Sicherheitslücken in kritischen Steuerungsgeräten von Kraftwerken und Umspannwerken

Andreas Klien, OMICRON electronics, Österreich

Kiev, Ukraine, 17. Dezember 2016, kurz vor Mitternacht

ANDY GREENBERG SECURITY JUN 12, 2017 8:00 AM

‘Crash Override’: The Malware That Took Down a Power Grid

In Ukraine, researchers have found the first real-world malware that attacks physical infrastructure since Stuxnet.

„Industroyer/Crash Override“
Erste Malware im Umspannwerk

OMICRON

Operational Technology (OT) im Stromnetz

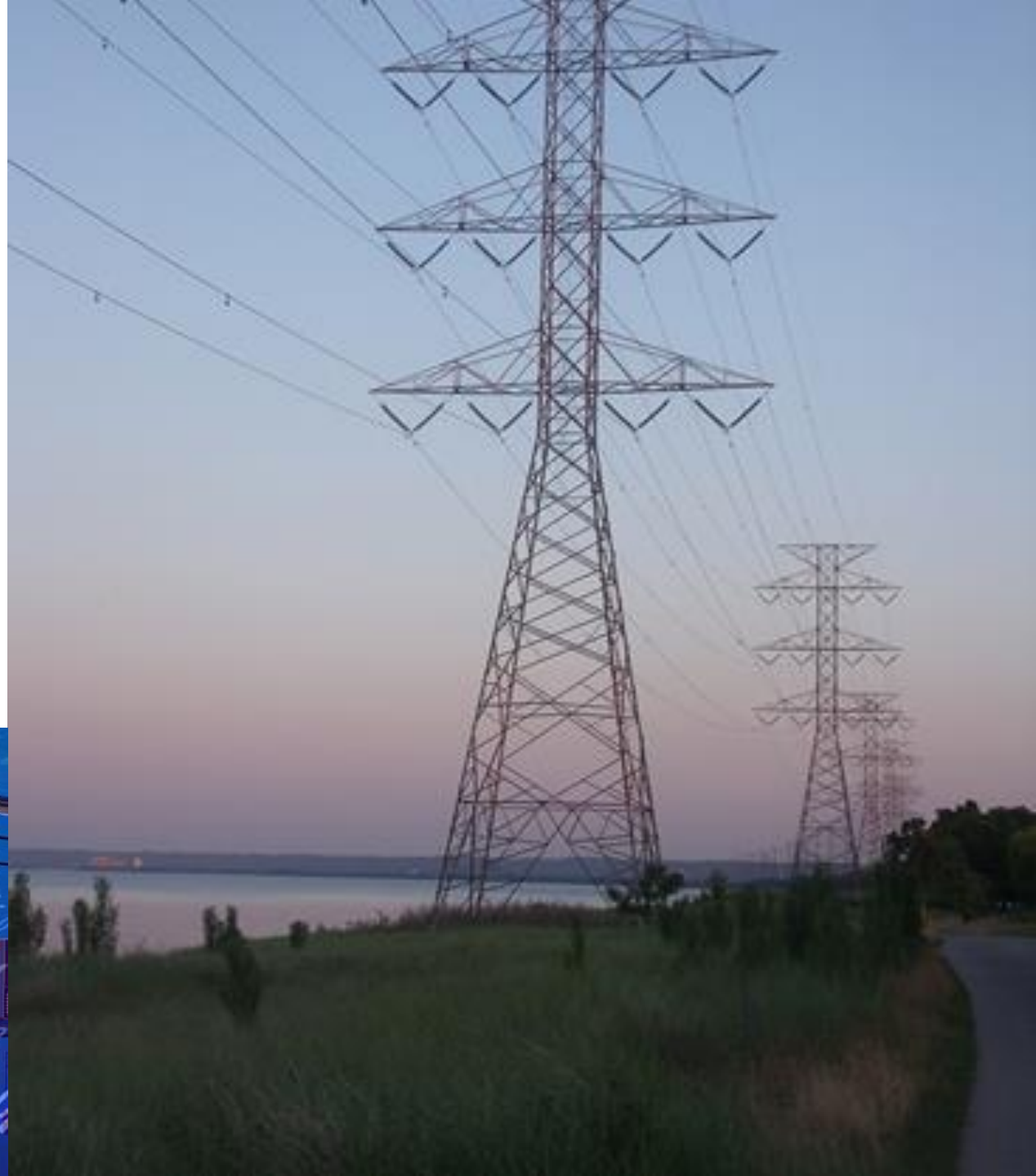
- OT = Computersysteme um physikalische Vorgänge zu steuern
  - Industriesteuerungen in Fabriken (z.B. SPS und SCADA)
  - Steuerungen in Umspannwerken und Kraftwerken

- Cyber Security in der Energieversorgung besteht aus IT- und **OT-Security**

Schutz- und Steuergeräte

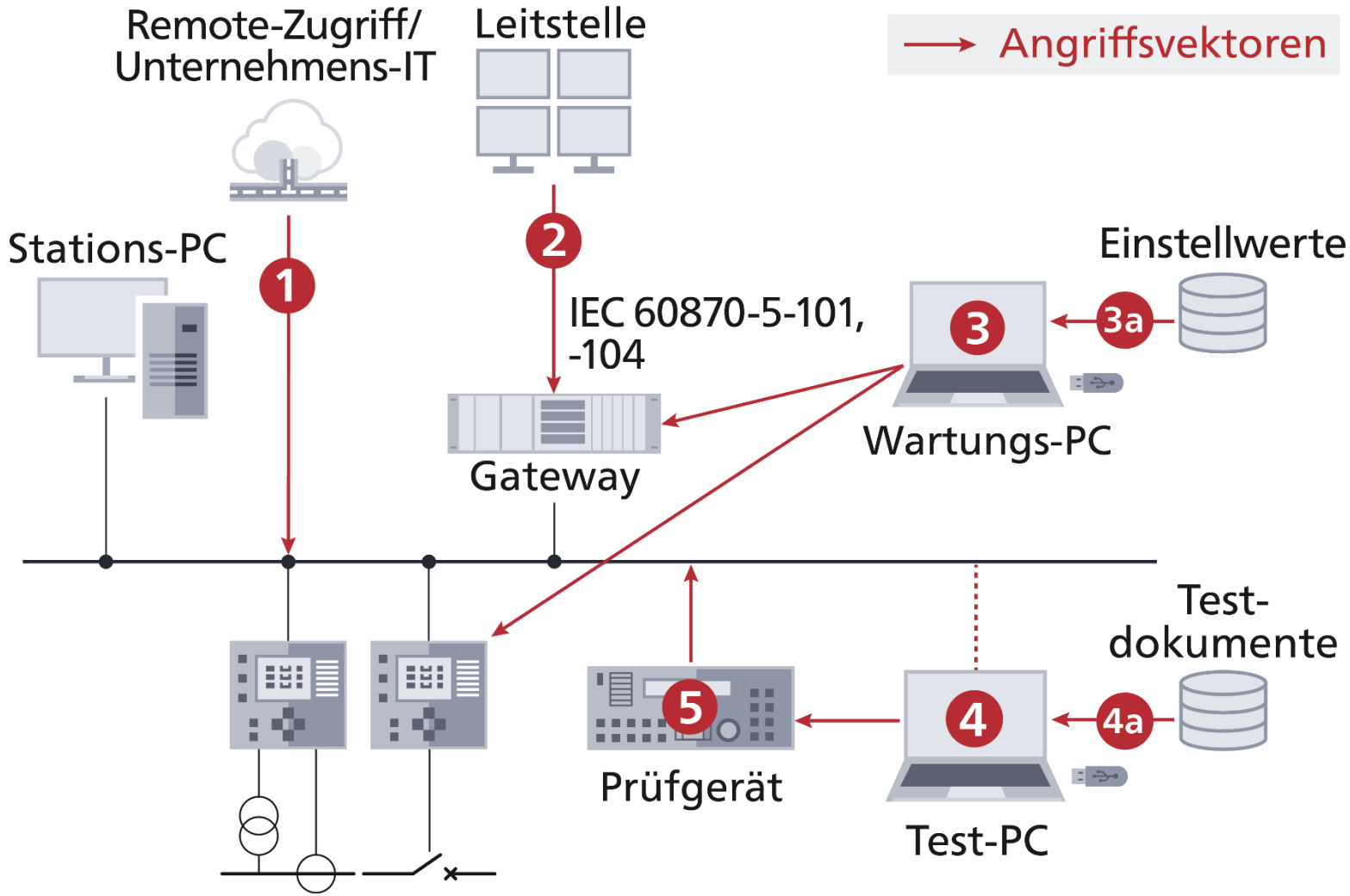
- Schützen z.B. Stromleitungen und Trafos vor Kurzschlüssen

- Sind Computer mit
  - Strom-/Spannungseingängen
  - Netzwerkschnittstellen
  - Webinterface
  - ...



Das Problem

Noch mehr Probleme



DoS-Angriffe auf Schutzrelais

- Industroyer 1 (Ukraine, Dez. 2016) nutzte DoS-Schwachstelle in Schutzrelais aus
  - Nur ein UDP Paket notwendig
  - CVE-2015-5374
- „Denial-of-Service“ bei Schutzrelais:
  - Kein Schutz der Leitung/des Trafos mehr.
- Patch wäre seit Juli 2015 verfügbar gewesen.

Europa, 2022

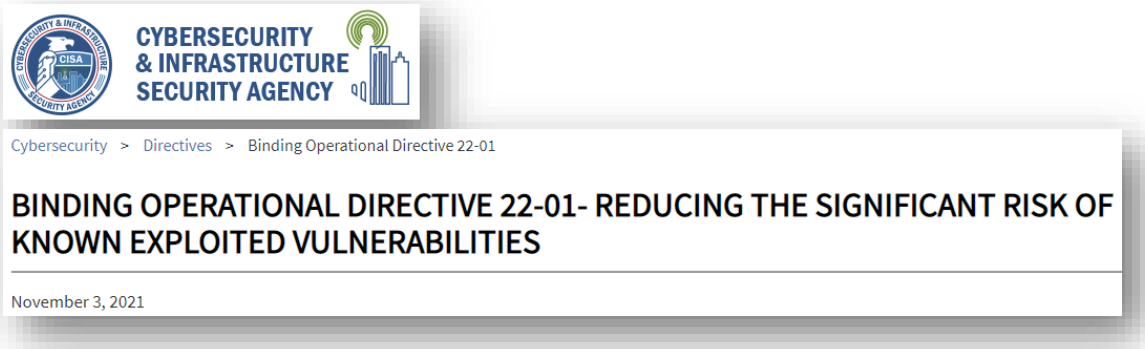
- Es sind immer noch tausende Relais mit dieser Firmware überall in Europa im Einsatz.

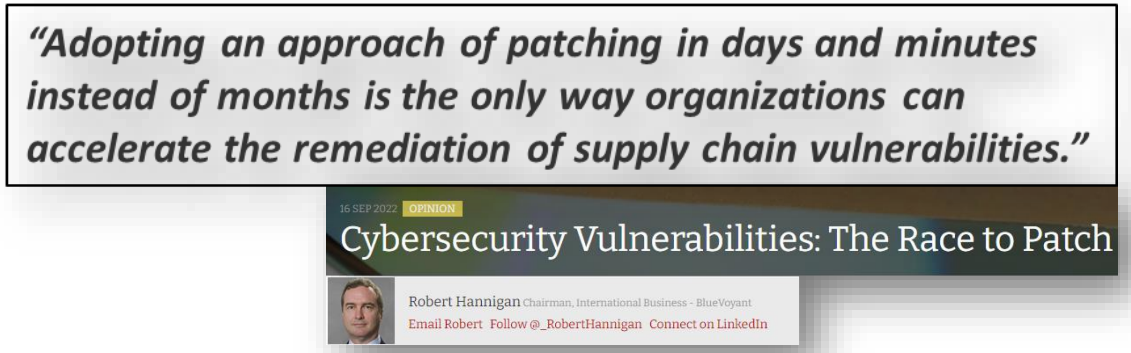
Exploit für CVE-2015-5374:

Quelle: exploit-db.com

„EVUs müssen endlich anfangen zu patchen!”

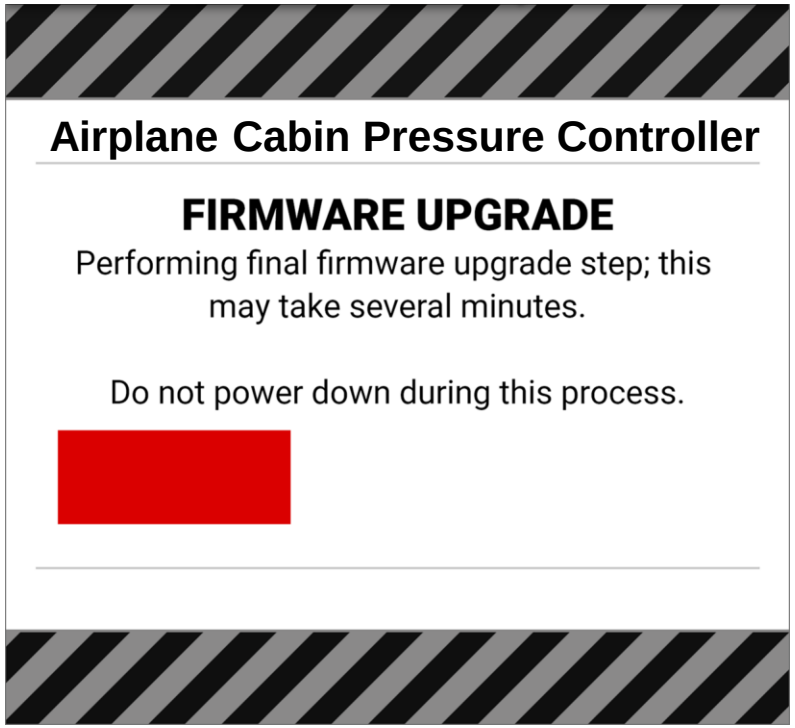
- *“Warum sind da immer noch Schutz- und Steuergeräte mit jahrealter Firmware,*
  - *mit jahrealten Schwachstellen,*
  - *und sogar mit bekannten Exploits?”*





OMICRON

Würden Sie das hier im Flug machen?



Grund 1: Leitungsfreischaltungen

- Patching erfordert meist die Abschaltung von Hochspannungsleitungen bzw. Generatoren.

DEUTSCHE WIRTSCHAFTSNACHRICHTEN

Stromnetz überlastet: Erneuerbare werden immer öfter abgeriegelt

Das deutsche Stromnetz liefert nicht genug Kapazität für die Erneuerbaren. (Foto: dpa)

Grund 2: Es ist Software!

Das Risiko, einen Patch aufzuspielen, kann höher sein, **als ihn nicht aufzuspielen**.

- Patches haben neue Bugs.
- Patches verhalten sich auf verschiedenen HW-Revisionen unterschiedlich.
- Patches können Nebeneffekte auf die programmierte Logik haben.


WIRED

LILY HAY NEWMAN SECURITY AUG 11, 2022 1:28 PM

Sloppy Software Patches Are a 'Disturbing Trend'

The Zero Day Initiative has found a concerning uptick in security updates that fail to fix vulnerabilities.


CSO

Why patching quality, vendor info on vulnerabilities are declining

It's getting harder to assess the impact of patching or not patching, and too many patches don't fully fix the problem. It's time to pressure vendors.

By Susan Bradley
Contributing Writer, CSO | AUG 24, 2022 2:00 AM PDT

OMICRON

Wie teste ich, ob nach dem Update alles noch funktioniert?

- Schutzfunktionen mit hunderten von Einstellparametern.
  - Bäume auf Leitungen werfen?
  - Nein. Mittlerweile gut automatisiert testbar.
- Logikfunktionen mit dutzenden von Schaltern.
  - Eine Schaltkombination dauert Minuten.
- Übertragung von hunderten Signalen und Messwerten Richtung Leitstelle.
  - Messwerte ändern und Leitstelle anrufen?

OMICRON

Risiko-Management statt blindes Patchen

1. Welche Schwachstellen gibt es für meine OT-Hersteller überhaupt?
2. Welche meiner Geräte sind betroffen?
3. Wie groß ist das Risiko?
4. Welche Abhilfe-/Minderungsoptionen gibt es?
5. Was könnte ich tun, bis wir *wirklich* etwas tun können?

Security Advisories mit meinen Geräten abgleichen

- Wie bestimme ich mein Risiko, wenn ich ein Security Advisory bekommen habe?

- Ich bin nur betroffen, wenn
  - das **Gerätemodell**, **Modulkonfiguration**
  - und **Firmware**-Version übereinstimmen
  - und die betroffenen Dienste zugänglich sind.

Bundesamt für Sicherheit in der Informationstechnik

CERT-Bund Meldungen

← ZURÜCK 1 2 3 ... 100 WEITER →

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

3.1 AFFECTED PRODUCTS

Hitachi Energy reported this vulnerability affects the following RTU500 series in which HCI Modbus TCP is

- RTU500 series CMU Firmware version 12.0.*
- RTU500 series CMU Firmware version 12.2.*
- RTU500 series CMU Firmware version 12.4.*
- RTU500 series CMU Firmware version 12.6.*
- RTU500 series CMU Firmware version 12.7.*
- RTU500 series CMU Firmware version 13.2.*

3.1 AFFECTED PRODUCTS

Siemens has reported that this vulnerability affects the following SICAM A8000 Web Server Module produc

- CP-8000 MASTER MODULE WITH I/O -25/+70°C (6MF2101-0AB10-0AA0): All Versions
- CP-8000 MASTER MODULE WITH I/O -40/+70°C (6MF2101-1AB10-0AA0): All Versions
- CP-8021 MASTER MODULE (6MF2802-1AA00): All Versions
- CP-8022 MASTER MODULE WITH GPRS (6MF2802-2AA00): All Versions

The affected protocol firmware utilized with the web server modules includes the following:

- AGPMT0 (AGP Master)
- DNPiT1 (DNP3 TCP/IP Server)
- DNPiT2 (DNP3 TCP/IP Client)
- DNPMT0 (DNP3 Master seriell)
- DNPST0 (DNP3 Slave seriell)
- ET83 (61850 Ed.1)
- ET85 (61850 Ed.2)
- MPCiT0 (MODBUS TCP/IP Client)

OMICRON

Präzises Anlageninventar nötig

- Mit zu wenig Geräteinformationen treffen **zu viele** Schwachstellen zu,
  oder man **übersieht** Schwachstellen.

- Beispiel: ICSA-22-195-16; Denial-of-Service in EN100 Ethernet module ... all firmware versions prior to v4.40

Darum wird ein präzises Anlageninventar gefordert in:

ISO/IEC 27001, Annex A.8 Asset Management, ISO/IEC 27019

ISA/IEC 62443-3-3 SR7.8

Herausforderungen mit Security Advisories

- Security Advisories bekommt man meist als PDF per E-Mail von jedem Hersteller separat.
- Pro Hersteller 60-200 Advisories pro Jahr.
- Pro Advisory ca. 10-20 Gerätetypen betroffen.

Beispiele:

"Affected are medium voltage drives manufactured since 2015 and prior to 2022"

"Affected are all versions between V2.5 (including) and V2.7 (excluding)"

"Affected are ACME 14 SW *installations installed from material dated earlier than 2020-09-15"*

OMICRON

Licht am Ende des Tunnels – Automatisierbarkeit

Es gibt maschinenlesbare Beschreibungen dieser Anlagen!

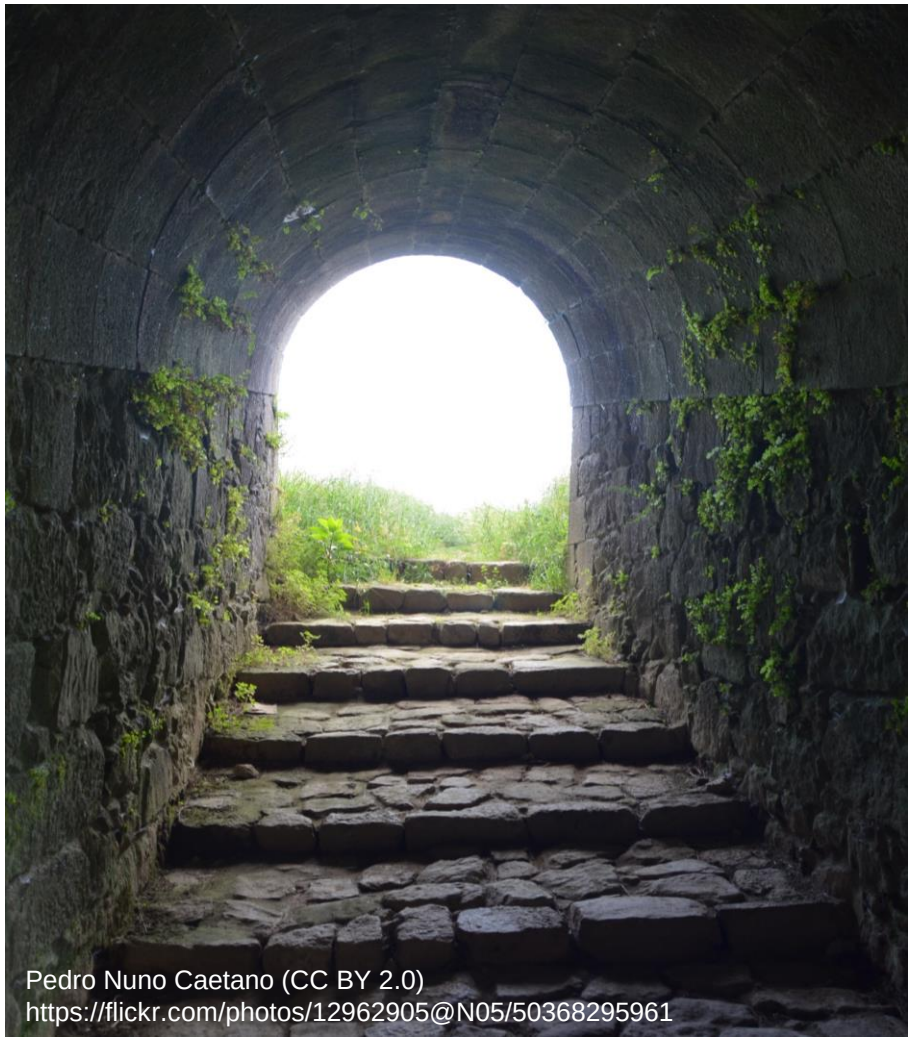
Projektdateien in „IEC-61850-SCL-Format“

- Beschreiben die Geräte und das Netzwerk

Security Advisories in CSAF-Format

- Beschreiben Schwachstellen maschinenlesbar

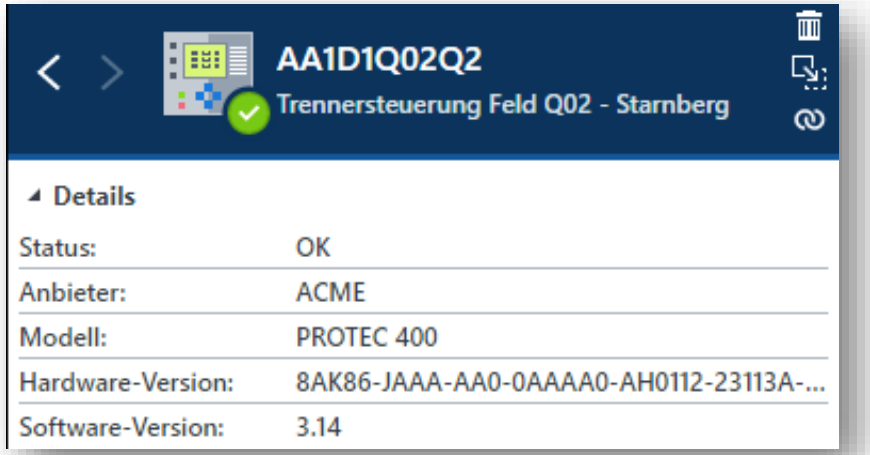
Einzigartige Möglichkeiten, Prozesse zu automatisieren!

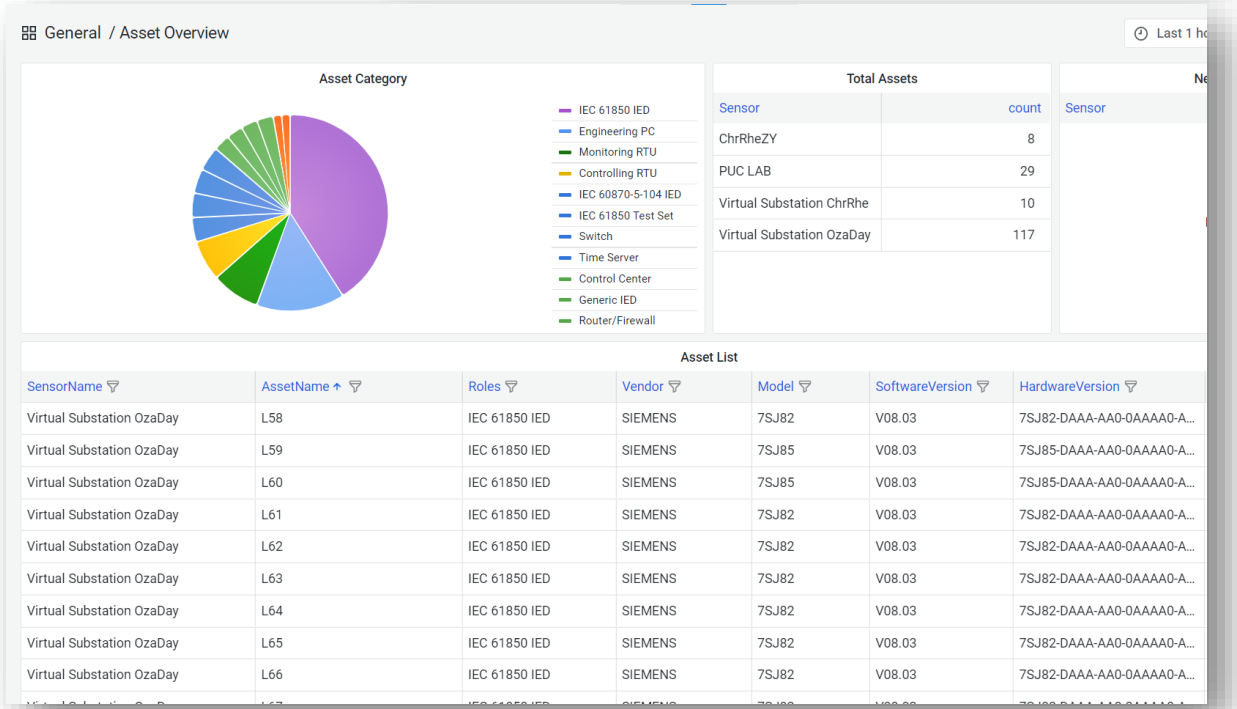


Automatische Inventar-Erstellung

- StationGuard erfasst Geräteinformationen über
  - Passive Betriebsmittelauflistung
  - Engineering-Dateien: SCL und CSV
  - Aktive Geräteabfrage

- Export und Import für Synchronisierung mit anderen Systemen





OMICRON

OASIS Common Security Advisory Framework

- Maschinenlesbares, standardisiertes Format für Security Advisories.
- Mehrere große OT-Anbieter veröffentlichen bereits mit CSAF.
- Eine große Verbesserung gegenüber PDFs, die per E-Mail verschickt werden!

https://csaf.io

Es gibt aber noch viel zu tun...

Beispiele für CSAF-Feld product_version_range:

"Medium voltage drives manufactured since 2015 and prior to 2022"

"All versions between V2.5 (including) and V2.7 (excluding)"

"ACME 14 *installations installed from material dated earlier than 2020-09-15"*

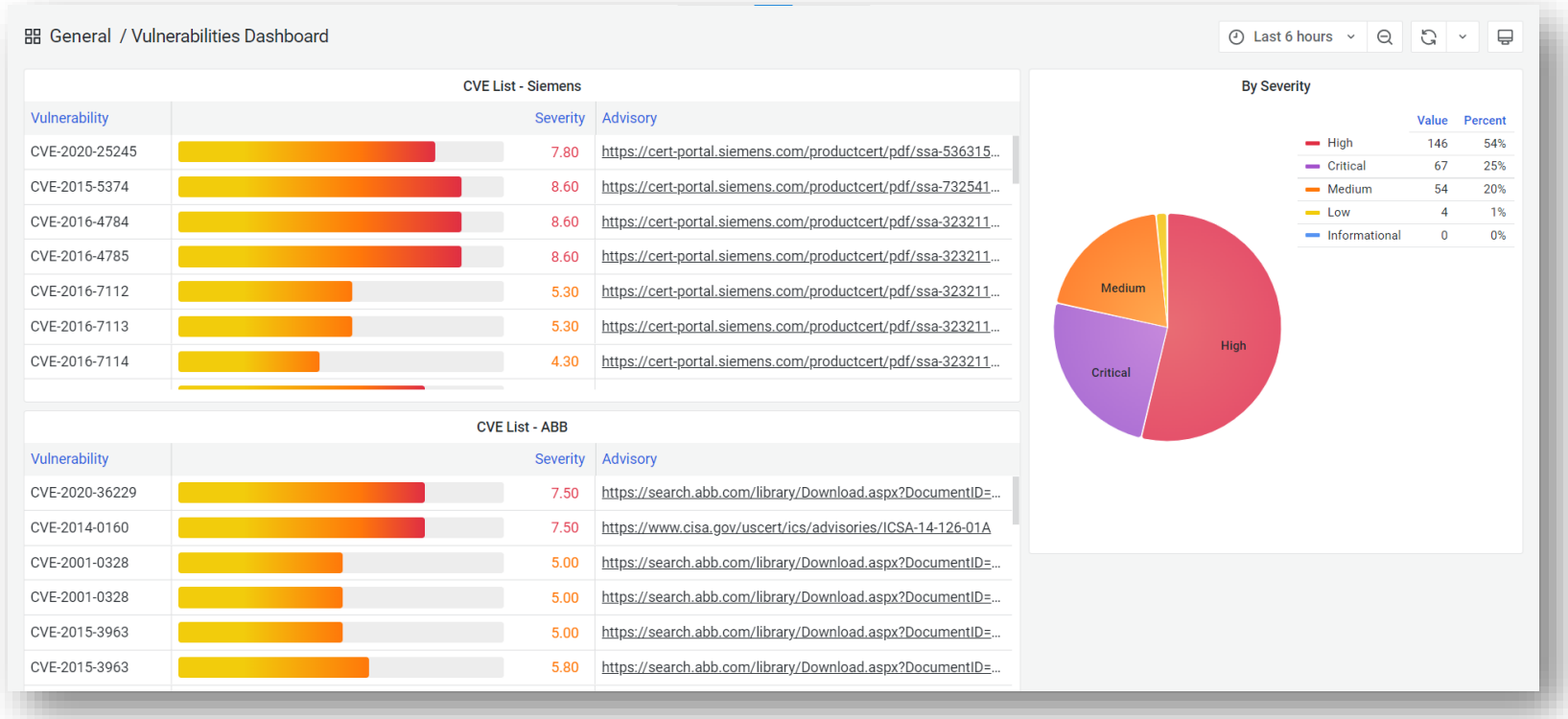
OMICRON

Wie lösen wir dieses Problem?

- Unsere Experten erstellen „von Hand“ eine Schwachstellendatenbank mit Metainformationen.
- Damit können wir automatisiert, nur die zutreffenden Schwachstellen anzeigen.

Gerätetypen-Datenbank

OT-Schwachstellen Datenbank



OMICRON

Unser Ziel: Zusammenarbeit zwischen OT und IT unterstützen

- IT- und OT*-Techniker:innen müssen zusammenarbeiten, um das Stromnetz vor Cyberangriffen zu schützen.

- Wir wollen diese Zusammenarbeit effizienter machen.

*OT = Operational Technology, die IT in der Steuerungstechnik

OMICRON

Wie StationGuard zur Sicherung des Stromnetzes beiträgt

Sichtbarkeit

- Macht Risiken und Schwachstellen sichtbar

Anlageninventar (Asset Inventory)

- Genaueste und detaillierteste Betriebsmitteldatenbank

Schwachstellen-Management

- Überblick und Einsicht in alle Geräte-Schwachstellen

Angriffe erkennen und Bedrohungen analysieren

- Eingebautes Anlagenwissen ermöglicht weniger Fehlalarme, einfachere Alarmanalyse und schnellere Reaktionsprozesse.

OMICRON

Zusammenfassung

- IT- und OT- muss zusammenarbeiten, um das Energienetz zu schützen.
- Das Stromnetz zu patchen ist nicht einfach.
- Es gibt jedoch Potential für Automatisierung beim Risikomanagement.

Vielen Dank für die Aufmerksamkeit!