Bernd Koberwein
Head of Security Services
BearingPoint AT
+43 664 81 61 874
bernd.koberwein@bearingpoint.com

OT Security
Sicherer Fernzugriff

22.02.2023

Deutsche Messe
Technology Academy

BearingPoint®

Industrieumgebungen im Fadenkreuz von Cyberkriminellen

- Cyberangriffe auf Industrieumgebungen haben über die letzten Jahre deutlich zugenommen
- OT hat grundlegend andere Zielsetzung und Prioritäten als IT Umgebungen (Safety, Availability, Integrity)
- Weniger Dynamik in OT-Umgebungen, aber deutlich mehr Einschränkungen hinsichtlich Changes
- Hohe Dynamik in der Bedrohungslandschaft erfordert schnelle Reaktion auf neue Schwachstellen (20k neue Vulnerabilities pro Jahr)
- Sehr lange geplante Lebensdauer von Anlagen im Gegensatz zur IT
- Oftmals eingeschränkte Kontrolle über installierte Komponenten und starke Abhängigkeit von Lieferanten
- Automatisierungskomponenten können oft nicht gepatched werden und Upgrades sind aufwändig und teuer
- In der Regel kein Security Monitoring und keine Security Kontrolle

Am häufigsten angegriffene Industrien in Europa

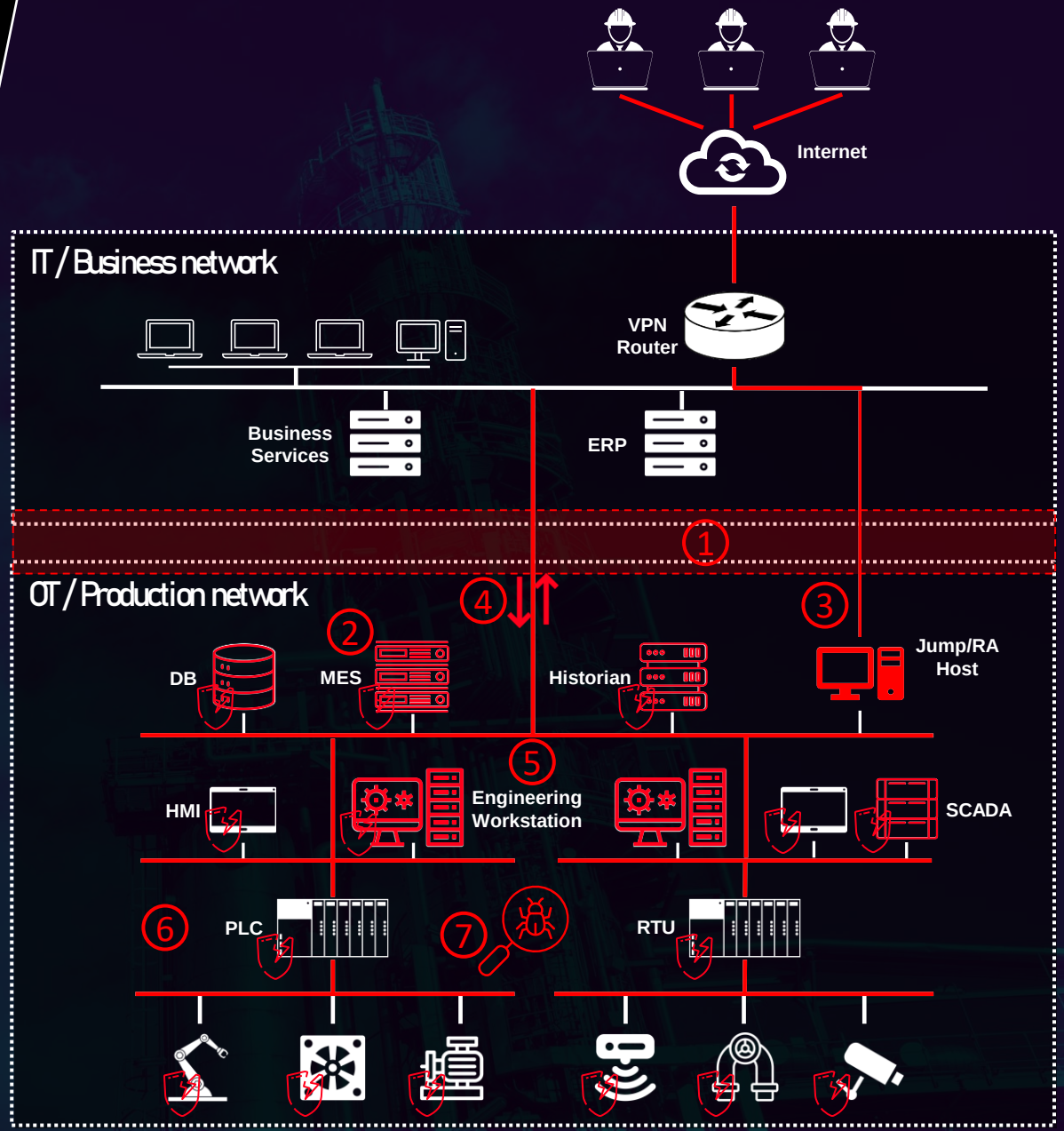
Sector	2019	2020	2021	2022
Manufacturing	8	2	**1**	**1**
Finance and Insurance	1	1	2	2
Professional and business services	5	5	3	3

Source: IBM Security X-Force Threat Intelligence

BearingPoint®

Technische Herausforderungen in OT Umgebungen

1. Fehlende/schwache Trennung IT/OT
2. Veraltete Systeme / Software (end of life), kein Patching möglich oder verfügbar
3. **Unsichere Fernzugriffe**
4. Unreglementierter Datenverkehr
5. Keine/unzureichende Segmentierung
6. Kein Asset/Vulnerability Management
7. Kein Monitoring und Anomalieerkennung



BearingPoint®

Anlagen-/Maschinenbauer vs. Anlagenbetreiber

Trotz unterschiedlicher Zugänge zum Thema benötigen beide Seiten eine Technologie, die Sicherheit und Effizienz ermöglicht

Aus Sicht der Anlagen- und Maschinenbauer

- Benötigen einheitliche Zugriffsart für eigene Techniker (nicht 20 verschiedene Clients für unterschiedliche Kunden)
- Anlagen sind untereinander nicht vernetzt, somit Vereinheitlichung oder zentrales Management schwierig
- Haben teilweise keine Compute-Infrastruktur vor Ort, auf der Lösungen gehostet werden können (oder müssen dafür bezahlen)
- Haben oft Anlagen auf der ganzen Welt und benötigen niedrige Latenzen um effizient arbeiten zu können
- Verbinden sich oft auch auf die Steuerungsebene / L1 mit proprietärer Software

Aus Sicht der Anlagenbetreiber

- Haben eine oder mehrere Anlagen die über eine einheitliche Fernzugriffslösung verwaltet werden soll
- Haben eigene Techniker, die sowohl von intern, als auch von extern Wartungstätigkeiten durchführen sollen
- Benötigen granulare Kontrolle über Zugriffe und Aktivitäten
- Haben oft mehrere Lieferanten die mit eigenen Lösungen arbeiten wollen
- Haben keine oder wenig Kontrolle über die Software mit der die Anlagen- und Maschinenbauer zugreifen
- Verbinden sich hauptsächlich auf Komponenten in Prozess- oder Betriebsleitebene (Windows/Linux)

Fernzugriffstechnologien im OT Umfeld

- VPN (Virtual Private Network)
  - Entweder Site2Site Tunnel oder Client
  - Verschlüsselte Verbindung, Protokollunabhängig, Unterstützt MFA
  - Erlaubt direkte Verbindung auf Endgeräte
- VNC (Virtual Network Computing)
  - Erstellt in den späten 90ern
  - Plattformunabhängige Fernsteuerungslösung
  - Server / Client Architektur, Kommerzielle Lösung unterstützt MFA (TOTP)
  - Over-the-should monitoring auf der Zielmaschine möglich
- RDP (Remote Desktop Protocol)
  - Fernsteuerungslösung primär für Windows
  - Server / Client Architektur, Unterstützt MFA (aber relativ aufwändig)
  - Kein Over-the-shoulder monitoring
- TeamViewer
  - Plattformunabhängige Fernsteuerungslösung für Desktops
  - Server / Client Architektur, Unterstützt MFA (TOTP)
  - Erlaubt Over-the-shoulder Monitoring

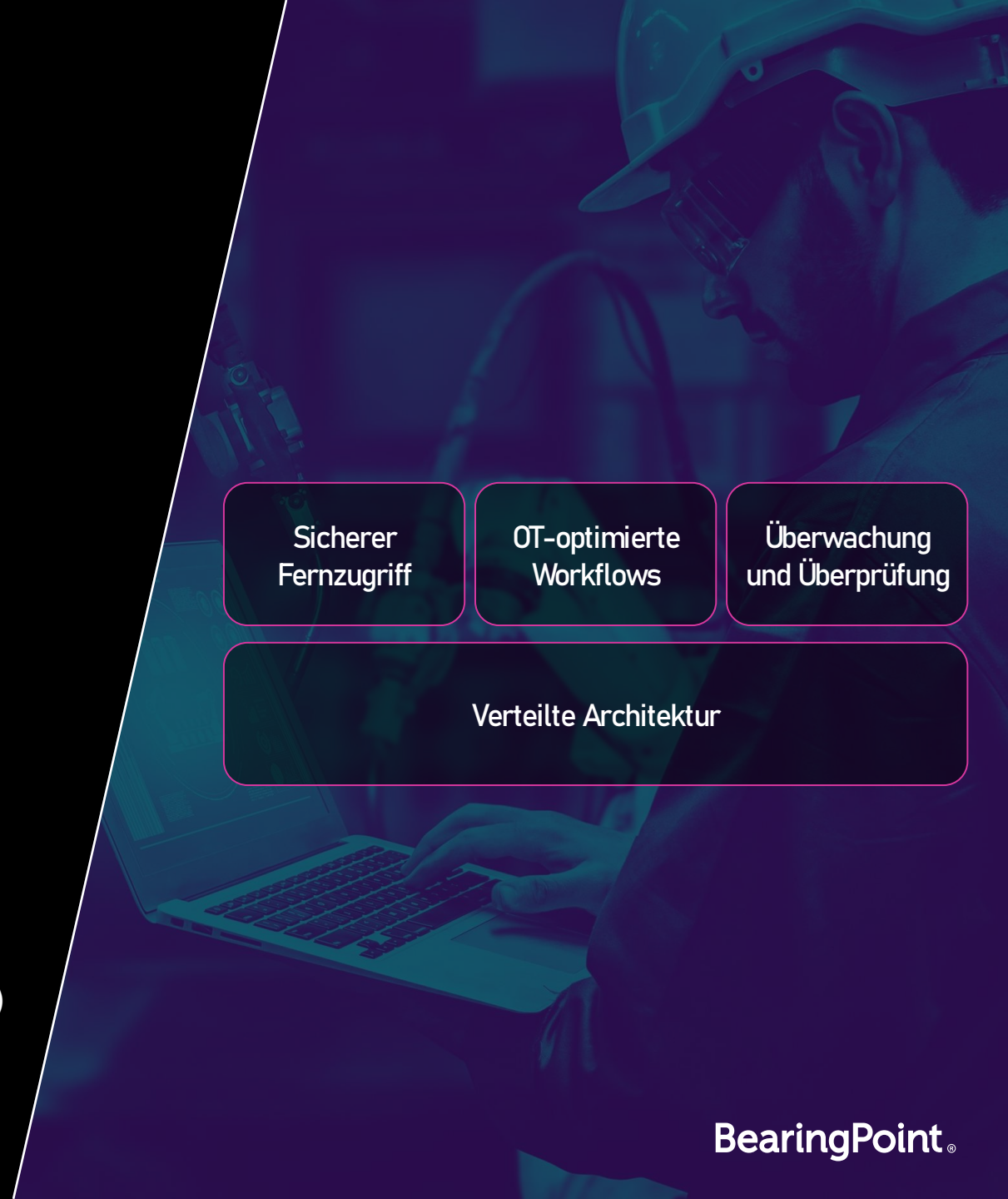
Risiken / Einschränkungen

- Erfordern offene Ports nach außen
- Erfordern Patching/Upgrades
- Konfigurationsfehler
- Multi-Faktor Authentifizierung
- Einschränkung der Zugriffe kompliziert
- Eingeschränkte Recording Möglichkeiten
- Kaum Audit Log Granularität
- Wenig Kontrolle über Zeit und Tätigkeit
- Anfälligkeit für Supply-Chain Attack
- Uneingeschränkter Dateitransfer

BearingPoint®

Technische Anforderungen an moderne OT-Fernzugriffslösungen

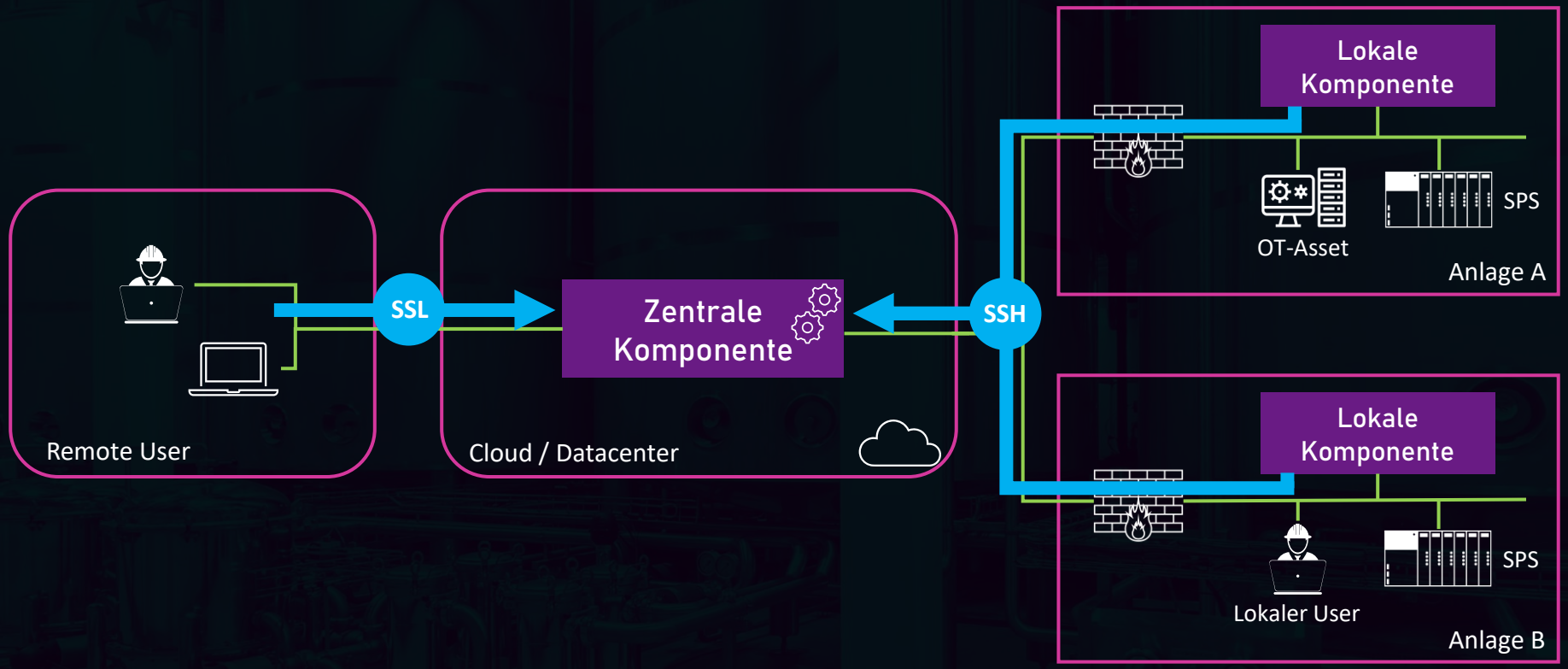
- Hohe Verfügbarkeit
- Keine Inbound Connections (offene Ports)
- Breite Unterstützung von Protokollen (z.B. SPS Direktverbindung)
- Multi-Faktor Authentifizierung
- Lückenloses Audit Log
- Freigabeprozess für Fernzugriffe
- Live Videomonitoring
- Videoaufzeichnung für Wartungsaktivitäten
- Granulare Zugriffssteuerung (User/Gruppen und Geräte)
- Sichere Dateiübertragung
- Integration mit zentralen Identify Providern (SAML, AD, …)
- Integration mit Drittthersteller-Securitylösungen (Antivirus, SIEM, …)
- Keine proprietären Clients notwendig (z.B. VPN Client)
- Verschiedene Deployment Modelle (virtualisiert, auf eigenständiger Hardware)



BearingPoint®

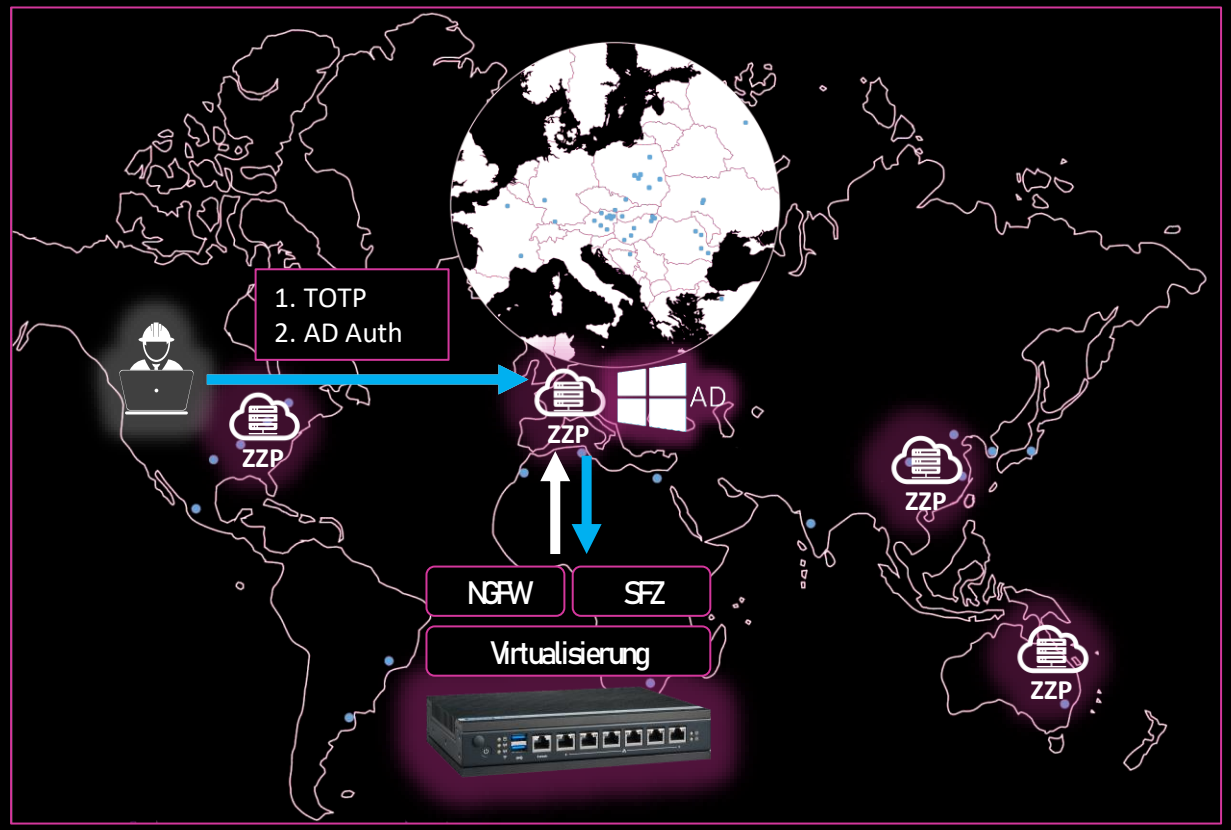
Architektur moderner Fernzugriffslösungen

Durch eine „two-tier architecture“, also eine mehrschichtige Architektur, wird die Exponierung nach außen vermieden und die Angriffsfläche reduziert



BearingPoint®

Use Case – Produzierendes Unternehmen mit globaler Präsenz



Fakten

- Ca. 60 Standorte global verteilt; teils sehr abgelegen
- Vielzahl an Lieferanten die Fernzugriff benötigen
- Support- und Technikerteams an mehreren Standorten
- Verschiedene Zugriffsmethoden im Einsatz

Herausforderungen

- Exponierte Ports für Fernzugriffe
- Kein MFA
- Kein Logging, Monitoring, Auditing
- Jump Hosts mit Vollzugriff auf Anlagennetz; keine Einschränkung
- Keine Ad-hoc Freigabe möglich; Tunnel bestehen dauerhaft
- Keine lokale Server-Infrastruktur an vielen Standorten

Lösung

- Vier **Zentrale Zugriffspunkte** gehosted in der Cloud; dadurch niedrige Latenzen zu Standorten
- Anbindung an **Active Directory** für zentrales Usermanagement
- **Unabhängige Hardwarelösung** (rugged) für schwierige Umgebungen
- **Virtualisierung** für zentrales Management, Monitoring, Upgrades…
- Next-Gen Firewall und **Sichere Fernzugriffskomponente**

BearingPoint®

Industrial Cyber Security Handbook

Free Download

industrialsecurity.at

BearingPoint

BearingPoint®

Think digital.
Act agile.
Manage innovation.

Together we are more than business

BearingPoint ist ein unabhängiges Management- und Technologieberatungsunternehmen mit europäischen Wurzeln und globaler Reichweite.

Wir unterhalten Niederlassungen an mehr als 40 Standorten und entwickeln mit 5.500 Mitarbeitern innovative Strategien für neue und bestehende Geschäftsmodelle und konzipieren und implementieren digitale Lösungen und Services für führende Unternehmen und öffentliche Institutionen.

Mit unseren Kompetenzen in den Bereichen Managementberatung, agile Transformation, technologiebasierte Business Services und smarte BearingPoint-Softwarelösungen setzen wir uns gemeinsam mit unseren Kunden und Partnern aktiv für messbaren und nachhaltigen Geschäftserfolg ein.

Zu den Kunden von BearingPoint gehören führende Unternehmen und Organisationen. Das globale BearingPoint-Netzwerk mit mehr als 10.000 Mitarbeitern betreut Kunden in über 75 Ländern.

Bernd Koberwein
Head of Security Services
BearingPoint AT
+43 664 81 61 874
bernd.koberwein@bearingpoint.com

BearingPoint®