CERT@VDE –
The cybersecurity platform for industrial small and medium-sized enterprises (SME)

Andreas Harner, Head of CERT@VDE
Hamburg, January 2018
Industrial IoT (IIoT) or Industry 4.0

IT based automation devices based on classic operation systems

classic fieldbuses replaced by Ethernet-based buses

Worldwide access to the sensors: through the Cloud!

...enterprises of the Industrial Automation have to cope with vulnerabilities in their products!
## Security differences between Office-IT and Process-IT

<table>
<thead>
<tr>
<th></th>
<th>Process-IT, Industrial Control Systems (ICS)</th>
<th>Office-IT, Office-Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Virus-Programs</td>
<td>unusual / difficult to apply</td>
<td>usual / easy to apply</td>
</tr>
<tr>
<td>product life cycle</td>
<td>up to 20 years and longer</td>
<td>3 - 5 years</td>
</tr>
<tr>
<td>real-time requirement</td>
<td>very high</td>
<td>low: delays are acceptable</td>
</tr>
<tr>
<td>application of patches</td>
<td>not regular / unplanned</td>
<td>regular / planned</td>
</tr>
<tr>
<td>security tests / audits</td>
<td>no common practice</td>
<td>planned und partly mandatory</td>
</tr>
<tr>
<td>outsourcing</td>
<td>rarely</td>
<td>standard</td>
</tr>
<tr>
<td>physical security</td>
<td>varies from low until high</td>
<td>high (esp. Critical Infrastructures)</td>
</tr>
<tr>
<td>vulnerability handling</td>
<td>SME: immature</td>
<td>standard</td>
</tr>
</tbody>
</table>

---

*VDE*
...need of a „coordinating PSIRT“ in Germany for ICS...

Common Position:

- „….we, the SMEs of the Industrial Automation need a trustworthy, neutral, independant platform based on an institution with a wellknown reputation…“
  \(\rightarrow\) VDE e.V. (registered association, non-profit)“

\(\rightarrow\) Within european time zone – able to speak German – able to speak „Automation“
Scope of CERT@VDE

Process-IT (PIT)

Office-IT

Operational Assets
Production Equipment
Sensors and Actuators

On-Premises IT

Cloud IT

shop-floor

office-floor
The VDE e.V. - Association for Electrical, Electronic & Information Technologies

- Knowledge transfer in the VDE network of experts
- Partner for educational and technological policies
- Youth development

- VDE|DKE is the German member of IEC and of CENELEC

- Interoperability – Safety – Security - Usability

non-profit
1879
- Foundation of the first “Berliner Elektrotechnik-Vereins“: Proposed by Werner v. Siemens:
  - Safety… for electrical systems
  - Exchange of information … between power operators and manufacturers

1893
- Foundation of VDE (by Adolf Slaby and Georg Wilhelm von Siemens)

**Historical interrupt or „why VDE“?**

Electrical Safety → Functional Safety → Cybersecurity
Today’s situation: vulnerability handling in SMEs

- unorganized approaches
- SMEs feel overstrained (CVSS, CVE,..)
- ICS Cert „speaks“ English and is not in the European timezone
- no access to the CERT-community
- → no / limited resources for vulnerability handling
  → no PSIRT
  → no routine in interacting with CERTs
- → no trusting instance in Germany
  → restricted trust in governmental organisations
- reactions happen secretly:
  → no collaboration
  → no exchange of information
  → no cross-company interaction
  → many partial solutions
- no/collaboration
Further drivers for CERT@VDE

- Technical threat level
- Economic importance
- Political situation
- Standards
1. Protect enterprises
   - Foster economy

2. Increase the ability to analyse and to react on cyber threats
   ...to fight against cyber espionage and cyber sabotage
   - Strengthen CERT-structures:
     - Attract resources and personnel...
IEC 62443: Normative requirements in standards for industrial security

General
- 1-1 Technology, concepts and models
- 1-2 Master Glossary of terms and abbreviations
- 1-3 System security compliance metrics
- 1-4 System security lifecycle and use case

Definitions
- Metrics

Policies and procedures
- 2-1 Requirements for an IACS security management system Ed 2.0 Profile of ISO 27001/27002
- 2-2 Implementation guidance for an IACS security management system
- 2-3 Patch management in the IACS environment (TR)
- 2-4 Requirements for IACS solution suppliers

System
- 3-1 Security technologies for IACS (TR)
- 3-2 Security risk assessment and system design
- 3-3 System security requirements and security levels

Component
- 4-1 Secure product development lifecycle
- 4-2 Technical security requirements for IACS products

Process requirements
- Functional requirements
Closing the gap: CERT@VDE

- Manufacturer (HW and SW)
- Operator (asset owner)
- National / international CERT community
- Machine builder or Integrator

- Provides components
- Has own production: is an operator too!

© VDE Verband der Elektrotechnik Elektronik Informationstechnik e. V.
Added values for CERT@VDE cooperation partners

- **cross-company** discussions and interaction on the trustworthy and secure environment of CERT@VDE (anonymous, if required) → motivates to collaborate!
- information hub between CERT community and automation industry

Qualified information exchange between manufacturers, operators, integrators and CERT community

→ **Responses** to threats/detected vulnerabilities: **structured and faster!**

**Single Point of Contact:**
- for operators to find contact persons of the manufacturers
- for operators to find published security information of all their suppliers in one place
- for manufacturers to address customers and integrators using their products
- supports the communication with other CERTs (e.g. ICS-CERT) for the constituency
- supports the communication with reporters of vulnerabilities („White-Hat Hacker“…):
  → „**Coordinated Disclosure**“
- collects and provides industry-specific security information for the constituency
Added values for CERT@VDE cooperation partners – II.

<table>
<thead>
<tr>
<th>Coordination when fixing vulnerabilities and support on publication of advisories.</th>
<th>CVE number assignment (lack of routine in SMEs dealing with CVSS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>elaborate Best Practices by the constituency, for the constituency</td>
<td></td>
</tr>
<tr>
<td>events and workshops for the automation industry to improve processes, to raise awareness and to promote the importance of CERTs</td>
<td></td>
</tr>
<tr>
<td>▪ image boost for the cooperation partners</td>
<td></td>
</tr>
<tr>
<td>▪ institutionalisation of PSIRT structures inside the SMEs is encouraged</td>
<td></td>
</tr>
</tbody>
</table>
Willkommen bei CERT@VDE

Das CERT@VDE unterstützt KMU bei IT-Sicherheitsvorfällen im Bereich der Automatisierungsindustrie über Organisationsgrenzen hinweg.

Aufgaben und Leistungen

- Ermöglicht einen herstellerübergreifenden Austausch auf einer neutralen, vertrauenswürdigen und sicheren Plattform, unter Wahrung der Anonymität.
- Koordiniert die Unterstützung beim Schließen von Sicherheitslücken.
- Ist der Austausch über geeignete Vorgehensweisen an.
- Bereitgestellte zielgruppenorientierte Schwachstelleninformationen aus diversen Quellen auf und macht diese verfügbar.
- Veranstaltet Workshops für die Automatisierungsindustrie.
- Mitarbeitet gemeinsam mit seinen Partnern Best Practices.

mehr ...

In Kooperation mit:

- BECKHOFF
- Endress+Hauser
- PEPPERL+FUCHS
- PHOENIX CONTACT
- Weidmüller

Zukünftige Termine

- TF-CSIRT meeting & FIRST Regional Symposium Europe 06.02.2018 09:00
  (Europe/Berlin) – Steigenberger Hotel Hamburg, Hotelgeorgenstr.G 3, 20459 Hamburg
- IT-Sicherheit – eine Chance für den Wirtschaftsstandort Deutschland
  27.03.2018 10:30
  (Europe/Berlin) – NH Collection, Friedrichstraße 96 (am Bahnhof Friedrichstraße), 10117 Berlin Mitte

Vergangene Termine

Nachrichten

- Neuer Verordnungsentwurf für ein einheitliches europäisches IT-Sicherheitsnetzwerk erstellt am 15.01.2018
- TRIRIS/TRITON/4ATMAN ICS Malware erstellt am 08.01.2018
- Meltdown und Spectre erstellt am 05.01.2018

Team:
1 Head
2 IT-Sec-Managers
1 BDM + marketing

Web:
https://cert.vde.com

Advisories

Collaboration platform based on „Mattermost“

Member:
- „Deutscher CERT Verbund“
- Accredited in „TI-TF-CSIRT“
Thank you for your attention!

Andreas Harner
Head of CERT@VDE
Phone: +49 69 6308 392
andreas.harner@vde.com