White paper

Av: Mats Karlsson Landré,
OT-säkerhetsexpert på Sectra

Varför en SOC-tjänst gör det möjligt att följa VA-branschens regler

En allt mer central del i VA-branschens säkerhetsarbete är cybersäkerhet. Våra digitala system är helt avgörande för en effektiv produktion. Möjligheten till manuell drift finns fortfarande i viss mån, men även då är man beroende av fungerande digitala komponenter.

En god cybersäkerhet kräver att många olika säkerhetsåtgärder fungerar tillsammans och att de samverkar för bästa effekt. Det alla säkerhetsåtgärder har gemensamt är att de förutsätter att larm och säkerhetspåverkande händelser i anläggningen övervakas så att åtgärder snabbt vidtas för att hantera situationer där en viss säkerhetsåtgärd inte räckte till.

Att köpa säkerhetsövervakning som tjänst (”Security Operations Center” – SOC) är ett mycket kostnadseffektivt sätt att få professionell säkerhetsövervakning dygnet runt. Som bieffekt förstärks effekten av redan existerande säkerhetsåtgärder genom att deras förmågor kan samlas och samverka sinsemellan. Exempelvis kan indikationer från brandväggar i nätverket, larm från virusskydd i servrar och loggar från applikationer vägas samman till en mycket tydlig lägesbild.

Med en tjänst för säkerhetsövervakning av OT- och IT-system kan VA-bolag möta de regulatoriska krav som ställs från Cybersäkerhetslagen (NIS2) och Säkerhetsskyddslagen, men också att uppnå en högre grad av säkerhet genom att ta hänsyn till råd från Svenskt Vattens Säkerhetshandbok P-118 samt krav från den internationella standarden för säkerhet i Industriella Automations- och Kontrollsystem IEC 62443. Att införa en SOC är en viktig pusselbit att stärka den egna förmågan att upptäcka incidenter och lägger en utmärkt grund för det systematiska säkerhetsarbetet som minskar risken att tillgängligheten av vatten och avloppstjänster påverkas.

Cybersäkerhetslagen, NIS2-direktivet och MSB:s föreskrifter

Den nya Cybersäkerhetslagen[1] som utgår från NIS2-direktivet väntas träda i kraft i mitten av januari 2026 och ersätta tidigare lagstiftning baserad på NIS-direktivet[2]. Jämfört med tidigare lagstiftning omfattas nu även avloppshantering för VA-branschens del.

Den nya Cybersäkerhetslagen ställer krav på att samhällskritiska verksamhetsutövare ska vidta proportionella och riskbaserade åtgärder för att säkerställa cybersäkerheten, något som är avgörande för samhällsviktiga tjänster. Som verksamhetsutövare ska man kunna analysera störningar och incidenter där resultatet skyndsamt ska rapporteras till myndigheterna. En förutsättning för denna rapportering är att verksamhetsutövaren har förmågan att samla in och analysera säkerhetsloggar för att förstå ett händelseförlopp, något som även är viktigt för att snabbt kunna åtgärda incidenter.

MSB, Myndigheten för Samhällsskydd och Beredskap, har tagit fram föreskrifter[3] baserat på Cybersäkerhetslagen. Dessa föreskrifter är tänkta att gälla för alla typer av verksamheter med undantag för vissa digitala tjänster där PTS, Post- och Telestyrelsen, ger ut föreskrifter.

1. Cybersäkerhetslagen
2. Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
3. Remisser om föreskrifter och allmänna råd

SECTRA
Knowledge and passion

I föreskrifterna läggs stort fokus på förmågan att tidigt upptäcka och agera på säkerhetsincidenter för att minimera deras skadeverkning. Det ställs direkta krav på övervakning som kan upptäcka intrång och andra incidenter. En naturlig komponent i säkerhetsövervakning är insamling och analys av säkerhetsloggar.

Även om föreskrifterna inte uttryckligen ställer krav på att säkerhetsövervakning ska ske dygnet runt finns en rad starka formuleringar kring att incidenter ska upptäckas skyndsamt och att behovet av realtidsövervakning ska hanteras. Det finns förstås ett starkt egenvärde i att säkerhetsövervakning är aktiv dygnets alla timmar och årets alla dagar. Värdet av en övervakning dagtid eller genom sporadisk analys blir begränsat, samtidigt som det krävs en relativt stor grupp av säkerhetsspecialister för att kunna bemanna dygnet runt på årets alla dagar. Detta faktum gör säkerhetsövervakning i egen regi ogörligt för de flesta organisationer.

Ett begrepp som genomsyrar både Cybersäkerhetslagen och MSB:s föreskrifter är proportionalitet. Alltså tanken att man genom riskanalyser ska hitta de områden i verksamheten där säkerhetsåtgärder skulle göra störst nytta och kunna fokusera sina resurser där. En annan viktig förmåga är att kunna mäta och utvärdera sina säkerhetsåtgärder. Detta går hand i hand med proportionaliteten eftersom det säkerställer verklig nytta hos de åtgärder man förlitar sig på. Säkerhetsövervakning kan lämna ett avgörande bidrag till både proportionalitet och mätbarhet genom att synliggöra hur effektiva övriga säkerhetsåtgärder är i praktiken.

Ett annat viktigt begrepp i föreskrifterna från MSB är Sektorkritiska system. Det är de system som man behöver för att bedriva den verksamhet som orsakar att man omfattas av Cybersäkerhetslagen. För Sektorkritiska system ställs speciellt höga krav på exempelvis nätverkssegmentering, säkerhetsövervakning, dokumentation, fysiskt skydd, backuper och att öva återställning efter ett haveri. Det är rimligt att de säkerhetssystem som skyddar Sektorkritiska system håller minst samma standard som de system de skyddar, vilket gör valet av exempelvis säkerhetsövervakning helt avgörande för anläggningens totala säkerhet.

Att leverera tjänster för säkerhetsövervakning ställer mycket höga krav på leverantörens eget säkerhetsarbete för att säkerställa att leverantören inte blir en språngbräda in till kundernas produktionsmiljöer. Därför är det naturligt att denna typ av verksamheter själva omfattas av NIS2 och Cybersäkerhetslagen under begreppet ”utlokaliserade säkerhetstjänster”. EU har via sin cybersäkerhetsmyndighet ENISA sedan 2024 publicerat detaljerade krav[4] på dessa. Arbete pågår inom ENISA med certifieringskrav för att kunna visa att den här typen av verksamhet håller en hög kvalitet och säkerhet. I föreskriften finns krav på att hantera behovet av att välja certifierade leverantörer av exempelvis säkerhetstjänster.

Kräver NIS2 att du har säkerhetsövervakning?

MSB:s föreskrifter till Cybersäkerhetslagen ställer ett antal tydliga krav på förmågor i verksamheten som bara är möjliga att möta med en välutvecklad säkerhetsövervakning. För VA-verksamheter gäller att 4 timmars nedsatt funktionalitet i ett produktionssystem räcker för att det ska räknas som en incident som ska rapporteras. För att undvika detta krävs alltså mycket snabb upptäckt och hantering av säkerhetsproblem.

Förskrifterna är också tydliga med att:

- Säkerhetspåverkande händelser i nätverk och system ska loggas.
- Intrångsdetektion ska användas och upptäckta händelser ska loggas.
- Säkerhetsövervakning bör ske i realtid för att kunna upptäcka incidenter snabbt.
- Loggarna ska skyddas mot obehörig åtkomst och skada. Exempelvis nämns att loggar bör samlas i ett centralt övervakningssystem som ska separeras från övriga system.
- Föreskrifterna trycker på att loggar från olika källor ska kunna jämföras.
- Senast inom 24 timmar ska ni kunna rapportera vad som faktiskt inträffat.

> *“MSB:s föreskrifter till Cybersäkerhetslagen ställer ett antal tydliga krav på förmågor i verksamheten som bara är möjliga att möta med en välutvecklad säkerhetsövervakning.”*

4. Kommissionens genomförandeförordning 2024/2690

- Ni ska kunna fatta beslut om att incidenten är över baserat på insikter om vad angriparen gjort och inte gjort.
- Efter en incident ska ni lämna en slutrapport där ni drar slutsatser baserat på vad som faktiskt ledde till att incidenten inträffade och hur upprepning ska förhindras.
- Föreskrifterna tar upp behovet av att ha förberett stöd från leverantörer inför en kris. Den egna personalen ska kunna fokusera helt på att stötta verksamheten istället för att exempelvis analysera loggar.
- Ni ska hantera behovet av att köpa tjänster på säkerhetsområdet som är certifierade enligt EU:s cybersäkerhetsakt.

Säkerhetsskyddslagen

För VA-bolag som till någon del omfattas av säkerhetsskyddslagen[5] gäller enligt SÄPO:s föreskrifter[6] för säkerhetsskydd att verksamhetsutövaren ska logga händelser i informationssystem som har betydelse för säkerhetskänslig verksamhet.

Verksamhetsutövaren ska kunna upptäcka funktionsstörningar, skadlig inverkan, obehörig åtkomst och försök till påverkan på den säkerhetskänsliga verksamheten så att åtgärder kan vidtas för att försvåra och hantera säkerhetsincidenter. Man ska även logga händelser som ändring och användning av systemadministrativa behörigheter. I Säpo:s vägledning för säkerhetsskydd av informationssystem[7] beskrivs hur en SOC bör inrättas för övervakning av sina system och ett centraliserat system ska implementeras för att kunna analysera säkerhetshändelser.

En viktig skillnad mot Cybersäkerhetslagen är att Säkerhetsskyddslagen enbart ställer krav på skydd mot ”antagonistiska hot”, d.v.s. fientligt inställda personer. Cybersäkerhetslagen talar istället om ”allriskansats”, alltså att alla typer av hot mot digital säkerhet ska hanteras.

I praktiken kan det alltså finnas tillfällen när Säkerhetsskyddet behöver kompletteras med det som brukar kallas verksamhetsskydd för att uppnå ett skydd som motsvarar kraven från Cybersäkerhetslagen.

I jämförelse med Cybersäkerhetslagen och MSB:s föreskrifter går kraven enligt Säkerhetsskyddslagen och SÄPO:s föreskrifter längre på flera områden. Ett tydligt exempel är att säkerhetsloggar ska bevaras och analyseras i minst 10 år. Detta ställer stora krav på de tekniska lösningar som används för att övervakningen ska bli praktiskt genomförbar och ekonomiskt försvarbar.

Svenskt Vattens Säkerhetshandbok P118

Branschorganisationen Svenskt Vatten gav 2023 ut *Säkerhetshandbok för VA-verksamhet (P118)*[8] för att stödja VA-aktörer med sitt säkerhetsarbete. Handboken karaktäriserar hur ett gott säkerhetsarbete ser ut för att skydda datorbaserade system:

”Generellt handlar ett gott säkerhetsarbete om förmågan att löpande kunna identifiera nuläget samt kritiskt analysera beroenden och potentiella sårbarheter. Det gäller att få till en robust hantering av och kontinuitet hos verksamhetens datorbaserade system. Detta kräver att verksamheten övervakar interna nätverk och samtidigt beaktar omvärldshändelser så att viktiga relevanta uppdateringar och skyddsåtgärder kan vidtas på kort tid.”

Handboken beskriver vikten av tydliga och dokumenterade incidentrutiner, att skillnaden på säkerhetsutmaningar är stora mellan administrativa IT-system och driftsnära OT-system, att genomföra regelbundna utbildningar och säkerhetsövningar, samt att noggrant hantera valet mellan molntjänster och lokal drift av system. Den betonar också förebyggande åtgärder såsom multifaktorautentisering, segmentering av nätverk, sårbarhetsanalyser, backuprutiner och beredskap för att snabbt upptäcka och hantera incidenter.

5. Säkerhetsskyddslag (2018:585) | Sveriges riksdag
6. PMFS 2022:1
7. Informationssäkerhet: Vägledning i säkerhetsskydd
8. Säkerhetshandbok för VA-verksamhet (P118-digital version) | Vattenbokhandeln

SECTRA
Knowledge and passion

Motsvarande krav och hänsyn ska även överföras på de säkerhetstjänster som används. Har man exempelvis valt att enbart använda lokalt placerade system, istället för molntjänster, blir en naturlig följd att exempelvis säkerhetsövervakning ska ske med lokalt placerad utrustning.

Egen rådighet, utländskt inflytande och sekretess

Säkerhetsövervakning är en mycket central del av en organisations säkerhetsarbete. Det innebär också att tjänsten behöver levereras på ett sätt som i sig är säkert och som garanterar dess funktion även när omvärldsläget förändras till det sämre.

Många vill undvika onödiga yttre beroenden genom att välja lösningar som inte är beroende av molnleverantörer, internettjänster eller andra funktioner som ligger utanför parternas egen kontroll. Särskilt viktigt är att insamlingen av loggar kan ske oavbrutet och att de ständigt analyseras.

Ett allt vanligare krav vid upphandling av tjänster för säkerhetsövervakning är att tjänsten ska levereras i Sverige och endast ha svensk personal som hanterar känsliga uppgifter. I en förlängning av samma resonemang ställs allt oftare kravet om ett tydligt och spårbart svenskt ägande av leverantören som företag.

IEC 62443

IEC 62443 är en serie internationella standarder som fokuserar på cybersäkerhet för industriella kontroll- och automationssystem (IACS), även benämnda OT-system. Dessa standarder täcker hela livscykeln för säkerhet, från design och utveckling till drift och underhåll av OT-system och komponenter. Lagstiftning inom IT- och OT-säkerhet, såsom NIS2-direktivet, förhåller sig ofta till internationella standarder som IEC 62443. Även om uppfyllande av standarden inte automatiskt innebär juridisk efterlevnad, utgör den ett effektivt verktyg för att strukturera och dokumentera cybersäkerhetsarbetet i linje med lagkrav.

IEC 62443-2-1[9] för ledningssystem för ägare av IACS är uppdelade i moduler, så kallade Security Program Elements (SPE) för IACS-säkerhet. Dessa SPE:er täcker flera områden nödvändiga för effektiva ledningssystem för IACS-säkerhet som exempelvis rutiner för organisationsfrågor, nätverkssegmentering och härdning av komponenter. Att införa en SOC-tjänst uppfyller många krav som ställs i IEC 62443-2-1.

SPE 7 i IEC 62443-2-1 beskriver krav på att organisationen har policys och rutiner för händelse- och incidenthantering i industriella kontroll- och automationssystem för att uppnå förmåga att upptäcka och förhindra säkerhetsincidenter. Det innebär att det ska finnas processer för att upptäcka, analysera och åtgärda avvikelser och incidenter i systemet, samt rapportera dessa i rätt tid till rätt person. Man ska också arbeta proaktivt med att identifiera och åtgärda sårbarheter i sin miljö. Vidare ska all relevant information loggas på ett säkert sätt och sparas under en tillräcklig tidsperiod. Loggarna ska innehålla detaljerad information som möjliggör spårbarhet och tidskorrelerad analys, vilket är avgörande för att förstå händelseförlopp och identifiera potentiella säkerhetshot.

SPE 4 i IEC 62443-2-1 säger att man ska stärka skyddet i sina komponenter, exempelvis med hjälp av härdning. En tjänst för säkerhetsövervakning kan analysera om kritiska system eller komponenter har onödiga portar öppna eller om nätverkstrafik går mellan komponenter utan kryptering och meddela kunden detta. På så sätt kan kunden systematiskt härda sina komponenter och förbättra sin säkerhet för att minska riskerna att attacker mot systemet kan uppstå.

Lämpliga krav på säkerhetsövervakning

I en tid där ett aktivt cybersäkerhetsarbete är en självklarhet blir det allt tydligare att en stark förmåga till säkerhetsövervakning är helt avgörande. Eftersom det krävs stora resurser för att bygga upp en sådan förmåga är det i de flesta fall bara realistiskt att köpa den som tjänst.

> *“Det innebär att det ska finnas processer för att upptäcka, analysera och åtgärda avvikelser och incidenter i systemet, samt rapportera dessa i rätt tid till rätt person.”*

9. Standard - Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners IEC 62443-2-1:2024 - Swedish Institute for Standards, SIS

SECTRA
Knowledge and passion

För att säkerställa att den tjänst man väljer verkligen motsvarar de behov som produktionen ställer finns några viktiga områden som man bör överväga att ha med som krav:

- **Verksamhetsförståelse** – Har leverantören erfarenhet av leverans till er sektor? Förstår leverantörens personal typiska utmaningar och krav i verksamheten? Förstår leverantörens personal de unika förutsättningarna för övervakning i OT-miljöer?

- **Tjänstens tekniska utformning** – Är tjänstens tekniska plattform utformad på ett sätt som är lämplig för övervakning av er produktionsplattform? Finns rätt insamlingsmetoder för att inte riskera att påverka produktionen? Om så behövs, finns fysiskt begränsad envägskommunikation (”nätverksdiod”) tillgänglig? Kan aktiv åtgärd erbjudas via exempelvis EDR-teknik?

- **Lokalt placerad utrustning** – Kan leverantörens utrustning placeras i era lokaler för att möta produktionens behov av lokala system och för att säkerställa att övervakningen inte är beroende av yttre system som internet eller molntjänster? Kan övervakningen fungera under pågående säkerhetsincident om verksamhetens internetanslutning tas ner som en förebyggande åtgärd?

- **Ö-drift** – Under vilka förutsättningar ska leverantören erbjuda en opåverkad tjänst trots att anläggningen körs i ö-drift? (Alltså att verksamhetens system är bortkopplade från yttre system och eventuellt även utan yttre tillförsel av el.)

- **Unika anläggningsbehov** – Är er anläggning beroende av någon speciell teknik eller kommunikationsprotokoll som det är avgörande att övervakningen kan hantera?

- **Kontinuerlig övervakning** – Har leverantören förmåga att hantera en incident alla tider på dygnet? Detta kan vara viktigt för att begränsa skadeverkningar även om produktionen inte pågår 24/7/365.

- **Proaktiva värden** – Skall leverantören sammanställa månatliga eller kvartalsvisa rapporter av viktiga händelser, insikter och lärdomar? Finns behov av att leverantören löpande presenterar förslag på förbättringar baserat på icke-kritiska larm kan vara stort för produktionens robusthet. Detta bör även inkludera områden som inte har säkerhetspåverkan men som skulle kunna höja tillförlitligheten hos verksamhetens system.

- **Egen rådighet** – Ska leverantören erbjuda er direkt åtkomst till sammanställd information i övervakningssystemet alternativt egen åtkomst för att arbeta med hotjakt mm?

- **Övningar** – Förväntas leverantören delta i era övningar och penetrationstester?

- **Leverantörens eget uppfyllande av NIS2** – Hur planerar leverantören att själv möta kraven från Cybersäkerhetslagen samt föreskrifter från EU och PTS på deras egen organisation?

- **Leverantörens planering för kommande EU-certifiering** – Har leverantören planer på certifiering enligt ”EU Managed Security Services Certification[10]”? Att kravställa detta från leverantörer finns med i MSB:s föreskrifter.

- **Internationella beroenden** – Levereras tjänsten i Sverige av svensk säkerhetskontrollerad personal?

10. EU Managed Security Services Certification

- **Ägarbilden** – Finns något större utländskt ägande i leverantören?
- **Säkerhetsskydd** – Kan leverantören ingå SUA-avtal eller motsvarande? Vilken typ av säkerhetsgranskning genomgår personalen? Håller lokalerna där verksamheten bedrivs tillräckligt hög skyddsklass? Uppfyller leveransen krav enligt SÄPO:s vägledningar?
- **Höjd beredskap och krig** – Har leverantören krigsplacerat nyckelpersonal?
- **Stöd kring myndighetsrapportering** – Erbjuder leverantören rätt stöd i samband med att ni behöver rapportera det som MSB:s föreskrifter benämner som ”betydande incident”, ”betydande sårbarhet” eller ”betydande cyberhot”?

Om Sectra

Sectra hjälper myndigheter och försvar i Europa att skydda samhällets mest känsliga information och kommunikation.

Inom området för säker kommunikation utvecklas produkter och tjänster som skyddar delar av samhällets mest känsliga information och kommunikation. Sectra har varit en ledande leverantör inom cybersäkerhet sedan 1978. Vi har levererat rådgivning och övervakningstjänster med fokus på kritisk infrastruktur och industriella system, ofta kallat OT-säkerhet sedan 2016.

Bland våra kunder finns exempelvis producenter av dricksvatten, fjärrvärme, kemisk processindustri, tillverkande industri, elproducenter och tillverkare av cybersäkerhetsutrustning. Vi stöttar också myndigheter, IT-bolag och ingenjörsföretag med vår unika kompetens.

Sectra omfattas, precis som de flesta av våra kunder, av NIS2-direktivet och Cybersäkerhetslagen. Vi har dessutom tagit en aktiv roll i EUs utveckling av certifieringsscheman för säkerhetstjänster.

Sectra Communications AB • communications@sectra.com • communications.sectra.com
This is a marketing material and may be changed at any time without prior notice.
Sectra will not be held liable for any errors or misconceptions herein.
© 2025 -11 Sectra Communications

SECTRA
Knowledge and passion