NIS 2 APPROACH WITH CYBER SECURITY IN BUILDING AUTOMATION AND PHYSICAL SECURITY

Ing. Manuel Burger, MSc

Sales leader Europe Enterprise Business

w/o Germany

THE FUTURE IS WHAT WE MAKE IT

Honeywell

CUSTOMER CYBERSECURITY CHALLENGES

Sources:
[1]IBM Security. 2022. Cost of a Data Breach Report 2022, p7.
[2]Secureworks. 2022. https://cybersecurityventures.com/boardroom-cybersecurity-report/, p10.
[3]https://www.cybintsolutions.com/cyber-security-facts-stats/ .

$4.35M Durchschnittliche Kosten eines Datenverstoßes im Jahr 2022[1]

$9.44M Durchschnittliche Kosten eines Datenverstoßes in USA im Jahr 2022[1]

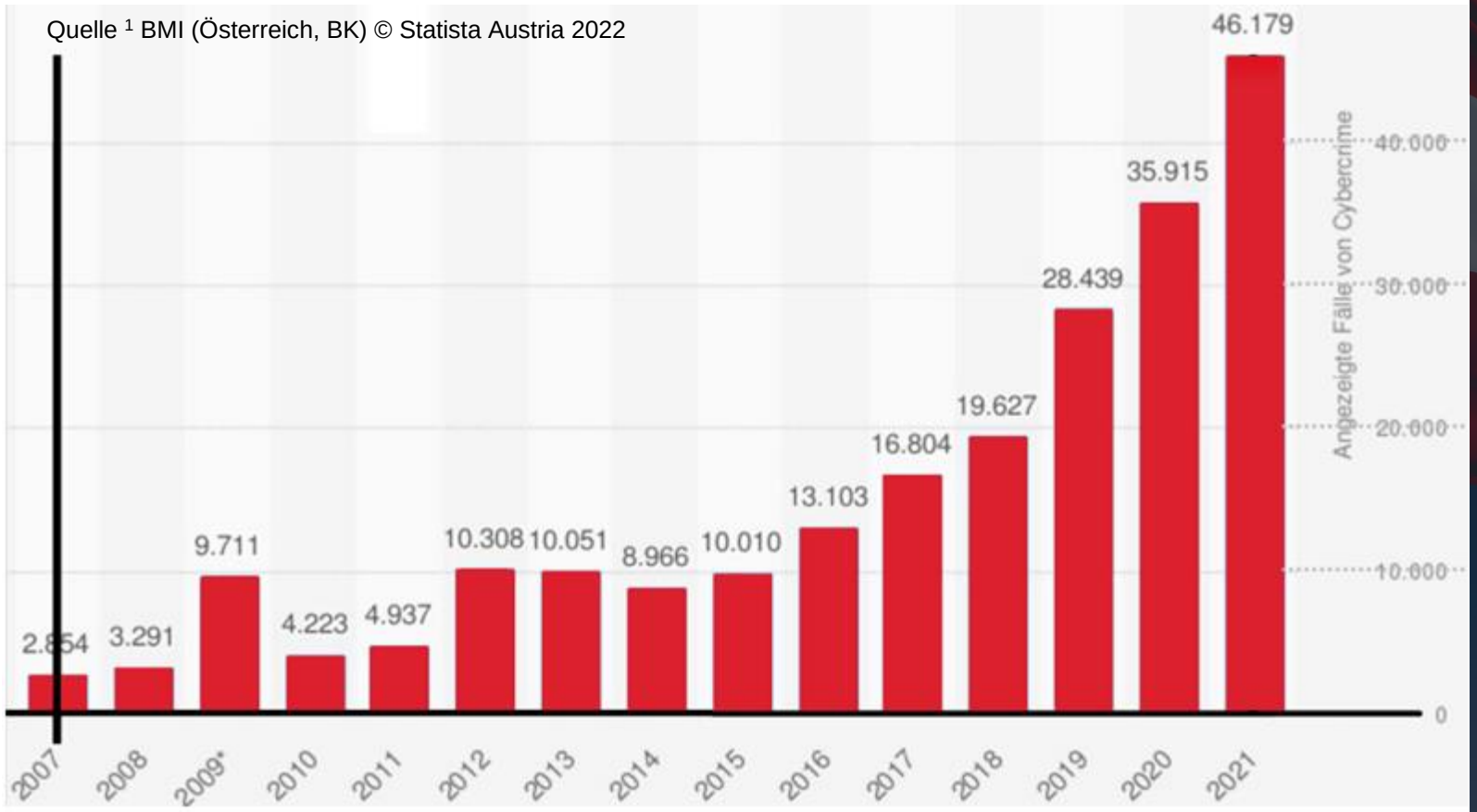
$7T Gesamtkosten von Cyber-Kriminalität weltweit bis 2022[2]

300% Anstieg der Cyberangriffe seit Covid-19[3]

10 Months Durchschnittliche Zeit bis zur Entdeckung eines Datenverstoßes[1]

1. **Minimierung von Betriebsstörungen**
   Sicherstellung, dass ein Plan für die Wiederherstellung nach einem Vorfall gegeben ist
2. **Sichern von geistigem Eigentum, Daten und personenbezogene Informationen**
3. **Vermeiden von Rufschädigung sowie Schaden der Marke.**
4. **Erfüllen von gesetzlichen Vorschriften**
   Einhaltung von behördlichen und branchenspezifischen Standards, um so etwaige Strafen zu reduzieren
5. **Minimierung potenzieller finanzieller Kosten**
   Vermeiden von möglichen Kosten für Wiederherstellung nach einem Desaster, Ransomware, Kosten aufgrund von Datenverlust, rechtliche Schritte, ….
6. **Beheben von Fachkräftemangel im Bereich Cybersicherheit**
7. **Aufechterhaltung von hoher Zuverlässigkeit, Sichtbarkeit und Sicherheit**
8. **Verbessern Sie die Cyberrisiko-Positionierung**
   Proaktivität und Vorbereitung vermitteln Vertrauen darüber, wie man einen Cyberangriff handhabt, wenn er auftritt

CYBER CRIME OFFENSES
REPORTED INCIDENCES | AUSTRIA 2007-2021



+28,6%

Anstieg angezeigter Cybercrime- Delikte in 2021[2]

+19,9%

Anstieg angezeigter Fälle von Datenbeschädigung, Hacking oder DDoS-Attacken in 2021[2]

+52,5%

Anstieg von Datenverarbeitungsmissbrauch in 2021[3]

Sources:
[1] BMI (Österreich, BK) © Statista Austria 2022
[2] ttps://bmi.gv.at/magazin/2022_07_08/06_Cybercrime_Report.aspx
[3] https://www.bundeskriminalamt.at/306/files/Cybecrime_2022_V20230517_webBF.pdf

ARE YOU PUTTING YOUR SITE'S SECURITY AND SAFETY AT RISK?

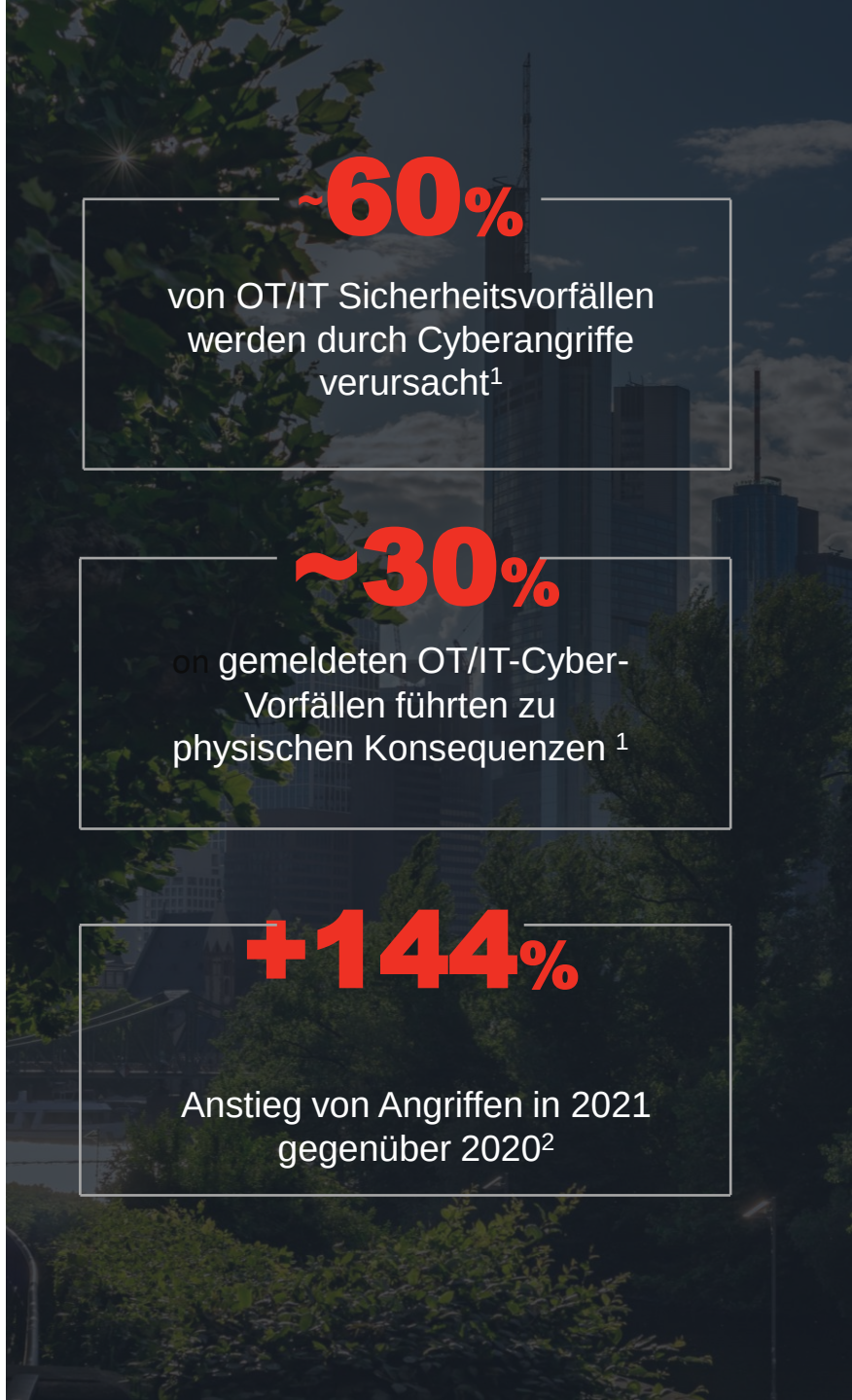
Sind **Betriebssystem-** und **Applikationssoftware** auf dem aktuellen Letztstand

Entspricht die **Hardware** den Cyber-Security Standards, wenn sie mit Ihrem Netzwerk verbunden sind?

Was passiert, wenn Ihre kritischen Systeme nicht den Cybersicherheitsstandards entsprechen? **Compliance**

Wird genug gemacht?

- Cybersicherheitsmaßnahmen müssen entsprechend Ihrer Betriebsumgebung und Risikobereitschaft umgesetzt werden
- Cybersicherheitsposition (Bedrohungen und Schwachstellen) muss kontinuierlich auf Abweichungen und Hinweise auf Kompromittierungen überwacht werden.
- Betriebssystem Versionen, Applikationsversionen sowie ggf. Firmware müssen auf Stand sein



Sources:
[1] Honeywell GARD Threat Intelligence Team, 2024
[2] Waterfall 2024, OT Security Incidents In 2021, [Accessed Jan 29, 2024

WHAT IF YOUR CRITICAL SYSTEMS ARE NOT CYBERSECURITY COMPLIANT?

Regierungsvorschriften und Unternehmensrichtlinien erhöhen die künftigen Erwartungen hinsichtlich besserer Transparenz bei Vorfällen sowie Einhaltung der Vorgaben!

Mögliche Ursachen der Probleme:

- Betriebssyteme nicht auf Letztstand bzw. fehlende kritische Updates
- Applikationssversionen sind nicht auf Letztstand
- Keine oder bedingte Verschlüsselung (inklusiv, ganzheitlich)
  - Unsichere Konfiguration
  - Unsichere Kommunikation
- Veraltete Technologien (RFID)
- Veraltete Schnittstellen
- Fehlen von ganzheitlichem Cyber-Security Ansatz (CRA?)

€5,5 Billionen

Geschätzte jährliche Gesamtkosten global der Cyber-Kriminalität in 2021[1]

Sources:
[1] Gesetz über Cyberresilienz | Gestaltung der digitalen Zukunft Europas

HONEYWELL APPROACH
SIA 62443 COMPLIANCE

Sources:
[1]https://www.securityinformed.com/news/honeywell-building-technologies-isa-iec-62443-4-1-process-certification-software-development-lifecycle-co-10449-ga-co-2173-ga.1681383591.html

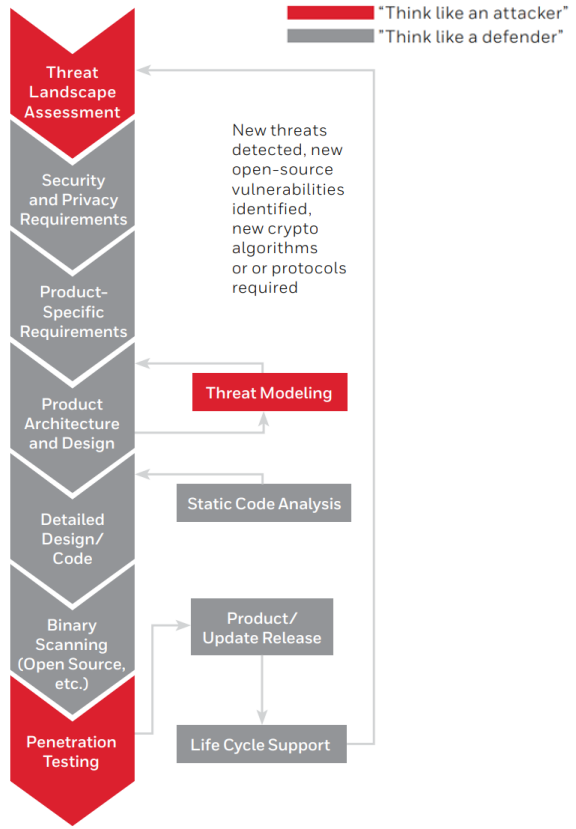
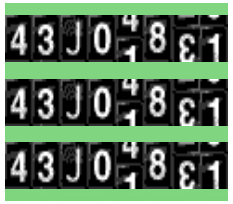


Figure: Example of a Secure Development Lifecycle based on international standards such as ISA/IEC 62443

Die ISA/IEC 62443-Standards definieren Anforderungen und Prozesse für die Implementierung und Aufrechterhaltung von sicheren, industriellen Automatisierungs- und Steuersystemen. Die **Zertifizierungsstandards** legen **bewährte Verfahren** für **Sicherheit** fest und bieten Möglichkeit, das **Sicherheitsniveau** zu **bewerten**.

HONEYWELL TOP PRIORITY
CYBER SECURITY COMPLIANCE



ISA/IEC 62443-4-1

Development

- Life cycle of secure software development
- Standard security requirements
- Threat modeling
- Review of secure code
- Penetration testing
- Advanced independent security testing

Design

- Security implementation guides
- Network planning
- Ports, services, protocols
- Password management
- System monitoring
- Disaster recovery plan

Implementation

- Defense in depth
- Network separation
- Hardening the hardware
- Hardening of the operating system
- Virus protection
- Host intrusion prevention
- Firewall

Incident Response

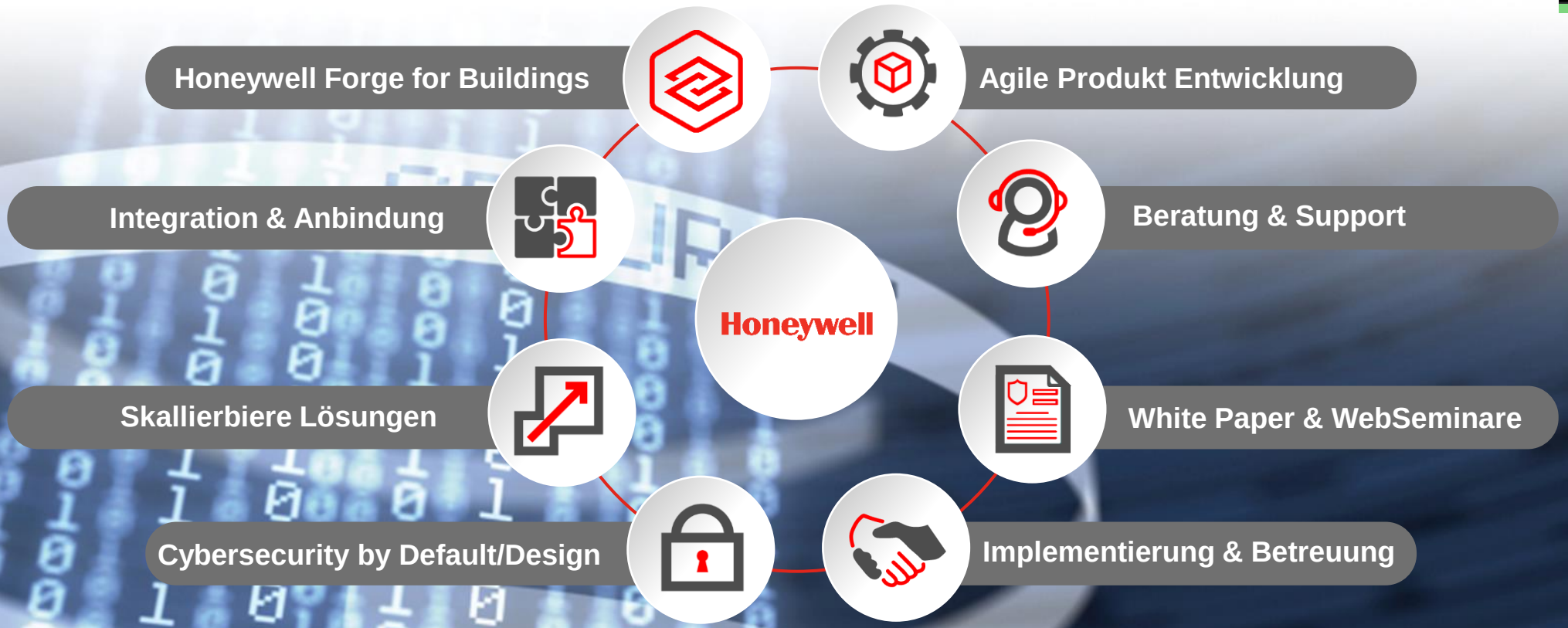
- Formal process
- Covers all Honeywell products and services
- Timely response and resolution
- Security notifications

Standards & Frameworks

- ITIL
- CPNI/SANS Top 20 Cyber Security Controls
- NIST Guidelines
- IEC/ISA 62443
- RMADS
- GPG13

+150 Mitarbeiter dezitiert CC | ~2.000 Mitarbeiter Teilzeit/Projekt bezogen

HONEYWELL CYBER SECURITY
VALUE PREPOSITION



Kundennutzen & Mehwerte | Generell CS als auch NIS2

BUILDING AUTOMATION
CYBER SECURE FOR US & CUSTOMER

NASDAQ: **HON** ~**750** sites | ~**99,000** employees | **Charlotte, NC** headquarters | **Fortune 500**

Aerospace

Unsere Produkte werden in praktisch allen kommerziellen und militärischen Flugzeugplattformen weltweit eingesetzt und umfassen Flugzeugantriebe, Cockpitsysteme, Satellitenkommunikation und Notstromsysteme.

Building Automation

Unsere Produkte, Software und Technologien sind in mehr als 10 Millionen Gebäuden weltweit im Einsatz und helfen unseren Kunden, ihre Einrichtungen sicher, energieeffizient, nachhaltig und produktiv zu gestalten.

Performance Materials and Technologies

Wir entwickeln fortschrittliche Werkstoffe, Prozesstechnologien, Automatisierungslösungen und industrielle Software, die Industrien auf der ganzen Welt revolutionieren.

Safety and Productivity Solutions

Wir verbessern die Leistung von Unternehmen sowie die Sicherheit und Produktivität von Arbeitnehmern durch automatisierte Materialhandhabung, Sprachscanning und mobile Computertechnologie, Softwarelösungen sowie persönliche Schutzausrüstung und Sensortechnologie.

Honeywell Connected Enterprise

Wir beschleunigen die digitale Transformation unserer Kunden mit Software und Lösungen für das industrielle Internet der Dinge (IIoT) über das Enterprise Performance Management-Angebot Honeywell Forge. Der Schwerpunkt von HCE liegt auf der Softwareentwicklung, vom Gateway bis zu den Endbenutzeranwendungen, und bringt Skalierbarkeit und Kompetenz in das gesamte Unternehmen Honeywell.

#futureshaper | Shaping the future across industries

BUILDING AUTOMATION
SCOPE AND OBLIGATION

Vor über 100 Jahren haben wir das Konzept der Energieeffizienz durch die Optimierung des Wohnkomforts durch Automatisierung eingeführt. Heute wird dieses Konzept in 10 Millionen Gebäuden, in denen unsere Technologie verwendet wird, neu definiert.

Bestehende Installationsbasis | Neue Technologien & Regulatorien

BUILDING AUTOMATION
NIS2 CHECK PHYSICAL SECURITY

Die grundlegende Zielsetzung der NIS-2-Richtlinie bleibt im Vergleich zur NIS-Richtlinie sinngemäß bestehen, nämlich in der Schaffung eines hohen gemeinsamen Niveaus der Cybersicherheit in der EU, dies aber in einem modernisierten Rechtsrahmen[1]

Maßnahme	Erläuterung
Policies	Richtlinien für Risiken und Informationssicherheit
Incident Management	Prävention, Detektion und Bewältigung von Cyberincidents
Business Continuity	BCM mit Backup Management, Disaster Recovery, Krisenmanagement
Supply Chain	Sicherheit in der Lieferkette
Einkauf	Beschaffung von IT- und Netzwerksystemen
Effektivität	Vorgaben zur Messung von Cyber- und Risikomaßnahmen
Training	Cybersecurity-Hygiene
Kryptographie	Vorgaben für Kryptographie und wo möglich Verschlüsselung
Personal	HR-Security
Zugangskontrolle	Zugriffskontrolle
Asset Management	Information Security Management System (ISMS)
Authentifizierung	Einsatz von Multi-Faktor und SSO
Kommunikation	Sichere Kommunikationstools
Notfallkommunikation	Einsatz gesicherter Systeme (Sprach, Video und Text)

[2]

Source:
[1] Die neue NIS-2-Richtlinie , https://www.nis.gv.at/nis-2-richtlinie.html
[2] Plusserver, https://www.plusserver.com/blog/nis2-leitfaden-zur-umsetzung-der-security-richtlinie/

ALL CONNECTED SYSTEMS CAN FACE CYBER THREATS

IEC 62443-4-1 Internationale Norm

Zertifizierung nach ISO 27001

NIS-2 compliant IT-Systemen,
NAC, TLS1.2, IEEE 802.1X, IEC 62443-4-1

Einbruchmeldetechnik, Zutrittskontrolle, Videoüberwachung.Kommunikation, Crypto-Chip, Verschlüsselung, proprietäre BUS EMA/ZK

Komplettlösungen, SW/HW/3rdP, EN 60839 G4

PSIM, Incident Management, Compliance, WFs

MFA, SSO, Biomtrie, …

AES, TLS, Propritärer Bus

Technisch VdS Protokolle SecurIP, SIA-DC09

Thank you for your attention

Ing. Manuel Burger, MSc
Sales Specialist Security Products

Sales leader Europe Enterprise Business
w/o Germany

manuel.burger@honeywell.com
+43 664 810 55 71

vCard

THE FUTURE IS WHAT WE MAKE IT

Honeywell