SIEMENS

MobilityMatters
Over mobiliteit en veiligheid

Cyber security vanaf de voorkant

Overig nieuws door Redactie MobilityMatters | 29-11-2018

Naarmate we onze vitale infrastructuur verder automatiseren wordt cyber security steeds belangrijker. Siemens Mobility borgt dit van de tender- tot en met de onderhoudsfase en heeft hiervoor een specialistenteam in huis. Siemens AG heeft wereldwijd een traject uitgerold voor het beveiligen van haar producten en oplossingen: het Product & Solution Security-initiatief (PSS). In alle Siemens-organisaties zijn een PSS Officer (PSSO) en PSS Experts (PSSE) aangewezen. Zij zorgen ervoor dat cyber security vanaf de tenderfase via de engineering tot en met de servicefase van objecten is geborgd.

Erik Versteegt is sinds 1 oktober PSSO bij Siemens Mobility in Zoetermeer, dat onder meer sluizen, waterkeringen, bruggen, tunnels en signaalgevers op het hoofdwegennet automatiseert. Hij wordt ondersteund door vijf cyber security engineers (PSSE's). Het team kan ook een beroep doen op CERT (Computer Emergency Response Team), het dedicated cyber security team van Siemens in Duitsland. CERT test

en onderzoekt de eigen systemen van Siemens, maar kan dit ook voor klanten doen. Er werken binnen Siemens zo'n 1.275 Cyber Security Experts en dit aantal is groeiende.

Vanaf de voorkant

"Binnen de kantoorautomatisering (IT) is cyber security al ver gevorderd", aldus Versteegt. "Operationele technologie is echter anders dan informatietechnologie. Het Operating System Windows kan op Tunnelsystemen minder vaak worden geüpdatet dan bijvoorbeeld op een kantoorlaptop, omdat de kans bestaat dat de tunnelbesturing na een update niet meer naar behoren functioneert. Dit betekent dat we iedere update op voorhand uitgebreid moeten testen. Beschikbaarheid is alles in onze sector: onze automatiseringsoplossingen moeten voor 100% werken. Sluizen, tunnels en waterkeringen zijn dan ook kritische objecten. Voor ieder project brengen we aan de voorkant – vaak al in de tenderfase – de risico's en bedreigingen van het systeem in kaart. Op basis hiervan nemen we beveiligingsmaatregelen."

Koploper

"Nederland loopt qua cyber security voorop", vult Sales Consultant Services Harald Hofstede aan. "Veel van onze klanten hebben de eisen rond cyber security de afgelopen jaren aangescherpt, en scannen hun objecten op cyber security. Ze worden stelselmatig naar het bepaalde beveiligingsniveau getild. Voor nieuwe automatiseringsprojecten wordt cyber security vanaf de start meegenomen. We hebben dan intensief contact met de Security Operation Centers van onze klanten, die 24/7 hun eigen netwerken meten. We delen onze ervaringen om de bewustwording binnen ons domein te vergroten, zodat het netwerk en de installaties veiliger en betrouwbaarder worden en dus een hogere beschikbaarheid hebben. Een goed voorbeeld hiervan is het groeiboek Cyber Security dat, vanuit de netwerkorganisatie Centum Ondergrondsbouwen (COB), door afgevaardigden van marktpartijen en overheidsinstanties is opgesteld en waar wij als Siemens Mobility een significante bijdrage aan hebben geleverd."

Mens blijft risico

Op basis van defence in depth heeft Siemens cyber security geïntegreerd in de eigen processen. Het gaat niet alleen om beveiliging van informatie en installaties, maar ook om menselijk handelen. Versteegt: "De mens blijft binnen een automatiseringsomgeving het grootste risico. Cyber security gaat verder dan gerichte

aanvallen. Als iemand ergens in je systeem per ongeluk een geïnfecteerde USB-stick gebruikt kun je al het haasje zijn.”

Testomgevingen

Voor diverse objecten en netwerken borgt Siemens het hoogste level van cyber security tot en met de onderhoudsfase. Testen, updaten en patchen maken hier onderdeel van uit. Hofstede: “Nieuwe objecten hebben steeds vaker een eigen testomgeving. Dit is een absolute noodzaak en wordt gelukkig in toenemende mate gevraagd door opdrachtgevers. Een Windows-patch kan invloed hebben op het SCADA-systeem. Dit moeten we op voorhand kunnen controleren binnen de testomgeving, waarop we veldapparatuur kunnen aansluiten. Zodoende kunnen we een betere inschatting maken van het gedrag en de risico’s die het doorvoeren van een patch in een operationele omgeving met zich meebrengt.” Voor oudere systemen zonder eigen testomgeving heeft Siemens een virtueel cluster, een grote server om na iedere nieuwe update de gevolgen te simuleren voor de software die draait bij de klant. Het gaat dan niet alleen om Windows-updates, maar ook om updates van bijvoorbeeld de Siemens bediensoftware WinCC OA of patches voor de PLC firmware. “Eventuele kwetsbaarheden delen we meteen met de klant om vervolgens samen naar oplossingen te zoeken. Ook partijen die gebruik maken van Siemens oplossingen, die niet door onszelf zijn geinstalleerd kunnen bij ons terecht voor advies en ondersteuning. Op die manier borgen we de hoogste beschikbaarheid van de objecten die we automatiseren.”
