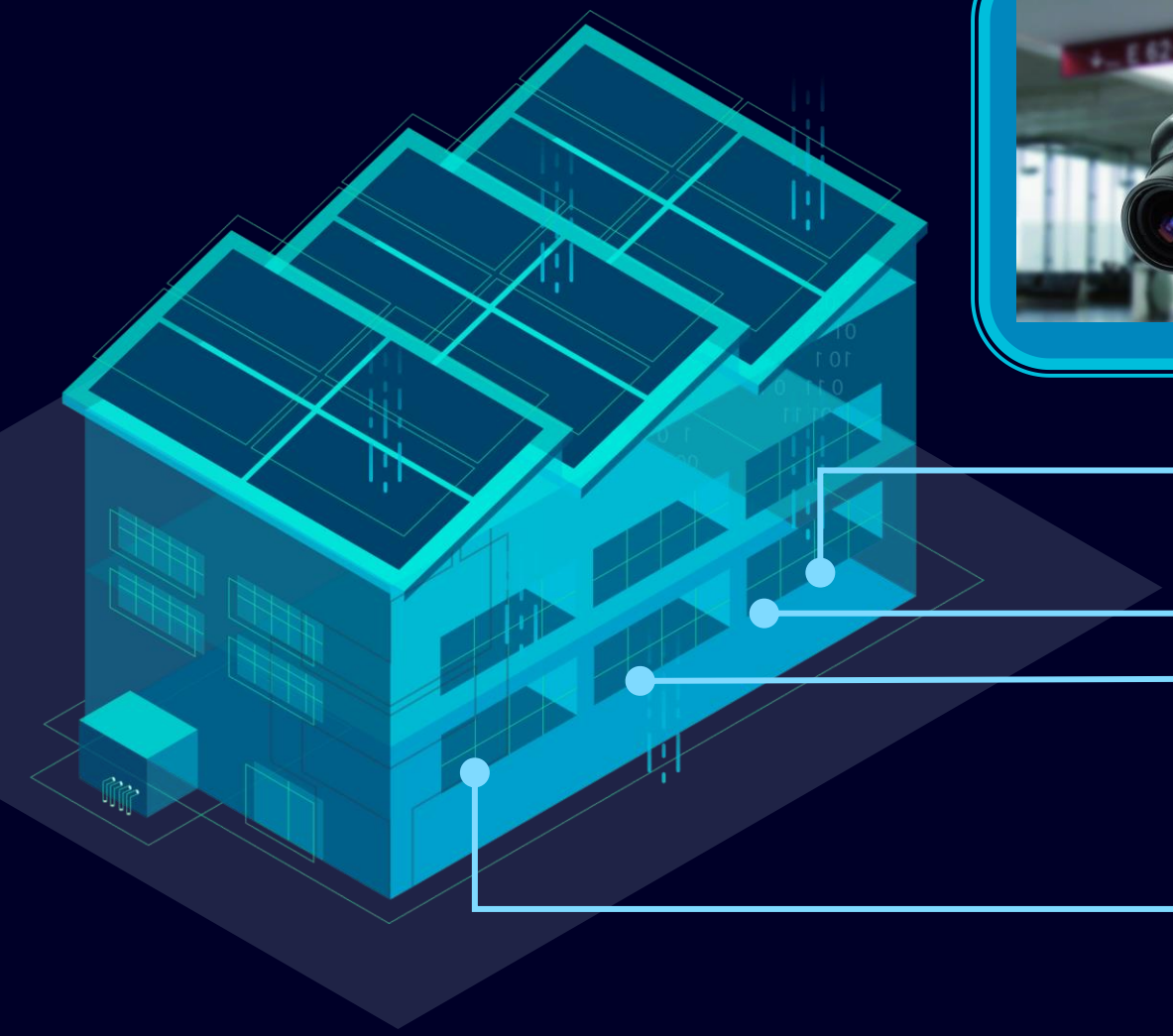
Cybersicherheit: Startklar für NIS2
IT & OT (Gebäude & Sicherheitstechnik)

Cybersecurity WKNÖ 2024

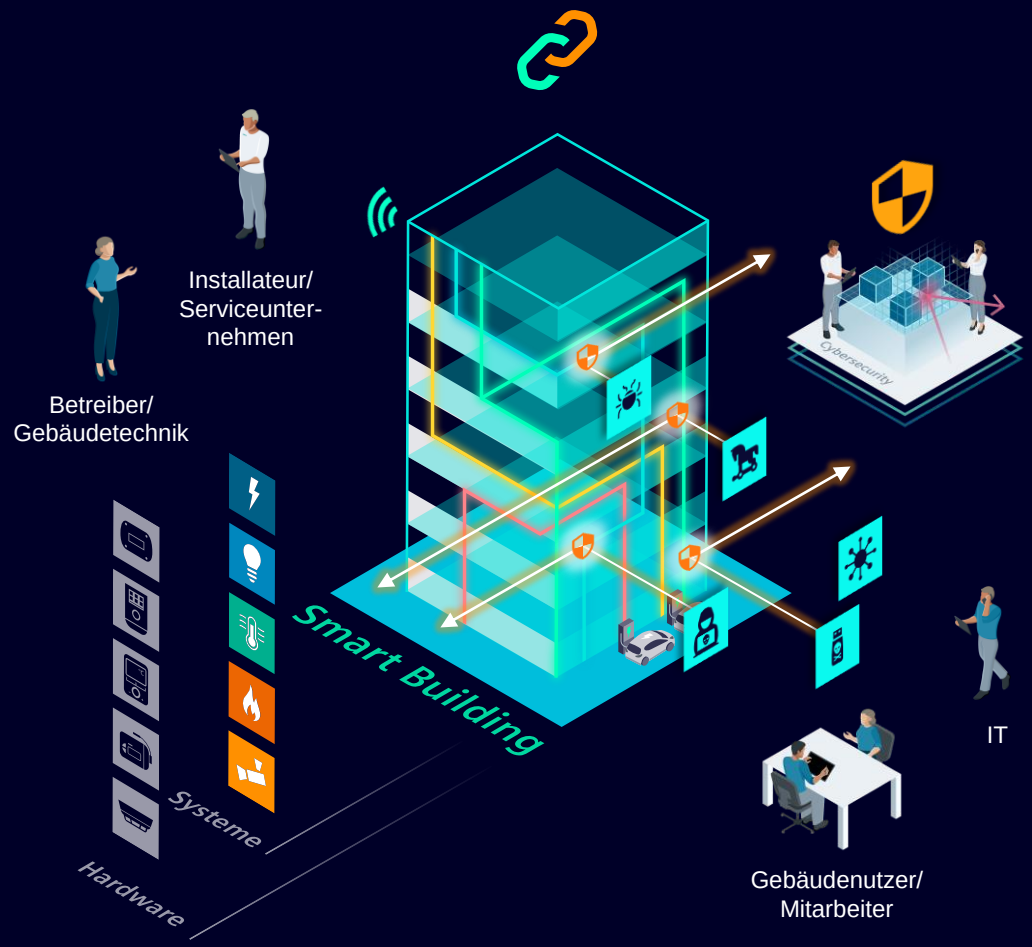
SIEMENS

Gestern gab es Kommunikationsinseln



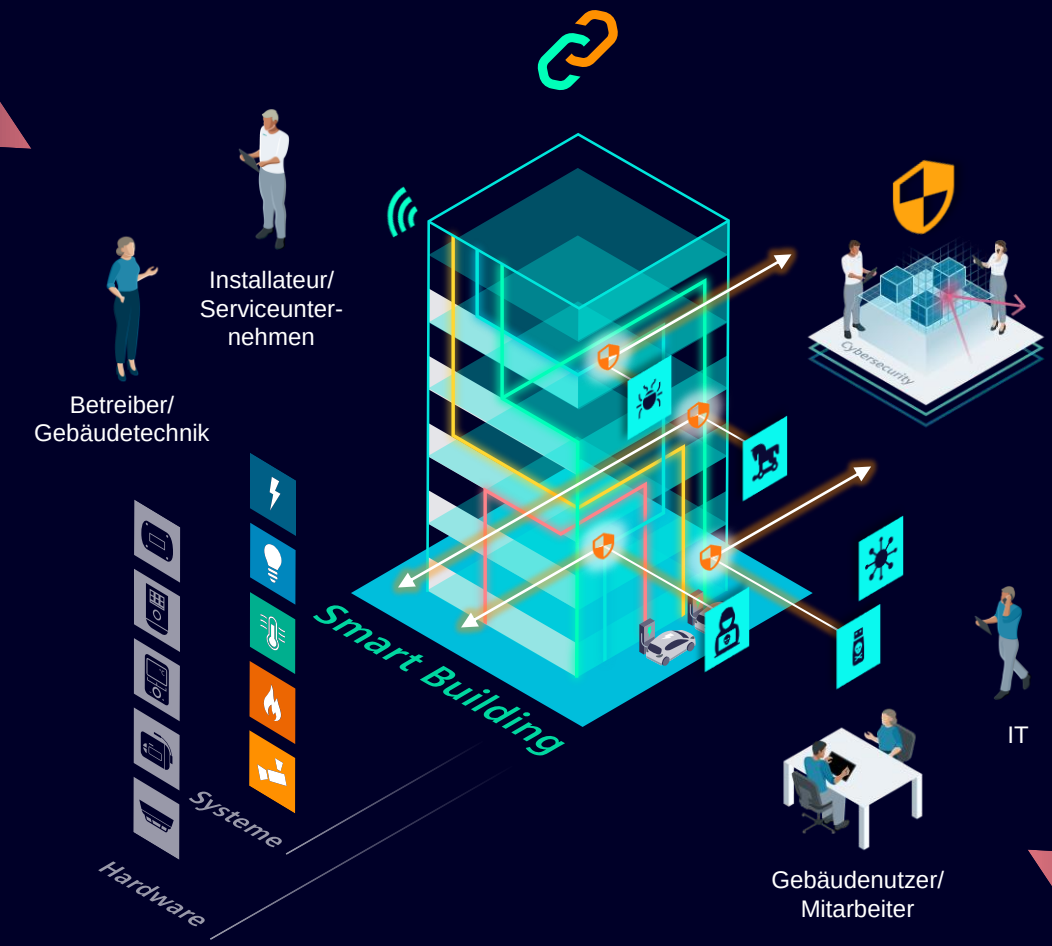
SIEMENS

Heute ist alles **vernetzt ...**



SIEMENS

… und **gefährdet**



SIEMENS

Cyberattacken
Die Bedrohung ist real und nimmt zu

In den letzten 5 Jahren ...

2019

LockerGoga / Über 40 Mio. Verlust

Norsk Hydro, Aluminiumproduzent und Stromversorger in Norwegen, von neuer Ransomware-Variante betroffen

2021

Neue, sich verändernde Bedrohungen

- Palfinger AG
- Salzburg Milch

- EKANS – OT/ICS-fähige Ransomware

- Colonial Pipeline
- Steelcase
- Honda usw.

2022

Österreich

- Stephansdom (Glocken)
- IMA Schelling Group
- Land Kärnten
- Universität Salzburg
- Med. Uni Innsbruck
- Wohnungsgenossenschaft 'Wien-Süd'
- Eglo Leuchten GmbH
- BRP-Rotax GmbH & Co KG
- Therme Bad Waltersdorf
- jö Bonus Club
- Österreichisches Verkehrsbüro

SIEMENS

Cyberattacken
Die Bedrohung ist real und nimmt zu

World‘s largest „economies“ *		
1.	USA	21,44 Bio US$
2.	China	14,14 Bio US$
3.	Cybercrime	8,0 Bio US$
4.	Japan	5,15 Bio US$
5.	Deutschland	4,0 Bio US$
6.	Indien	3,5 Bio US$
7.	Vereinigtes Königreich (UK)	2,83 Bio US$
8.	Frankreich	2,71 Bio US$
9.	Italien	1,99 Bio US$
10.	Brasilien	1,85 Bio US$

Quelle: IMF-International Monetary Fund und WEF-World Economic Forum, 2023
*) Billion = 1.000 Mrd.

SIEMENS

IT- und OT rücken zusammen

ZWEI SYSTEME | ZWEI ANFORDERUNGEN

Betriebstechnologie (OT) steuert Geräte

Informationstechnologie (IT) steuert Daten

Betriebstechnologie / **Operational Technology (OT)**

Überwachung und Steuerung von
- physischen Prozessen,
- Geräten und
- Infrastrukturen

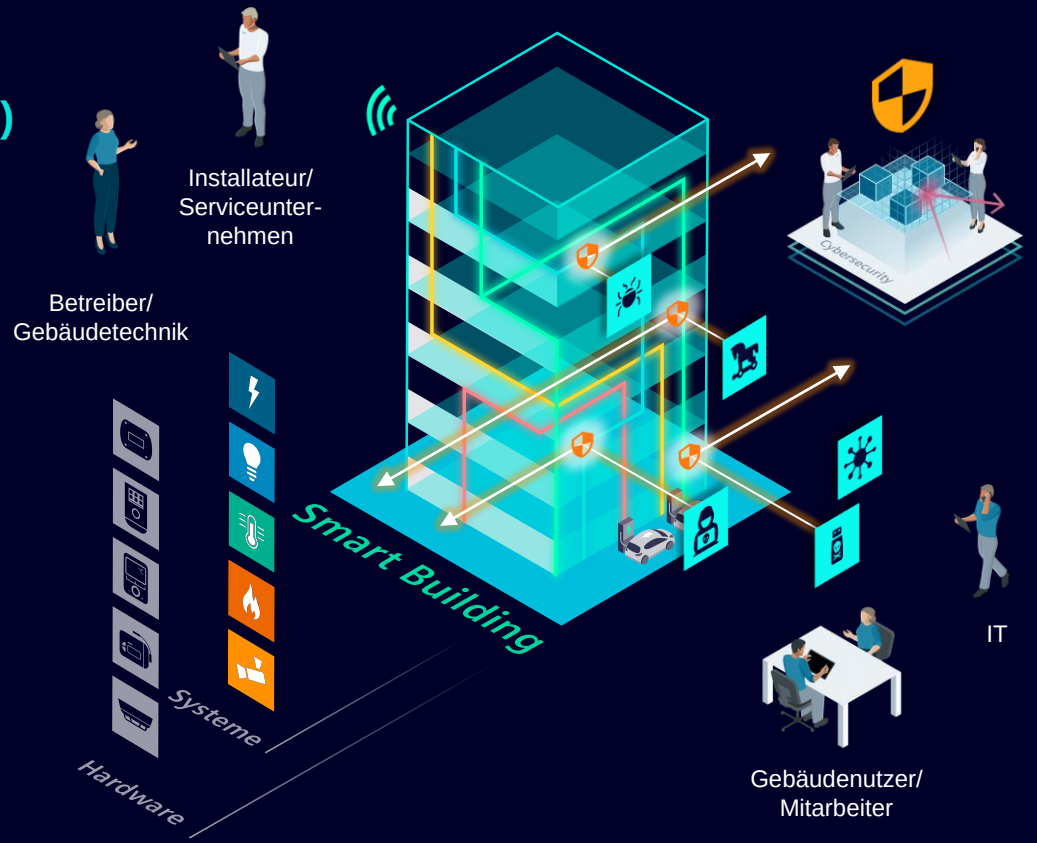
Beispiele:
- Gebäudeautomation,
- Energie- Management,
- Produktionsteuerung oder
- physische Sicherheitssysteme

SCHUTZZIELE

1. Verfügbarkeit (Availability)

2. Integrität (Integrity)

3. Vertraulichkeit (Confidentiality)



Informationstechnologie / **Information Technology (IT)**

umfasst alle Systeme zur Verarbeitung, Nutzung, Speicherung und zum Austausch von Informationen.

Beispiele:

Internet/E-Mail, Büro-Anwendungen, Auftrags-, Buchhaltungs-, Personal- und Dokumentenverwaltungs-Systeme

SCHUTZZIELE

1. Vertraulichkeit (Confidentiality)

2. Integrität (Integrity)

3. Verfügbarkeit (Availability)

SIEMENS

Die Herausforderungen sind in beiden „Welten“ ähnlich, aber die Realität sieht in der IT- und der Gebäudesicherheit ganz anders aus

OT-Domänen-Know-how ist entscheidend, um Abhängigkeiten zu verstehen und effektive Maßnahmen umzusetzen.

IT Security		OT Gebäude Security
Vertraulichkeit		**Verfügbarkeit und Safety**
3-5 Jahre	**Asset/Produkt lifecycle**	**Bis zu 40 Jahre**
Forced migration (z.B. PCs, Smartphones)	**Software lifecycle**	**Einsatz solange Ersatzteile verfügbar**
Hoch (> 10 “agents” auf office PCs)	**Möglichkeiten für Security SW**	**Gering** (alte Systeme ohne freie Ressourcen)
Niedrig (hauptsächlich Windows 10/11)	**Heterogenität**	**Hoch** (von Windows XP bis zu 11)
Standards basiert (agents & forced patching)	**Hauptschutzkonzept**	**Fall und Risiko basiert**

Frei verwendbar | © Siemens 2024

Überblick Maßnahmen – EU Richtlinie über die Resilienz kritischer Einrichtungen (CER)

a) **Vorsorge:** Präventionsmaßnahmen gegen Vorfälle, Disaster und Klimawandel;

b) **Physische Sicherheit:** Absicherung der ihrer Liegenschaften und Kritischen Infrastruktur mit physischen Schutzmaßnahmen, Perimeter Überwachung, Detektion, Zutrittskontrolle

c) **Krisen:** Reaktion auf Sicherheitsvorfälle, Abwehr und Begrenzung de Folgen solcher Vorfälle, Umsetzung von Risiko- und Krisenmanagementverfahren und -protokollen und vorgegebener Abläufe im Alarmfall;

d) **Wiederherstellung:** Business Continuity Management (BCM) und Maßnahmen zur Wiederherstellung nach Vorfällen — inkl. alternative Lieferketten;

e) **Personal:** Sicherheitsmanagement hinsichtlich der Mitarbeiter zu gewährleisten, durch Maßnahmen wie:
- Festlegung von Kategorien von Personal, das kritische Funktionen wahrnimmt,
- Festlegung von Zugangsrechten zu Räumlichkeiten, kritischen Infrastrukturen und zu sensiblen Informationen
- Einführung von Verfahren für Zuverlässigkeitsüberprüfungen im Einklang mit Artikel 14 (Zuverlässigkeitsüberprüfung)
- Benennung von Kategorien von Personal, die solche Zuverlässigkeitsüberprüfungen durchlaufen müssen, und der
- Festlegung angemessener Schulungsanforderungen und Qualifikationen.

f) **Awareness:** das Personal für die genannten Maßnahmen schulen und mit Informationsmaterial und Übungen sensibilisieren.

Nur ein umfassender Sicherheitsansatz auf Basis des Defense-in-Depth-Konzepts kann effektiven Schutz bieten

Mehrschichtiges Cyber Sicherheitskonzept

Sicherheits-risiken zwingen zum Handeln

Gebäudesicherheit
- Physischer Zugangsschutz
- Sicherheitsrichtlinien
- Sicherheitsüberwachung

Netzwerksicherheit
- Netzwerksegmentierung
- DMZ
- Firewalls
- VPN
- Verschüsselung
- ……..

Systemintegrität
- Systemhärtung
- Updates
- Patch-Management
- Authentifizierung und Zugriffsschutz

Produkt und Software Security
- *Security by Design*
- *Security by Default*

SIEMENS

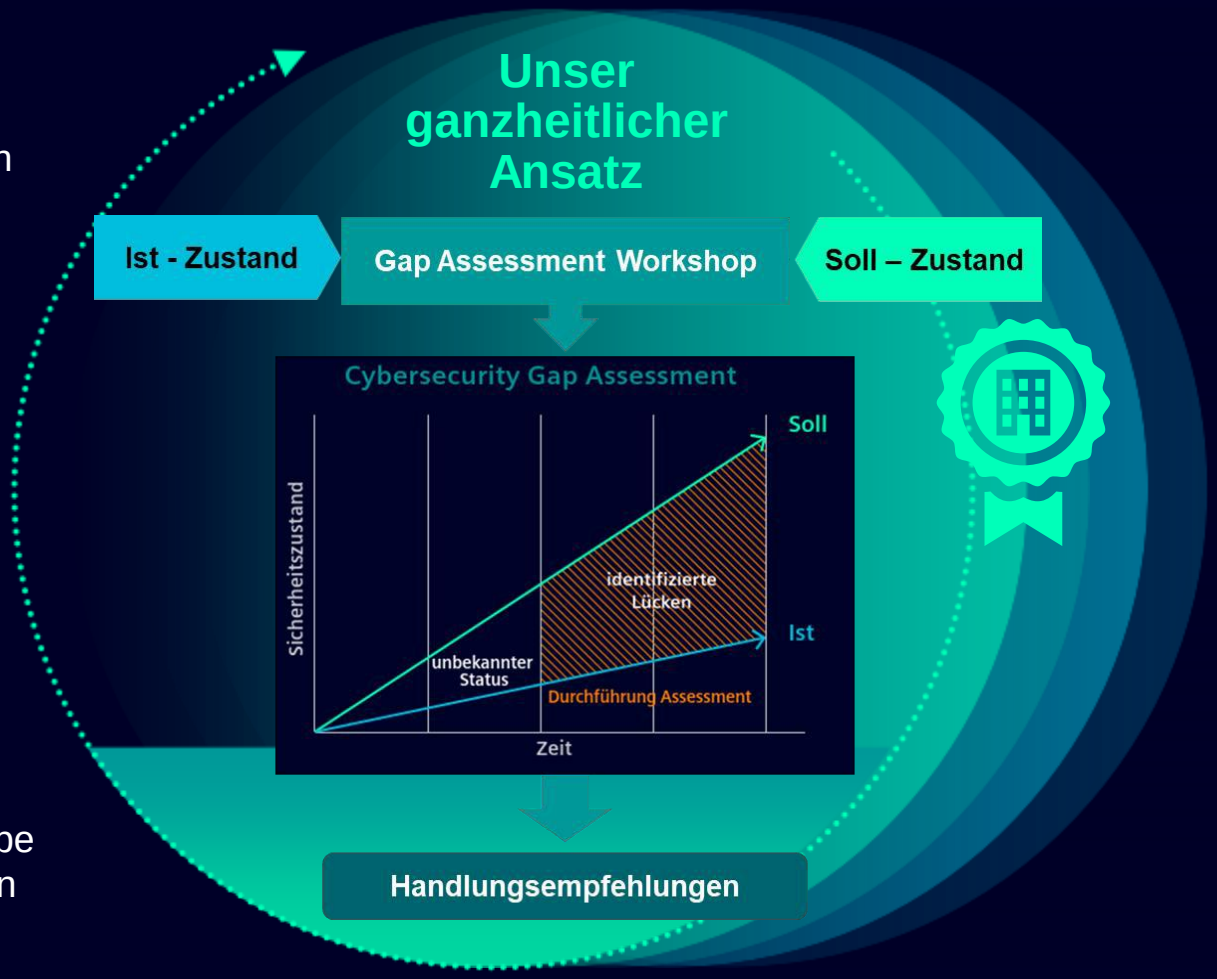
Smart Buildings ganzheitlich denken.
Unsere Lösungen für Ihre Herausforderungen: **Cyber Security GAP Assessment**

Ihre Anforderungen

- Schutzziel: Vermeidung von Störungen
- Transparenz über Cybersecurity-Lücken in der Gebäudetechnik

Ihre Herausforderungen

- Mangelnde Transparenz über Cybersecurity Maßnahmen in der Gebäudetechnik
- Steigende Anzahl von Cybersecurity Vorfällen erfordert die Steigerung der Cyber-Resilienz in der Gebäudetechnik
- Gebäudetechnik ist bisher nicht im Scope der IT-/ Cyber-Security-Verantwortlichen



Ihre Vorteile

Ganzheitliche Beurteilung des Cybersicherheitsstatus der Gebäudetechnik
Bereiche:
- Organisation
- Prozesse
- Technik

Transparenz für Entscheider und Management über vorhandene Lücken gegenüber dem IT-Sicherheitsstandard ISO 27001 bzw. der ISO/IEC 62443

Praxisorientierte Handlungsempfehlungen zur raschen Verringerung der kritischen Cyberrisiken

SIEMENS

Building Automation Protokoll

Was ist BACnet….

- Standardisiertes Kommunikationsprotokolls für Überwachung, Regelung und Energiemanagement von Gebäuden
- Offener Kommunikations-protokoll-Standard in der Gebäudeautomation
- Alle namhaften Gebäudeautomation-Lieferanten führen BACnet-Produkte
- Gestattet Einbindung in das Ethernet und Zugriff auf alle Anlagen des Betreibers
- Start der Entwicklung 1987, Standard seit 1995

BACnet bis jetzt…

1 Sehr stark verbreitet

- Verwendung in ~70% aller kommerziellen Gebäudemanagement -systemen

2 Keine Verschlüsselung

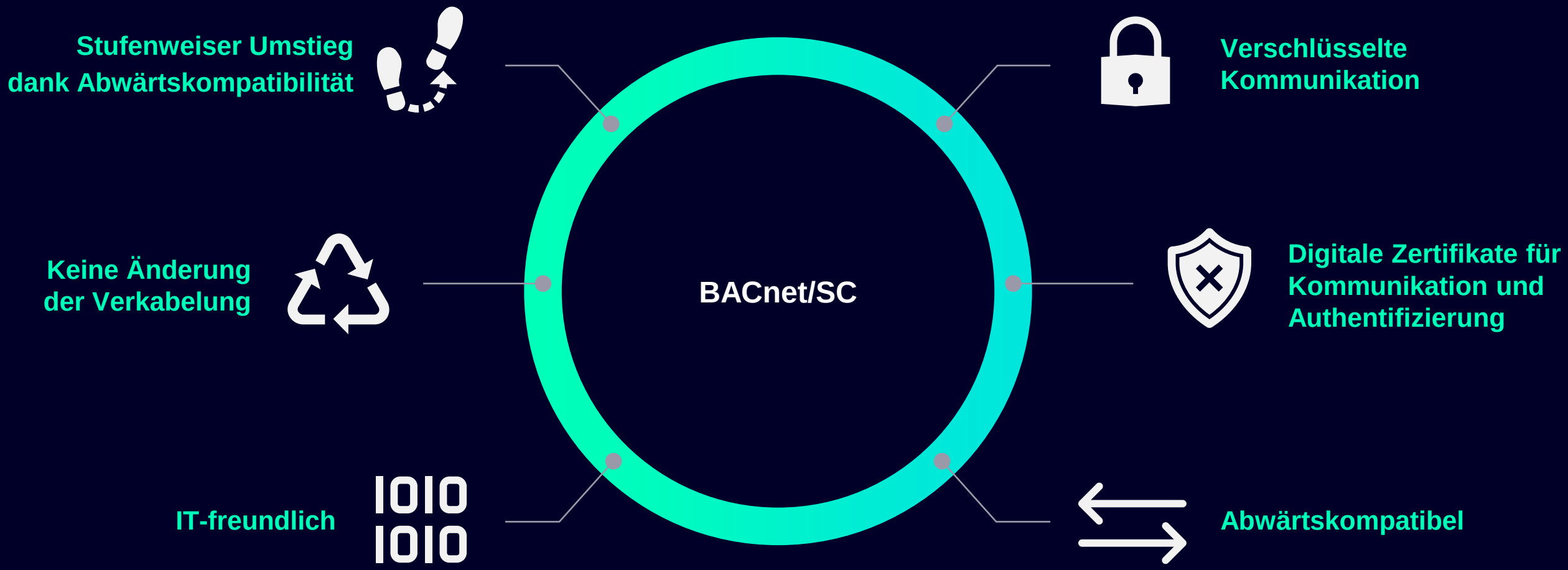
- Kommunikation in Klartext

3 Keine Authentifizierung

- Nicht fälschungssichere Kommunikation

SIEMENS

Vorteile von BACnet Secure Connect



SIEMENS

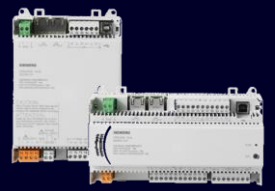
BACnet SC Portfolio

Desigo CC

Die Managementplattform zur Vernetzung aller Disziplinen im Gebäude

Desigo PXC-Controller

Frei programmierbare Controller für HLK-Anlagen und Integrationsfunktionen



Desigo DXR-Controller

Frei programmierbare Raum-Controller

Brandschutzklappen-steuerung

Frei programmierbares Brandschutzklappensystem mit Abschaltmatrix

SIEMENS

Kontakt

Herausgeber: Siemens AG Österreich

Ing. Martin Krammer
Business Development Manager – Cyber Security
Smart Infrastructure
Siemensstraße 90
1210 Wien
Österreich

Telefon +43 664 80117 213 75

E-Mail martin.krammer@siemens.com

SIEMENS