VOICE
CIO Service GmbH

CYBER SECURITY COMPETENCE CENTER
Blinde Flecken in der Produktion

it-sa 2022

Dokumentation vom 27.10.2022
Erstellt von COMPLION AG, Köln

Ihr Experte des VOICE e.V. Cyber Security Competence Center

IT-SA 2022

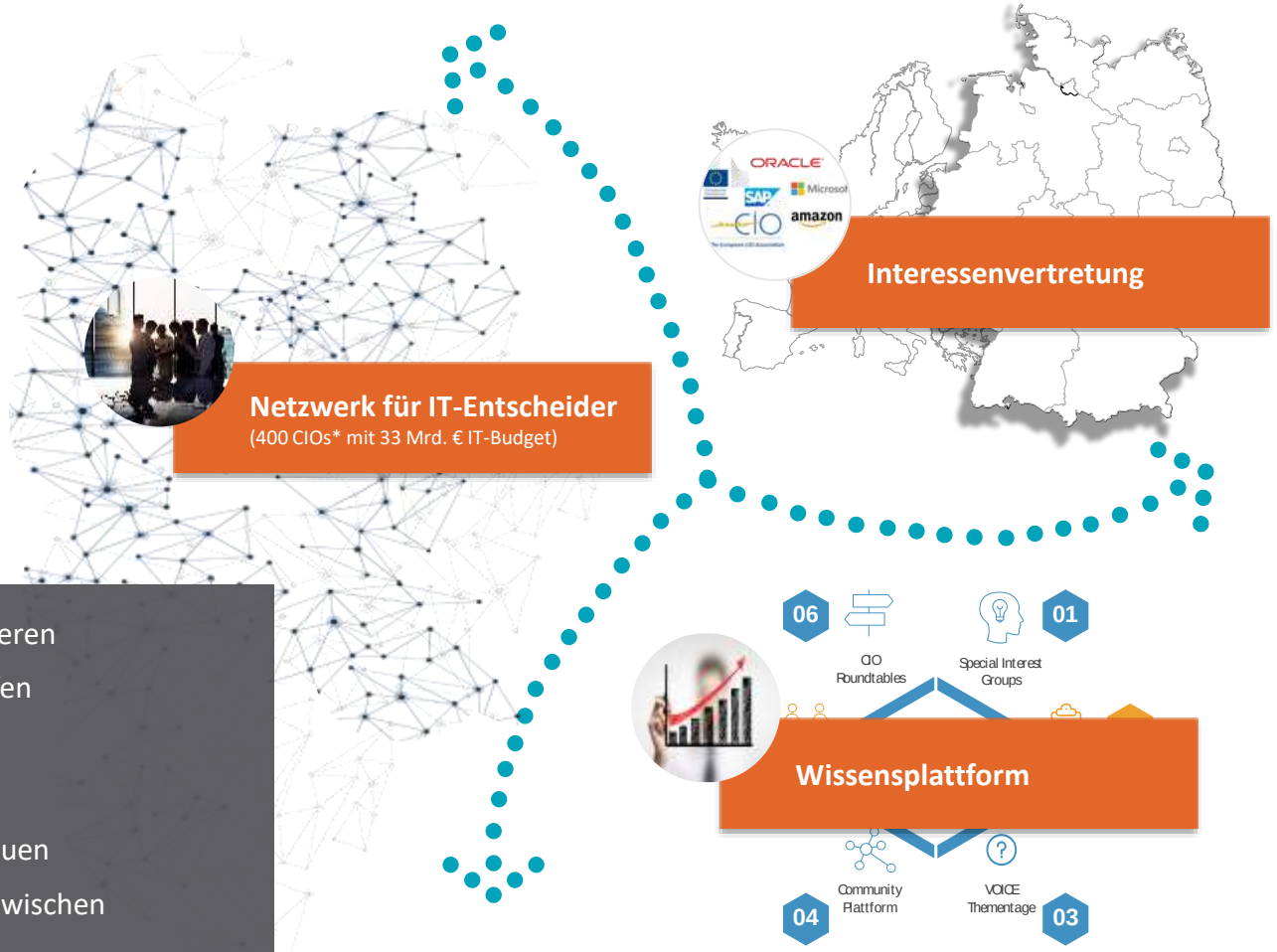
TOBIAS PHILIPSEN

- IT-Security Experte (Governance)
- Internationales Strafrecht im Cyberraum
- Cybersicherheit und Lagebild
  (VOICE Cyber Security Competence Center)

- tobias.philipsen@complion.de

VOICE e.V.: einer der wichtigsten Anwenderverbände; mehr als 400 Mitgliedsunternehmen

IT-SA 2022



- ✓ Offen, aber geschützt kommunizieren
- ✓ Faire Rahmenbedingungen schaffen
- ✓ Erfolgreich vernetzt agieren
- ✓ Agenda Setting
- ✓ Schnell gemeinsam Wissen aufbauen
- ✓ Förderung der Zusammenarbeit zwischen Business und IT
- ✓ Schnelle Hilfe bei Ihren Problemen

*Mitglieder sind ausschließlich IT-Anwenderunternehmen aller Größen und Branchen

VOICE, der Bundesverband der IT Anwender e.V., unterstützt durch COMPLION

COMPLION AG, SPEZIALISIERT AUF MANAGEMENTBERATUNG ZU COMPLIANCE-, RISIKO- UND IT SICHERHEITSTHEMEN, UNTERSTÜTZT DEN BUNDESVERBAND DER IT ANWENDER VOICE IN IT-FACHTHEMEN.

VOICE
CIO Bundesverband der IT-Anwender e.V.

Mission

- Netzwerk
- Roundtable, Fach-Workshops, Online Plattform
- Austausch von Erfahrungen und Fachwissen
- Steigerung der Wettbewerbsfähigkeit durch den Einsatz digitaler Technologien

Mitglieder

- Über 400 Mitglieder
- Größte Vertretung von Digital-Entscheidern der Anwenderseite im deutschsprachigen Raum
- DAX, MDAX und mittelständische Unternehmen

COMPLION

Unser Portfolio

- Managementberatung für Compliance, Risiko und IT-Sicherheitskonzepte von Konzernen
- Schwerpunkte: Software-Wirtschaftlichkeit, Softwarevertrags- und Nutzungskonzepte, Datenschutz und Cyber Security

Das Team

- Derzeit 20 sehr erfahrene sowie junge Kolleg:innen verschiedener Fachrichtungen
- Grundsätze: „Equality in Idea Generation“ & Work-Life-Balance
- Erfolgreiche Nachwuchskräften können Mitunternehmer werden

Cyber Compliance per Managed Service

THREAT INTELLIGENCE – THEMEN MIT GEFAHRENPOTENZIAL IM UNTERNEHMEN RICHTIG POSITIONIEREN

Die aktuelle IT-Sicherheitslage

- Mit **neuen Angriffstechniken** ist ständig zu rechnen → Resilienz !
- Der Großteil der heutigen Angriffe nutzt **Schwachstellen, die Wochen oder Monate bekannt** sind → Patch-Geschwindigkeit !
- Ausnutzung von Sicherheitslücken teils bereits **nach wenigen Stunden** → Prävention !

Das VOICE Cyber Security Competence Center

- Wöchentlicher **Managed Security Service**: kuratierte Produktion und Lieferung der aktuellen Cyber Threat Intelligence
- **Community Sharing** im Kreis von CISOs und Senior Experts (derzeit ca. 25 Unternehmen / Organisationen)
- Diskussion zur Bewertung, zu Priorisierungen und zum Austausch der **tagesaktuellen Handlungsnotwendigkeiten**
- Aufbau und Pflege einer hoch effektiven Community für **Prävention und Best Practices**

- VOICE liefert mit dem CSCC einen einzigartigen Service, den jedes Unternehmen und Organisation benötigt

VOICE Cyber Security Competence Center Webcast – Threat Intelligence on Demand

DER CSCC WEBCAST RICHTET SICH INSBESONDERE AN MITTELSTÄNDISCHE UNTERNEHMEN

Angebot

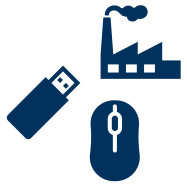
- **Zweiwöchentliche Multimedia-Veröffentlichung** (Audio, Video, Begleit-PDF) zum Streaming on Demand
- Audiopodcasts **direkt via allen gängigen Podcast Apps** (u.a. Apple Podcasts und Pocketcast) zu empfangen
- **Flash-Berichte** zu besonders kritischen Meldungen zwischen den regelmäßigen Veröffentlichungen (z.B. bei aktiv ausgenutzten Zero-Day-Lücken)

Inhalte

- Inhalte **speziell abgestimmt auf** die Sicherheitsinformationsanforderungen von **mittelständischen Unternehmen**
- Aufbau der **Lageberichte analog zur CSCC Community**: Attacks & Breaches, Threats & Vulnerabilities, Security Intelligence

Die Bedrohung von IT via OT und IoT ist in den letzten Jahren angestiegen.

IT-SA 2022



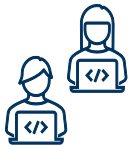
- Produktionsgeräte / Maschinen
- IoT-Geräte, die nicht in der IT angesiedelt sind
- Peripherals / Lizenzträger mit beschreibbarem Speicher

- Ansiedelung außerhalb der direkten IT-Verantwortung
- Geräte oft mehrere Jahrzehnte im Einsatz
- Gesteigerte Netzwerkkomplexität aufgrund von Segmentierungen

- Mehr als doppelte Anzahl an Meldungen mit Industrie-Bezug im CSCC im Jahr 2022 (vgl. 2021)
- Proof-of-Concepts für Angriffstechniken auf IT via OT immer häufiger diskutiert
- Russischer Angriffskrieg gegen die Ukraine betrifft seit erstem Tag Industrie und insb. Kritis

Häufig auftretende Probleme mit OT / IoT

IT-SA 2022



Starke Dezentralität der Verwaltungsressourcen

Keine Verfügbarkeit von Patches und Firmware Updates, insb. im Bereich IoT

Fehlende Patch-Zyklen aufgrund von Produktionsnotwendigkeiten

Eingeschränkte oder sogar fehlende Visibilität von Geräten

IDS / IPS eingeschränkt auf OT / IoT anwendbar

"Evil PLC Attack" Angriffsvektor demonstriert Nutzung von PLCs für die Verbreitung von Malware im Unternehmens-IT/ OT-Netzwerken.

CSCC LAGEBERICHT KW33

ATTACKS & BREACHES

THREATS & VULN'S

SECURITY INTEL

1. **Claroty:** Sicherheitsforscher:innen veröffentlichen Proof-of-Concept zur Ausnutzung mehrerer teils kritischer Sicherheitslücken in PLC Entwicklungsumgebungen von u.a. Rockwell Automation, Schneider Electric und General Electric

   - Betroffen: PLC Entwicklungsumgebungen von **Rockwell Automation** (Micro800 Control Systems Platform), **Schneider Electric** (Modicon Platform), **GE** (Mark VIe Platform), **B&R** (X20 System Platform), **Xinje** (XD Series Platform), **OVARRO** (TBox Platform) und **Emerson** (PACSystems Platform)

   Auszugsweise:

   - **KW28:** CVE-2022-26507 (CVSSv3: 9,8) Schneider Electric SCADAPack: Out-of-Bounds Write in *XML Decompression DecodeTreeBlock* von *AT&T Labs Xmill 0.7. A* -> Heap-basierter Buffer Overflow -> Senden einer nicht näher spezifizierten Input-Datei -> Remote Code Execution durch einen unauthentifizierten Remote-Angreifer

   Angriffsvektor:

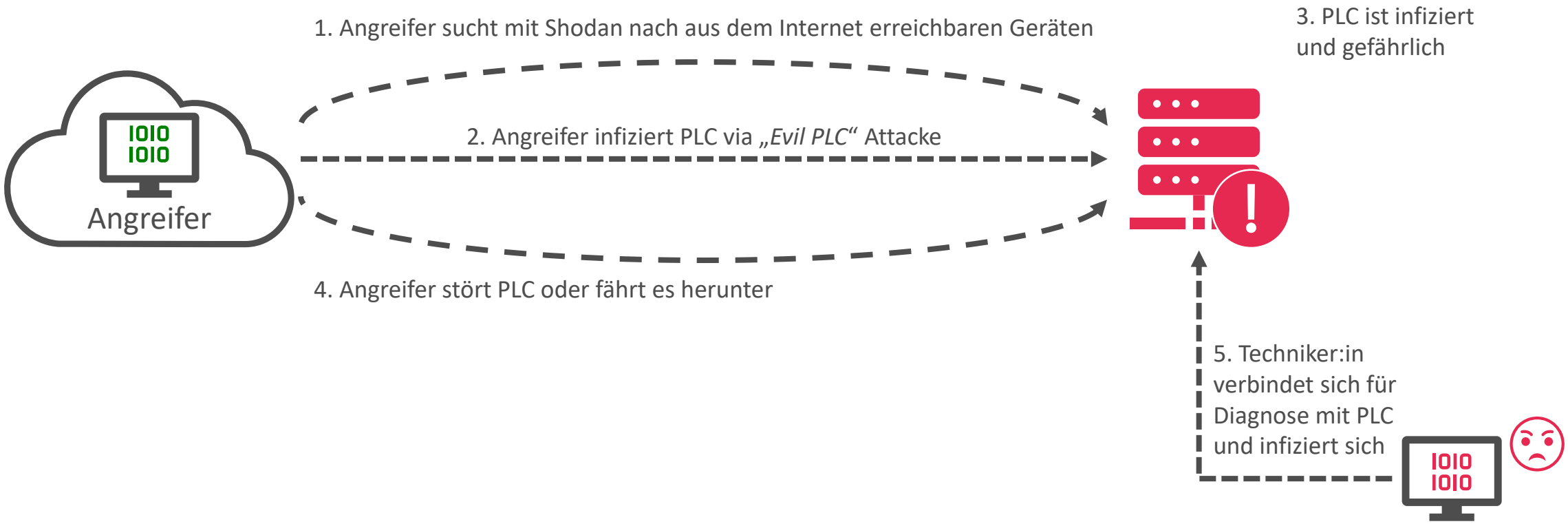
   - Angreifer scannt nach über Internet erreichbare und verwundbare PLCs
   - Injizieren von Schadcode auf PLC via vom Angreifer kontrollierter PLC-Entwicklungsworkstation
   - PLC wird mit Entwicklungsworkstation verbunden -> Parsen des Schadcodes vom schadhaften PLC in PLC-Entwicklungsumgebung
   - Verbreitung via PLC-Entwicklungsumgebung im Operational Technology (OT)-Netzwerk

   → **Updates einspielen**; **Netzwerksegmentierung**, **-Hygiene** und **Traffic Monitoring**

   Claroty – Webseite | CSO Online – Artikel

"Evil PLC Attack" Angriffsvektor demonstriert Nutzung von PLCs für die Verbreitung von Malware im Unternehmens-IT/ OT-Netzwerken.

CSCC LAGEBERICHT KW33



Vendor	Platform	Arch	Tested Model (CPU Module)	RTOS Firmware	Engineering Workstation	Protocol	Root Cause	CVE
OVARRO	TBOX	ARM	TBOX LT2-530	Linux	TwinSoft	Custom Modbus (Port 502/TCP)	ZipSlip / Path Traversal	CVE-2021-22650
B&R (ABB)	X20 System	ARM/x86	X20CP1585	VxWorks	Automation Studio	ANSL (Port 11169/TCP) INA2000 (Port11159/TCP or UDP)	ZipSlip / Path Traversal	CVE-2021-22289
Schneider Electric	Modicon (M349, M580)	ARM	M340, M580	VxWorks	EcoStruxure Control Expert (Unity Pro)	Modbus / UMAS (Port502/TCP)	Memory Corruption (Heap Overflow)	CVE-2022-26507
General Electric	MarkVIe	PPC (BE)	MarkVIe IS220UCSAH1A	QNX Neutrino	ToolBoxST	SDI (Port5311/TCP)	ZipSlip / Path Traversal	CVE-2021-44477, CVE-2018-16202
Rockwell Automation	Micro Control Systems	ColdFire	Micro820	ThreadX	Connected Components Workbench CCW)	CIP (Port 44818/TCP)	Unsafe Deserialization	CVE-2021-27475, CVE-2021-27471, CVE-2021-27473
Emerson	PACSystems	X86	Rx3i	VxWorks	PAC Machine Edition	SRTP (Port 18245/TCP)	ZipSlip / Path Traversal	CVE-2022-2788
Xinje	XDPPro	ARM	XD/E PLC	VxWorks	XD PLC Program Tool	Modbus UDP (Port 502/UDP)	ZipSlip / Path Traversal	CVE-2021-34605, CVE-2021-34606

Die Möglichkeiten zur Risikomitigation im Bereich OT / IoT lassen sich in drei Kategorien einteilen.

IT-SA 2022

Awareness & Prevention

- Nutzung von Threat Intelligence zu Bedrohungen gegen OT / IoT (u.a. Voice CSCC)
- Kommunikation der Bedrohungslage an das Management
- Zuständigkeiten für OT-Security im Unternehmen klären
- Asset Management for OT / IoT optimieren

Detection, Response & Recovery

- Visibilität erhöhen (u.a. über Einbindung in Überwachungstools)
- Endpoint Detection & Response auf OT anpassen
- OT in Recovery Prozesse nach Cyberattacken integrieren
- Identity & Access Management für OT prüfen

Continuous Improvement

- Pen-Testing für Netzwerkauditierung
- Austausch nicht patchbarer Geräte (wenn möglich) / Patch-Zyklen für OT reviewen
- Stärkere Einbindung von IT-Sicherheitsanforderungen in Beschaffungsprozesse
- Regelmäßige Schulungen und Awareness-Trainings

VOICE
Bundesverband der IT-Anwender e.V.

VOICE – Bundesverband der IT-Anwender e.V.
Büro Berlin: Invalidenstraße 91 | 10115 Berlin
Büro München: Riedenburger Str. 2 | 81677 München (Postadresse)

+49 30 2084 964 70

voice-info@voice-ev.org

www.voice-ev.org

VR 31149B | Geschäftsführung: Wolfgang Storck

/company/voice-ev

/CIOVoice