

Identifizieren Sie Blind-Spots innerhalb Ihrer OT-Security

Mareike Redder, Produktmanagement cbb software GmbH
Benedikt Heintel, CISO Viega GmbH & Co. KG

KURZVORSTELLUNG

Mareike Redder

Mareike Redder ist als Ingenieurin der angewandten Informationstechnik seit 2018 bei der cbb software GmbH tätig.

Seit 2022 verantwortet Mareike Redder das Produkt Management der cbb software GmbH. Vor ihrer jetzigen Rolle war sie als Accountmanagerin tätig.

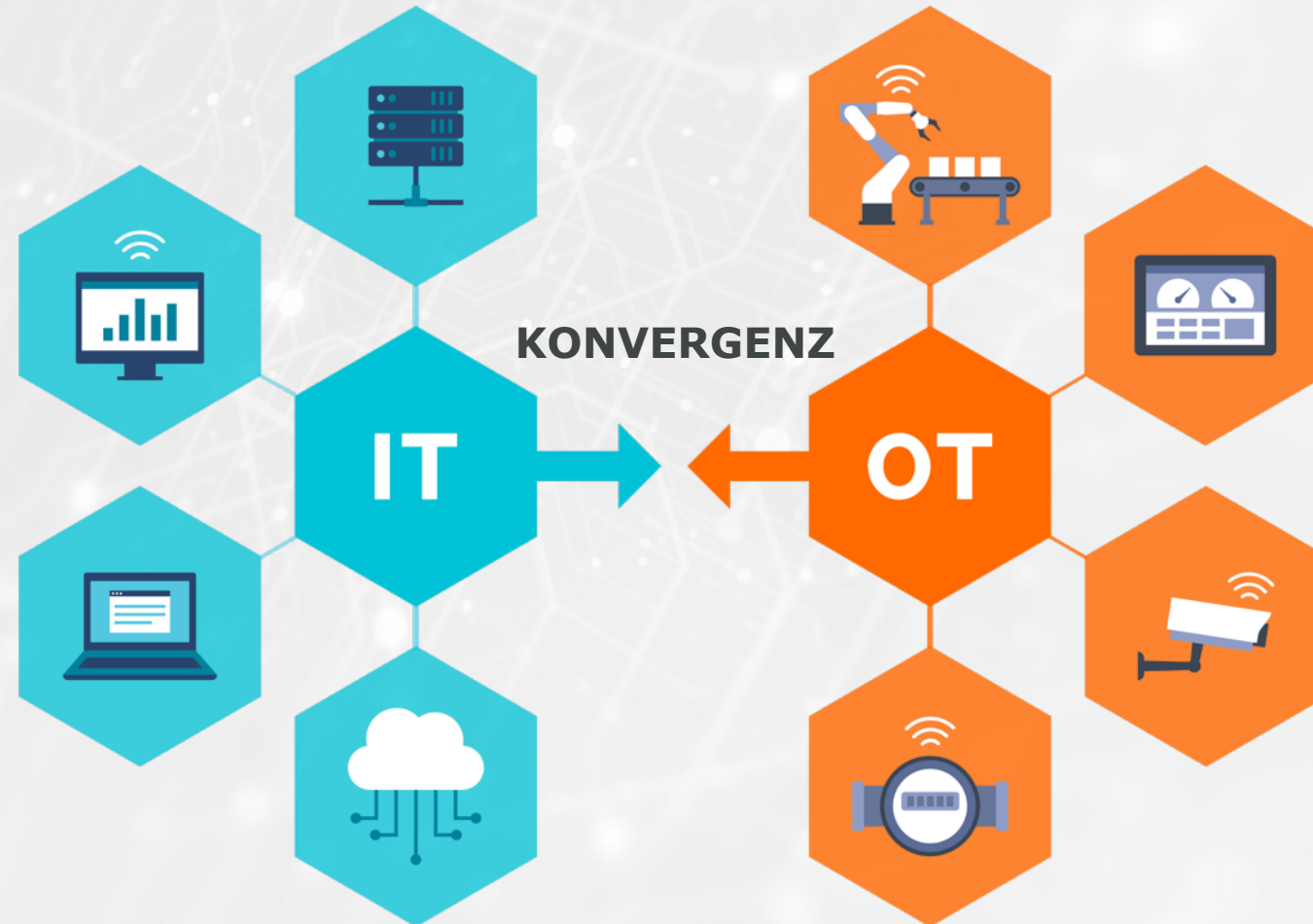
Die cbb software GmbH bietet seit mehr als 25 Jahren schlüsselfertige Produkte in den Bereichen Konnektivität, Sicherheit, Analytik und Energie. Ob Automotive, Gebäudetechnik oder Industrie cbb ist der internationale Partner für digitale Transformation.

Bereits nach ihrem Studium 2012 konnte Mareike Redder Erfahrungen in der Flugzeugindustrie eines amerikanischen Unternehmens sowie in der Leitung von technologiegetriebenen Forschungsprojekten im Energiesektor sammeln.



ABGRENZUNG IT & OT

WARUM IT/OT-KONVERGENZ?



CYBERCRIME IN DEUTSCHLAND

EINE STETIG WACHSENDE BEDROHUNG



3 von 4 Unternehmen

sind jährlich Opfer von Cyber-Angriffen



€ 203 Mrd. Schaden

pro Jahr,
alleine in Deutschland



436k Schadprogramme

weltweit, täglich...

**Das Gefahrenpotenzial für Unternehmen wächst stetig,
bei gleichzeitigem Bedarf nach Digitalisierung und Datentransparenz.**

AKTUELLE BEDROHUNGSLAGE

ES KANN JEDEN TREFFEN



Continental

August 2022

- Cyberangriff blieb wochenlang unbemerkt
- Ransomware Hackergruppe hat 40 TB Datenvolumen abgegriffen
- Angeblich auch Interna von namhaften Kunden aus Automobilbranche
- Daten stehen im Darknet zum Verkauf (für 50 Mio. Dollar)



Aurubis

Oktober 2022

- Hackerangriff auf IT-Infrastruktur
- Systeme präventiv heruntergefahren und vom Internet getrennt
- Produktion in Teilen betroffen,
- Wareneingang und -ausgang manuell aufrechterhalten



STEICO

März 2023

- Cyberangriff am 01.03.23
- Produktionsbetrieb und Verwaltung betroffen
- Aktuell unklar, ob Ransomware-Angriff mit Lösegeldforderung
- Taskforce mit Datenforensikern und Sicherheitsexperten eingerichtet

KURZVORSTELLUNG

Benedikt Heintel

Benedikt Heintel ist ein ausgewiesener Experte im Bereich der IT-, OT- und Informationssicherheit und derzeit als Chief Information Security Officer (CISO) bei der Viega Gruppe tätig. Viega ist ein führender Hersteller von Pressverbinder für Rohrleitungen und sensorgestützte Spülung. Darüber hinaus ist er ein aktiver Auditor für Informationssicherheits- Managementsysteme auf der Grundlage der ISO 27001.

Bevor er zu Viega kam, war Benedikt Heintel als Informationssicherheitsbeauftragter bei einem Mautunternehmen tätig. Zudem arbeitete er als Projektleiter für sicherheits- und technologieorientierte Projekte bei einem Engineering Dienstleister. Hierbei konnte er wertvolle Erfahrungen in Projekten für führende Unternehmen aus verschiedenen Branchen, darunter Telekommunikation, Finanzen und öffentliche Verwaltung, sammeln.



WHAT ABOUT YOU?





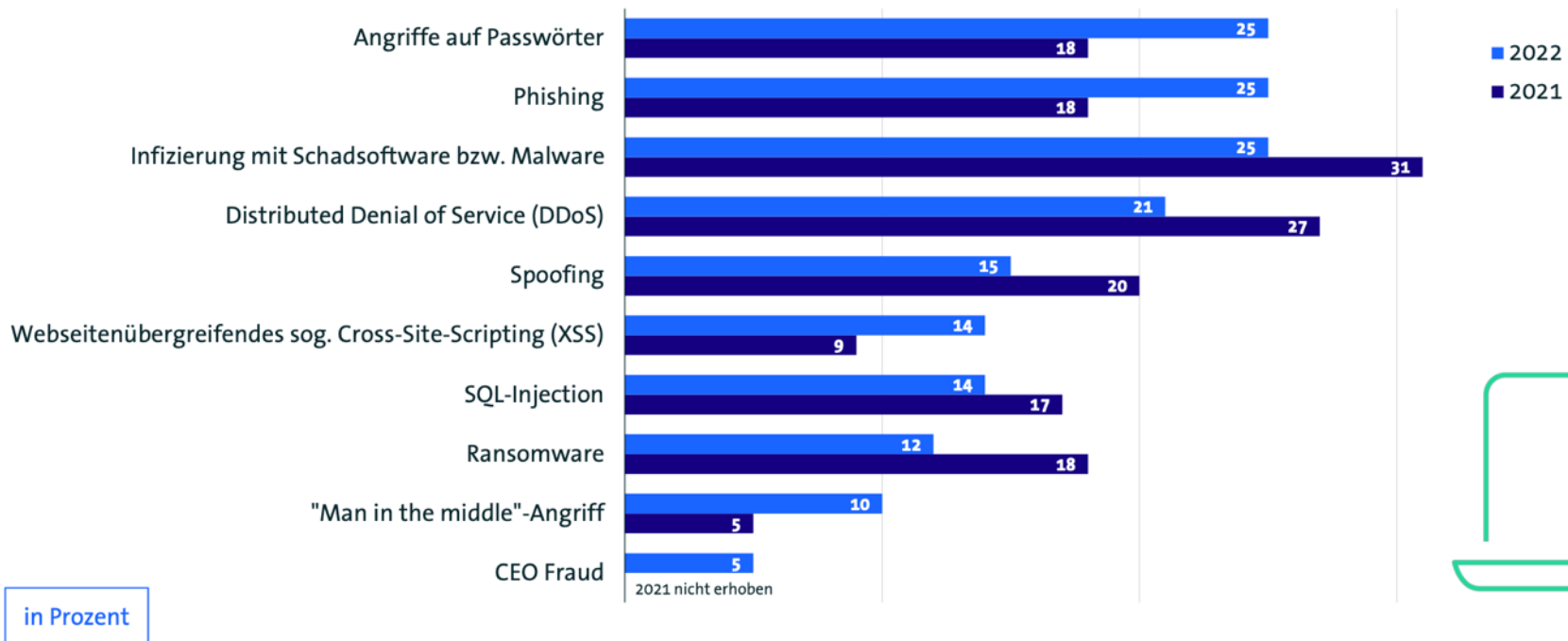
**DO YOU KNOW
YOUR ENEMY?**

TÄTERPROFILE

WAS IST BEKANNT?

Häufigere Schäden durch Phishing & Passwortdiebstahl

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?



Basis: Alle befragten Unternehmen (n=1.066) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022



HOW TO SECURE OT SYSTEMS?

**DO YOU
SLEEP WELL?**





BESSER SCHALFEN MIT DEM edge.SHIELDOR

KONVENTIONELLE OT-LÖSUNGEN

SEGMENTIERUNG + FIREWALL + ASSETMANAGEMENT

- ✓ Segmentierung von Netzwerken
- ✓ Freischaltung oder Sperrung von Ports
- ✓ Eine Lösung, um die Sicherheit zu erhöhen

- Keine intelligente Prüfung der Inhalte
- Umfangreiche IT Administration der Subnetze nötig
- Bedarf regelmäßiger Anlagenupdates
- Weiterhin Sicherheitslücken durch notwendige Services (VPN, Dateiaustausch,...)

**Und das Netzwerk kommt schnell einem
Schweizer Käse gleich...**

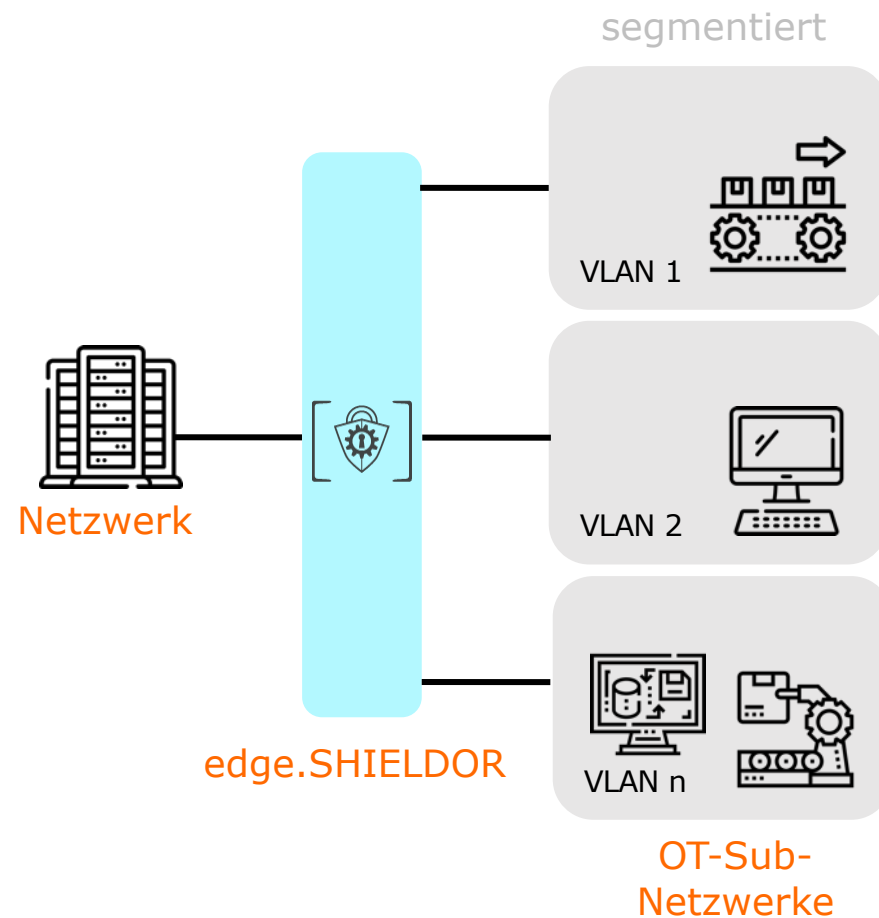


OT-SECURITY NEU GEDACHT ANFORDERUNGEN

- ✓ Risikomanagement und -bewertung
- ✓ Patch-Management
- ✓ Netzwerksegmentierung
- ✓ Identitäts- und Zugriffsmanagement
- ✓ Überwachung und Erkennung
- ✓ Kein Vendorlock – erweiterbare Architektur
- ✓ Datensicherheit und Datenwiederherstellung

OT-SECURITY NEU GEDACHT

UMFÄNGLICH ABGESICHERT MIT DEM edge.SHIELDOR*

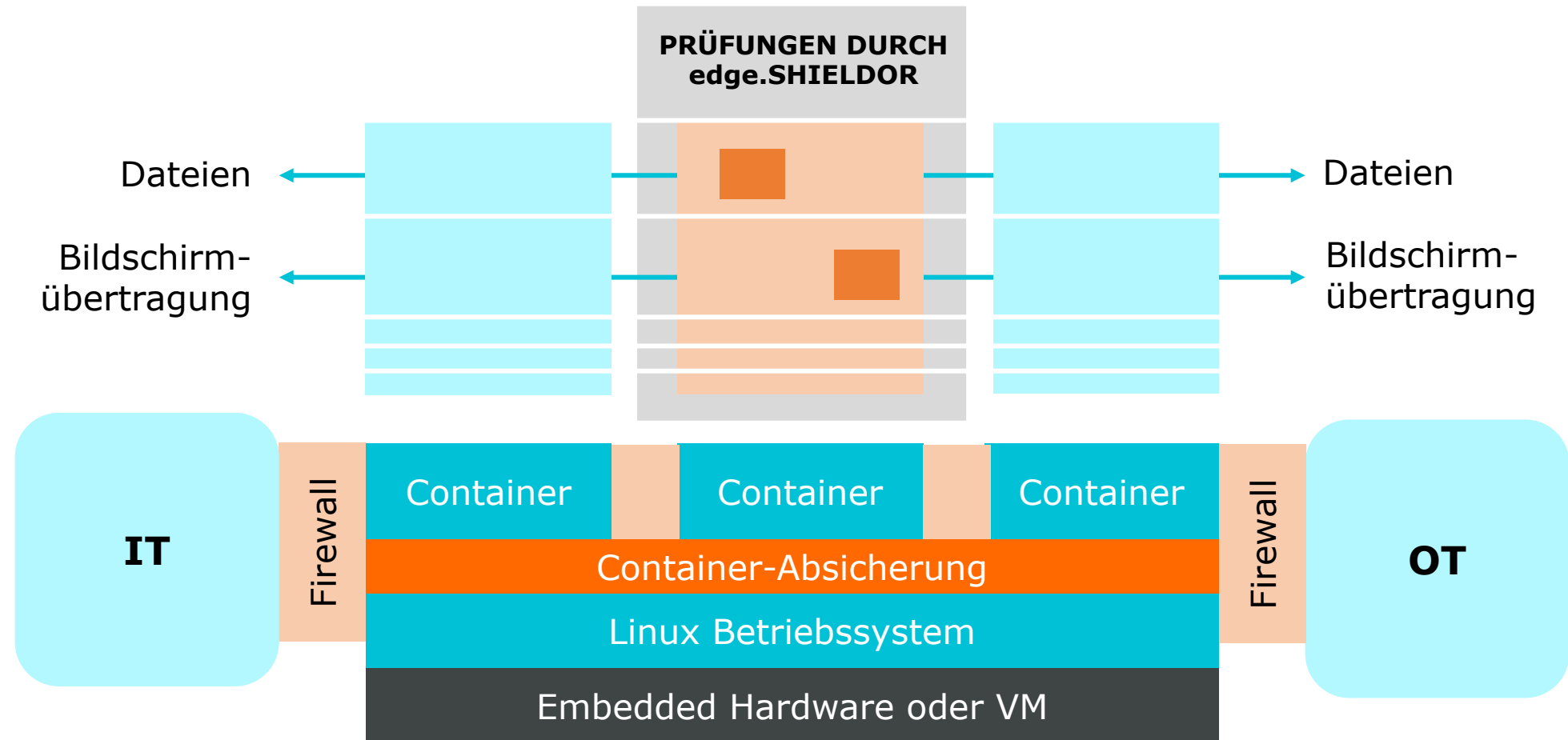


Eine Lösung, viele Vorteile

- ✓ **Keine Softwareupdates** alter Anlagen/Maschinen nötig
- ✓ **Gesamter Informationsfluss** zwischen IT und OT über den edge.SHIELDOR
- ✓ Eine durchgehende **Zero-Trust Architektur** aufbauen
- ✓ **Zentrale Verwaltung** aller Subnetze reduziert Aufwand
- ✓ **Homogene Lösung** für alte und neue Anlagen erzeugen für eine **vereinheitlichte IT/OT**
- ✓ **Kein aufwändiges Retrofitting**
- ✓ Automatisierte planbare **Updateroutinen**

OT-SECURITY NEU GEDACHT

SICHERHEITSKONZEPT



LEISTUNGSVERSPRECHEN & USPs



Kein Retrofit notwendig,
dadurch Kostenersparnis

Reduktion der Gefahr
einer Netzwerk-
kompromittierung durch
Entkopplung

Kompatibilität zu
edge.PORTFOLIO bietet
zusätzliche Analytik &
Prozessdatenerfassung

Unterstützung von
Drittsoftware durch
Container Lösung

Zentrale Verwaltung aller
Teilnetze durch eine
Managementoberfläche

Keine Softwareupdates
alter Anlagen /
Maschinen nötig

Der edge.SHIELDOR setzt für Sie da an, wo klassische
OT-Security Lösungen aufhören!



IT WORKS JUST LIKE A TIME MACHINE!

WATCH NOW!



KEY TAKEAWAYS





**LET'S
DISCUSS!**

SIE HABEN FRAGEN? WIR HELFEN IHNEN GERNE WEITER!

Mareike Redder
Produktmanagement

E: mareike.redder@cbb.de

cbb software GmbH
Isaac-Newton-Straße 8
D-23562 Lübeck

T: +49 451 39771- 0

M: info@cbb.de

W: www.cbb.de

cbb software GmbH
Mitglied der Viega Group seit 2018

Geschäftsführung: Benjamin Pieritz