#18: Risico’s als gevolg van digitale verbinding

Milan Lopuhaä-Zwakenberg
Informatica, Universiteit Twente

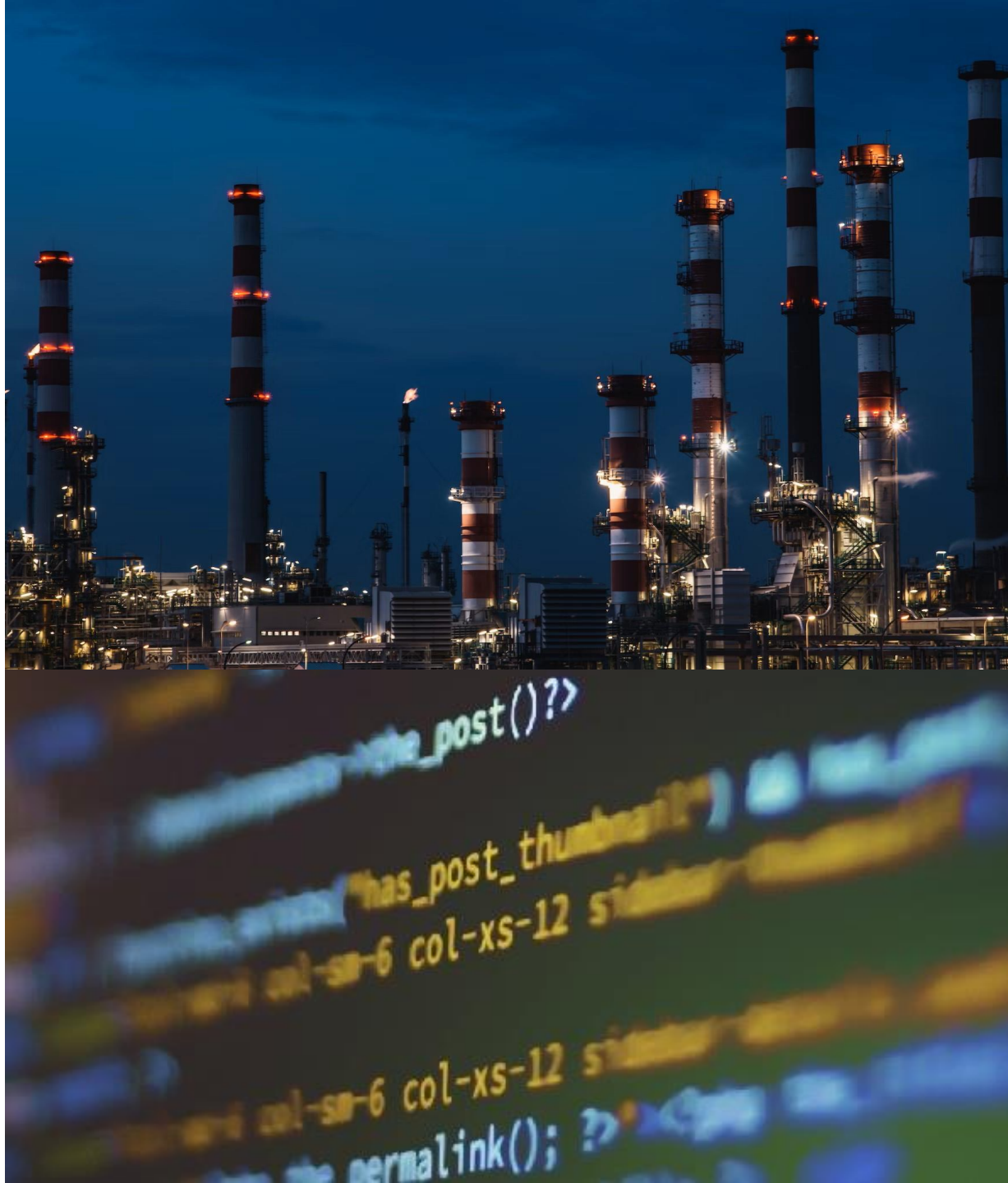


Foto: Maksym Kaharlytskyi

Foto's: Mufid Majnun, Ethan Wilkinson

Achtergrond

Safety: risico op schade (mens, omgeving,…) door het niet functioneren van systemen

Security: systeem functioneert ondanks risico's door bedreigingen

Achtergrond

Doel SDN: Nederlandse chemische industrie veiligste ter wereld (safety)

- (Cyber)security kan impact hebben op safety:
  - Ransomware-aanval kan systeem platleggen
  - Cyberaanval kan systeem overnemen
- Meer en meer digitale verbondenheid
- NIS-2, CER: cybersecurity moet op orde zijn

Onderzoeksvraag: Hoe staat het met de safety van de Nederlandse chemische industry m.b.t. cybersecurity?

Siegfried, Brenntag, and Symrise hit by cyberattacks

Companies say hacker activity caused temporary production shutdowns

by ***Melody M. Bomgardner***

May 27, 2021 | A version of this story appeared in **Volume 99, Issue 20**

Chemical Industry a High value target for Cyber attacks

Leave a comment / Industry news / By Matthew Reynard

The Chemical industry is facing an onslaught of Cyber attacks. A UK Government study from 2021 estimated that Cyber attacks created a loss of £1.3 Billion for companies operating within the chemical industry.

US chemical plants risk disastrous cyberattacks relying on guidance a decade out of date

Foto: c&en, Fundamentals First, chemistryworld

Achtergrond

Onderzoeksvraag: Hoe staat het met de safety van de Nederlandse chemische industry m.b.t. cybersecurity?

Voor dit onderzoek:

- *Process safety*
- m.b.t gevaarlijke stoffen
- Bij BRZO-bedrijven

Foto: The Chemical Engineer, Steve Froebe

Methodologie

Interviews met:

- SDN
- VNCI
- DCMR
- TKI Chemie
- Ministerie I&W
- Sitech

Hoofdvragen:

- Hoe staat het met inzicht, weerbaarheid t.o.v. cybersecurity?
- Hoe kunnen deze verbeterd worden en wat staat verbetering in de weg?

Resultaten: vraag #1/7

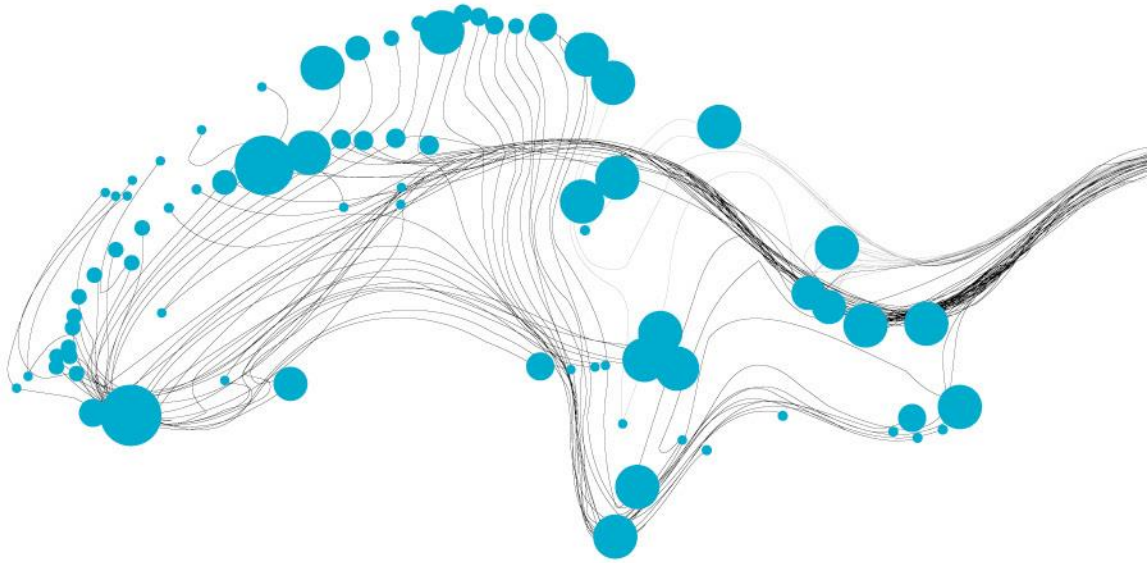
Hebben BRZO-bedrijven voldoende inzicht in de kwetsbaarheid/weerbaarheid?

- Grote bedrijven waarschijnlijk wel (maar ook niet altijd!)
- Kleine bedrijven waarschijnlijk niet
- Vraag bedrijven zelf!

Resultaten: vraag #2/7

Wat staat voldoende inzicht in de weg?

- Awareness: wat zijn de risico's?
- Kennis: wat kun je er tegen doen?
  - Wie dan?



Resultaten: vraag #3/7

*Voorzover inzicht er **wel** is, wat zijn de zwakke plekken?*

- Mensen
- Link IT-OT
- Vraag bedrijven zelf!

Resultaten: vraag #4/7

Welke maatregelen zijn nodig?

- Awareness:
  - Bedrijfsniveau
  - Werknemerniveau
- Geïntegreerd risicomanagement
- Cybersecurity op hetzelfde niveau als safety

Resultaten: vraag #5/7

Welke barrières zijn er tot het implementeren van maatregelen?

- Tijd
- Kennis (werknemers met kennis van OT én cybersecurity)
- Verschil tussen IT en OT
- Vraag bedrijven zelf!

Resultaten: vraag #6/7

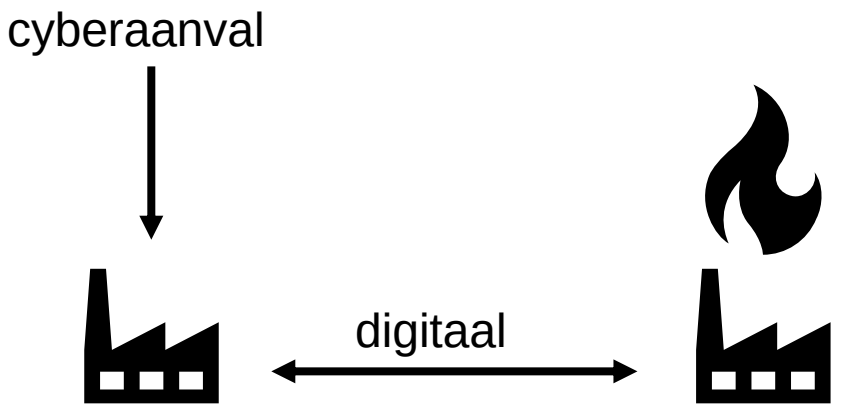
Wat heeft cybersecurity-wetgeving nodig om succesvol geïmplementeerd te worden?

- Transparantie en duidelijkheid
- Cybersecurity moet niet clashen met safety-wetgeving
- Integrale toezichthouders (wie dan?)

Resultaten: vraag #7/7

Hebben bedrijven inzicht in digitale cascade-effecten?

- Kan invloed hebben op ‘klassieke’ domino-effecten
- Nieuw, waarschijnlijk alleen grote bedrijven
- Vraag bedrijven zelf!



Conclusies

Wat is de staat van cybersecurity m.b.t. process safety?

1. **Vraag bedrijven zelf!**
2. Grote bedrijven waarschijnlijk ok, kleine bedrijven minder
3. Grootste risico's/benodigdheden:
    1. Awareness (op bedrijfs- en medewerkersniveau)
    2. Kennis/expertise in cybersecurity én OT
    3. Link IT/OT
    4. Geïntegreerd risicomanagement

Aanbevelingen

- Gedetailleerde *case studies*, juist bij kleine bedrijven
- Holistische *Threat detection* in gecombineerde IT/OT-omgevingen
- Geïntegreerd, kwantitatief safety/security-risicomanagement
- Onderzoek naar digitale cascade-effecten, juist bij kleine bedrijven