JOANNEUM RESEARCH DIGITAL

Kritisch, aber verwundbar: Die Cybersecurity-Herausforderungen in OT-Systemen

JOANNEUM RESEARCH

CyberSecurity: Lagebild 2025 - 1.7.2025

Branka Stojanovic

Die Bedrohungslage

- **Cyberangriffe** auf kritische Infrastrukturen **nehmen stark zu**
  - In diesem Jahrzehnt hat sich ihre Zahl jedes Jahr **mehr als verdoppelt**
- Durch die stärkere **Vernetzung** entstehen **neue Herausforderungen** bei der **Datensicherheit**
  - z. B. größere Angriffsflächen
- Der Einsatz von **KI-Tools** kann die Sicherheit verbessern – bringt aber **auch Risiken** mit sich
  - KI wird sowohl für „gute“ als auch für „schlechte“ Zwecke genutzt

Operational Technology (OT)

Operational Technology (OT) auf einen Blick

- **Was ist OT?**
  - Technologische **Rückgrat kritischer Infrastrukturen**
  - **Unterscheidet sich von IT** (Informationstechnologie)
  - Kontrolliert und überwacht **physische Prozesse** (z. B. SCADA-Systeme)
  - Fokus auf **Sicherheit, Echtzeitfähigkeit und Langlebigkeit**
- **Zunehmende Komplexität**:
  - Neue Technologien führen zu **komplexeren OT-Systemen**
  - **IoT, Edge und Cloud-Anwendungen** bringen zusätzliche **Sicherheitsrisiken**

Kritisch - und dennoch verwundbar

- **Veraltete Protokolle & schwache Authentifizierung** werden weiterhin genutzt
- **Patching ist selten**, da OT-Systeme rund um die Uhr laufen
- **Fehler beeinträchtigen Sicherheit, Umwelt und Vertrauen**
- **KI bringt Innovation – aber auch neue Risiken**

Photo by ChatGPT

OT-Systeme werden immer komplexer – basieren aber oft auf fragiler technischer Basis.

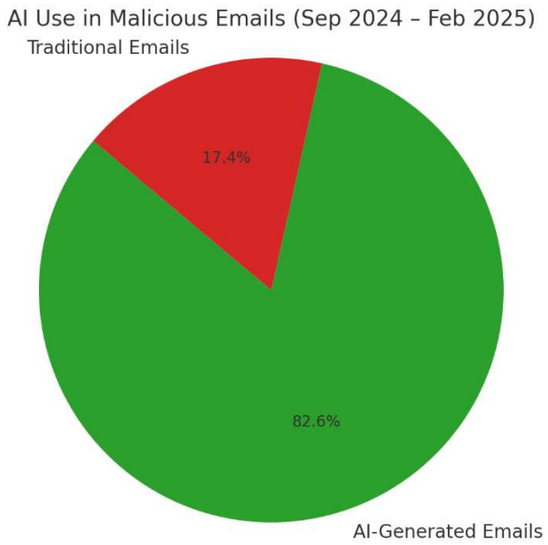
Bedrohungslage 2025

- **Ransomware-Angriffe +46 %** im 1. Quartal 2025
- **CISA warnt**: Zunehmende Aktivitäten von **„weniger professionellen Angreifern“** mit öffentlich zugänglichen Tools
- **Wasser- und Energiesektor** bleiben besonders gefährdet (Laut WEF-Bericht)

https://industrialcyber.co/reports/new-honeywell-2025-cyber-threat-report-reveals-ransomware-surges-46-percent-with-ot-systems-as-key-targets
https://www.cisa.gov/news-events/ics-advisories/icsa-25-140-09

LLM-Boom & OT-Sicherheit – Phishing-Angriffe

- Analyse von **386.000 schadhafte E-Mails** (Sep 2024 – Feb 2025):
  - **82,6 %** nutzten **KI-generierte Inhalte**
  - **+17,3 %** Anstieg im Phishing-Aufkommen



- **CISA warnt**:
  „Phishing bleibt einer der Hauptangriffswege – nun verstärkt durch Tools wie ChatGPT.“
- In OT-Vorfällen (z. B. LockBit, Black Basta):
  - Der **erste Zugriff erfolgt häufig über Phishing** bei Ingenieur:innen oder Dienstleistern
- **KI-generierte E-Mails** sind besser formuliert und überzeugender –
  → höhere Klickrate

https://securitytoday.com/articles/2025/04/15/report-82-percent-of-phishing-emails-used-ai.aspx?utm_source=chatgpt.com
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a?utm_source=chatgpt.com

LLM-Boom & OT-Sicherheit - Phishing-Angriffe

Altmodische Phishing-E-Mail (ohne KI)

From: it-support@your-water-plant.net
To: Admin Team
Subject: URGENT: Password Confirm

Dear Admin,

We doing a secuirty update. Please confirm your password to keep
system running:

http://your-water-plant-secure-login[.]com

Failure to comply will cause shut down of SCADA panel.

Thanks,
IT Support

LLM-gestützte „Next-Gen“-Phishing-E-Mail

From: Julia Kraus <j.kraus@eu-water-isac.net>
To: Michael Fischer <m.fischer@rheingau-water.de>
Subject: [Ticket #62443] Firmware Hotfix for GE Fanuc RX3i PLCs – Action Needed Before 18:00

Hi Michael,

following yesterday’s joint ISAC call about CVE-2025-36535, we have coordinated directly with GE to provide an interim firmware hot-fix that prevents unauthenticated Modbus writes to the RX3i CPU. The patch has been validated by two member utilities (see attached SHA-256 checksums).

Because your SCADA asset inventory (last updated 13 May) lists seven RX3i racks in Pump Station A and Booster C, we recommend applying the hot-fix before peak-demand tonight:

▶ Download (via secure portal):
https://portal.eu-water-isac.net/auth/patch-rx3i-24-06-25?cid=548712

After installing, please upload the log bundle so we can mark the ticket closed.

Let me know if anything is unclear—I’m on Signal if you need a quick chat.

Best regards,
Julia Kraus | OT-CERT Engineer
European Water ISAC – Incident Response Desk
j.kraus@eu-water-isac.net • +49 151 555 01234

LLM-Boom & OT-Sicherheit - Phishing-Angriffe

Generisch adressiert („Dear Admin“)

Personalisierte Inhalte basierend auf Rollen, Geräteinventar oder tatsächlichen Schwachstellen

From: it-support@your-water-plant.net
To: Admin Team
Subject: URGENT: Password Confirm

Dear Admin,

We doing a secuirty update. Please confirm your password to keep
system running:

http://your-water-plant-secure-login[.]com

Failure to comply will cause shut down of SCADA panel.

Thanks,
IT Support

From: Julia Kraus <j.kraus@eu-water-isac.net>
To: Michael Fischer <m.fischer@rheingau-water.de>
Subject: [Ticket #62443] Firmware Hotfix for GE Fanuc RX3i PLCs – Action Needed Before 18:00

Hi Michael,

following yesterday's joint ISAC call about CVE-2025-36535, we have coordinated directly with GE to provide an interim firmware hot-fix that prevents unauthenticated Modbus writes to the RX3i CPU. The patch has been validated by two member utilities (see attached SHA-256 checksums).

Because your SCADA asset inventory (last updated 13 May) lists seven RX3i racks in Pump Station A and Booster C, we recommend applying the hot-fix before peak-demand tonight:

▶ Download (via secure portal):
https://portal.eu-water-isac.net/auth/patch-rx3i-24-06-25?cid=548712

After installing, please upload the log bundle so we can mark the ticket closed.

Let me know if anything is unclear—I'm on Signal if you need a quick chat.

Best regards,
Julia Kraus | OT-CERT Engineer
European Water ISAC – Incident Response Desk
j.kraus@eu-water-isac.net • +49 151 555 01234

LLM-Boom & OT-Sicherheit - Phishing-Angriffe

Häufig mit schlechter Sprache oder Rechtschreibfehlern

```
From: it-support@your-water-plant.net
To: Admin Team
Subject: URGENT: Password Confirm

Dear Admin,

We doing a secuirty update. Please confirm your
password to keep
system running:

http://your-water-plant-secure-login[.]com

Failure to comply will cause shut down of SCADA
panel.

Thanks,
IT Support
```

Gut formuliert, technisch präzise und überzeugend

```
From: Julia Kraus <j.kraus@eu-water-isac.net>
To: Michael Fischer <m.fischer@rheingau-water.de>
Subject: [Ticket #62443] Firmware Hotfix for GE Fanuc RX3i PLCs – Action
Needed Before 18:00

Hi Michael,

following yesterday's joint ISAC call about CVE-2025-36535, we have
coordinated directly with GE to provide an interim firmware hot-fix that
prevents unauthenticated Modbus writes to the RX3i CPU. The patch has been
validated by two member utilities (see attached SHA-256 checksums).

Because your SCADA asset inventory (last updated 13 May) lists seven RX3i
racks in Pump Station A and Booster C, we recommend applying the hot-fix
before peak-demand tonight:

▶ Download (via secure portal):
https://portal.eu-water-isac.net/auth/patch-rx3i-24-06-25?cid=548712

After installing, please upload the log bundle so we can mark the ticket
closed.

Let me know if anything is unclear—I'm on Signal if you need a quick chat.

Best regards,
Julia Kraus | OT-CERT Engineer
European Water ISAC – Incident Response Desk
j.kraus@eu-water-isac.net  •  +49 151 555 01234
```

Aktuelle Angriffe: Energie & Industrie

- **Schneider Electric** meldet eine **Cyberattacke auf das interne Projekt-Tracking-System**, das sich angeblich in einer isolierten Umgebung befand (Nov 2024)
- Die Gruppe **HellCat** gibt an, folgende Daten **exfiltriert** zu haben:
  - Über **40 GB** aus dem internen **JIRA-System**
  - Enthält **Projekte, Tickets, Plugins und über 400.000 Benutzerdaten**
- Geforderte Lösegeldsumme: **150.000 US-Dollar**
- **Dritter Vorfall bei Schneider innerhalb von 18 Monaten**

https://cyberscoop.com/schneider-electric-energy-ransomware-hellcat/

CYBERSCOOP

RANSOMWARE

Schneider Electric reports cyberattack, its third incident in 18 months

The ransomware group HellCat claims responsibility for the cyberattack and threatens to dump 40GB.

BY CHRISTIAN VASQUEZ • NOVEMBER 5, 2024

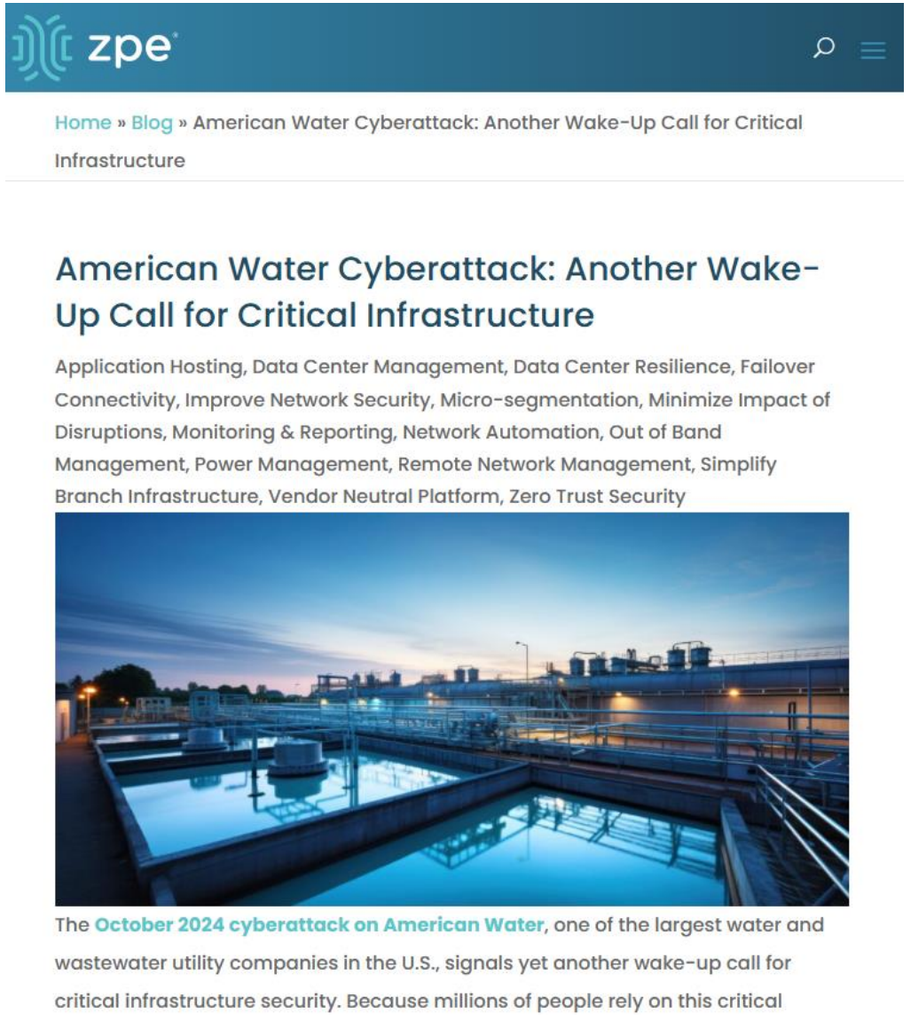
Listen to this article 2:34 Learn more.

Facade of the headquarters building of Schneider Electric, a French multinational company specializing in digital automation and energy management (Getty Images)

Aktuelle Angriffe: Wassersektor

- Das Unternehmen **American Water Works Co. Inc.** –
  der **größte regulierte Wasser- und Abwasserversorger der USA** –
  war Ziel eines **Cyberangriffs**,
  der das **Kundenportal und die Abrechnungsdienste** lahmgelegt hat
  (Okt 2024)

- **Wer war betroffen?**
  - Über **14 Millionen Menschen** in **14 Bundesstaaten**
  - Einschließlich **18 Militärstandorte**



https://zpesystems.com/american-water-cyberattack-another-wake-up-call-for-critical-infrastructure/

Quelle: https://www.youtube.com/watch?v=6-SXUbdnPr4 https://www.youtube.com/watch?v=T7OQbb_-x-U

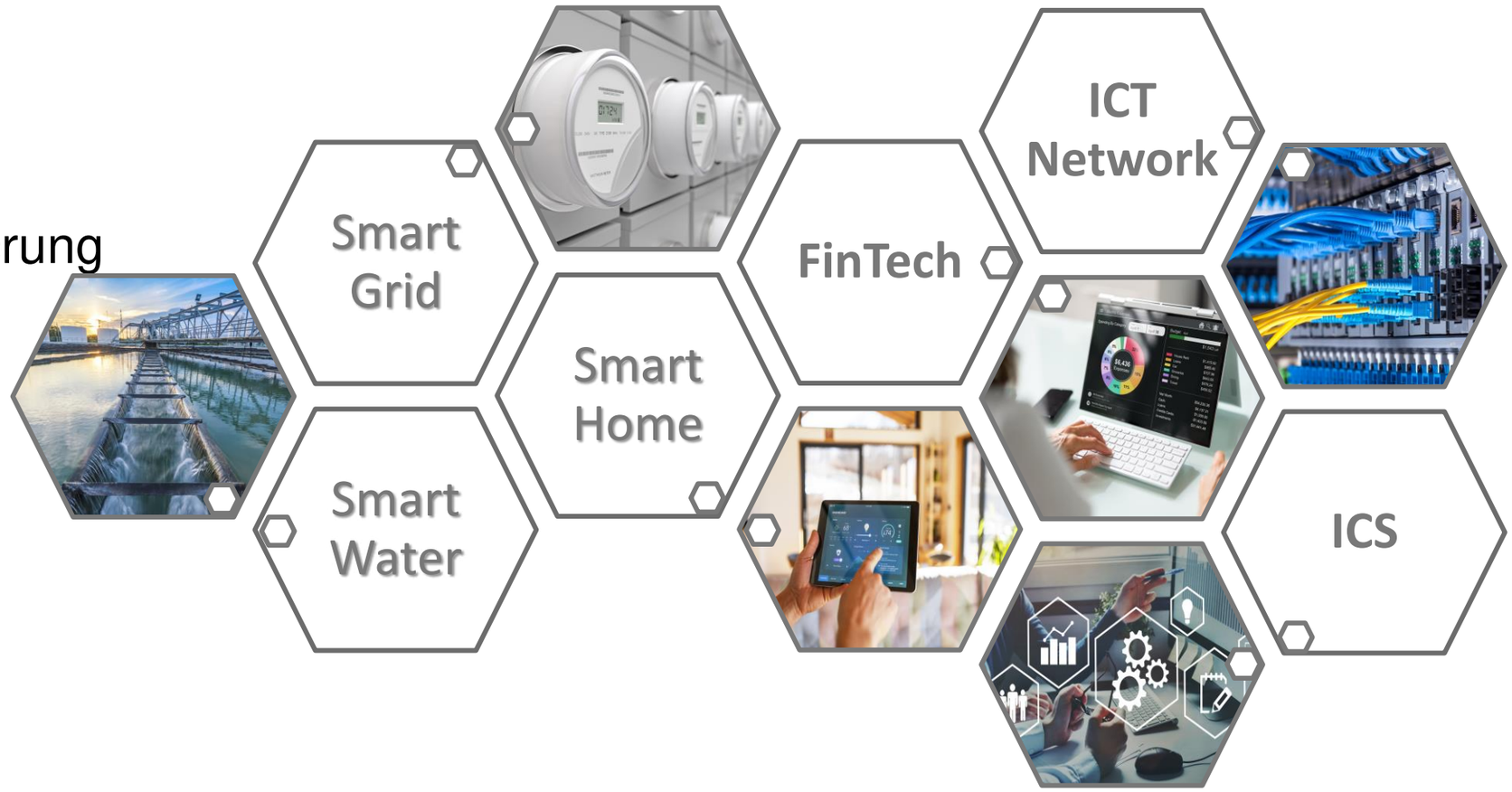
Resilienz

- *“Die Fähigkeit eines Systems, sich auf Störungen vorzubereiten, sie aufzunehmen, sich davon zu erholen und sich an neue Bedingungen anzupassen –insbesondere bei Vorfällen im Zusammenhang mit Cyberangriffen.”*

Cyber Resilience of Networks and Systems, Springer, Kott & Linkov eds.

IT/OT-Resilienz und Sicherheitsforschung bei JR

- **Security-by-Design**
  - Automatisierte Sicherheitstests
  - Bedrohungsmodellierung
- **KI und Sicherheit**
  - Resilienz durch KI-gestützte Methoden
  - Sicherheit von KI-Systemen



JOANNEUM RESEARCH DIGITAL

SeRWas

- **Sichere & resiliente Wasserwirtschaft**
  - **Förderprogramm**: FFG KIRAS 2023
  - **Fokus**: Verbesserung der Cybersicherheit im österreichischen Wassersektor
  - https://projekt-serwas.at/
- **Projektfokus & JR-Beiträge**
  - Verbesserung des **Cyber-Schutzes** für Wasserwirtschaft durch gezielte Methoden und Tools
  - Entwicklung von **KI** zur frühzeitigen Erkennung von Cyberangriffen
    - Einsatz von **Edge AI** / **Tiny AI** für eingebetteten Echtzeitschutz
  - Wissensvermittlung zur Förderung von **Awareness** und **Best Practices**
  - Durchführung von **Risikoanalysen und Bedrohungsmodellierung** für die Wasserverteilung

Bundesministerium
Land- und Forstwirtschaft,
Regionen und Wasserwirtschaft

TU Graz

GRAZ HOLDING

xylem
Let's Solve Water

ipCENTER
Raum für Bildung

Photo by Orhan Akbaba: https://www.pexels.com/photo/water-flowing-from-pipes-17882783/

JOANNEUM RESEARCH DIGITAL

Ausblick 2025-2030

- **KI-gesteuerte Angriffe** auf physische Infrastruktur und Prozessleitsysteme
- **Deepfakes & Social Engineering** gegen Personal in Leitwarten und Bereitschaftsdiensten
- **Post-Quanten-Kryptografie**: Umstieg auf neue Verschlüsselungsstandards
- **Strengere Regulierung**: Gesetzgeber erhöhen die Haftung von Infrastrukturbetreibern

Photo by Pixabay: https://www.pexels.com/photo/blue-bright-lights-373543/

Conclusion – Was können wir tun?

- **OT-Systeme sind kritisch**, aber oft nur unzureichend geschützt
- **Cybersicherheit muss ein zentraler Bestandteil** der OT-Strategie sein
- **Enge Zusammenarbeit** zwischen IT, OT und Management ist entscheidend
- **KI verändert** sowohl **Bedrohungen** als auch **Verteidigungsstrategien** – jetzt handeln!!

Photo by JOANNEUM RESEARCH

KI – zwischen Risiko und Chance für mehr Cybersicherheit.