Smarta tips • Smarta tips • Smarta tips • Smarta tips • Smarta tips • Smarta tips •

Digitala dörrar på glänt – hur skyddar vi VA-anläggningar mot cyberattacker?

Vattenförsörjning och dess infrastruktur hör till de viktigaste funktionerna i vårt samhälle. Den digitala omvandlingen av VA-industrin innebär många miljö- och resursmässiga fördelar men öppnar samtidigt upp för en ny hotbild i form av cyberattacker.

Digitaliseringen berör hela samhället. Inom VA-industrin utökas den snabbt med mängder av funktioner som ställer nya krav på befintliga anläggningar. Tekniska möjligheter som till exempel integrering av stora mängder data och fjärrstyrning lägger grunden för en mer resurseffektiv och miljövänlig vattenhantering.

Men samma utveckling medför även att vi öppnar nya dörrar till känsliga delar av verksamheten. Med ökad digital exponering ökar risken för olika typer av attacker utifrån som lätt kan sprida sig in i verksamheten. Även system som saknar externa uppkopplingar kan påverkas genom oavsiktliga misstag inne på en anläggning vilket kan resultera i driftsstörningar.

Starkare hotbild. Idag måste alla som driver industriell verksamhet räkna med nya risker och hotbilder ur både tekniskt och organisatoriskt perspektiv. Den digitala sårbarheten har skapat en marknad för illegala intrång befolkad av nya aktörer som arbetar utifrån vitt skilda bevekelsegrunder.

En färsk sammanställning av hotbild och incidenter visar att samhällsviktiga funktioner som vattenanläggningar är högintressanta mål för brottslingar som vill tjäna pengar, men även för statliga aktörer med andra motiv. Deras kompetens och metoder blir allt mer sofistikerade, vilket kräver en heltäckande syn på säkerhet i hela organisationen för att kunna möta och stoppa en ström av intrångsförsök som ständigt söker nya vägar.

Nya krav och direktiv. Inom EU finns det så kallade NIS-direktivet som blev svensk lag 2018. Det ska säkerställa skyddet av en mängd olika områden klassade som samhällsviktig infrastruktur. NIS-direktivet är utformat för att skydda drift och informationssäkerhet inom anläggningarnas system och att säkra systemen för attacker utifrån.

Detta medför nya krav på den som driver den här typen av anläggningar. Leverans och distribution av dricksvatten identifieras som en samhällsviktig verksamhet med rapporteringsskyldighet, vilket innebär en skyldighet att jobba aktivt och regelbundet med dessa frågor. Råkar du ut för någonting är du rapporteringsskyldig och beredskap måste finnas för hur den rapporteringen ska gå till.

Direktivet gäller alla aktörer över en viss storlek men för många vattenanläggningar i landet kan det vara en teknisk och organisatorisk utmaning att få fram något som liknar en helhetssyn över verksamheten. Förr var dessa anläggningar isolerade öar som kunde låsas in med stängsel och grindar men idag finns förutom de fysiska portarna också mängder av digitala dörrar som kan stå på glänt utan att någon märker det.

Professionella riskanalyser. Med erfarenhet och kunskap i både drift och informationshantering går det att skapa säkerhetssystem som ser till helheten i både vattenanläggningar och andra industriella verksamheter. På Siemens utgår vi från den mest heltäckande standarden för säkerhet i industriella informations- och styrsystem, IEC 62443, för att säkerställa alla aspekter av säkerhet, både tekniska och organisatoriska. Vårt arbete innefattar anläggningens hela livscykel och gäller såväl systemägare som produkt- och tjänsteleverantörer.

Oavsett om du bygger nytt eller ser över en befintlig anläggning är det viktigt att identifiera eventuella risker och att säkerhetsaspekterna är med i projektplanen från början. Att tidigt kunna upptäcka incidenter, interna såväl som externa, innan de leder till störningar är ett effektivt sätt att höja säkerheten. Våra metoder låter oss utvärdera en anläggnings säkerhetsstatus och baserat på detta ta fram en åtgärdsplan.

Heltäckande säkerhetslösningar. På så sätt kan vi tidigt isolera kritiska faktorer för att integrera de rätta säkerhetslösningarna även i komplexa system. Vi har en komplett portfölj av lösningar och tjänster för att implementera och upprätthålla rätt säkerhetsnivå för varje specifik anläggning.

Idag måste vi behandla alla industriella anläggningar som potentiella måltavlor. VA-anläggningar är tack vare sin samhällsbärande funktion extra intressanta för professionellt utförda, koordinerade cyberattacker. Ett angrepp mot ett vatten- och avloppssystem kan medföra stora konsekvenser även vid en begränsad incident.

Det har aldrig varit viktigare att ta ett helhetsgrepp på informationssäkerheten. Vi har lång erfarenhet inom VA-industrin och kan erbjuda de senaste industriella säkerhetslösningarna. ■

siemens.se/vatten
siemens.com/industrial-security
urban.haglund@siemens.com