Cybersecurity

Cybersecurity in tijden van corona

Ken je netwerk!

Door Joeri van der Kloet

Nu in veel bedrijven minder personeel op de werkvloer aanwezig is, is het risico dat er minder inzicht en toezicht is op de cybersecurity binnen het bedrijf. Niet alleen omdat fysieke toegang wellicht makkelijker is dan normaal, maar ook omdat er minder zicht is op informatiestromen binnen de operationele processen.

“Als je ter plekke geen zicht hebt op je proces, kan je dan de informatiestromen op processorniveau nog wel vertrouwen?” Sebastiaan Koning, senior consultant bij Hudson Cybertec, legt de vinger op de zere plek: minder personeel op de werkvloer resulteert vaak in minder inzicht in het proces. En dan gaat het niet over de bovenliggende automatiseringslagen, maar dieper in de installatie: de processoren, ofwel de PLC’s. “Juist die PLC is je laatste redder in nood, waar je altijd op moet kunnen vertrouwen. Als er een overstroming plaatsvindt, een sluis een noodstop moet krijgen, of er ergens een chemische brand uitbreekt, moet die automatiseringslaag feilloos werken. Als die systemen gecorrumpeerd zijn, heb je in zo’n situatie een levensgroot probleem”, aldus Koning.

In tijden van corona

Goede cybersecurity zit hem niet uitsluitend in de technische kant. Dus alleen het plaatsen van firewalls is zeker niet voldoende. De mens op de werkvloer én de organisatie zijn, samen met de techniek, de drie pijlers waar cybersecurity op rust. In tijden van corona zijn die twee niet-technische pijlers anders dan anders. En dat kan gevolgen hebben voor cybersecurity, weet Koning: “Minder mensen op de vloer betekent minder overzicht. Zonder goede toegangsbeveiliging kunnen mensen gemakkelijker binnenkomen en minder snel worden opgemerkt. Een crimineel met verstand van zaken trekt ergens een camera of een PLC los, sluit een laptop aan die zich voordoet als die camera of PLC en hij kan zo je bedrijfsnetwerk op.”
Bij een minder goede fysieke controle wordt een sluitende cybersecurity, vooral in de operationele omgeving, belangrijker. Koning: “Door het thuiswerken mis je de digitale bescherming die je binnen de muren van je bedrijf wel hebt. Ook al probeer je het thuiswerken goed in te richten, je hebt er toch minder controle op. In de praktijk zullen mensen niet heel snel vanuit huis inloggen op een installatie, maar toch is dat niet ondenkbaar.”

Beperkt

Als installaties toch benaderd moeten worden vanuit een ander netwerk, moet dat veilig gebeuren. Koning: “Dat hele protocol moet voldoen aan de IEC62443-norm, de internationale cybersecuritynorm voor Industrial Automation & Control Systems (IACS). Daarbij breng je op een slimme manier segmenteringen aan in je netwerken en systemen. Die richt je vervolgens zo in dat als er een ‘breach’ plaatsvindt, de schade beperkt blijft tot een gedeelte van je installatie.”
Op afstand kunnen inloggen op het netwerk hoeft niet per se een probleem te zijn, maar alleen als voldaan is aan een aantal voorwaarden. “Werk daarbij met een protocol waarbij degene die inlogt alleen de hoognodige rechten krijgt binnen de gekaderde systemen”, legt Koning uit. “Het is niet slim om iemand op afstand op een engineer workstation te laten komen, waarbij alle PLC’s in de installatie kunnen worden benaderd. Er is in het operationele domein ook helemaal geen reden om iemand op afstand bij je PLC’s te laten.”

Ken je netwerk

Aan de andere kant is het zeker wel nuttig om informatie op afstand te kunnen uitlezen. Koning: “Dat geeft veel mogelijkheden om processen in de gaten te houden. Maar je kunt die mogelijkheid ook gebruiken om het netwerk zelf te monitoren. ‘Ken je netwerk’ zeggen wij bij Hudson Cybertec altijd. Want hoe kun je op bepaalde communicatie vertrouwen als je zelf geen inzicht in die communicatie hebt? Je hebt inzicht nodig in de onderlinge componenten en op de manier waarop die componenten met elkaar communiceren.”

In de praktijk is dat in de IT (informatietechnologie) beter geregeld dan in de OT (operationele technologie). “Dat is verklaarbaar”, vindt Koning. “Vanwege de ‘legacy’ (veroudering van systemen, red.) en de snelheid waarmee ontwikkelingen in de OT plaatsvinden. Maar wil je het veilig maken, zal je toch echt moeten beginnen met je netwerk goed in kaart brengen.” Dat er nu een crisis aan de gang is, wil niet zeggen dat deze tijd ongeschikt is voor het aanscherpen van de cybersecurity, integendeel. Koning: “Ik zou zeggen: doe het juist nu, want heel veel zaken en delen van de installaties zijn op dit moment minder in bedrijf. Je kunt er nu juist vaak beter bij dan onder normale omstandigheden. Een deel van het inventarisatiewerk kunnen we ook middels online interviews al doen.”

OT-monitoring

Het is van groot belang, en niet alleen nu, om precies te weten welke activa er zijn en dat het netwerkverkeer inzichtelijk is, zodat niets aan het toeval wordt overgelaten. “Hiervoor maken wij gebruik van onze OT-monitoring-oplossing”, legt Koning uit. “Deze meet onder andere afwijkingen in het netwerkgedrag binnen het OT-netwerk. Deze gedetecteerde afwijkingen kunnen duiden op een cyberaanval, maar ook op ongeoorloofde toegang tot systemen of zelfs ongeoorloofde ‘setpointwijzigingen’. De Hudson Cybertec-oplossing voor OT-monitoring is specifiek voor het OT-domein ontwikkeld en verder geoptimaliseerd.”
Aan de hand van een voorbeeld bij de waterschappen, maakt Koning duidelijk hoe dat werkt. Het draait om het verschil tussen ‘intrusion detection’ en ‘intrusion prevention’. “IT gaat altijd voor prevention”, weet Koning. “Maar daarmee leg je soms ook je proces deels plat. Neem nu de waterschappen: een gemaal gebruikt in de regel tussen de 0 tot 80 procent van het vermogen om water weg te werken. Als een waterschap ineens op 100 procent van z’n vermogen begint te draaien, legt een ‘prevention systeem’ het gemaal plat, want er zou een cyberaanval kunnen plaatsvinden. Als je die monitoring te rigide maakt, snij je jezelf in de vingers, want bij hevige regenval moet dat gemaal toch echt op 100 procent kunnen draaien, ook al komt dat bijvoorbeeld maar eens per jaar voor. Intrusion detection gaat daar flexibeler mee om: die maakt wel die melding, maar zorgt ervoor dat als de procesoperator dat wil, het gemaal toch op 100 procent kan draaien. Detectie en alarmering dus, in plaats van blokkering.”

Ketenveiligheid

Ondanks dat OT-cybersecurity nog lang niet op het niveau is van IT-cybersecurity, ziet Koning wel ontwikkelingen. “Bedrijven die hun IT- en OT-kant goed op orde hebben, kijken vaak ook al verder dan alleen hun eigen installatie. Er zijn bedrijven die zeggen: ‘Als je zaken met ons wilt doen, zal jouw bedrijf ook conform IEC 62443 moeten functioneren. Ketenveiligheid dus. Maar nogmaals, het begint bij jezelf: ken je netwerk!”

Meer info:
www.hudsoncybertec.com