Livsmedelsverket

Riskanalys som verktyg

Ett utbildningsmaterial för dricksvattenleverantörer som omfattas av NIS-regleringen

Författare:
Anders Lindström.

Omslag: Livsmedelsverket

Innehåll

1. Inledning

Detta dokument riktar sig till verksamheter som bedriver produktion och distribution av dricksvatten och som behöver stöd i att komma igång med riskanalys som en del av sitt systematiska informationssäkerhetsarbete. Beskrivningarna i detta dokument syftar till att fungera utbildande och ska inte ses som rekommendationer eller krav på hur riskanalyser ska genomföras.

2. Bakgrunden till riskanalys

En grundläggande aktivitet i en verksamhets säkerhetsarbete är att avgöra vilka åtgärder som är lämpliga för att uppnå tillräcklig säkerhet. Formuleringen ”lämpliga säkerhetsåtgärder” återkommer ofta i olika regelverk och lagstiftningar. För att komma fram till vad som är lämpliga säkerhetsåtgärder finns två huvudsakliga aspekter att hantera

1. Vad är tillräcklig säkerhet, vad är det som ska uppnås?
2. Hur avgör vi vilka åtgärder som är lämpliga för att vi ska uppnå tillräcklig säkerhet?

Detta informationsmaterial beskriver hur metoder för riskanalys kan användas som verktyg för att hitta svar på båda frågorna, och hur riskanalys kan användas för att få en viktig del av det systematiska informationssäkerhetsarbetet på plats.

2.1 Säkerhet – en nivå av skydd

För att reda ut vad tillräcklig säkerhet är behövs först en förståelse för vad säkerhet är. Säkerhet kan sägas vara en viss nivå av skydd från någon slags negativ händelse. För att det ska finnas en nytta med säkerhet behöver det vara tydligt vad som ska skyddas och vad det ska skyddas mot - samt hur starkt skyddet måste vara.

I en modern bil tar förare och passagerare på sig säkerhetsbälten och har en mängd säkerhetssystem i bilen som ska skydda vid en krock eller annan olycka. Skyddet i bilen är anpassat till de hot (trafikolyckor) mot människan (det som ska skyddas) som skulle kunna förekomma under bilfärden. Hade bilen däremot färdats i en krigszon, hade skyddet på bilen behövt vara dimensionerat för helt andra hot. Den skyddsvärda människan som färdas i bilen är densamma, men det hade till exempel behövts mindre och kraftigare fönsterrutor, förstärkt plåt i dörrarna och starkare motor. Hade sådana bilar använts i normala fall hade sådant som höga kostnader för inköp och service, framkomlighet, minskad bekvämlighet och miljöpåverkan blivit problematiska. Nivån av skydd hade alltså varit felaktigt anpassad till behovet, dvs. säkerhetsåtgärderna hade inte varit lämpliga.

Hur starkt skyddet behöver vara relaterar till hur stor risk som kan accepteras – utan vetskap om hur stor risk som är acceptabel så går det heller inte att avgöra om det satsats för mycket eller för lite resurser på säkerhetsåtgärderna. Det blir då svårt att ha en uppfattning om huruvida säkerhetsarbetet och investeringar i åtgärder är rimliga.

3. Vad ska skyddas?

Livsmedelsverkets föreskrifter om informationssäkerhetsåtgärder för samhällsviktiga tjänster inom sektorn leverans och distribution av dricksvatten (LIVSFS 2022:2) ställer krav på att leverantörer av samhällsviktiga tjänster ska ta fram och underhålla aktuella förteckningar över bland annat tillgångar i form av nätverksansluten hård- och mjukvara. En förteckning över tillgångar fungerar som ett ingångsvärde till en riskanalys eftersom förteckningen gör det tydligt vad som ska skyddas.

Det kan krävas en del arbete för att komma fram till alla tillgångar som bör ingå i en sådan förteckning, därför kan det vara effektivt att först fokusera på att identifiera så kallade guldägg, dvs. de system eller komponenter som behöver fortsätta fungera på grund av de stora konsekvenser det får om de får ett avbrott. Om anställda med erfarenhet och kunskap om verksamheten tillsammans går igenom och letar efter guldäggen har de goda möjligheter att relativt snabbt att komma fram till vilka de är. Avsnittet Riskanalys i praktiken beskriver mer kring vilka som bör delta.

För att efterleva föreskriften måste samtliga tillgångar förtecknas, så arbetet är inte färdigt enbart för att guldäggen identifierats. Det ger dock en grund för att komma igång med riskanalysen, och arbetet med identifiering av tillgångar kan fortsätta parallellt med att riskanalyser för de guldägg som identifierats påbörjas. Ett riskanalysarbete kan lätt fastna i startgroparna på grund av att det blir för omfattande, så det kan underlätta att inte ha allt för höga ambitioner för arbetets inledande skede, även om riskanalysen på sikt behöver bli heltäckande. För att riskanalyser ska ge ett värde behöver de göras kontinuerligt och återkommande, så det är naturligt att riskanalyserna förbättras över tid i takt med att verksamheten lär sig och metoden utvecklas.

4. Metoder för riskanalys

När det blivit tydligt vilka tillgångar som finns och vad som ska skyddas är det möjligt att gå vidare till att titta på en metod för riskanalysen. För att arbetet med riskanalys, och i förlängningen informationssäkerhetsarbetet, ska bli systematiskt behövs en metod som är anpassad och fungerar för verksamheten och som kan återanvändas varje gång riskanalysen ska uppdateras. På så vis blir analysen och resultatet förutsägbart och personoberoende och det blir möjligt att över tid följa hur arbetet med riskhanteringen har fungerat.

Det finns standarder för riskanalysmetoder som går att använda för att etablera en metod i den egna verksamheten. Det är också bra att undersöka internt om det redan finns en beslutad metod som ska användas, så att en ny metod inte bryter mot interna riktlinjer.

Generellt kan det sägas finnas två huvudsakliga metoder. Den ena metoden är att utgå från de identifierade tillgångarna och först avgöra deras respektive värde. Värdet av en tillgång baseras på en klassning av konsekvenser av förlorad konfidentialitet, riktighet och tillgänglighet hos tillgången. Sedan görs en individuell bedömning av möjliga negativa omständigheter och händelser som hotar respektive tillgång. Den andra metoden är att utgå ifrån en mer generell analys av identifierbara hot mot verksamheten och dess IT-miljöer för att i nästa steg säkerställa att alla individuella tillgångar har rätt nivå av skydd.

Traditionellt har den förstnämnda metoden varit populär och den gick relativt bra att använda när de skyddsvärda tillgångarna var få och lätta att avgränsa, identifiera och värdera. I dagens mer komplexa miljöer och omvärld kan det vara enklare att använda den senare metoden och fokusera på identifierbara hot. Utifrån NIS-lagens perspektiv har metoden i sig ingen betydelse för regelefterlevnad, utan leverantörer kan själva välja vilken metod som passar bäst i deras verksamhet.

Detta material fokuserar på att använda en metod som utgår ifrån en generell identifiering av hot och därefter en bedömning av risk, det vill säga den senare metoden. Andra metoder kan också vara relevanta, men syftet är här att ge en förståelse för hur en verksamhet komma igång med riskanalysarbetet.

5. Identifierbara hot

När riskanalysen genomförs bör deltagare som har kunskap om vilka hot eller negativa omständigheter som kan inträffa i system och nätverk som används för produktion och distribution av dricksvatten medverka. Anställda med olika kompetenser, till exempel IT, nätverk, dricksvatten (operatör, ingenjör eller dylikt), informationssäkerhet, etc. kan belysa olika perspektiv och identifiera olika typer av hot, så det underlättar att deltagare med olika roller i organisationen medverkar och det höjer kvalitén på analysen. Till exempel kan sannolikt någon som arbetar som driftsingenjör lättare identifiera hot i form av felaktigt handhavande eller misstag i SCADA-system medan någon från IT kan lyfta fram hot mot tekniska miljöer och infrastruktur i form av t.ex. sårbarheter eller hackerattacker.

Inför riskanalysen kan det vara värdefullt att göra en så kallad omvärldsbevakning för att få en bättre uppfattning om vilka hot som branschen generellt arbetar med att hantera, sårbarheter i utrustning som används, sannolikhet för att hot ska inträffa osv. Vanligt är en så kallad passiv omvärldsbevakning som baseras på att söka igenom och läsa olika informationskällor tillgängliga på internet. Det finns också säkerhetsbloggare och organisationer som regelbundet skickar ut nyhetsbrev med information om nya hot och sårbarheter. Ofta kan den stora informationsmängd som går att hitta på internet vara svår att sortera, så omvärldsbevakning bör göras till en återkommande aktivitet i det systematiska informationssäkerhetsarbetet så att verksamheten lär sig vilka källor som är användbara. Det finns även bibliotek av hot som kan användas som ett underlag för att identifiera sådana som är relevanta för dricksvattenproduktion.

Det kommer att vara svårt att identifiera samtliga hot vid en första riskanalys, men det är inte meningen att arbetet ska ses som en engångsaktivitet som därefter vara färdigt. Systematiskt informationssäkerhetsarbete innebär att konsekvent och förutsägbart göra kontinuerliga förbättringar, så det är därför inte nödvändigt att ha ambitionen att riskanalysen ska vara komplett efter första genomförandet. Medvetenhet och kunskap om hot utvecklas över tid vilket medför att identifiering av hot och genomförande av riskanalyser också förbättras över tid om de utförs systematiskt och återkommande, samt om verksamheten kontinuerligt utvärderar och förbättrar processen.

6. Sammanvägd riskbedömning

En risk kan sägas bestå av två komponenter – sannolikheten för att en negativ händelse eller ett hot ska inträffa och konsekvensen om det inträffar. Ett hot med hög sannolikhet och hög konsekvens innebär naturligt sammanvägt en hög risk. För att förutsägbart kunna göra den sammanvägda bedömningen behöver verksamheten definiera de nivåer av sannolikhet och konsekvenser som ska användas i riskanalysarbetet.

6.1 Konsekvensnivåer

Riskanalys med hänsyn till NIS-regleringen behöver ske utifrån perspektivet av hot som kan påverka tillhandahållandet av den samhällsviktiga tjänsten, dvs. leverans och distribution av dricksvatten. I riskanalysen går det också att ta hänsyn till andra konsekvenser som till exempel ekonomiska förluster, minskat förtroende eller påverkan på varumärke. För syftet här är nivåerna satta utifrån konsekvenser för leveransen av den samhällsviktiga tjänsten om ett hot skulle realiseras. Nedan följer exempel på nivåer som skulle kunna användas vid konsekvensbedömning, men utifrån NIS-lagens perspektiv kan en leverantör själv välja nivåer och beskrivning som är anpassade efter verksamhetens omständigheter.

Konsekvensnivå	Beskrivning
4. Allvarlig	Avbrott eller störning i leveransen av dricksvatten som är längre än godtagbart och kräver undantagsåtgärder för att säkerställa vattenförsörjning. Omfattande omprioriteringar av verksamheten.
3. Betydande	Avbrott eller störning i leveransen av dricksvatten som kan hanteras av abonnenterna utan större påverkan. Stora omprioriteringar av verksamheten.
2. Måttlig	Avbrott eller störning i leveransen av dricksvatten utan påverkan på abonnenter, men som kräver omprioriteringar av verksamheten för att hantera.
1. Försumbar	Avbrott som har en försumbar påverkan på leveransen av dricksvatten och inte kräver några omprioriteringar av verksamheten utan kan hanteras som del av daglig drift.

6.2 Sannolikhetsnivåer

Sannolikheten beskriver hur troligt verksamheten bedömt att ett hot ska inträffa, ofta utifrån ett mått på en frekvens på hur ofta en händelse vanligtvis inträffar. Det kan vara svårt att säga exakt hur sannolika vissa hot är och hur ofta de kan inträffa, särskilt om de aldrig förekommit tidigare, men med definierade nivåer brukar det ändå vara möjligt att göra en rangordning

mellan hoten. Även om det till exempel är svårt att avgöra exakt hur frekvent en överbelastningsattack förekommer, så brukar det vara möjligt att göra bedömningen om den är mer eller mindre frekvent än till exempel ett strömavbrott. Vid varje genomförd riskanalys är det också möjligt att justera bedömningen baserat på nya erfarenheter, vilket gör att bedömningen så småningom blir rimlig.

Bedömning av sannolikhet brukar bli bättre om den sker i grupp eftersom olika personer kan komma med olika perspektiv. Sannolikhet för hot av mer intern karaktär som till exempel misstag eller handhavandefel kan också vara svårare att bedöma för den som själv riskerar att begå dem, så det är bra att deltagare med olika utgångspunkt får diskutera för att komma fram till en så rimlig bedömning som möjligt.

Nedan följer exempel på nivåer som skulle kunna användas för sannolikhetsbedömning. Återigen har en leverantör själv möjlighet att välja nivåer och beskrivningar som är anpassade efter verksamhetens omständigheter.

Sannolikhetsnivå	Förväntad frekvens/förekomst
4. Mycket hög sannolikhet	Ca. 1 gång/månad eller oftare
3. Hög sannolikhet	Ca. 1 gång per år
2. Medelhög sannolikhet	Ca. 1 gång vart 10:e år
1. Låg sannolikhet	Mer sällan än vart 10:e år

6.3 Bedömning, sammanvägning och resultat

När en bedömning av ett hot ska göras är det naturligt att det finns existerande åtgärder på plats som kan påverka såväl konsekvens som sannolikhet. Reservkraft kan göra att konsekvensen av ett kortare elavbrott i en datorhall blir försumbart. Upparbetade och dokumenterade rutiner för kontinuerliga säkerhetsuppdateringar av system gör att sannolikheten minskar att en känd sårbarhet i programvara utnyttjas av en hacker. Ett syfte med riskanalysen är att avgöra om det krävs ytterligare åtgärder för att hantera en risk, så därför bör hänsyn tas till existerande åtgärder när bedömningen görs. För att det ska bli tydligt på vilka grunder bedömningen är gjord bör en förteckning eller beskrivning av de existerande åtgärderna som påverkar konsekvens eller sannolikhet inkluderas i dokumentationen från riskanalysen.

När sannolikheten och konsekvensen för ett hot är bedömt enligt de definierade nivåerna behöver det ske en sammanvägning för att komma fram till riskvärdet. Ofta brukar det ske med hjälp av en matris där risken kan värderas och kategoriseras. Nedan finns ett exempel på hur en sådan riskmatris kan se ut.

Konsekvens					
	4. Allvarlig	M	H	H	EH
	3. Betydande	M	M	H	H
	2. Måttlig	L	M	M	H
	1. Försumbar	L	L	M	M
		1. Låg	2. Medelhög	3. Hög	4. Mycket hög

Sannolikhet

I matrisen representerar ’L’ en låg risk, ’M’ en medelhög risk, ’H’ en hög risk och ’EH’ en extra hög risk. Det sammanvägda riskvärdet ska ligga till grund för prioritering av åtgärder för hantering av identifierade risker, så det kan ibland behövas justeringar av matrisens utformning så att prioriteringen blir rimlig. En verksamhet kan ha beslutat att alla risker som har ett sammanvägt värde av Medelhög risk ska hanteras inom 6 månader. Om det i riskanalysen tagits upp många hot med försumbar konsekvens, men mycket hög frekvens så kan det då vara relevant att den sammanvägda bedömningen blir Låg för just den typen av risker så att prioriteringen av åtgärder blir rimlig. För dricksvattenproduktion kanske avbrott i kommunikationslänkar till ytterstationer sker med hög frekvens, men verksamhetens erfarenhet kan vara att konsekvensen av ett sådant avbrott oftast är försumbar eftersom utrustningen inte är beroende av att länken är konstant tillgänglig. Det behövs då ingen ytterligare åtgärd för att hantera risken, men den har ändå analyserats för att påvisa detta faktum. Notera att oavsett verksamhetens egen bedömning av risken, kan ett hot av detta slag, om det inträffar, ändå vara en rapporteringspliktig incident enligt NIS-lagen. De bedömningsnivåer verksamheten sätter upp ska alltså inte avgöra om en incident är rapporteringspliktig utan detta är styrt av MSB:s föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster (MSBFS 2018:9, 8 kap.). Nedan finns ett exempel på en justerad riskmatris.

Konsekvens					
	4. Allvarlig	M	H	H	EH
	3. Betydande	M	M	H	H
	2. Måttlig	L	M	M	H
	1. Försumbar	L	L	L	L
		1. Låg	2. Medelhög	3. Hög	4. Mycket hög

Sannolikhet

6.4 Beslut om åtgärd

För att åstadkomma en systematik och förutsägbarhet i hur identifierade risker åtgärdas behöver det finnas beslutade riktlinjer om hantering och prioritet som är baserade på den

sammanvägda bedömningen. En sådan riktlinje kan också innehålla instruktioner om när en risk kan accepteras utan åtgärd av verksamheten, och vem i organisationen som i så fall får fatta ett sådant beslut. Det är med denna riktlinje verksamheten formellt sätter en nivå på hur stor risk man är villig att utsätta sig för och vem som är riskägare för den specifika risken. Nedan följer ett exempel på hur en sådan riktlinje kan utformas. Utifrån NIS-lagens perspektiv kan en leverantör själv utforma en riktlinje som är anpassad efter verksamhetens omständigheter.

Risknivå	Beskrivning
Extra hög risk	För risker på denna nivå ska åtgärder omedelbart införas för att sänka sannolikheten eller mildra konsekvensen. Enbart högsta ledningen har beslutsmandat att acceptera en risk på denna nivå och ska därmed alltid vara riskägare för risken. Ett sådant beslut ska alltid ske i ett beslutsfört forum och dokumenteras.
Hög risk	Åtgärder för att hantera risker på denna nivå ska införas inom 3 månader. Chef för aktuellt verksamhetsområde har mandat att fatta beslut om lägre prioritering eller längre tidsfrist och ska därmed alltid vara riskägare för risken. Ett sådant beslut ska dokumenteras i riskanalysen. Enbart högsta ledningen har mandat att acceptera en risk på denna nivå. Ett sådant beslut ska ske medvetet och dokumenteras.
Medelhög risk	Åtgärder för att hantera risken ska införas inom 12 månader. Riskägare har mandat att fatta beslut om lägre prioritering eller längre tidsfrist, samt mandat att fatta beslut om att acceptera risken. Sådana beslut ska dokumenteras i riskanalysen.
Låg risk	Risken ska bevakas men kräver ingen ytterligare åtgärd. Ny bedömning görs vid nästa riskanalys.

7. Riskanalysen i praktiken

Det kan vara bra att dela upp riskanalysen i mindre delar så att arbetet med att genomföra riskanalysen inte blir för betungande för verksamheten. Av samma orsak kan det underlätta att inte sätta för höga ambitioner för hur heltäckande den initiala riskanalysens resultat ska bli. En riskanalys som ska identifiera samtliga tillgångar och hot kommer lätt att blir stor och riskerar därmed att aldrig komma igång – och kanske därför aldrig leder till några åtgärder. Att inleda arbetet med ambitionen att identifiera guldäggen och bedöma de huvudsakliga hoten ger dock en bra start och lägger grunden för fortsatt arbete. Arbetet med riskhantering är inte färdigt när riskanalysen och åtgärdsplanen är framtagen, utan är en del i ett kontinuerligt förbättringsarbete.

Bjud in till möten

Bjud in deltagare till två möten, ca. 2-3 timmar vardera, det första för att identifiera tillgångar, det andra för att identifiera hot och göra riskanalysen. De som ska delta behöver tillsammans ha kunskap om;

- Verksamheten
- IT - infrastruktur och system som används för tillhandahållandet av den samhällsviktiga tjänsten
- Hur systemen används
- Hot och negativa händelser som kan inträffa
- Existerande åtgärder

För att få bra underlag vid genomförandet av en riskanalys kan det vara bra att ge deltagarna förhandsinfo om hur analysen går till och be dem reflektera över kring vilka hot som bör analyseras. De kanske har läst om någon händelse som skulle kunna inträffa i den egna verksamheten, eller så känner de till något som skett det senaste året som kunde ha utvecklats till en incident. Kanske har de noterat någon brist i säkerhet eller rutiner som de oroar sig över, och som därför behöver tas upp vid analysen.

När riskanalysen genomförs behöver en utpekad person dokumentera resultatet, dels så att det blir användbart för att ta fram åtgärdsplan, och dels så att det kan fungera som underlag för att rapportera till ledningen eller för att uppvisa regelefterlevnad vid en tillsyn. Sådan dokumentation bör utformas så den kan återanvändas i framtida riskanalyser. När nästa riskanalys sker behöver deltagarna se över sådana hot som tagits upp tidigare för att bedöma om risken kvarstår, samt bygga på med ytterligare hot om sådana finns. Om verksamheten genomför en återkommande riskanalys och kommer fram till att det inte finns ytterligare risker som behöver hanteras betyder inte det att aktiviteten varit resultatlös, utan det är helt enkelt en indikation på att nivån av säkerhet är lämplig.

Ett exempel på hur dokumentation från en riskanalys kan se finns att ladda ned på Livsmedelsverkets webbplats, www.livsmedelsverket.se/nis.

7.1 Formulera hoten för att underlätta bedömning

Som framgått av tidigare avsnitt innehåller en riskanalys ett stort mått av bedömning och resultatet kommer att bli beroende av deltagarnas erfarenheter och kunskaper. För att underlätta bedömningen är det därför bra att försöka vara relativt specifik i formuleringen av det hot som ska bedömas. Det blir då även lättare att hitta lämpliga åtgärder för att hantera den risk som uppstår på grund av hotet. Nedan följer ett par exempel för att visa på vilka olika sätt en hotbeskrivning kan formuleras.

7.1.1 Exempel 1

Svårbedömd hotbeskrivning

Ransomware-attack mot verksamheten.

Hotbeskrivning som underlättar bedömning

Tekniker från underkonsult ansluter egen dator smittad med ransomware som sprider sig i SCADA-miljön. Samtliga komponenter i miljön måste sättas upp igen från grunden.

Den första beskrivningen är för generell för att det ska vara möjligt att bedöma sannolikheten. Det är också svårt att avgöra vad konsekvensen blir eftersom det inte anges vilka komponenter som påverkas av attacken.

I den andra beskrivningen blir det tydligare.

- Kanske har deltagarna vetskap om hur vanligt det är att tekniker ansluter egen dator när de jobbar i SCADA-miljön så att det är möjligt göra en bedömning av sannolikheten att verksamheten blir utsatt. Förmodligen har de även en uppfattning om underkonsulters tekniska säkerhetsåtgärder och kan bidra med detta till bedömningen.
- Med deltagare med kunskap om IT-miljöerna finns också möjlighet att avgöra hur stor sannolikheten är att ett ransomware kan spridas i produktionsmiljön och det går att få en uppfattning om hur det står till med backuper och vilken tid det tar att återställa.
- När det är tydligare vilka system som påverkas av hotet går det bättre att få en uppfattning om hur vattenförsörjningen påverkas. Hänsyn kan till exempel behöva tas till hur länge vatten i reservoarer kan försörja invånarna, och om det är möjligt att återställa system inom den tiden.

Med den tydligare beskrivningen går det också att bedöma inom vilka områden det kan sättas in åtgärder om risken behöver hanteras ytterligare.

- Alternativa arbetssätt för underkonsulters tekniker kan övervägas.
- Säkerhetskrav kan behöva ställas på underkonsulters utrustning om det är absolut nödvändigt att den ska kopplas in.

- Åtgärder kan införas för att ytterligare segmentera nätverk så att en attack på en komponent är mindre sannolik att sprida sig i produktionsmiljön.
- Tekniska lösningar för backuper kan behöva ses över så att ransomware inte förstör kopior som används för återställning.
- Rutiner för återställning kan ses över och övas för att få ned tiden för återställning.

7.1.2 Exempel 2

Svårbedömd hotbeskrivning

Strömavbrott i 5 timmar

Hotbeskrivningar som underlättar bedömning

- *Strömavbrott i stadskärnan som påverkar kommunhuset där primär datorhall finns. Strömavbrottet pågår i mindre än 5 timmar.*
- *Strömavbrott i stadskärnan som påverkar kommunhuset där primär datorhall finns. Strömavbrottet pågår i mer än 5 timmar.*
- *Strömavbrott i hela kommunen. Det påverkar kommunhuset där primär datorhall finns samt vattenverk A där sekundär datorhall finns. Strömavbrottet pågår i mer än 10 timmar.*

I den första beskrivningen går att ana att det finns reservkraft för att hantera drift av en datorhall i upp till 5 timmar, och det kanske är möjligt att avgöra baserat på historik hur sannolikt det är att ett sådant avbrott ska ske. Om hotet delas upp som i exemplet blir det dock lättare att göra en bedömning av sannolikheten och framförallt konsekvensen av olika strömavbrottssituationer. I den utförligare beskrivningen framgår att det finns en sekundär datorhall som är möjlig att växla över till vid ett avbrott, dvs. det finns befintliga åtgärder på plats som också behöver ingå i bedömningen av risken.

8. Åtgärdsplanen

Baserat på riktlinjen om hantering och prioritet som beskrivs i avsnittet *Beslut om åtgärd* ska verksamheten ta fram och besluta om en åtgärdsplan. När beslut tas om åtgärd är det nödvändigt att bedöma om vald åtgärd sänker risken tillräckligt för att ytterligare åtgärder inte ska behöva vidtas. Kanske sänker en viss åtgärd sannolikheten för att ett hot ska inträffa, men den sammanvägda risken är fortfarande är så pass hög att ytterligare åtgärder krävs för att mildra konsekvenserna när det inträffar.

I åtgärdsplanen behöver det vara tydligt vem som är ägare för risken och vem som är ansvarig för införande av åtgärder. Det behöver även finnas en tidplan för när en åtgärd ska vara införd så att det går att följa upp hur arbetet med införande av åtgärder fortskrider. Riskägarskap är också reglerat i Livsmedelsverkets föreskrifter. Det kan vara en fördel att dokumentera åtgärdsplanen i anslutning till riskanalysen så att det blir tydligt vilka risker respektive åtgärd ska hantera.

Ett exempel på hur dokumentation av en åtgärdsplan kan se ut finns att ladda ned på Livsmedelsverkets webbplats, www.livsmedelsverket.se/nis.

9. Formalisera riskanalysarbetet

Om informationssäkerhetsarbetet och systematiska genomföranden av riskanalyser ska fungera över tid behöver ledningen ta ett formellt ansvarig för att sådana uppgifter genomförs. En ledning eller motsvarande funktion med mandat behöver besluta att arbetet ska göras, hur arbetet ska gå till samt vilket ansvar som ska delegeras till lämpliga roller inom verksamheten.

Det är inte ovanligt att ett gediget säkerhetsarbete sker i en verksamhet oavsett om ansvaret är tilldelat, men ofta blir säkerhetsarbetet beroende av en eller flera eldsjälar som känner ett personligt ansvar för detta och därmed gör bra saker. Den typen av personberoende behöver undvikas då personberoenden utgör risker i sig.

Vid revision eller tillsyn kan verksamheten också komma att behöva uppvisa underlag som visar hur verksamheten jobbar med riskanalyser. I dessa fall är det vanligt att gå igenom dokumentation som visar *hur* riskanalysen ska göras och sedan bevis på *att* arbetet faktiskt är utfört på det sättet. Regelefterlevnaden går lättare att bedöma om verksamheten kan visa upp en beskrivning av en rutin eller riktlinje för att sedan visa upp dokumentation från den genomförda riskanalysen. Den typen av dokumentation kan också vara helt nödvändig att ha på plats för att följa relevanta lagar och regler. Samma förhållningssätt går att applicera på de flesta typer av reglerad verksamhet inom informationssäkerhetsområdet – visa att verksamheten bestämt hur saker ska göras och visa sedan att verksamheten faktiskt gjort som den har bestämt.

Ett exempel på hur en riktlinje om riskanalys kan se ut finns att ladda ned på Livsmedelsverkets webbplats, www.livsmedelsverket.se/nis.


Livsmedelsverket