HUDSON CYBERTEC

Legacy & Patch Management voor IACS

Sebastiaan Koning – Hudson Cybertec

1

Sebastiaan Koning

- Senior Cybersecurity Consultant
- 15 jaar ervaring met OT systemen
- Specialisme in OT-netwerken
  - Sterke focus op cybersecurity
- Verschillende functies
  - Technisch
  - Organisatorisch

2

Programma

- Patchen in IACS: wél of niet doen?
- Patchprocedure voor IACS
- Wat te doen als patchen niet mogelijk is
  - Functioneel
  - Architectuur
  - Monitoring

3

Patchen in IACS: wél of niet doen?

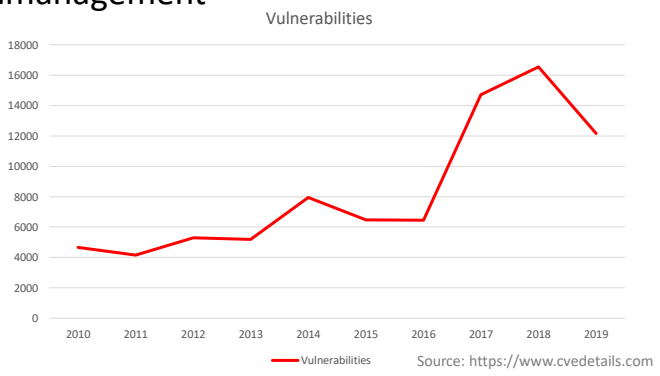
4

Wanneer patchen

- “If it ain’t broken, don’t fix it”
  - Waarom patchen als het werkt?
  - Er moet altijd een reden zijn
- Maar er zijn ook cyberdreigingen
  - Kwetsbaarheden
  - Gerichte aanvallen
  - Bijkomstige schade

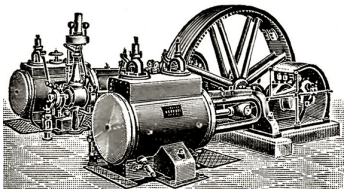
Waarom wél patchen?

- Patchen is niet altijd te vermijden
- Maak wél gebruik van patchmanagement



Legacy assets

- Hoe oud zijn deze assets?
- Wat zijn de risico's?
  - Cyber
  - Fysiek (voeding, mechanisch)
- Bestaan er patches?
- Bestaat de producten óf de fabrikant nog?
- Wat zijn de gevolgen als een update mislukt?
- Is er wel een reden dat een update nodig is?



Risico's bij updaten legacy assets

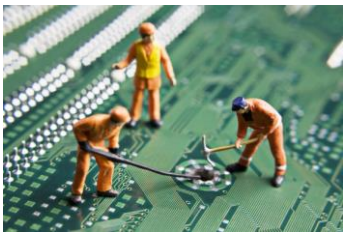
- Afwijkende werking na update
- Corrupte configuratie
- Apparaat (her-)start niet
  - Firmware defect
  - Hardware defect
- Geen kennis meer
  - Pensioen

Ongecontroleerde updates (1/2)

- Updates van assets worden elders beheerd
  - (Outsourced) IT
  - Applicaties werken niet meer na update
  - Ongeplande updates en herstarts

Ongecontroleerde updates (2/2)

- Onderhoudspartij voert updates uit zonder procedure
  - Externe partij of andere afdeling
  - Gebrek aan afstemming
  - Risico op compatibiliteitsissues met andere assets
  - Mogelijk afwijkend gedrag na update

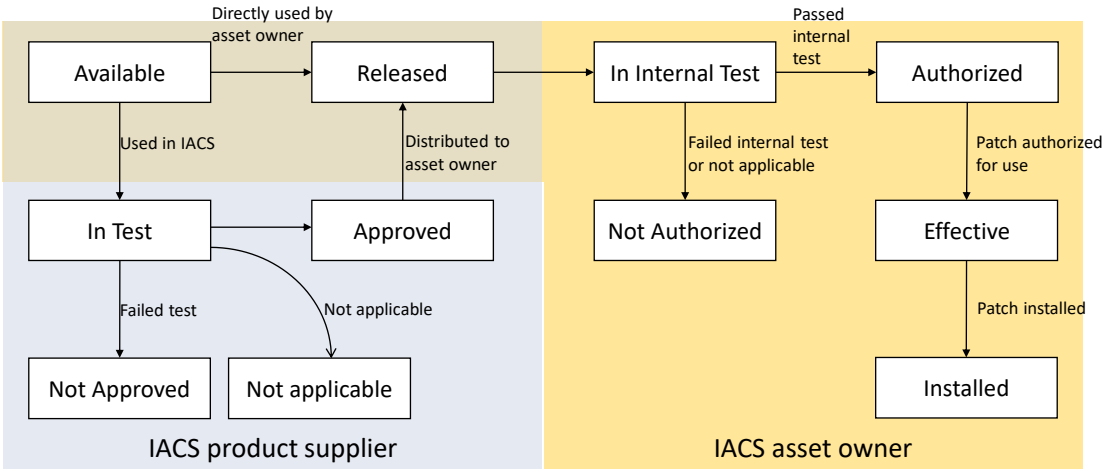


Know your network!

- Ken de samenstelling van je systeem!
- Welke assets?
- Welke dataflows?
- Wat zijn de kwetsbaarheden?
- Wat zijn de risico's?
- Wat is de impact?

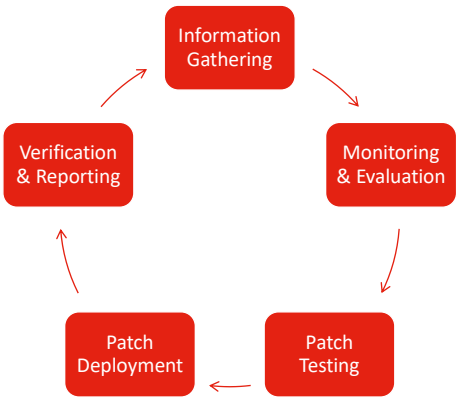
The Patch State Model

The Patch State Model (IEC 62443-2-3)



The patch process

The Patch Process

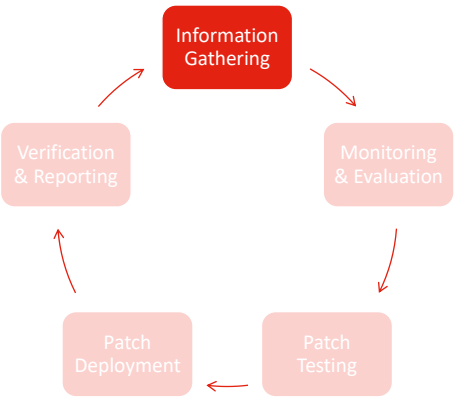


15

The Patch Process

Information gathering

- Inventory
- Supplier relationships
- Supportability
- Assess existing environment
- Categorize and classify assets

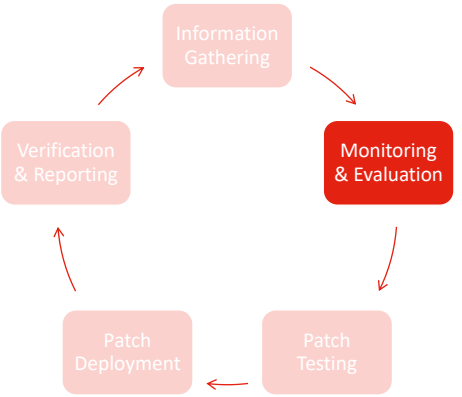


16

The Patch Process

Monitoring & Evaluation

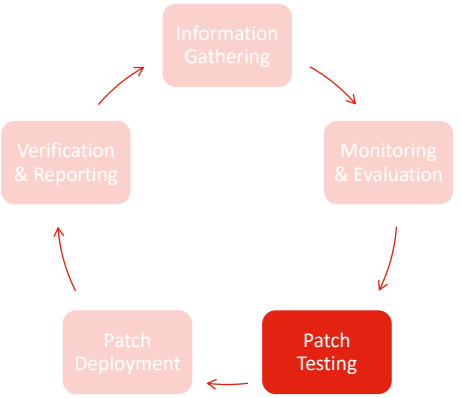
- Monitor & ID patches
- Determine applicability
- Risk assessment
- Decision



The Patch Process

Patch testing

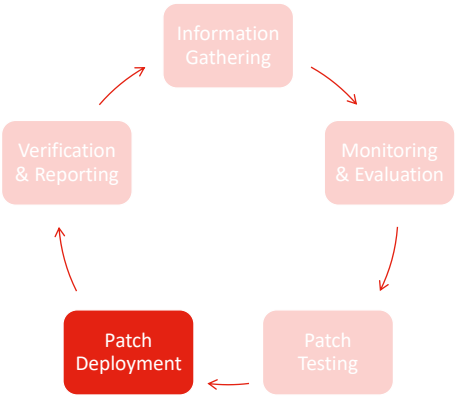
- File authenticity
- Review changes
- Install procedure
- Qualification & verification
- Removal/roll-back procedure
- Risk mitigation



The Patch Process

Patch deployment

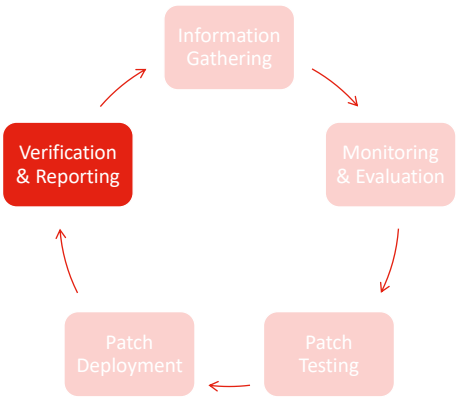
- Notification
- Preparation
- Scheduling
- Deployment



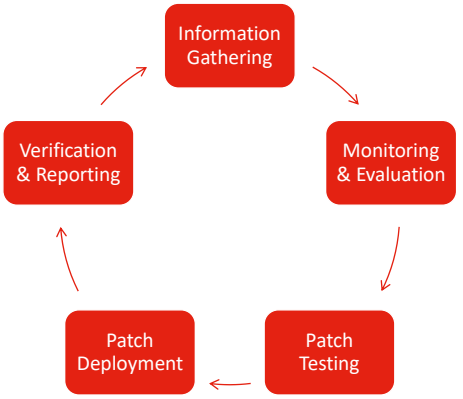
The Patch Process

Verification & reporting

- Verification
- Training
- Documentation



The Patch Process



21

Patching and IACS

22

Patching and IACS - challenges

- Patching = changing
- (Un-) Available Maintenance window
- Specialized environments/software
  - Warranty
  - Vendor approval
  - Vendor testing <> end-user situation
- Possible impact

Patching and IACS – points of attention

- Setup a clear RACI
- Up-to-date (complete) asset-lists
- Verify backups
- Test-facilities similar to production
- Track, validate and report
- Emergency procedure
- Phased rollout

Wat te doen als patchen niet mogelijk is?

25

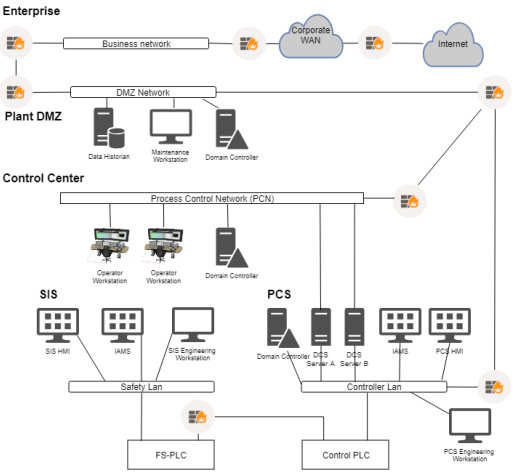
Patching binnen IACS – Mitigerende maatregelen

- Organisatorisch
  - Beleid en procedures
  - Bewustwording
  - Standaardiseren
- Technisch
  - Firewalls (inclusief end-points)
  - Uitschakelen of verwijderen van features
  - Hardening
  - Anticiperen op product lifecycles
  - Virtual patching…

26

Patching binnen IACS – Virtual patching

- Virtual Patching
  - Signature based
  - Detecteren / Beschermen
  - Plaatsing is essentieel
  - Tijdelijke maatregel



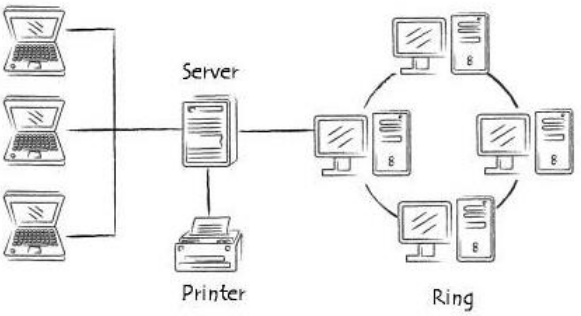
Zones & Conduits (IEC 62443)

Zones & conduits op basis van IEC 62443 (1/2)

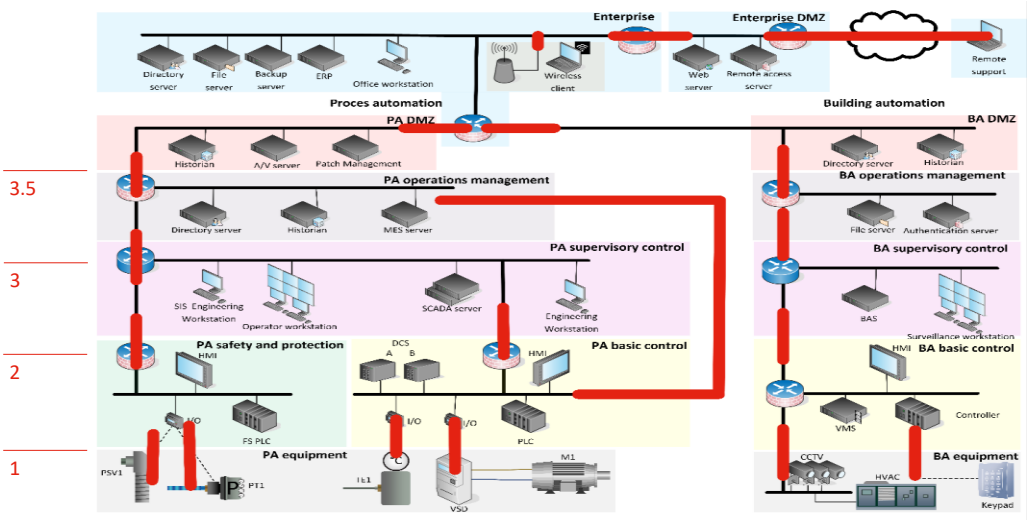
- Zones
  - Groepeer assets op basis van:
    - Functionaliteit
    - Locatie
    - Verantwoordelijke organisatie
    - Resultaten van de risico-inventarisatie
  - Overeenkomstige security vereisten per zone

Zones & conduits op basis van IEC 62443 (2/2)

- Conduits
  - Verbinding tussen zones
  - Logische verbinding



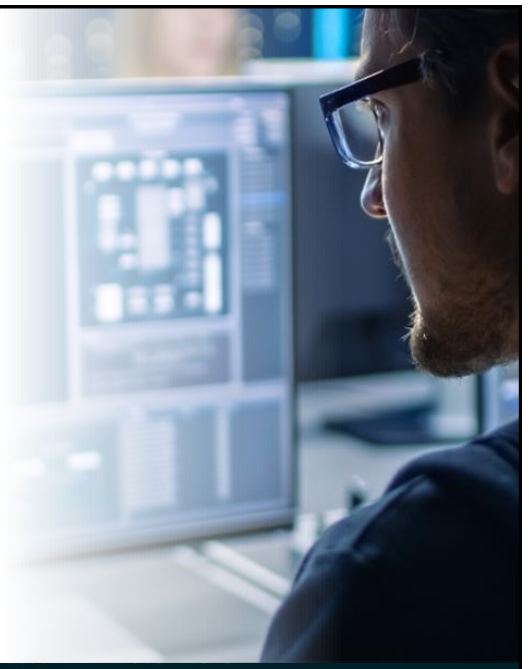
Voorbeeld



Impact van zones & conduits

- Snelste Quick-Win voor een hogere cyberweerbaarheid
- Beperkt de verspreiding van risico's
- Kan aanpassing vergen aan de architectuur
  - En tijdelijke onderbreking van het proces

Monitoring



Waarom geen firewalls of IPS?

- Firewalls brengen risico's met zich mee:
  - Verstoring OT data
  - Single-point-of-failure
  - Vaak geen herkenning van OT protocollen
  - Niet geschikt voor fail-safe en real-time communicatie

Monitoren (1/2)

- Passieve uitlezing
- Geen verstoring van communicatie
  - Geen firewall of IPS
- Maak gebruik van Anomaly Detection
  - Herkennen van normale datapatronen
  - Triggeren op afwijkingen

35

Monitoren (2/2)

- Kies voor een OT gerichte oplossing
  - Herkenning van OT protocollen en datapatronen
- Direct toepasbaar!
  - Zelfs op oude installaties
- Asset Management

36

HUDSON CYBERTEC

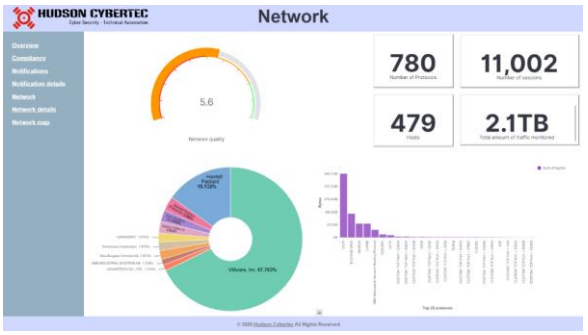
OT Network & Compliance Monitoring (1/3)

- U heeft altijd een actueel inzicht in:
  - Uw werkelijk aanwezige assets
  - Kwetsbaarheden en dreigingen
  - Het netwerkverkeer en afwijkingen
  - De kwaliteit van het netwerkverkeer
  - Compliance monitoring op:
    - Internationale standaarden (IEC 62443, ISO 27001, NIST, etc)
    - Wet- en regelgeving (Wbni, BIO, CSIR, Vewin, etc)
  - Nederlandse/Duitse innovatie

HUDSON CYBERTEC

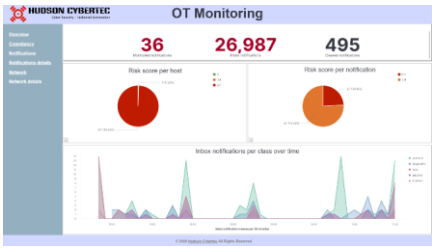
OT Network & Compliance Monitoring (2/3)

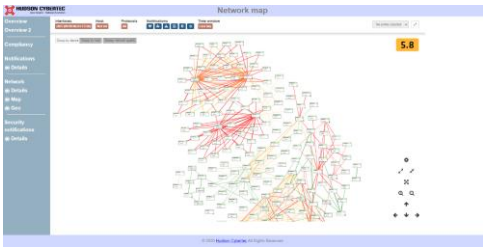
- Intelligent Anomaly Detection
- Ontwikkeld vanuit 100% OT perspectief
  - Geen doorontwikkeling vanuit IT
- OT protocol herkenning
  - Voorkomen van false-positives

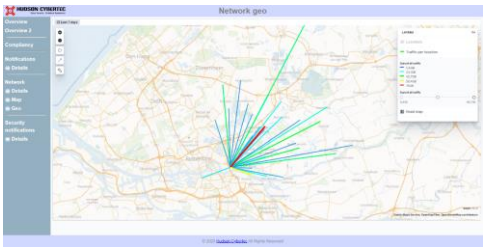


HUDSON CYBERTEC

OT Network & Compliance Monitoring (3/3)







26 t/m 30 oktober 2020 | Online kenniswek
INDUSTRIAL CYBER SECURITY

39
HUDSON CYBERTEC

39

Latest and actual information:

Follow us on

26 t/m 30 oktober 2020 | Online kenniswek
INDUSTRIAL CYBER SECURITY

40
HUDSON CYBERTEC

40

41

HUDSON CYBERTEC

Contact:

Laan van ‘s-Gravenmade 74
2495 AJ Den Haag
www.hudsoncybertec.com
070 – 2500717
info@hudsoncybertec.com

42