Cyber meets Safety

Geen safety zonder cybersec

Safety staat in de procesindustrie al jarenlang hoog op de agenda, terwijl dat voor cybersecurity pas recent relevant is geworden. Toch is de tegenstelling tussen cybersecurity en safety een vrij arbitraire tegenstelling. Er zijn weliswaar verschillen tussen de twee begrippen, maar er zijn zeker ook overeenkomsten. Sterker nog, zonder goede cybersecurity kan je ook geen safety realiseren, menen Marcel Jutte, Managing Director, en William van der Veen, Senior Safety/Security Consultant, beiden werkzaam bij Hudson Cybertec.

urity

Redactie Process Control

Een Safety Instrumented System (SIS) is de 'last automated line of defense' van een productieproces in de industrie en is als zodanig vastgelegd in de IEC 61511 norm.

Een SIS is daarmee feitelijk een geautomatiseerde bewaking van het proces om in geval van nood het proces gecontroleerd veilig af te schakelen en een rampscenario te voorkomen. Na het SIS is er dus geen geautomatiseerd systeem dat ingrijpt om een ophanden zijnde calamiteit te voorkomen. Naast de reeds genomen schadebeperkende/reducerende maatregelen blijft alleen nog de oplettendheid van operators over om na een calamiteit in te grijpen om zo serieuze schade en letsel te beperken.

Offline

Maar die SIS systemen zijn steeds vaker het doelwit van cyberaanvallen, weet Van der Veen. "Door in het beginstadium van een cyberaanval het SIS systeem buiten werking te stellen, of offline te krijgen, kan in een vervolgstadium van de aanval serieuze schade aan de productie-installatie en letsel aan medewerkers toegebracht worden. Dat zijn dus serieuze aanvallen met potentieel grote schades tot gevolg. Het laat ook goed zien dat er onderdelen van het proces zijn waar safety en cybersecurity heel dicht bij elkaar komen."

Intrinsiek veilig

Laten we eerst eens kijken naar die overeenkomsten tussen safety en cybersecurity, want volgens Van der Veen zijn die er wel degelijk. "Cybersecurity en safety vergen een vergelijkbare aanpak en methodologie om de risico's te beheersen. Middels een risicoanalyse (RVA) dienen risico's geïdentificeerd te worden, geanalyseerd of geprioriteerd en daarna gemitigeerd of gereduceerd middels maatregelen."
Ook de volgorde van risicoreductiestappen is bij cybersecurity min of meer hetzelfde als bij safety. "Je begint met de risico's; eerst maak je de systemen intrinsiek veilig, zodat een gevaar simpelweg niet aanwezig is. Denk bij safety voor mechanische gevaren aan het beperken van de snelheid van bewegende delen en denk bij cybersecurity aan het segmenteren of zoneren (DMZ invoeren) van het industriële netwerk", legt Van der Veen uit.

PBM's en passwords

Na deze eerste stappen kunnen technische maatregelen genomen worden: hekken in geval van safety, firewalls in geval van cybersecurity. Om de nog overgebleven risico's te beheersen, moeten procedurele maatregelen genomen worden, bijvoorbeeld door Persoonlijke Beschermings Middelen in geval van safety, of door een goed wachtwoordbeheer voor cybersecurity. Als laatste dient men informatie te verschaffen over de restrisico's. "Dan moet je bij cybersecurity en bij safety vooral denken aan awareness training", licht Van der Veen toe.

SIL en SL

Nog een overeenkomst tussen safety en cybersecurity is dat voor beiden in een methode is voorzien voor de beoordeling of waardering van systemen met betrekking tot de betrouwbaarheid en veiligheid van de processen. "Wat Safety Integrity Levels (SIL) zijn voor safety, zijn Security Levels (SL) voor cybersecurity", vertelt Van der Veen. "Middels SL's kan de mate van cybersecurity weerbaarheid van IACS beschreven worden. Ook zijn SL's een maatstaf voor de capaciteit van producten om aan een bepaald cybersecurity niveau te kunnen voldoen."

V&G

Verschillen tussen safety en cybersecurity zijn er echter ook. Safety is al lange tijd een bekend onderdeel van de bedrijfsvoering van industriële bedrijven. Onder andere duidelijke wet- en regelgeving op het ge-

William van der Veen, Senior Safety/Security Consultant, werkzaam bij Hudson Cybertec.

bied van safety heeft er toe geleid dat safety gemeengoed is geworden. "Vaak heeft een bedrijf een V&G-plan of een onderhoudsplan waar, naast Arbo ook safety in is uitgewerkt", vertelt Van der Veen.
Ook is er een financieel aspect. Omdat safety gemeengoed is geworden, zijn er ook vaak specifieke budgetten voor safety.

CSMS

Voor cybersecurity is het bovenstaande nog veel minder het geval, weet Jutte. "Bij cybersecurity moet vaak eerst nog het management overtuigd worden van het nut en de noodzaak, voordat er budget vrijgemaakt wordt. Ook moet vaak eerst nog een Cyber Security Management Systeem (CSMS) ingericht worden om alle aspecten, namelijk mens, proces en techniek, te beheersen op het gebied van cybersecurity-risico's en het opstellen van een cybersecurityplan. Het cybersecurityplan is feitelijk dat wat een V&G plan is voor safety. Wij helpen veel bedrijven bijvoorbeeld door een CSMS in te richten of door het invullen van een CISO/COSO rol."

IDS

Men kan aan de voordeur maatregelen nemen om een aanval te voorkomen. Daarmee is een succesvolle aanval echter niet uit te sluiten. In tegenstelling tot safety, waar elke consequentie uit den boze is, worden bij cybersecurity ook achter de voordeur maatregelen getroffen, waarbij de consequenties van een aanval beperkt worden, bijvoorbeeld door een backup plan of continuity plan. "En als er een succesvolle aanval heeft plaatsgevonden, kan dat middels monitoring (IDS) snel geconstateerd worden en mogelijk de daders achterhaald worden", vertelt Jutte. "Zonder monitoring worden helaas veel (digitale) incidenten afgedaan als onverklaarbare of "technische" storingen."

Verder kijken

Waar bij safety de gevaren zijn te omschrijven in een eindige lijst, moet men bij cybersecurity altijd rekening houden met mogelijk nieuwe kwetsbaarheden, zoals zero days (bedreigingen die nog niet algemeen bekend zijn). "De mogelijke gevolgen in het geval van cybersecurity zijn ook vaak lastiger voor te stellen dan bij safety", weet Jutte. "Maar de gevolgen kunnen minstens zo groot of kwalijk zijn. Bovendien moet je bij cybersecurity verder kijken dan je denkt. Je hebt het dan over de continuïteit van de hele organisatie."

Borgen

Volgens Van der Veen is er een integrale aanpak van zowel safety als cybersecurity nodig om de continuïteit van de bedrijfsvoering te borgen. "Hierbij zijn zowel cybersecurity als safety van belang", meent hij. "Wanneer een bedrijf de cybersecurity niet geregeld heeft, is de safety ook niet geborgd. Cyberrisico's introduceren weliswaar niet perse nieuwe gevaren met betrekking tot safety, maar de genomen safety beheersmaatregelen kunnen wel buiten werking gesteld worden door gebrekkige cybersecurity. Dan heb ik het nog niet eens over milieuschade en imagoschade."

IEC 61511 vs IEC 62443

Organisatorisch is het nog lastig om safety en cybersecurity integraal aan te pakken, weet Van der Veen: "Je kunt safety en cybersecurity bijvoorbeeld niet tegelijk in dezelfde RVA meenemen. Ondanks de overeenkomsten is de benadering van cybersecurity risico's een andere dan die van safety risico's. Waar de IEC 61511 een framework is voor het managen van Safety Instrumented Systems in de procesindustrie, is de IEC 62443 een framework voor het managen van cybersecurity voor systemen in de OT." (Operationele Technologie, red.).

Marcel Jutte, Managing Director, werkzaam bij Hudson Cybertec.

Cyber-certificering

De IEC 62443 is inmiddels de wereldwijd geaccepteerde cybersecurity normenreeks voor Industrial Automation & Control Systems (IACS). De normenreeks beschrijft middels het opzetten van een CSMS en middels uit te voeren RVA's, hoe de Security Levels (SL's) bepaald kunnen worden, zodat de risico's en kwetsbaarheden van veiligheidssystemen beheerst kunnen worden. "Op deze manier maak je de safety van de processen weerbaarder tegen aanvallen zoals Triton", verduidelijkt Jutte.
"Safety is nu onderdeel van CE-markering. In de nabije toekomst zal iets soortgelijks ook voor cybersecurity gaan gelden. Er zal middels een RVA aangetoond moeten worden dat de genomen mitigerende maatregelen afdoende zijn om de cyberrisico's en cyber-kwetsbaarheden van de betreffende IACS te beheersen. Ook is de verwachting dat cybersecurityproducten een "cyber-certificering" krijgen om hun cybersecurity capability mee aan te geven, vergelijkbaar met SIL", besluit Jutte.

Over Hudson Cybertec

Hudson Cybertec is al jaren actief betrokken bij de ontwikkeling en totstandkoming van de IEC 62443 en wordt internationaal beschouwd als de IEC 62443 Subject Matter Expert (SME). Ze zijn een leveranciersonafhankelijke dienstverlener van cybersecurity consultancy en diensten, welke wereldwijd betrokken is bij cybersecurity trajecten voor de operationele technologie (OT) en de daaraan gekoppelde IT-omgevingen. De focus ligt op een holistische aanpak van cybersecurity, waarbij de aspecten mens, organisatie en techniek centraal staan. Hudson Cybertec is gespecialiseerd in het uitvoeren van RVA's en het schrijven van cybersecurity beleid. Als partner van het Nederlands Normalisatie Instituut (NEN) verzorgt Hudson Cybertec een 3-daagse training Cyber Security for Industrial Automation & Control Systems (IACS), getiteld "Take control over your security risks with the IEC 62443". Tijdens het driedaagse programma raakt u bekend met relevante cybersecurity terminologie, krijgt u een uitstekend begrip van de IEC 62443 norm en leert u uw nieuwe kennis en vaardigheden toe te passen binnen de praktijk van uw eigen organisatie.

Direct inschrijven kan via deze URL: https://www.hudsoncybertec.com/en/inschrijven/
U kunt ook op www.processcontrol.nl de link vinden en extra informatie vinden als u zoekt op 'IACS training'.