Stroomversnelling in watermanagement 4.0 een goede zaak voor cybersecurity?

De strijd tegen hackers, scriptkiddies en kleine foutjes

Door Michael Theuerzeit

"Objecten in de watersector hebben een lange levensduur, waardoor gemalen, sluizen en waterbehandelingssinstallaties nog worden aangestuurd met computers en bijbehorende bedieningssystemen die allang niet meer gangbaar zijn", weet Marcel Jutte, managing director bij Hudson Cybertec. Zijn bedrijf is gespecialiseerd cybersecurity en heeft vaak te maken met waterinfrastructuur. De oude systemen in regelkamers zijn volgens hem zeer gevoelig voor hackers en scriptkiddies. Een mogelijke oplossing zijn patches, stukjes software die automatisch updates aanbrengen en codes veranderen.

Testen

Het gebruik van patches maakt het centraal beheer volgens Jutte eenvoudiger en geeft de netwerkomgeving een betere bescherming. Patches zijn binnen de it-sector een beproefde manier om kwetsbaarheden te verhelpen. Echter, niet alle softwareleveranciers kunnen met patches overweg en het uitrollen van een patch kan ertoe leiden dat een controlesysteem niet meer naar behoren functioneert. "Gelukkig testen de meeste leveranciers nu belangrijke besturingssysteempatches, om te zien of hun software daar goed mee om kan gaan", zegt Jutte.

Veel SCADA/HMI-systemen staan in de procesautomatiseringsomgevingen die nu, min of meer, aan elkaar gekoppeld worden via de centrale regelkamers. Hierdoor ontstaan in de centrale regelkamers extra 'entrypoints' voor deze systemen. Daarmee staan de centrale regelkamers gelijk voor een nieuwe uitdaging: implementatie van een goed beheersbeleid voor de systemen die de installaties monitoren.

Aanvallers

Onderlinge spionage lijkt volgens Jutte in de Nederlandse watersector nauwelijks een rol te spelen. Terroristen kunnen proberen het drinkwater te vergiftigen, waarbij ze de sensoren die dit zouden moeten meten, buiten werking stellen. "Gelukkig is de kans hierop ook nog steeds klein. Een groter gevaar zit wellicht in het onbedoeld foutief handelen door de medewerkers zelf", zo denkt Jutte. "Bij een verregaande integratie van systemen, kan een simpele fout verregaande gevolgen hebben. En dan zijn er nog de reguliere hackers en scriptkiddies, die vanuit nieuwsgierigheid kijken hoever ze kunnen binnendringen in systemen en mogelijk onbedoeld voor schade zorgen."

Risicogedreven aanpak

Jutte: "Midden in de dynamiek van watermanagement 4.0 moet de watersector goed oog houden voor het cybersecurityniveau van hun procesautomatisering. De Europese NIS-directive dwingt waterbedrijven tot een risicogedreven aanpak van cybersecurity, zoals deze wordt beschreven in bijvoorbeeld de IEC 62443." De drinkwatersector heeft dan ook baat bij een sectorbrede risicoanalyse, in overeenstemming met de IEC 62443, en een uniforme aanpak van security-assessments. Jutte stelt dat zijn bedrijf hiervoor een speciale tool heeft, die duidelijk kan aangeven waar bedrijven en organisaties staan qua cybersecurity.

De verregaande automatisering van het waterbeheer en de waterbehandeling heeft veel voordelen. Denk aan efficiencyverbetering en kostenbesparing. Maar dit watermanagement 4.0 heeft ook een keerzijde. Door de koppeling en integratie van systemen via het internet, kan de infrastructuur kwetsbaarder worden. Hoe bescherm je je bijvoorbeeld tegen terroristen, hackers en 'scriptkiddies'? Of, misschien nog belangrijker: hoe zorg je ervoor dat een klein foutje door een medewerker geen desastreuze gevolgen krijgt?

Marcel Jutte, managing director bij Hudson Cybertec