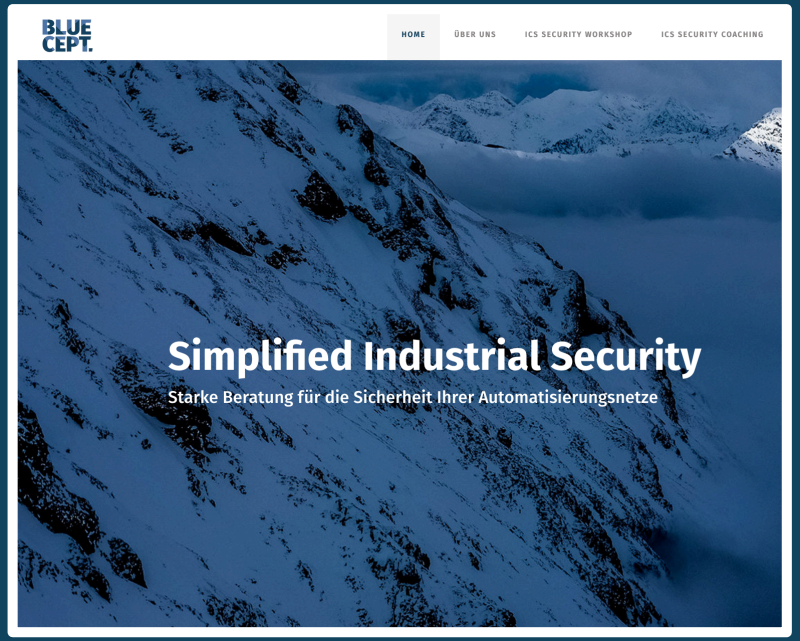
Spielzeugauto war gestern, schon mal nen Kran gesteuert?

sichere industrie

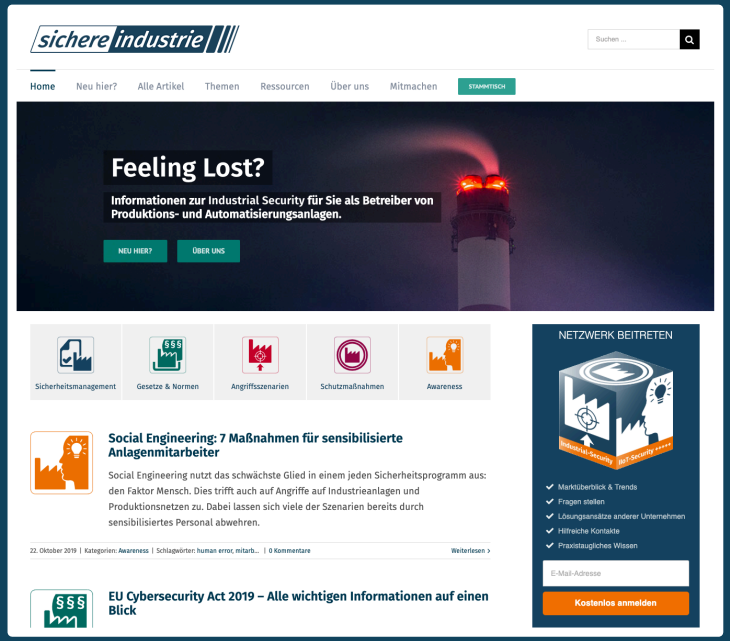
Fernwartung im Anlagennetz

Vorgehen und Best-Practises

01. Juli 2020 - Max Weidele

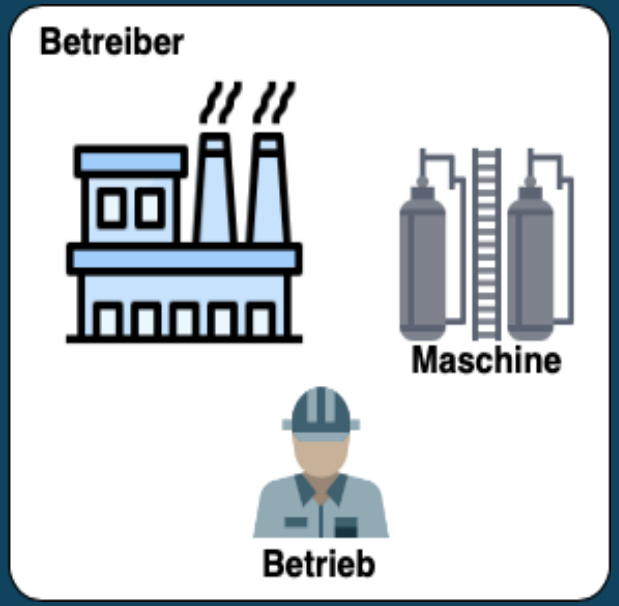


www.bluecept.com



www.sichere-industrie.de

Fernwartung und ihre Rollen



Fernwartung ?

Die Übersicht

- Brandmeldeanlagen
- Windkraftanlagen
- Baumaschinen (Bagger, Kräne, Radlader)
- Haushaltsgeräte (Kaffeemaschinen, Waschmaschinen, Trockner und Kühlschränke
- Wasser- und Atomkraftwerke
- Heizungen
- Klimaanlagen
- Videoleinwände, z.B. am Timesquare
- DSL-Router
- Elektronische Systeme in Gefängnissen
- Tansportschiffe und -flugezeuge
- Autonome Autos
- Überwachungskameras
- Industrie-Roboter, z.B. in der Automobil-Industrie
- Mars-Rover
- u.v.m.

Quelle: bluecept.com / sichere-industrie.de

Herausforderungen

- Vielzahl an Lösungen im Feld
- Sensibilität der Zielsysteme
- Diskussionen zwischen Betreiber/Lieferant

Phasen eines Fernwartungsprojekt

Anforderungen

Architektur

Organisation

Betrieb

Anforderungen

Preflight Check

Nr.	Fragestellung
1	Anzahl der Administratoren
2	Anzahl der Operatoren
3	Anzahl der Zielsysteme
4	Anzahl u. Name der Lieferanten
5	Anzahl interner Fernwarter
6	Anzahl interner Programmiergeräte

Quelle: bluecept.com / sichere-industrie.de

Lieferanten-Check

Nr.	Fragestellung
1	Art des Wartungsvertrags/-zugangs
2	Art der Zielsysteme
3	Zugriffsfrequenz des Lieferanten
4	Anzahl der Fernwarter
5	Ansprechpartner bei Lieferant
6	. . .

Quelle: bluecept.com / sichere-industrie.de

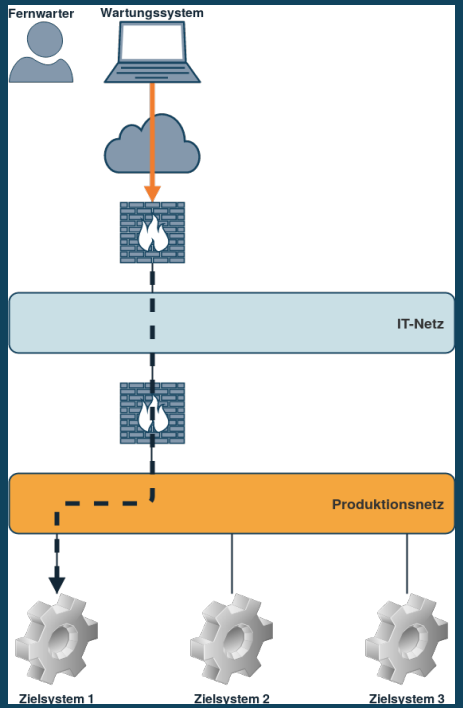
Anforderungskatalog an eine Lösung

Nr.	Kategorien
1	Anforderungen an den Hersteller
2	Performance & Skalierbarkeit
3	Wartbarkeit & Zukunftsicherheit
4	Benutzerfreundlichkeit
5	Installation & Inbetriebnahme
6	. . .

Quelle: bluecept.com / sichere-industrie.de

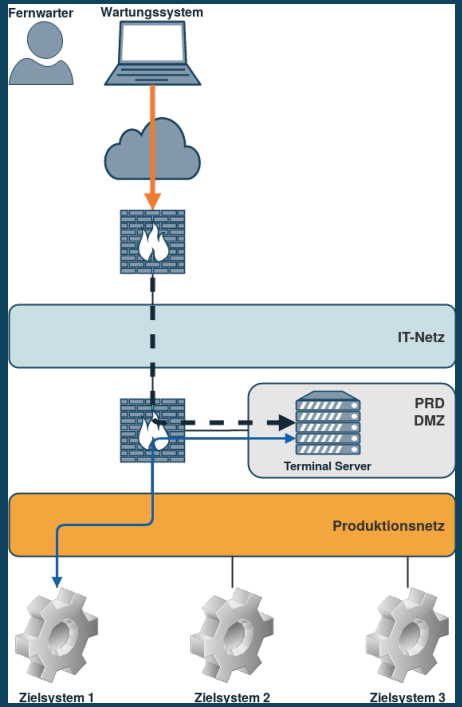
Architektur

Architekturmodelle:
VPN zu Firewall



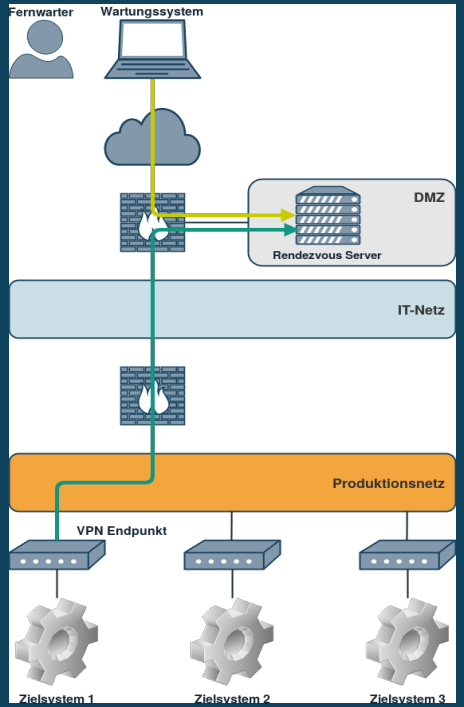
Quelle: bluecept.com / sichere-industrie.de

Architekturmodelle:
Jumphost-Ansatz



Quelle: bluecept.com / sichere-industrie.de

Architekturmodelle:
Rendezvous-Ansatz



Quelle: bluecept.com / sichere-industrie.de

Security berücksichtigen

Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IN DER PRODUKTION

Fernwartung im industriellen Umfeld

BSI-Veröffentlichungen zur Cyber-Sicherheit

Systeme zur Prozesssteuerung, Fertigung und Automatisierung – subsumiert unter dem Begriff Industrial Control Systems (ICS) – sind inzwischen ähnlichen Bedrohungen ausgesetzt wie konventionelle IT-Systeme. Aufgrund von betrieblichen oder wirtschaftlichen Gründen besteht häufig die Anforderung, eine Fernwartung der Systeme über öffentliche Netze vornehmen zu können. Derart angelegte Fernwartungszugänge führen dazu, dass industrielle Anlagen sehr viel stärker exponiert werden und somit zugleich einer gestiegenen Bedrohungslage ausgesetzt sind. Industrielle Fernwartungskomponenten müssen daher heute ein hinreichendes Sicherheitsniveau erfüllen.

Das Spektrum der am Markt verfügbaren Lösungen für Fernwartung im industriellen Umfeld ist sehr groß. Die Angebote reichen von VPN-Lösungen über Cloud-basierte Ansätze bis hin zu Provider-Lösungen im Bereich Machine-to-Machine (M2M). Die Produkteigenschaften einzelner Lösungen unterscheiden sich dabei teilweise signifikant. Die vorliegende Empfehlung gibt einen Überblick über die generischen Anforderungen für industrielle Fernwartung gemäß dem Stand der Technik. Es sei explizit darauf hingewiesen, dass Bestandslösungen auf Basis von analogen oder ISDN-Modems sowie die direkte Internetanbindung von Komponenten wie Speicher-programmierbaren Steuerungen (SPS) nicht dem aktuellen Stand der Technik genügen.

1 Architektur

Die folgenden Anforderungen sollten bereits bei der Planung und Integration einer Fernwartungslösung beachtet werden:

- ✔ Einheitliche Lösung: Besonders in größeren Infrastrukturen sollte möglichst eine einheitliche Lösung zum Einsatz kommen. Dies verringert sowohl die Anzahl der Angriffsvektoren als auch die Komplexität (kein „Wildwuchs").
- ✔ DMZ: Die Fernwartungskomponente sollte sich möglichst in einer vorgelagerten Zone (DMZ) befinden und nicht direkt im Produktionsnetz lokalisiert sein. Fernwartungszugänge dürfen nicht dazu führen, dass vorhandene umgangen werden. Vielmehr sind Firewalls geeignet, um beispielsweise erlaubte IP-Adressbereiche für eine Fernwartung festzulegen.
- ✔ Granularität der Kommunikationsverbindungen: Der Fernwartungszugriff sollte möglichst nicht pauschal pro (Sub)Netz erfolgen, sondern vielmehr feingranular pro IP und Port geregelt werden können. Dies minimiert die „Reichweite" von Fernwartungszugängen und beschränkt somit auch die Folgen einer Kompromittierung. Ein möglicher Ansatz ist beispielsweise der Aufbau von 1:1-Verbindungen mittels SSH statt der Kopplung ganzer Netze durch IPsec.

Quelle: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_108.pdf

Autor: Bundesamt für Sicherheit in der Informationstechnik

Organisation

Wichtige Prozesse

Nr.	Kategorien
1	Allgemeine Organisation (z.B. Verantwortlich)
2	Einkauf & Beschaffung
3	Systemadministration und -verwaltung
4	Prozesse für den Betrieb
5	. . .

Quelle: bluecept.com / sichere-industrie.de

Betriebskonzept

Betriebskonzept

Nr.	Inhalt
1	Organisatorisches
2	Incident Response Plan
3	Regelung von Support
4	Neubeschaffung /-beantragung von Zugängen
5	…

Quelle: bluecept.com / sichere-industrie.de

Zusammenfassung

Zusammenfassung

Anforderungen

Architektur

Organisation

Betrieb

https://www.sichere-industrie.de/industrial-iiot-security-themen/industrie-fernwartung/

Max Weidele

max.weidele@sichere-industrie.de

- Industrial & IIoT Security Stammtisch
- Best-Practises
- Marktüberblick & Trends
- Hilfreiche Kontakte

www.sichere-industrie.de