

# BERT EN BORIS ONDERSCHATTEN SECURITY NIET



en &  
nware in  
strie

ilig en  
k mijn  
e(s)?

# Hoe groot is de kans op een cyberincident?

## TRITON Malware Targeting Critical Infrastructure

### Could Cause Physical Damage

Almi Smart Machini  
bestanden terug te

26 februari 2018 om 12:20 uur

Thursday, December 14, 2017 Wang Wei

Share 2.96k Share 711 Tweet Share

Een jaar geleden werd Almi S  
Vriezenveen getroffen door e  
dat had grote financiële gevo  
delen, wil directeur Frank Lar  
hiervoor waarschuwen. De gr  
toch niet, nou ga daar maar n  
ledereen overkomen, dat is ir



Almi Smart Machining uit Vriezi  
in handen van een hacker. Het is al meer dan een jaar  
geleden, maar het zit nog heel diep. 'Alles was versleuteld.  
Niet alleen alle interne computers, maar ook de externe NAS-  
server inclusief onze interne back-up. Tja, dan sta je wel even  
heel raar te kijken', vertelt Frank Landhuis, directeur van Almi.

#### Alles versleuteld

Even terug in de tijd. Het was dus 18 januari 2017. 'Nee,  
eindelijk werd de staat door de hacker een dag eerder

Security researchers have uncovered another nasty piece of  
malware desig  
systems (ICS  
threatening a



Cause

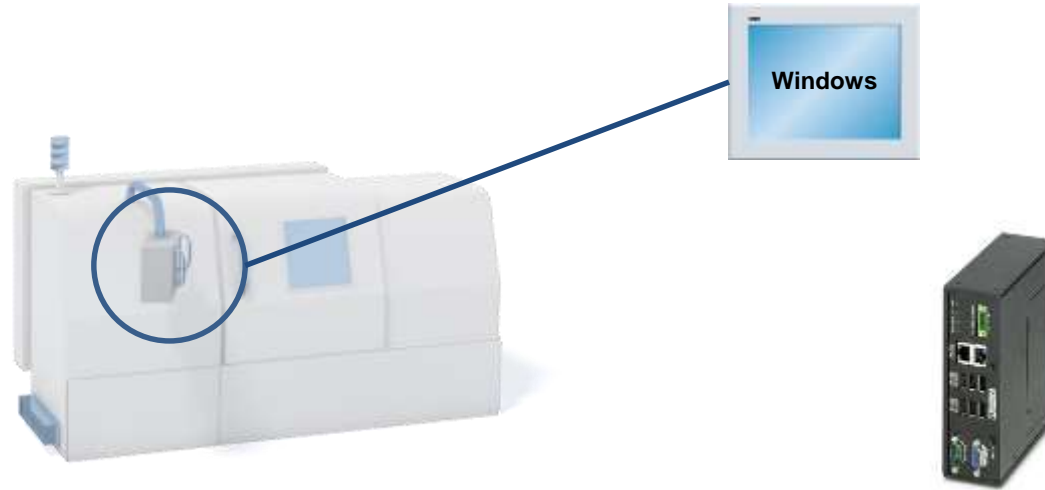
'Alles wa  
interne co  
NAS-serve  
Tja, dan sta  
vertelt Fran

Meer over

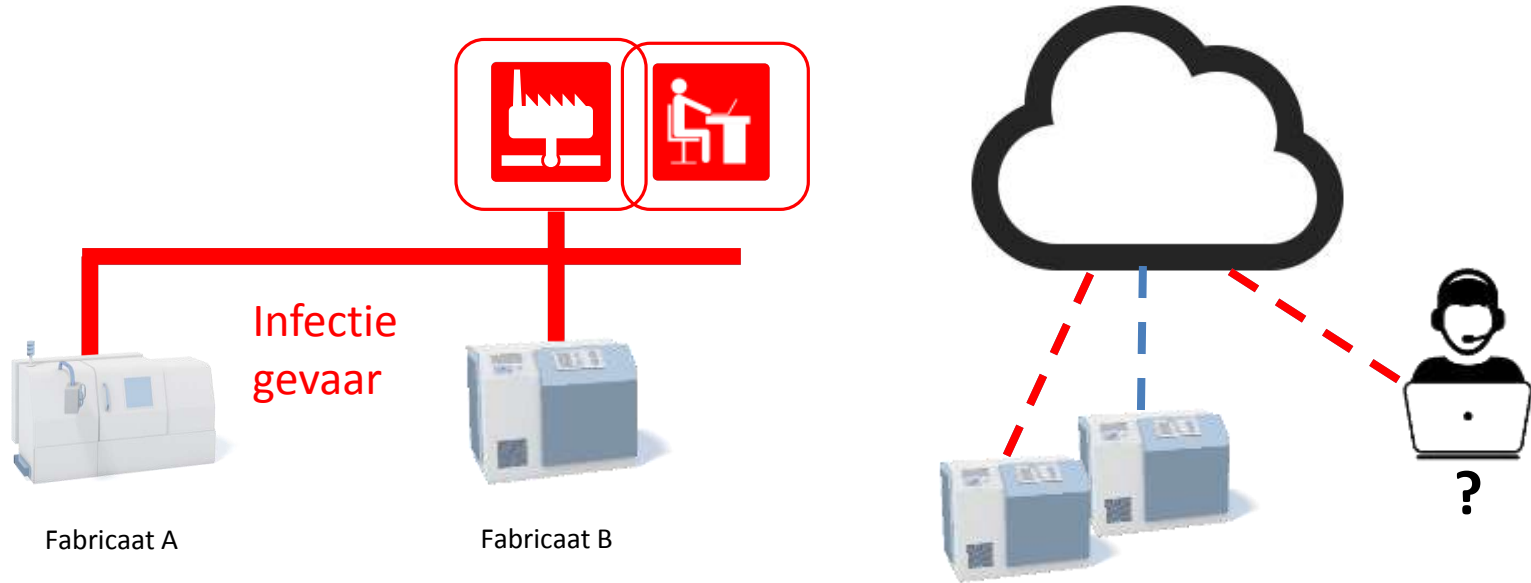
15 maart 2018 ••• Hart van Holland Nijkerk

Industrial Ethernet

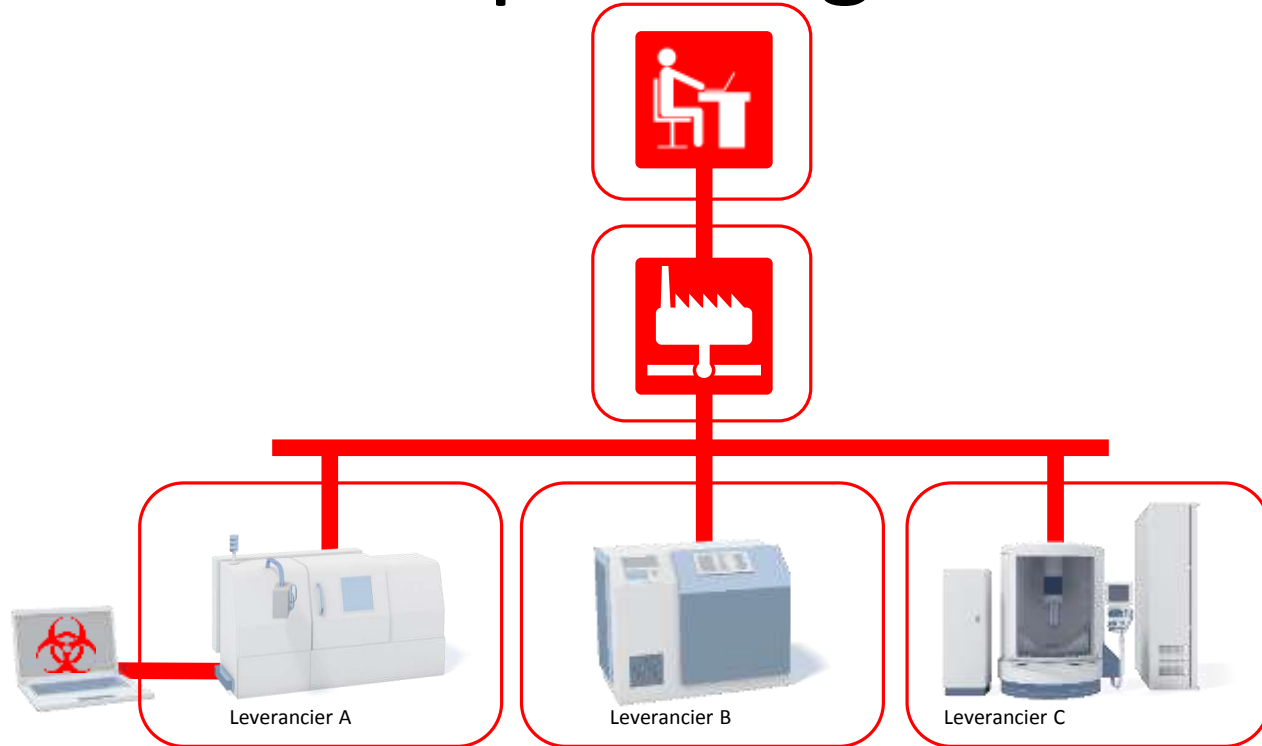
# Hoe dan?



# Hoe dan?



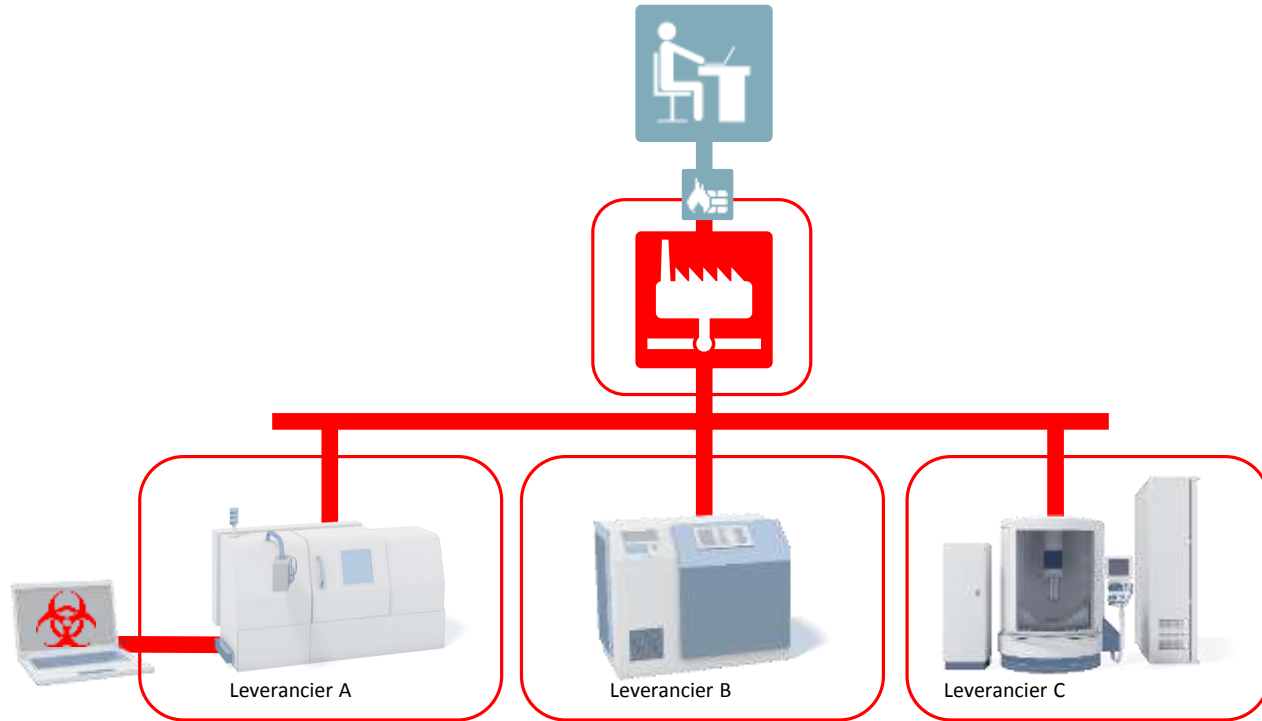
# Oplossing?



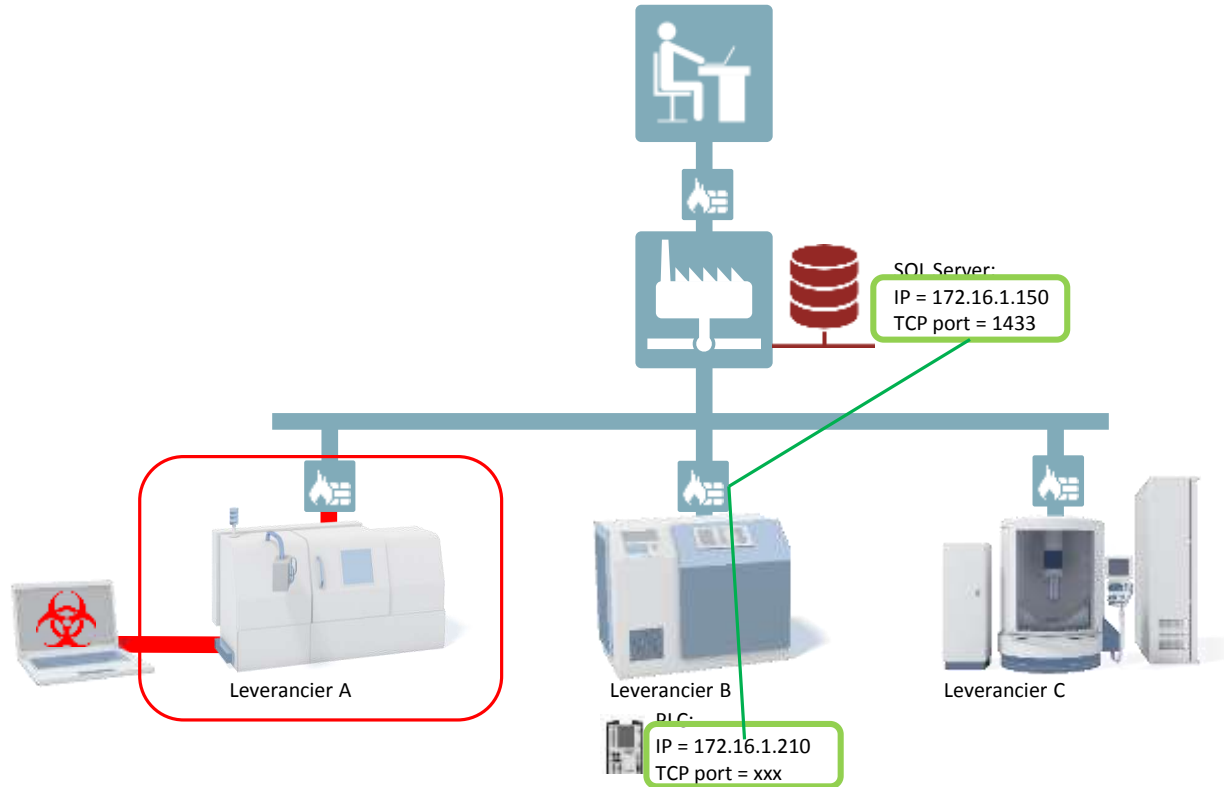
15 maart 2018 ••• Hart van Holland Nijkerk

## Industrial Ethernet

# Oplossing: segmentatie

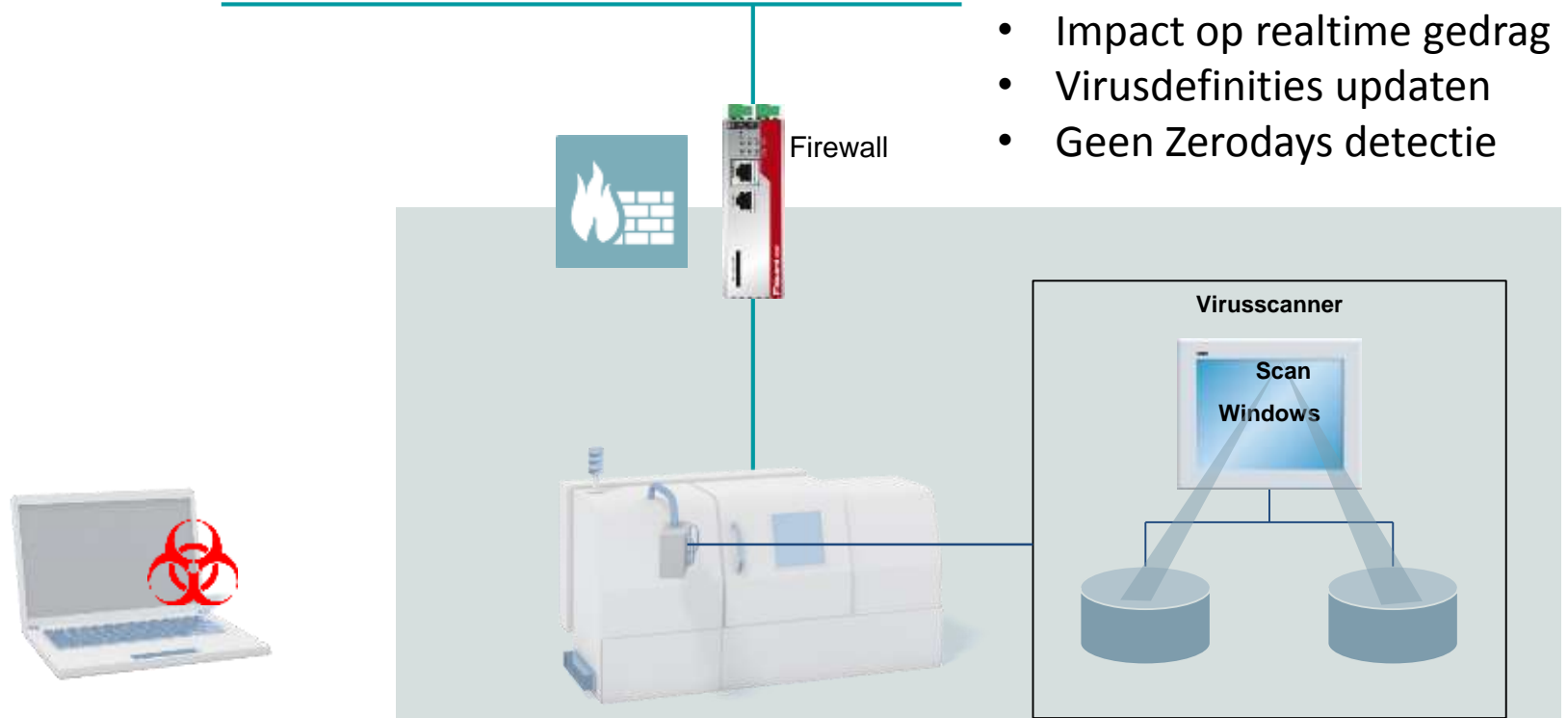


# Oplossing: segmentatie + firewall



# Oplossing: Virusscanner?

Ethernet



15 maart 2018 ••• Hart van Holland Nijkerk

Industrial Ethernet



# Beter:



Ethernet

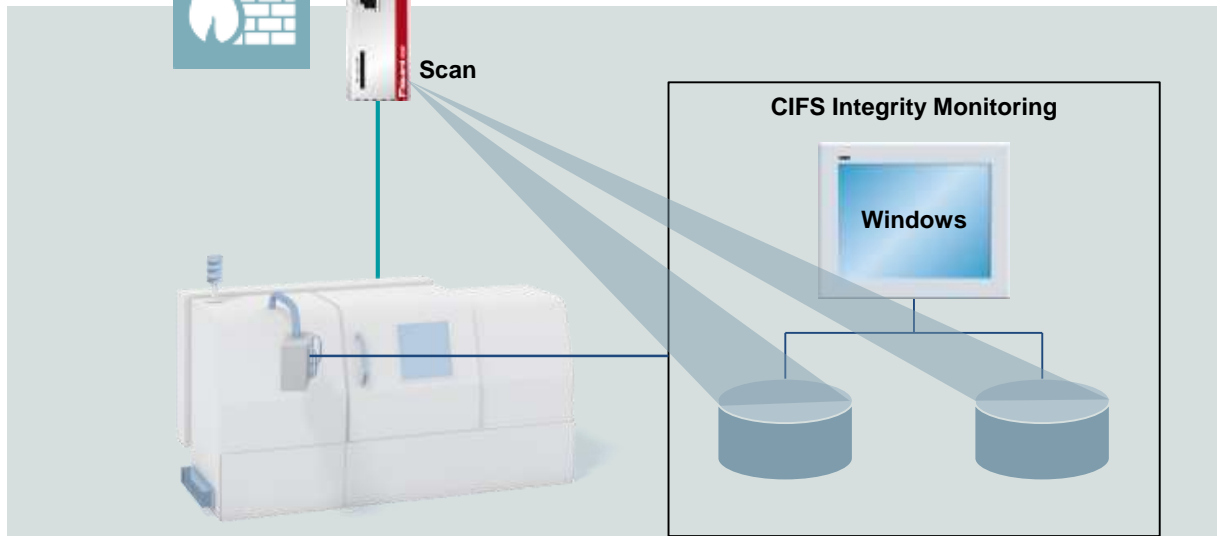


**CIFS Integrity Monitoring**  
Monitort het filesystem van de PC en geeft een alarmmelding wanneer er ongeautoriseerde wijzigingen optreden

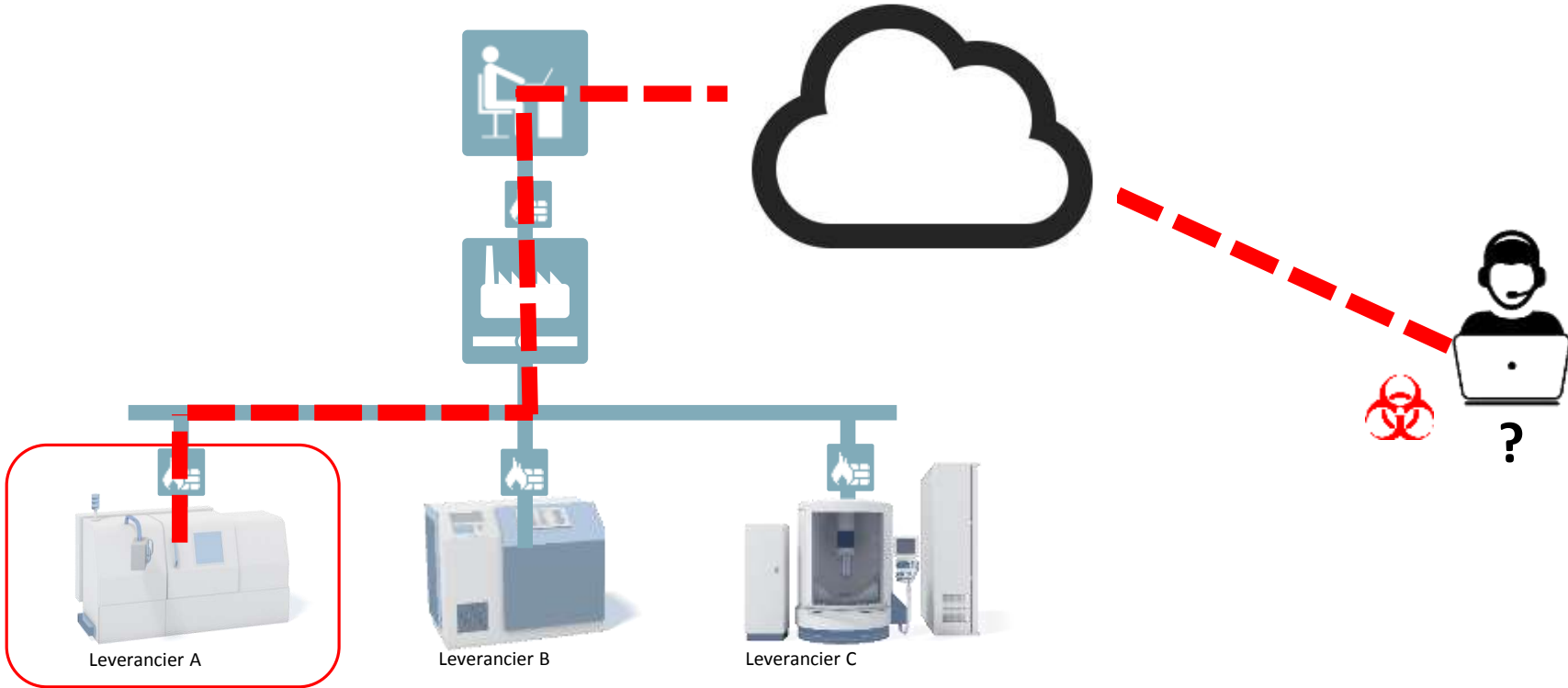


Firewall  
CIFS Integrity Monitoring

Scan



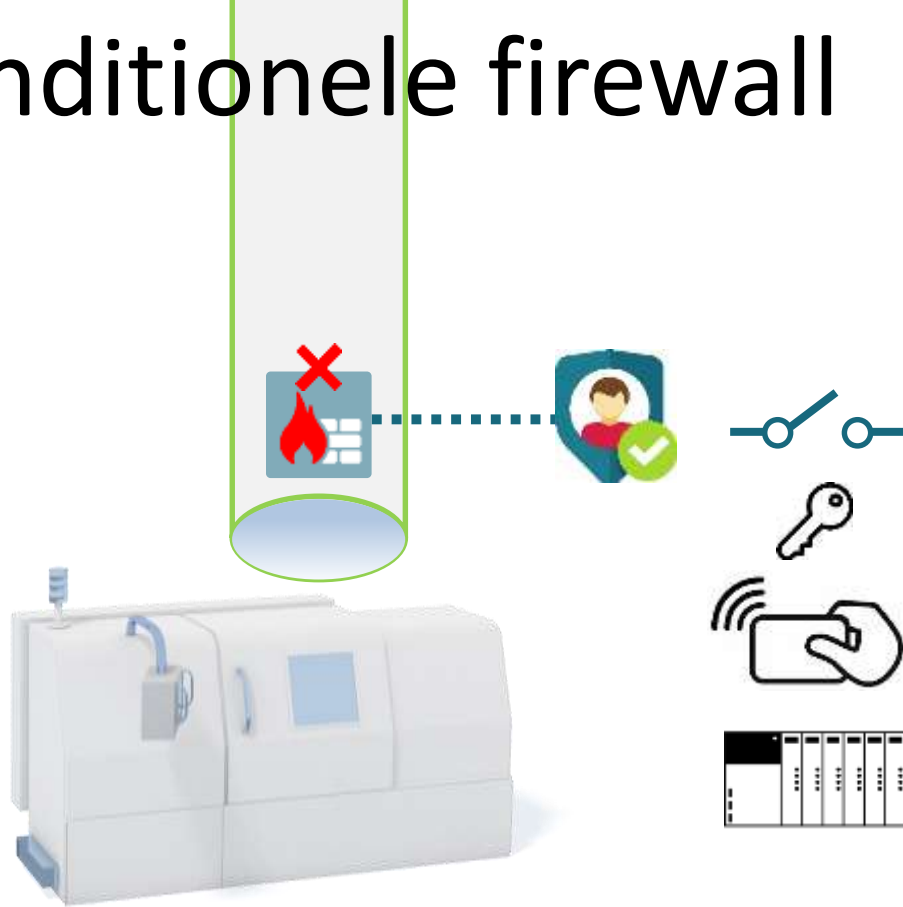
# Best? Conditionele firewall



# Best? Conditionele firewall



# Best? Conditionele firewall



15 maart 2018 ••• Hart van Holland Nijkerk

Industrial Ethernet

# Samenvatting

Virussen en Ransomware zijn ook een bedreiging voor de industrie. Dit komt door het toepassen van Industriële PC's in combinatie met de afwezigheid van Security maatregelen.

Maatregelen kunnen bestaan uit:

- Segmentatie van het netwerk om verspreiding tegen te gaan
  - Virusscanners op de Industriële Pc's, maar dit kent nadelen
  - Integrity monitoring om veranderingen te kunnen detecteren
  - (Conditionele) Firewallregels in VPN verbindingen om ook hier aan segmentatie te kunnen doen.
- 
- Voor andere/overige slimme oplossingen: bezoek onze stand of neem contact met mij op.

# Dank u wel voor uw aandacht!



PHOENIX CONTACT B.V.  
Hengelder 56  
Postbus 246  
6900 AE Zevenaar  
[www.phoenixcontact.nl](http://www.phoenixcontact.nl)

**Sjoerd Hakstege - van Eekhout**

Technisch Specialist  
Network & Security

[shakstege@phoenixcontact.nl](mailto:shakstege@phoenixcontact.nl)  
Tel.: +31 316 59 17 20  
Mobiel: +31 683 56 24 04



15 maart 2018 ••• Hart van Holland Nijkerk

## Industrial Ethernet