SDN innovatieproject #18

De impact van cybersecurity op de procesveiligheid van gevaarlijke stoffen in de Nederlandse chemische industrie

Milan Lopuhaä-Zwakenberg

Stefano Nicoletti

Reza Soltani

Mariëlle Stoelinga

Formal Methods & Tools, Informatica, Universiteit Twente

UNIVERSITY OF TWENTE.

SAFETY DELTA NEDERLAND

vinden, verbinden, vernieuwen in veiligheid

1. Inleiding

In de chemische industrie is veiligheid van groot belang. Hiermee wordt niet alleen de veiligheid voor de werknemers zelf bedoeld, maar ook de veiligheid van de fabriek en de omgeving, bijvoorbeeld als er door een ongeluk een lekkage van gevaarlijke stoffen ontstaat. SDN heeft als doel de Nederlandse chemische industrie de veiligste ter wereld te maken.

Hoewel de chemische industrie enigszins achterloopt op andere industrieën qua digitale verbondenheid (1), speelt digitale verbondenheid ook in de chemische industrie een steeds grotere rol, en heeft zeker na de coronapandemie een vlucht genomen (2). Deze digitalisering heeft grote positieve effecten op de bedrijfsoperationaliteit en het samenwerken met de keten, maar brengt ook het risico op cyberaanvallen met zich mee. Een bekend voorbeeld is de ransomware-aanval op Colonial Pipeline in 2021, waarbij het bedrijf 4,4 miljoen dollar in Bitcoin heeft betaald om de oliepijplijn weer in gebruik te kunnen nemen (3). Naast de financiële gevolgen zorgde het gebrek aan functioneren van de pijplijn voor enkele dagen voor brandstoftekorten in delen van de VS.

Naast gevolgen op financieel gebied en voor de bedrijfsvoering kunnen cyberrisico's ook gevolgen hebben voor de veiligheid (safety): als de industrial control systems (ICS) van een bedrijf met het internet verbonden zijn, dan zou een cyberaanvaller die hier toegang tot heeft de procesparameters kunnen beïnvloeden, met mogelijke gevaarlijke situaties tot gevolg. Dit is geen hypothetisch scenario: uit onderzoek van Bridewell blijkt dat 93% van de organisaties in de Britse kritieke nationale infrastructuur een succesvolle cyberaanval op hun ICS of OT-omgeving heeft gehad (4).

Het is dus van groot belang dat de cybersecurity van ook de Nederlandse chemische industrie dusdanig op orde is, dat de de resulterende risico's op de veiligheid voldoende beperkt zijn. Hoezeer dit op dit moment het geval is, is echter de vraag. Uit een recent onderzoek van Fox-IT in opdracht van DCMR (5) blijkt dat chemische bedrijven zeer verschillen in hun cybervolwassenheid, variërend van nauwelijks bestaand tot tot goed voorbereid. Deze resultaten roepen de vraag op hoezeer de veiligheid in het geding komt door een gebrek aan cybervolwassenheid.

1.1 Onderzoeksvragen

Dit rapport is het eindresultaat van een SDN-onderzoek uitgevoerd aan de Universiteit Twente, Het voornaamste doel is te bepalen wat de staat is van de cybersecurity in de Nederlandse chemische industrie met betrekking op veiligheid. Hierbij richten we ons voornamelijk op de procesveiligheid met betrekking tot de transport, opslag en verwerking van gevaarlijke stoffen, in de ±400 chemische bedrijven die onder de BRZO-wetgeving vallen (*Besluit Risico's Zware Ongevallen*), de Nederlandse wetgeving voor bedrijven die grote hoeveelheden gevaarlijke stoffen verwerken. Naast de vraag wat de huidige staat van cybersecurity is, onderzoeken we ook wat SDN kan doen om deze te verbeteren. Dit leidt tot de volgende twee onderzoeksvragen:

1. *Wat is de staat van de cybersecurity in BRZO-bedrijven t.o.v. de procesveiligheid van gevaarlijke stoffen?*
2. *Indien nodig, wat moet er gebeuren om de staat van de cybersecurity te verbeteren, en hoe kan SDN hieraan bijdragen?*

4. Conclusies

De voornaamste conclusie die uit dit onderzoek getrokken kan worden is de chemische industrie op dit moment onvoldoende voorbereid is op cyberincidenten die impact kunnen hebben op de procesveiligheid. Dit gebrek aan voorbereiding blijkt al uit het bewustzijn van de risico's op bedrijfsniveau, dat in veel bedrijven, voornamelijk de kleinere, onvoldoende aanwezig is. Dit bewustzijn is noodzakelijk om ervoor te zorgen dat er voldoende tijd, geld en personeel gestoken wordt in cybersecurity. Dat laatste is uit zichzelf ook al een bottleneck, aangezien er maar weinig mensen te vinden zijn met voldoende kennis van zowel cybersecurity als de OT-omgeving.

Omdat het huidige onderzoek bestond uit interviews met voornamelijk brancheorganisaties, kan een vollediger beeld verkregen worden door ook bedrijven zelf te betrekken. Met name kleinere bedrijven zijn hierbij interessant, omdat deze naar verwachting geen specifiek cybersecurityteam hebben, en waarschijnlijk de grootste kwetsbaarheden bevatten.

Op grond van de interviews zijn er voor BRZO-bedrijven wel een aantal globale aanbevelingen te maken. Ten eerste is er bewustzijn nodig, zowel op bedrijfsniveau, om te zorgen dat er voldoende aandacht besteed wordt aan cybersecurity, als op mederwerkersniveau, om de risico's van vaak voorkomende aanvallen zoals phishing te beperken. Daarnaast is het van groot belang om goed aandacht te schenken aan de link tussen de IT- en OT-omgevingen, omdat cyberaanvallen die van deze verbinding gebruik kunnen maken, kans maken om de procesveiligheid te beïnvloeden. Een goed uitgangspunt is de *security by design*-filosofie, waarbij al bij het ontwerp wordt nagedacht over mogelijke aanvallen en hoe die kunnen worden tegengegaan. Ook is het belangrijk om aan geïntegreerd risicomanagement te doen, waarbij cybersecurity en safety beiden beschouwd worden, zowel apart als in mogelijke interacties. Tot slot is het van groot belang om ook rekening te houden met cascade-effecten die veroorzaakt kunnen worden door kwetsbaarheden bij ketenpartners.

5. Aanbevelingen voor vervolgonderzoek

Naast de aanbevelingen voor bedrijven uit het vorige hoofdstuk kunnen, op basis van het huidige onderzoek, ook een aantal aanbevelingen gedaan worden op het gebied van innovaties of vervolgstudies.

1. *Case studies*: Waar dit rapport een globaal overzicht geeft, zou een case study bij een chemisch bedrijf een concreet en gedetailleerd beeld kunnen geven van hoe cybersecurity impact kan hebben op de procesveiligheid bij dat bedrijf. Vooral een kleiner bedrijf dat nog minder heeft nagedacht over deze relatie is hierbij interessant, omdat het juist deze bedrijven zijn waar potentieel de grootste risico's liggen. Hierbij moet wel gezegd worden dat deze bedrijven waarschijnlijk ook het minst snel te interesseren zijn in zo'n case study.
2. *Threat detection in geconvergeerde IT/OT-omgevingen*. Er kan gekeken worden naar hoe geautomatiseerde threat detection vormgegeven kan worden, niet alleen specifiek voor het IT- of OT-systeem van de organisatie, maar als algeheel systeem in de gehele digitale infrastructuur. Dit is van belang omdat cyberaanvallen potentieel de IT-omgeving gebruiken om de OT-omgeving te bereiken, en om deze aanvallen te detecteren moet er op een holistische manier met alerts omgegaan worden. Daarnaast moet deze threat detection gecombineerd worden met geautomatiseerde preventie en responsstrategieën.
3. *Geïntegreerd, kwantitatief risicomanagement.* Om de interactie tussen (cyber)security en veiligheid goed te begrijpen is het nodig om methodes van risicomanagement te hebben die beiden combineren. Door dit op een kwantitatieve wijze te doen, kan ook bijgedragen worden aan het bewustzijn: de impact van cybersecurity kan daarmee uitgedrukt worden in termen van bijvoorbeeld fysieke schade of geldelijk verlies, wat een duidelijke motivatie geeft om de weerbaarheid tegen cyberaanvallen te verdedigen. Een mogelijkheid hierbij is om *fault tree analysis*, dat al in de chemische industrie gebruikt wordt, te combineren met de *attack tree analysis* uit cybersecurity.
4. *Onderzoek naar digitale cascade-effecten.* Er moet onderzoek gedaan worden naar de potentiële impact van digitale cascade-effecten op de procesveiligheid. Dit kan gecombineerd worden met het vorige punt om een digitale tegenhanger te krijgen van bestaande mitigatie van fysieke domino-effecten: in plaats van een berekening die uitwijst hoe ver twee fabrieken van elkaar af moeten staan om het overslaan van brand te voorkomen, een berekening die vertelt tot op welke hoogte twee bedrijven digitaal verbonden kunnen zijn zonder dat de veiligheidsrisico's te groot worden. Ook hierbij zijn case studies belangrijk, voornamelijk bij kleine bedrijven, te meer omdat via deze cascade-effecten incidenten bij een klein bedrijf ook impact kunnen hebben op grotere bedrijven in dezelfde keten.