Software und Digitalisierung

Sichere Fernwartung

Beispiele von Fernwartungsarchitekturen für einen sicheren Remote Service



Software und Digitalisierung

Sichere Fernwartung

Beispiele von Fernwartungsarchitekturen für einen sicheren Remote Service

Vorwort

Fernwartung zur Aufrechterhaltung der Funktionsfähigkeit von Maschinen und Anlagen ist seit vielen Jahren Tagesgeschäft im Maschinen- und Anlagenbau. Um den Zugriff auf Maschinen sicher und zuverlässig zu gewährleisten, haben sich verschiedene technische Lösungen etabliert. Für den Anbieter von Fernwartung ist es jedoch häufig eine Herausforderung, den Kunden von der eingesetzten Lösung zu überzeugen, viele zeitintensive Diskussionen mit der IT-Abteilung des Kunden sind nötig. Nicht selten fordert der Kunde eine eigene Lösung, die aber nicht unbedingt sicherer ist, als die vom Maschinenhersteller angebotene. Das führt dazu, dass der Maschinenhersteller mehrere Lösungen bereithalten muss, um im Anwendungsfall die richtigen Zugangsdaten zu haben.

Dieses Dokument dient als Argumentationshilfe, um dem Kunden die verschiedenen Lösungen mit Vor- und Nachteilen zu erläutern und um eine Basis für das Erarbeiten eines gegenseitigen Konsenses für eine sichere Fernwartung zu schaffen.

Der VDMA-Arbeitskreis „Sichere Fernwartung“ hat verschiedene Fernwartungsarchitekturen, wie sie häufig anzutreffen sind, mit Vor- und Nachteilen beschrieben.

Im folgenden Dokument werden verschiedene Fernwartungsarchitekturen miteinander verglichen und deren Vor- und Nachteile beschrieben. Dabei sind grundlegende Anforderungen zur Security zu berücksichtigen, die unabhängig von den Architekturvarianten immer zu berücksichtigen sind.

Interessen der beteiligten Stakeholder

In allen Architekturen sind mindestens der Maschinenhersteller als Anbieter des Fernwartungsdienstes sowie der Betreiber als Nutzer zu berücksichtigen. Je nach Größe des Betreibers können auch hier unterschiedliche Interessengruppen involviert sein, etwa der Produktionsbereich, dessen besonderes Interesse der Verfügbarkeit und Produktivität gilt, sowie der IT-Bereich, der für das Security-Management verantwortlich ist.

Jeder Stakeholder hat seine eigene, legitime Sicht auf Security und Effizienz, die zu unterschiedlichen Anforderungen speziell an die Kontrollierbarkeit von Fernwartungsverbindungen führen und im Rahmen der Betrachtung von Vor- und Nachteilen der Architekturen berücksichtigt werden.

Allgemeine Anforderungen

Einige Aspekte sind jedoch bei allen möglichen Architekturen gleich:

- Das Bedürfnis nach einer fehlerfrei produzierenden Maschine
- Das Bedürfnis nach einer schnellen und effizienten Fehlerbehebung (-> online, ohne Reisezeiten)
- Das Bedürfnis nach einem in allen beteiligten Organisationen durchführbaren und skalierbaren Teleservice Prozess (Herstellerseitig bzgl. Einfachheit und Gleichheit für den Kundendienst und Betreiberseitig bzgl. Kontrollier-, Steuer- und Nachvollziehbarkeit)
- Das Bedürfnis aller Beteiligten, dass nur autorisiertes Fachpersonal an der Maschine arbeitet (vor Ort sowie remote)
- Fernwartung greift in die Maschinen und Anlagen ein, sie sollte daher nur in Abstimmung zwischen allen Parteien stattfinden und mit dem Betriebszustand der Maschine oder Anlage synchronisiert sein.
- Durch die Eingriffe können gewollt oder ungewollt Nebenwirkungen eintreten. Es ist die gemeinsame Aufgabe aller Beteiligten, durch entsprechende Sicherheitsmaßnahmen technischer und organisatorischer Art entsprechende Risiken zu minimieren. Zu dieser Risikominimierung können beispielsweise Prozesse gehören, die sicherstellen,
  - dass für die Wartung verwendete Systeme gehärtet sind, regelmäßig auf Schwachstellen geprüft und mit sicherheitsrelevanten Updates versorgt werden
  - dass kritische Systeme in zutrittsbeschränkten Bereichen installiert und nur von berechtigten Personen administriert werden

- dass entsprechend der Aufgabenstellung alle personenbezogenen Zugänge bei Beendigung der Beschäftigung oder Änderung der Position abgeschaltet werden und bei Gruppenzugängen die Passwörter bei Austritt geändert werden
- dass das Personal regelmäßige Security-Schulungen erhält
- dass die Verfügbarkeit der Fernwartung durchgehend gegeben ist, z.B. durch regelmäßige Probeverbindungen, damit eventuelle Veränderungen in der Einsatzumgebung, Ablauf von elektronischen Zertifikaten usw. nicht erst im Ernstfall entdeckt werden
- Ausgeschiedene Servicetechniker dürfen keinen Zugriff mehr auf diese Systeme mehr haben.

Allgemeine Infrastruktur

Hier wird von einer generell häufig anzutreffenden Netzwerk-Infrastruktur ausgegangen.
In Abbildung 1: oben ist das Netzwerk des Maschinenherstellers dargestellt. Das ist ein Firmennetz, ähnlich dem beim Betreiber, wird hier aber vereinfacht als ein Bereich dargestellt. In der Übersicht als „Remote-Ebene beim Maschinenhersteller“ bezeichnet.

Darunter kommt das Internet, über dieses wird der Kanal für die Fernwartung aufgebaut. Hier können sich separate Module für die Fernwartung befinden, in der Regel von Drittanbietern.

Alles unterhalb gehört zum Betreibernetzwerk. In aller Regel segmentieren die Betreiber ihre Netzwerke und schaffen Übergänge zwischen den Schichten durch DMZs.
[1]

So wird eine Fernwartungsverbindung in der Regel die zentrale DMZ des Betreibers durchqueren müssen (Unternehmensebene – Level 4). Danach wird diese Verbindung in aller Regel auch noch mindestens ein weiteres Netzwerk durchqueren müssen, die DMZ der Industrial Zone (Lokale Betriebsebene – Level 2/3).
[2]

Erst von dort besteht ein Zugang zum eigentlichen Maschinennetzwerk beim Betreiber (Steuerungs- und Feldebene – Level 0/1).
Die unterschiedlichen Fernwartungsstrukturen nutzen unterschiedliche Verbindungen und Richtungen des Verbindungsaufbaus. Letztlich ist aber immer das Ziel, eine Verbindung vom Maschinenhersteller bis zur Feldebene herzustellen.

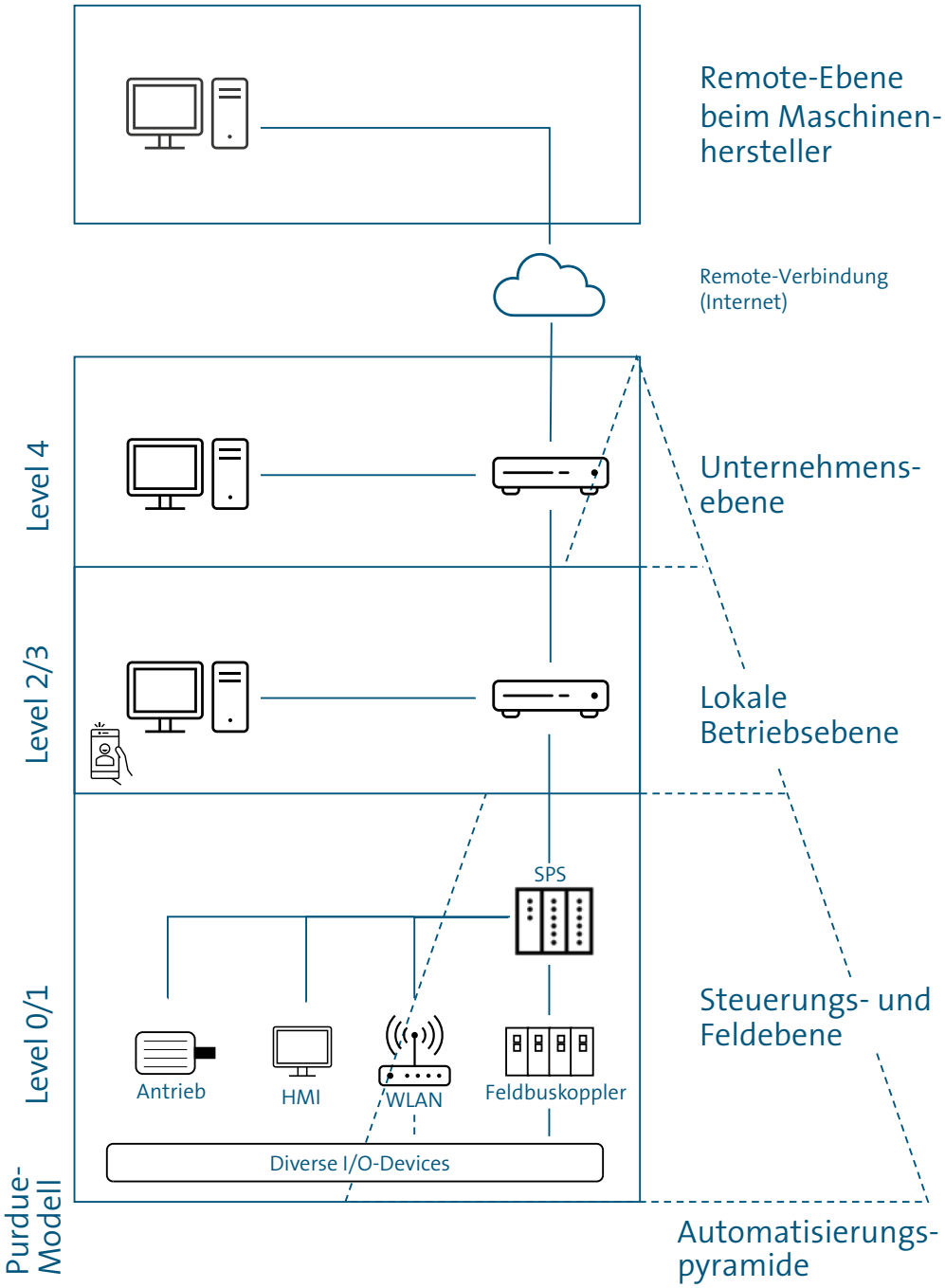
Unter Verbindung wird hierbei eine Virtual Private Network (VPN)-Verbindung verstanden, innerhalb derer die eigentliche Fernwartung über weitere Protokolle erfolgt. Ist der VPN-Tunnel etabliert, ist innerhalb des VPN-Tunnels die Richtung des Verbindungsaufbaus nicht mehr relevant. Jedoch sollte der VPN-Tunnel von innen (Betreiber) nach außen aufgebaut werden.

VPN-Tunnel haben den Vorteil, dass Vertraulichkeit und Integrität der Verbindungen innerhalb des VPNs durch kryptographische Methoden sichergestellt werden können. Systematisch haben sie dadurch auch den Nachteil, dass Art und Inhalt der Fernwartung nicht überwacht werden können.

Das Risiko ist abhängig von Sicherheit der jeweils gewählten Lösung

Abbildung 1

Beschreibung Netzwerkinfrastruktur



VPN direkt (Legacy) über Betreibernetzwerk (Variante 1)

Beschreibung Infrastruktur / Richtung des Zugriffs

Diese Variante besteht bei vielen Betreibern für verschiedene Altmaschinen. Es wird hier vom Maschinenhersteller aus eine VPN-Verbindung direkt auf einen VPN-Server in der Feldebene hergestellt. Dazu müssen Durchgänge vom Internet durch alle Firewalls und DMZs bis zu diesem VPN-Server hergestellt werden. Diese Durchgänge sind von Jedermann aus dem Internet grundsätzlich zugreifbar (öffentliche IP-Adresse und Port wird weitergeleitet bis auf den VPN-Server). Oft befindet sich dieser VPN-Server als Hutschienenbauteil im Schaltschrank der Maschine und kann durch einen Schlüsselschalter deaktiviert werden.

Verantwortlichkeiten

In aller Regel wird der VPN-Server vom Maschinenhersteller gestellt. Er ist in diesen Fällen dafür verantwortlich, dass auf diesem Gerät Sicherheitsupdates soweit möglich eingespielt werden. Der Betreiber muss den Zugriff von außen auf diesen VPN-Server innerhalb der Servicezeiten aufrechterhalten.

Risiken

Wenn der VPN-Server Sicherheitslücken aufweist, bietet er ein geeignetes Ziel für einen Angriff von außen, da er direkt erreichbar ist. Wenn er vom Maschinenhersteller gestellt ist, kann der Betreiber den aktuellen Zustand diesbezüglich meistens nicht beurteilen.

Fehlkonfigurationen in den Firewall- bzw. Routingeinstellungen beim Betreiber ermöglichen evtl. einen Zugriff von außen auf andere Geräte innerhalb des Betreibernetzes oder verhindern einen VPN-Aufbau gänzlich.

Abhilfemaßnahmen

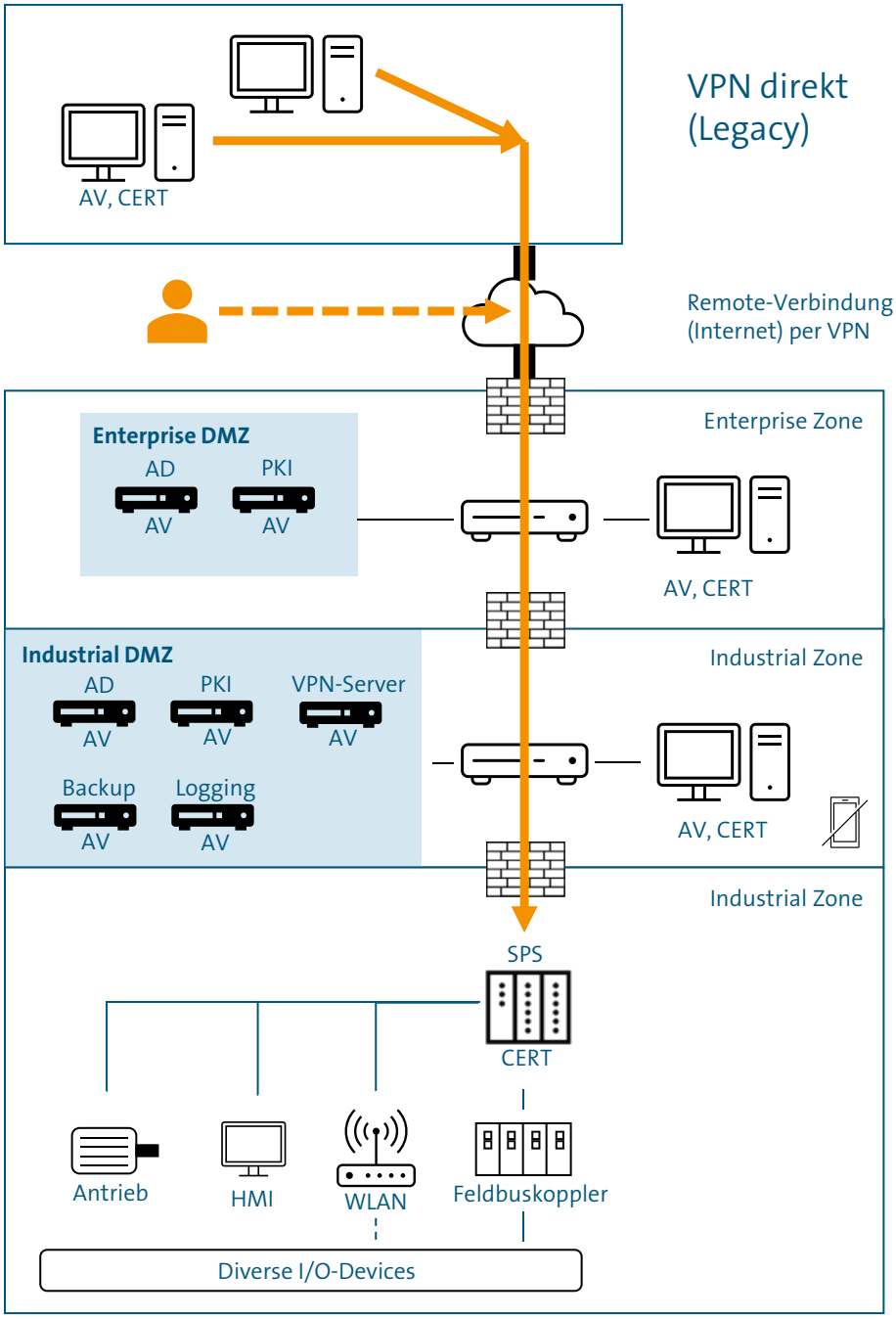
- Umbau auf eine sichere Variante

Bewertung des AK

- Umstellung auf endgültige Lösung sobald wie möglich (Konsens zwischen Betreiber und Hersteller)
- Für regelmäßige Fernwartungszugriffe aufgrund des hohen Wartungsaufwands und der Intransparenz für den Betreiber nicht geeignet
- Gefährlich, da die Verbindung tief ins Netz reingeht. Betreiber kann Inhalt nicht verifizieren, überprüfen
- Generell sollten die erlaubten Zugriffe von außen auf bestimmte Endpunkte innerhalb des Firmennetzwerkes auf ein Minimum reduziert werden.

Abbildung 2

VPN direkt über Betreibernetzwerk



Legende
AD: Active Directory, PKI: Public Key Infrastruktur
AV: Virenscanner, CERT: PKI-Zertifikat, DMZ: De-Militarized Zone

Erweiterung VPN direkt (Legacy) über Mobilfunk (Variante 2)

Beschreibung Infrastruktur / Richtung des Zugriffs

Diese Variante besteht bei vielen Betreibern für verschiedene Altmaschinen. Es wird hier vom Maschinenhersteller aus eine VPN-Verbindung direkt auf einen VPN-Server in der Feldebene hergestellt. Durch den Einsatz eines Mobilfunkrouters wird der Weg durch die Firewalls und DMZs des Betreibers umgangen und kann direkt auf die Maschine zugreifen. Wichtig: für den Verbindungsaufbau wird ein Mobilfunkrouter mit einer festen IP-Adresse benötigt. Hierfür gibt es spezielle Anbieter oder auch Angebote bei den bekannten Mobilfunkanbietern (bspw. Telekom Business Tarife). Der Router sollte auch so konfiguriert werden, dass nur von bestimmten Zieladressen zugriffen werden kann.

Verantwortlichkeiten

In aller Regel wird der VPN-Server inkl. Mobilfunkrouter vom Maschinenhersteller gestellt. Er ist dann meistens dafür verantwortlich, dass auf diesem Gerät Sicherheitsupdates soweit möglich eingespielt werden.

Risiken

Die öffentliche IP-Adresse ermöglicht den unerlaubten Zugriff von außen auf die Maschine. Etwas weniger Risiko [im Vergleich zu Variante 1], da der Weg nicht mehr durch die einzelnen Schichten des Netzwerks des Betreibers führt, sondern direkt auf die Maschine. Kommunikation in das Betreibernetzwerk kann mit einfachen Mitteln verhindert werden.

Die Abschaltung des Zugangs über diese Lösung kann nicht unbedingt zweifelsfrei festgestellt sein. Es kann sich die Maschine in einem zugriffsbereiten Modus befinden, ohne dass der Betreiber das feststellen kann.

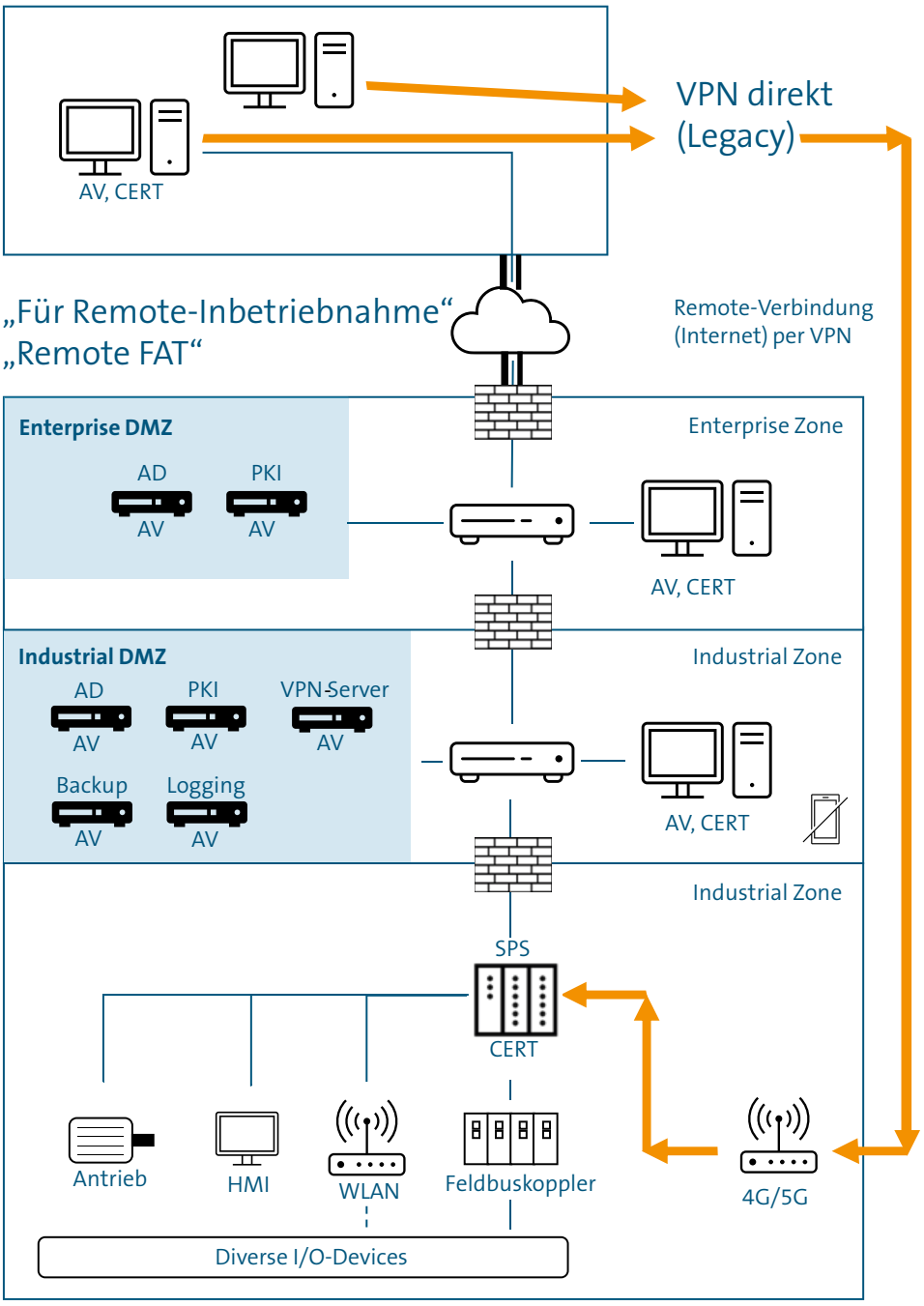
Abhilfemaßnahmen

Umbau auf aktuelle/empfohlene Variante

Bewertung des AK

- Nur als Zugriff während der Inbetriebnahme der Anlage, nicht dauerhaft
- Umstellung auf endgültige Lösung bei Abnahme; mögliche Lösung kann eine der nachfolgenden Varianten sein
- Für regelmäßige Fernwartungszugriffe nicht geeignet

Abbildung 3
VPN direkt über Mobilfunk



Legende
AD: Active Directory, PKI: Public Key Infrastruktur
AV: Virenscanner, CERT: PKI-Zertifikat, DMZ: De-Militarized Zone

Entkopplungssysteme: Beim Betreiber (Jump Hosts) (Variante 3)

Beschreibung Infrastruktur / Richtung des Zugriffs

Diese Variante wird von vielen Betreibern mit umfangreichen IT-Sicherheitsrichtlinien gefordert. Hierbei bietet der Betreiber einen VPN-Zugang in das Betreibernetzwerk an.

Der Betreiber stellt den VPN-Server

Üblicherweise ist das Ziel dieses VPN-Tunnels nicht direkt im Maschinennetz, sondern ein PC bzw. eine virtuelle Maschine irgendwo im Betreibernetz, z.B. in einer DMZ. Dieser wird mit Hilfe irgendeiner Fernsteuerungslösung ferngesteuert, z.B. VNC oder RDP. Von dort aus muss der Servicetechniker dann in mehreren Schritten weitere PCs oder virtuelle Maschinen fernsteuern und dabei jeweils Netzwerkübergänge innerhalb des Betreibernetzes überschreiten.

Es muss sich bei jedem weiteren Schritt wieder angemeldet werden. Je nach Sicherheitsrichtlinie des Betreibers können unterschiedliche Anmeldungen an den jeweiligen Jump-Hosts notwendig sein. Diese Zugangsdaten bei beschränkter Gültigkeit auch ablaufen und müssen dann z.B. halbjährlich erneuert werden.

Zum Schluss landet der Servicetechniker per Fernsteuerung auf einen (virtuellen) Service-PC, welcher direkten Netzwerkzugriff auf die Maschinenkomponenten hat. Es kann sein, dass hierfür ein lokaler Benutzer verwendet wird, so dass eine weitere Benutzername-Passwort-Kombination verwendet werden muss.

Dieser letzte PC muss alle benötigten Softwaretools für den Remoteservice installiert haben. Außerdem müssen dort, je nach Sicherheitsrichtlinie des Betreibers, auch alle Softwareprojekte für z.B. SPSen oder HMIs hinterlegt sein, denn ein Dateitransfer direkt auf den Service-PC ist je nach Sicherheitsrichtlinien des Betreibers nicht erlaubt, mindestens aber schwierig über mehrere Fernsteuerungsinstanzen hinweg.

Verantwortlichkeiten

Betreiber muss Funktionalität und Konten (Benutzername, Passwort, 2. Faktor) von VPN-Server und Jump Hosts sicherstellen.

Hersteller muss passenden VPN-Client, Prozess (Benutzername, Passwort, 2. Faktor), Fernsteuerungsclient nutzen. Bei verschiedenen Betreibern können sehr unterschiedliche Systeme im Einsatz sein. Auch die Authentifizierung kann sich hinsichtlich der Art und der Faktoren (Benutzername, Passwort, PIN, VPN-Token, E-Mail, App usw.) unterscheiden. Dies stellt für den Hersteller eine größere Herausforderung dar.

Wer stellt und wartet Service-PC?

- Allg. Wartung
- Installation Entwicklungssoftware
- Dateiübertragung für Projektdateien möglich? – Quarantäne-Instanz?

Risiken

- Generell eher geringes Risiko
- Hoher Prozessaufwand kann zu verringerter Effizienz/Verfügbarkeit der Fernwartung führen.

Abhilfemaßnahmen

Generell keine Abhilfe notwendig.

Empfehlung des AK

Solange die Hersteller dieser Lösung zustimmen und die Anforderungen erfüllen können, sowie der Betreiber die Nachteile (s.u.) in Kauf nimmt, kann diese Lösung umgesetzt werden und es besteht kein Bedarf an einer Änderung.

Bewertung des AK

Vorteile

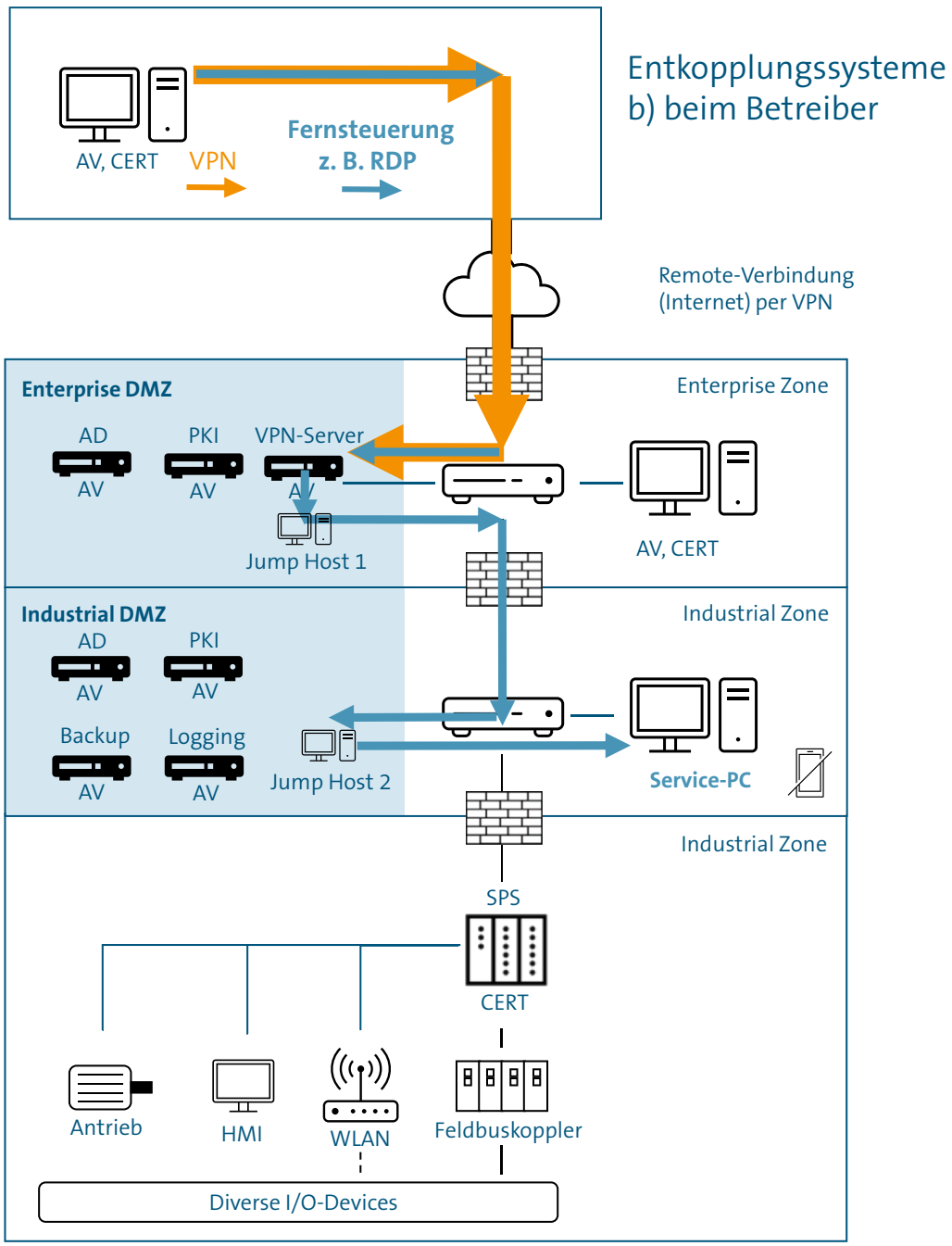
- Sicherheit hoch
- Remote-Service-Monitoring möglich
- Release-Management / Backup auf Service-PC ist möglich
- Software auf Service-PC (OS und Entwicklungspakete) kann eingefroren werden / dürfen altern

Nachteile

- Hoher Wartungsaufwand
- Hoher Investitionsaufwand
- Skaliert nicht aus Herstellersicht, hohe Varianz
- Evtl. problematische Prozesse
  - 24/7
  - Tokens / 2. Faktor
  - Passwortablauf/-wechsel
  - Zertifikatsablauf

Abbildung 4

Entkopplungssysteme



Legende
AD: Active Directory, PKI: Public Key Infrastruktur
AV: Virenscanner, CERT: PKI-Zertifikat, DMZ: De-Militarized Zone

Rendezvous-System Hardwarebasiert (beim Maschinenhersteller) (Variante 4)

Beschreibung Infrastruktur / Richtung des Zugriffs

Diese Variante wird von vielen Maschinenherstellern angeboten. Beim Maschinenhersteller ist ein hardwarebasiertes Rendezvous-System/VPN-Server installiert.

Die VPN-Verbindung wird von der Maschine zum Rendezvous-System aufgebaut. Für den Betreiber besteht nur die Notwendigkeit, eine Freigabe der Verbindung in seinen Firewalls umzusetzen. Dies könnte je nach technischer Ausprägung automatisch passieren (Konzept “Home Router”, alles Ausgehende ist erlaubt) oder die Vergabe spezieller Regeln oder Rechte umfassen. Oft befindet sich der VPN-Client als Hutschienenbauteil im Schaltschrank der Maschine und kann durch einen Schlüsselschalter aktiviert/deaktiviert werden.

Beim Maschinenhersteller sind Szenarien denkbar, bei denen die Servicetechniker die Verbindung zum Rendezvous-Server per VPN aufbauen. Direkte Anbindungen aus dem Hausnetz oder einem spezialisierten Servicenetz sind ebenso bekannt.

Der Servicetechniker könnte sich auch außerhalb des Hausnetzes des Maschinenherstellers befinden. Dies muss organisatorisch und vertraglich zulässig und abgesichert sein.

Verantwortlichkeiten

In aller Regel wird der VPN-Client vom Maschinenhersteller gestellt. Das Installieren eventueller Sicherheitsupdates muss abgestimmt werden, da der Maschinenhersteller nur während einer aktiven Fernwartungsverbindung Zugang zum VPN-Client hätte. Empfehlenswert ist ein übergeordnetes Managementsystem, um u.a. Updates auszurollen. Der Maschinenhersteller ist für den sicheren Betrieb des Rendezvous-Servers sowie die Anbindung seiner Servicetechniker (mit oder ohne VPN) verantwortlich.

Der Betreiber muss eventuell notwendige Freigaben für den Aufbau der VPN-Tunnel aufrechterhalten.

Risiken

Bei sachgerechter Konfiguration der VPN-Verbindungen sind diese kaum angreifbar. Angriffe und Fehlfunktionen würden daher an den Endpunkten und/oder der Verwaltung relevant.

Grundsätzlich erfordern Installation und Betrieb des Rendezvous-Servers Fachkenntnisse. Bei unsachgemäßem Vorgehen könnten eben genannte Probleme entstehen. Die Verfügbarkeit des Rendezvous-Servers ist entsprechend der Notwendigkeiten durch Redundanzen zu sichern.

In jedem Fall hat der Betreiber keine Kontrolle über die Kommunikation im VPN-Tunnel, so dass unabsichtlich (Fehlbedienung; Virus/Trojaner) oder sogar vorsätzlich Schadwirkungen hervorgerufen werden können.

Abhilfemaßnahmen

Hier ist sicherzustellen, dass nur berechtigte Benutzer im Hausnetz des Maschinenherstellers Zugriff auf den Rendezvous-Server erhalten, bei Verwendung von VPN-Tunneln durch die Servicetechniker ist sicherzustellen.

Beim Rendezvous-Server ist die saubere Trennung der Verbindungen relevant, über ein entsprechendes Management ist sicherzustellen, dass die Servicetechniker den richtigen Maschinen zugewiesen werden und nur diese ansprechen dürfen. Eine Kopplung zwischen den VPN-Tunneln verschiedener Maschinen (und damit verbundene Möglichkeiten gegenseitiger Beeinflussung) muss ausgeschlossen sein. Neben der Anwendung etwa eines Schlüsselschalters zur Aktivierung des VPN-Tunnels durch Personal an der Maschine kann durch verwaltete Firewall-Regeln im Betreibernetzwerk der Verbindungsaufbau kontrolliert und z.B. eine zusätzliche Freigabe durch Fertigungsleitung oder Security-Organisation durchgesetzt werden.

Bewertung des AK

Die beschriebene Architektur lässt sich auf hohem Sicherheitsniveau umsetzen, baut dabei aber allein auf die Security-Kompetenz und Vertrauenswürdigkeit des Maschinenherstellers. Insbesondere für kleinere Betreiber ohne eigene Expertise bietet diese Architektur eine bewährte Umsetzung. Für größere Betreiber bzw. kritische Anwendungen fehlt die Möglichkeit, die Fernwartung jenseits des „VPN-Tunnel an/aus“ detailliert zu steuern oder zu überwachen.

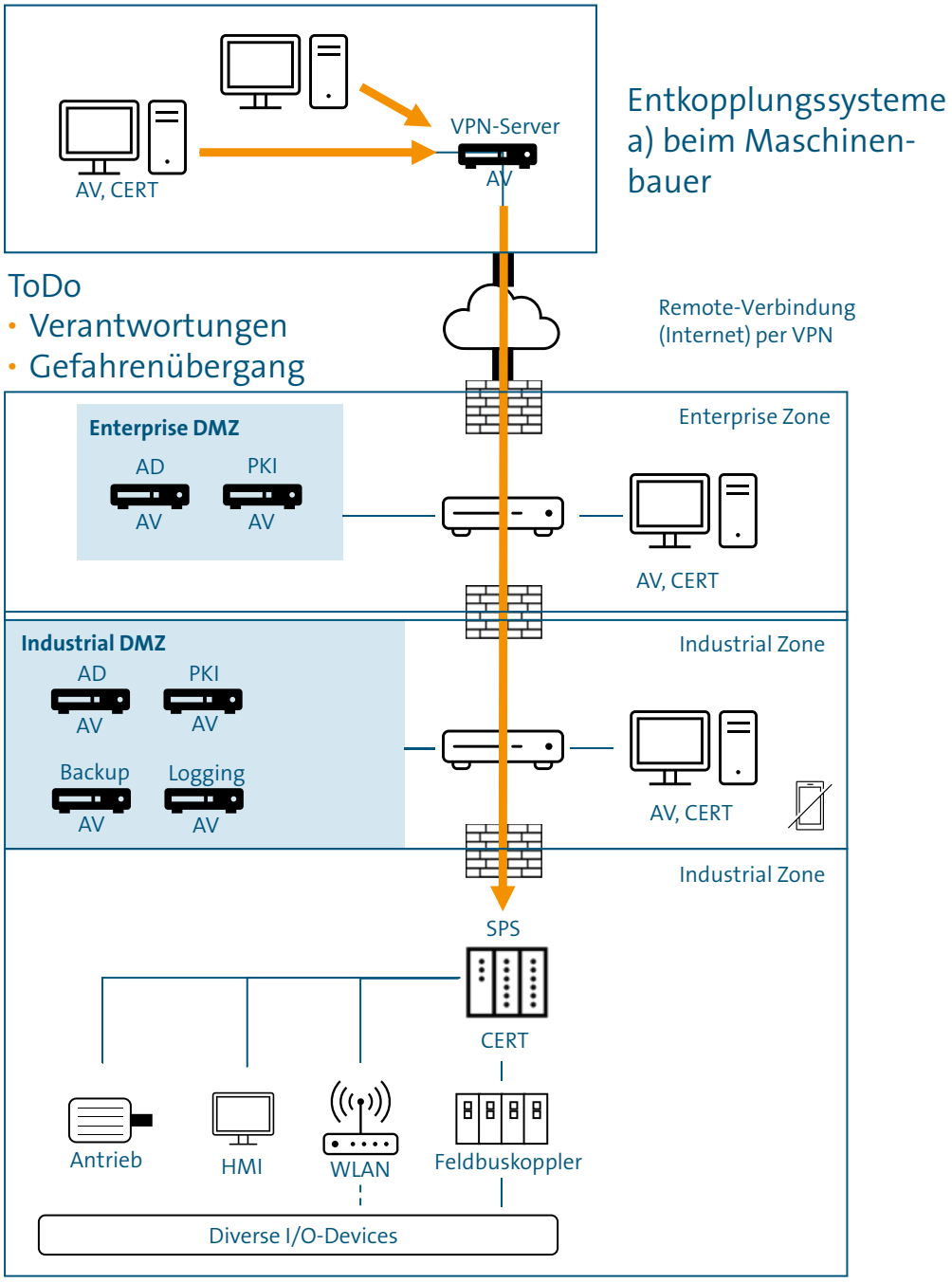
Vorteil

Hohe Kompetenzen, durch langjährige Erfahrungen.

Hohes Sicherheitsniveau, um eigene Kunden zu schützen – da ein Vorfall ein Imageverlust bedeuten könnte.

Abbildung 5

Rendezvous-System Hardwarebasiert beim Maschinenhersteller



Legende
AD: Active Directory, PKI: Public Key Infrastruktur
AV: Virenscanner, CERT: PKI-Zertifikat, DMZ: De-Militarized Zone

Rendezvous-System Hardwarebasiert (beim Betreiber) (Variante 5)

Beschreibung Infrastruktur / Richtung des Zugriffs

Diese Variante wird von vielen Betreibern mit umfangreichen IT-Sicherheitsrichtlinien gefordert, so dass der Betreiber die Hoheit über alle Fernwartungszugriffe hat.

In der DMZ des Betreibers ist in der Regel ein hardwarebasiertes Rendezvous-System/VPN-Server installiert.

Die VPN-Verbindung wird von der Maschine zum Rendezvous-System aufgebaut, so dass keine eingehende Verbindung in das Produktionsnetzwerk durch den Betreiber erlaubt werden muss. Umgekehrt baut der Servicetechniker des Maschinenherstellers eine VPN Verbindung zum Rendezvous-System/VPN-Server auf.

Analog zu Variante 4 kann sich der Servicetechniker auch außerhalb des Hausnetzes des Maschinenherstellers befinden. Für den Betreiber besteht nur die Notwendigkeit, eine Freigabe der Verbindung in seinen Firewalls umzusetzen. In der Regel befindet sich der hardwarebasierte VPN-Client unmittelbar vor der Maschine (hoher Sicherheitslevel) oder alternativ auch vor einer Produktionslinie (moderater Sicherheitslevel) und kann durch einen Schlüsselschalter aktiviert/deaktiviert werden.

Verantwortlichkeiten

Die für die Fernwartung benötigte Infrastruktur liegt beim Betreiber. Damit muss der Betreiber Fernwartungszugriffe für Servicetechniker per Konfiguration freischalten und in der Regel je nach Sicherheitsstufe Fernwartungszugriffe während des Betriebs explizit genehmigen. Der Maschinenhersteller muss die Freischaltung der Fernwartung für einzelne Servicetechniker beantragen.

Falls Betreiber und Maschinenhersteller die Kontrolle über die Fernwartung wollen, so sind auch Lösungen mit verschachtelten VPN Tunneln und revisionssicherer Aufzeichnung für beide Parteien üblich.

Risiken

Im Vergleich zu Variante 4 wird das Risiko durch die zentrale Verwaltung des Betreibers reduziert.

Abhilfemaßnahmen

Gemeinsam mit dem Betreiber müssen möglichst effiziente Prozesse implementiert werden, zur Verwaltung der Berechtigungen der Fernwartungszugriffe zwischen Servicetechnikern und Maschinen auf der Seite des Betreibers. Bei hohen Sicherheitsanforderungen ist eine Multi-Faktor Authentifizierung zu empfehlen beispielsweise mit einem Hardware-Authentifikator (Smartcard, USB Security Token Device), so dass Berechtigungen mehrfach unabhängig entzogen werden können.

Analog zur Variante 4 gelten die Maßnahmen zur Trennung von Verbindungen und zur Freischaltung. Die Umsetzung der Maßnahmen liegt allerdings in der Verantwortung des Betreibers.

Bewertung des AK

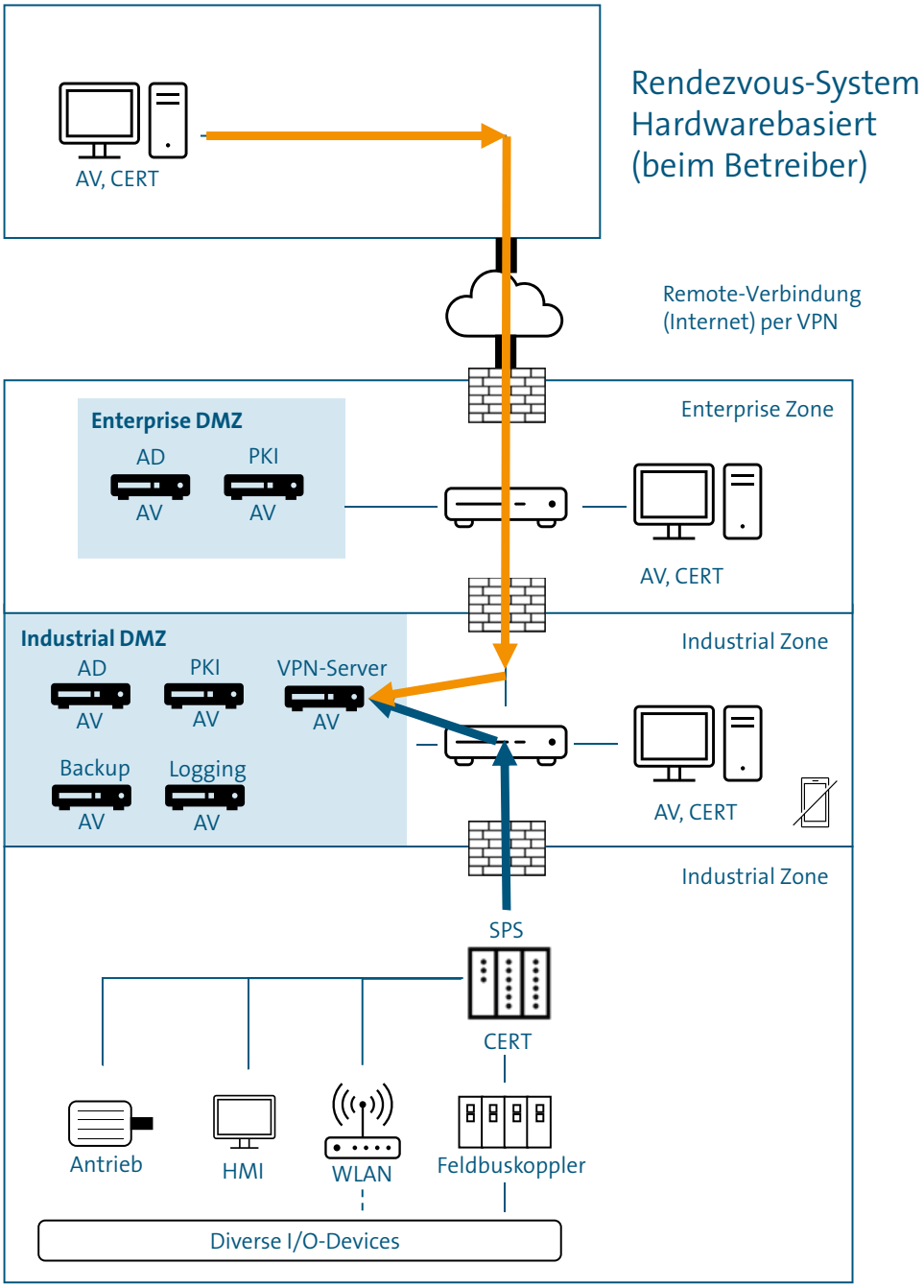
Die beschriebene Architektur lässt sich auf hohem Sicherheitsniveau umsetzen. Allerdings liegt die Hoheit der Fernwartung in der Regel vollständig beim Betreiber. Ein Zugriff auf Maschinen des Betreibers erfordert entweder die explizite Freischaltung durch einen Operator bei Anfrage einer Fernwartung oder die automatische Freischaltung der Fernwartung auf der Seite des Operators zu bestimmten vereinbarten Wartungsintervallen.

Vorteil

Hohe Akzeptanz bei Betreibern bzw. weite Verbreitung in unterschiedlichen Industriezweigen. Die Verantwortung liegt in diesem Fall beim Betreiber.

Abbildung 6

Rendezvous-System Hardwarebasiert beim Betreiber



Legende
AD: Active Directory, PKI: Public Key Infrastruktur
AV: Virenscanner, CERT: PKI-Zertifikat, DMZ: De-Militarized Zone

Rendezvous-System Cloud basiert (Variante 6)

Beschreibung Infrastruktur / Richtung des Zugriffs

Diese Variante und folgende haben sich aus Variante 4 entwickelt, und wird – je nach „Cloud-Affinität“ der Beteiligten – immer häufiger angeboten. Das Rendezvous-System/VPN-Server ist nun in der Cloud installiert.

Die VPN-Verbindung wird auch hier von der Maschine zum Rendezvous-System aufgebaut (also wieder „von innen nach außen“). Für den Betreiber besteht nur die Notwendigkeit, eine Freigabe der Verbindung in seinen Firewalls umzusetzen. Dies könnte je nach technischer Ausprägung automatisch passieren (Konzept “Home Router”, alles Ausgehende ist erlaubt) oder die Vergabe spezieller Regeln oder Rechte umfassen. Oft befindet sich der VPN-Client/Router als Hutschienenbauteil im Schaltschrank der Maschine und kann durch einen Schlüsselschalter aktiviert/deaktiviert werden

- Der Servicetechniker / Hersteller-Client stellt ebenfalls eine sichere Verbindung zum Rendezvous-System. Je nach Lösung stehen die gleichen Optionen bzgl. der verwendeten TCP-Ports wie beim Maschinen-Client zur Verfügung.
- Sowohl die Firewalls des Betreibers als auch des Herstellers müssen nur ausgehende Verbindung zum Rendezvous-System im Internet / Cloud erlauben und somit keine Weiterleitungsregeln konfigurieren müssen, die einen Kommunikationsaufbau aus dem Internet in das Netz des Herstellers oder Betreibers ermöglichen.

Verantwortlichkeiten

- Bei diesem Variante richten sich die Verantwortlichkeiten danach, wer den Cloud-Account und die Admin Hoheit über den darauf installierten VPN Server hat (Maschinenhersteller oder -betreiber)
- Der Betreiber muss in jedem Fall den Fernzugriff initiieren

Vorteile

- Keine eigene Hardware (VPN-Server) nötig: Nutzung IaaS / SaaS von Cloud-Provider (AWS, Azure, Alibaba): OPEX statt CAPEX
- Stand der Technik
- Gut skalierbare Lösung, die auch für den Maschinenhersteller empfohlen ist

Risiken / Nachteile

- Abhängigkeit vom Cloud-Anbieter („Lock In Effekt“).
- „VPN-Durchstich“ durch alle Netzwerkebenen vom Feld in die Cloud
- Cloud Security und Privacy / Vertragsbedingungen (SLA) s.
- Security nur so hoch, wie die Implementation der Lösung in der Cloud (ISO27001 bezieht sich nur auf Infrastruktur)
- Verletzung der lokalen Cyber-Gesetze z.B. Chinese Cyber Security Law, DSGVO, NIS2
- Vertragsdetails sind daher sehr wichtig; ggf. hoher Prüfaufwand
- Datenfolgeabschätzung (Cyber-Gesetze)

Abhilfemaßnahmen / Best Practice

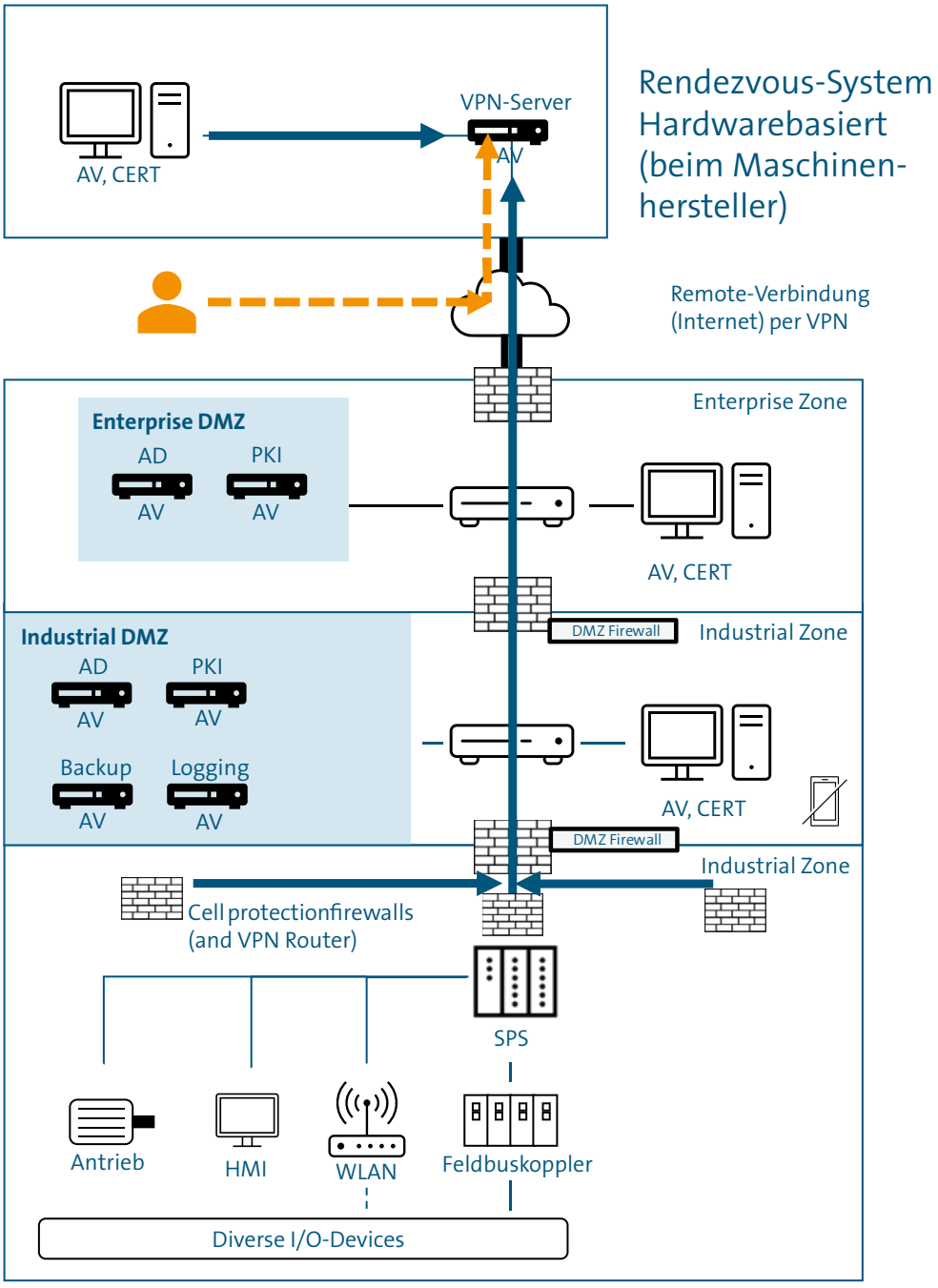
- Nur temporärer Zugriff (keine „stehende“ VPN Verbindung) Aktivierung z.B. über Schlüsselschalter als Digitaler Eingang am VPN-Router
- BSI Empfehlung für Cloud-Verträge

Bewertung des AK

- IT-Abteilungen großer Betreiber werden diese Methode favorisieren

Abbildung 7

Rendezvous-System Cloud basiert



Legende
AD: Active Directory, PKI: Public Key Infrastruktur
AV: Virenscanner, CERT: PKI-Zertifikat, DMZ: De-Militarized Zone

Rendezvous-System Hardwarebasiert hochverfügbar (Cloud) (Variante 7)

Beschreibung Infrastruktur / Richtung des Zugriffs

Diese Variante hat sich aus dem Variante 6 entwickelt, und wird – je nach „Cloud-Affinität“ der Beteiligten – immer häufiger angeboten. Das Rendezvous-System/VPN-Server ist auch hier in der Cloud installiert.

Hier gibt es ein zweites komplettes zweites Rendezvous-System in einer anderen Cloud oder in einem anderen Land. Hierdurch bildet sich ein komplett redundantes System, welches eine hohe Verfügbarkeit und einer hohen Ausfallsicherheit auszeichnet. Voraussetzung dabei ist, dass beide Rendezvous-Systeme über einen dauerhaft aufrechterhaltenen VPN -Tunnel miteinander verbunden sind.

Die VPN-Verbindung wird hier von der Maschine zu beiden Rendezvous-System aufgebaut (also wieder „von innen nach außen“). Für den Betreiber besteht nur die Notwendigkeit, eine Freigabe der Verbindung in seinen Firewalls umzusetzen. Dies könnte je nach technischer Ausprägung automatisch passieren (Konzept “Home Router”, alles Ausgehende ist erlaubt) oder die Vergabe spezieller Regeln oder Rechte umfassen. Oft befindet sich der VPN-Client/Router als Hutschienenbauteil im Schaltschrank der Maschine und kann durch einen Schlüsselschalter aktiviert/deaktiviert werden.

Der Servicetechniker / Hersteller-Client stellt ebenfalls eine sichere Verbindung zu einem der beiden Rendezvous-Systeme her. Je nach Lösung stehen die gleichen Optionen bzgl. der verwendeten TCP-Ports wie beim Maschinen-Client zur Verfügung.

Sowohl die Firewalls des Betreibers als auch des Herstellers müssen nur ausgehende Verbindung zum Rendezvous-System im Internet / Cloud erlauben und somit keine Weiterleitungsregeln konfigurieren müssen, die einen Kommunikationsaufbau aus dem Internet in das Netz des Herstellers oder Betreibers ermöglichen.

Verantwortlichkeiten

- Bei diesem Variante richten sich die Verantwortlichkeiten danach, wer den Cloud-Account und die Admin Hoheit über den darauf installierten VPN Server hat (Maschinenhersteller oder -betreiber)
- Der Betreiber muss in jedem Fall den Fernzugriff initiieren

Vorteile

- Keine eigene Hardware (VPN-Server) nötig: Nutzung IaaS / SaaS von Cloud-Provider (AWS, Azure, Alibaba): OPEX statt CAPEX
- Stand der Technik
- Gut skalierbare Lösung, die auch für den Maschinenhersteller empfohlen ist
- Zwei identische Fernwartungssysteme (und –workflow) für alle Endkunden, wo seine Maschinen „landen“
- Erhöhte Ausfallsicherheit aufgrund zwei Redundanter Rendezvous Systeme
- Gesicherte Zugelassene VPN Verdingung (VPN-Weiterleitung)
- Techniker Zugriff von außerhalb China über den Cluster Interconnect Datenabgleich Richtung des Zugriffs

- Rendezvous in der Cloud

- Clients haben eventuell zwei VPN Gegenstellen, mit denen sie sich verbinden könnten.

- Anwendungsfall eines separaten Rendezvous-Systems in China:
  - Keine Verletzung der lokalen Cyber-Gesetze z.B. Chinese Cyber Security Law, DSGVO, NIS – 2
  - VPN Verbindung von Maschine zum Rendezvous-System findet innerhalb von China statt

Risiken

- Abhängigkeit vom Cloud-Anbieter („Lock In Effekt“).

- „VPN-Durchstich“ durch alle Netzwerkebenen vom Feld in die Cloud

- Cloud Security und Privacy / Vertragsbedingungen (SLA) s.

- Security nur so hoch, wie die Implementation der Lösung (ISO27001 bezieht sich nur auf Infrastruktur)

Abhilfemaßnahmen

- Nur temporärer Zugriff (keine „stehende“ VPN Verbindung) [nicht optimal für OEM, falls es IoT Monitoring anstrebt]

- BSI Empfehlung für Cloud-Verträge

Bewertung des AK

Bei dieser Lösung handelt es sich um einen aktuellen Stand der Technik. Da es eine Standardisierte Lösung ist, ist diese auch für Maschinenhersteller empfohlen.

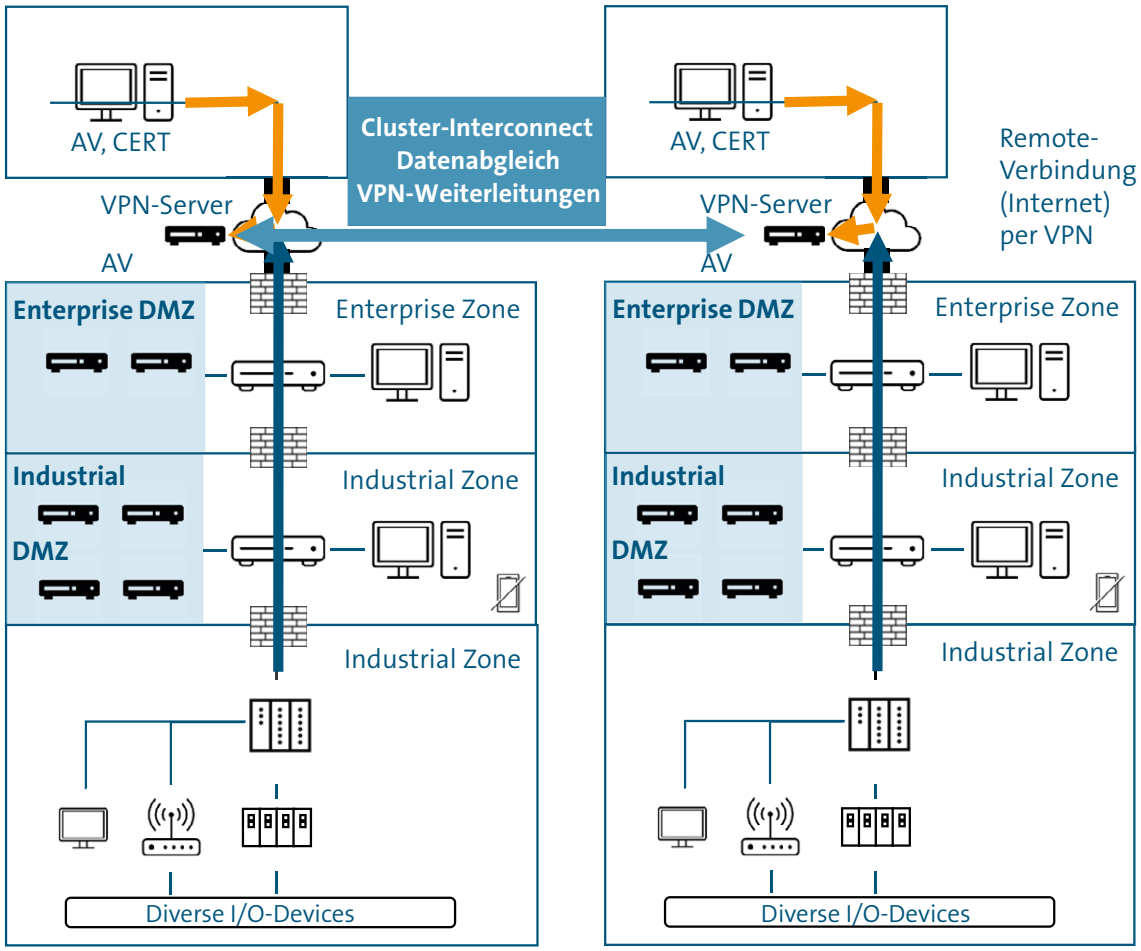
Wenn diese ab einer gewissen Größe auf eine Ausfallsicherheit angewiesen sind oder auch Kunden in einem Land wie China haben. Sollte eine Cloud von einem Ausfall betroffen sein, kann eine Fernwartung aller Kunden trotzdem gewährleistet werden, indem eine Verbindung ein die andere Cloud hergestellt wird.

Des Weiteren eine bessere Erreichbarkeit von Maschinen in Ländern mit VPN Beschränkungen. Bedingung hierfür ist aber, dass der VPN Tunnel registriert und zugelassen ist.

Zusätzlich werden die Latenzen verringert, wenn sich die Maschine in die geografisch nähere Cloud verbindet.

Abbildung 8

Rendezvous-System Hardwarebasiert hochverfügbar (Cloud)



Legende
AD: Active Directory, PKI: Public Key Infrastruktur
AV: Virenscanner, CERT: PKI-Zertifikat, DMZ: De-Militarized Zone

Rendezvous-System Softwarebasiert (Cloud) (Variante 8)

Beschreibung Infrastruktur

Die Infrastruktur besteht aus drei wesentlichen Komponenten

1. Rendezvous-System

Das softwarebasierte Rendezvous-System stellt die zentrale Schnittstelle zwischen dem Maschinen-Client auf Betreiberseite und dem Client auf der Herstellerseite.

Typischer Weise ist diese eine Cloud-basierte Applikation die weltweit über das Internet erreichbar ist. Es existieren aber auch Lösungen dieser Applikation, die Off Premise in einer Enterprise DMZ beim Hersteller oder Betreiber gehostet werden kann. Diese Variante wird hier nicht betrachtet.

Das Rendezvous-System erfüllt dabei folgende Aufgaben:

- Benutzerverwaltung für den Fernzugriff auf eine Anlage
- Festlegen der Berechtigung, welcher Benutzer auf welche Maschinenkomponenten zugreifen darf und über welche Kommunikationsprotokolle der Zugriff erfolgt
- Sichere Vermittlung der Datenkommunikation zwischen Maschinen-Client und Hersteller-Client
- Protokollierung (Audit Trail) sämtlicher Interkationen (Konfiguration des Rendezvous-Systems und Interaktionen während eines Fernzugriffs)
- Monitoring von Maschinenparametern
- Update der Maschinen-Clients

2. Maschinen-Client

Der Maschinen-Client steht je nach Lösung sowohl als ein Software-Applikation zu Installation auf einem PC-basiertem System bzw. virtuelle Maschine zur Verfügung oder bereits integriert und verschiedenen industrietauglichen Komponenten wie Switches, Firewalls und Routern inkl. WAN / WWAN Schnittstellen zur Verfügung.

Es stellt den sicheren Datenaustausch zwischen den Komponenten der Maschine und dem Rendezvoussystem her.

Eine weitere wesentliche Funktion ist die Übersetzung von IP-Adressen, so dass für einen Fernzugriffe die existierende IP-Adress-Struktur der Maschine nicht angepasst werden muss. Dies ist besonders wichtig für das Nachrüsten von existierenden Maschinen (Brown-Field-Applikationen) oder auch Serienmaschinen, die identische IP-Adress-Strukturen aufweisen.

Weiterhin ist es möglich, dass der Verbindungsaufbau des Maschinen-Client zum Rendezvoussystem durch externe Maßnahmen gesteuert (aktiviert/deaktiviert) werden kann.

Der Konfigurationsaufwand beschränkt auf die Konfiguration, wie dieser Client das Rendezvous-System und wie er sich zu authentifizieren hat.

3. Hersteller-Client

Der Hersteller Client stellt die sichere Kommunikation von dem PC zum Rendezvousserver her. Gemäß der konfigurierten Berechtigung auf dem Rendezvous-System erhält der Techniker des Herstellers nach erfolgreicher Authentifizierung Zugriff auf die Maschine bzw. den darin befindlichen Komponenten.

Richtung des Zugriffs

1. Zur Konfiguration des Rendezvous-System erfolgt in der Regel der Zugriff über den integrierten Web-Server des Rendezvoussystems.

2. Der Maschinen-Client baut selbständig eine sichere Verbindung mit dem Rendezvoussystem auf. Da am Markt verfügbaren Lösungen nutzen typischer weise den für HTTPs reservierten TCP-Port 443. Je nach Lösung stehen weitere TCP-Ports zu Verfügung oder können frei konfiguriert werden.

3. Der Hersteller-Client stellt ebenfalls eine sichere Verbindung zum Rendezvous-System. Je nach Lösung stehen die gleichen Optionen bzgl. der verwendeten TCP-Ports wie beim Maschinen-Client zur Verfügung.

   Vorteil dieser Lösung ist, dass sowohl die Firewalls des Betreibers als auch des Herstellers nur ausgehende Verbindung zum Rendezvous-System im Internet erlauben müssen und somit keine Weiterleitungsregeln konfigurieren müssen, die einen Kommunikationsaufbau aus dem Internet in das Netz des Herstellers oder Betreibers ermöglichen.

Verantwortlichkeiten

Hinsichtlich der Verantwortlichkeiten sind unterschiedle Szenarien zu Berücksichtigen. Neben dem Hersteller der Maschine und dem Betreiber der Maschinen spielt unter Umständen auch der Lieferant der Fernzugriffslösung und der Cloud-Betreiber eine wesentliche Rolle.

Risiken

- Verletzung der lokalen Cyber-Gesetze (DSGVO, NIS 2, Chinese Law)

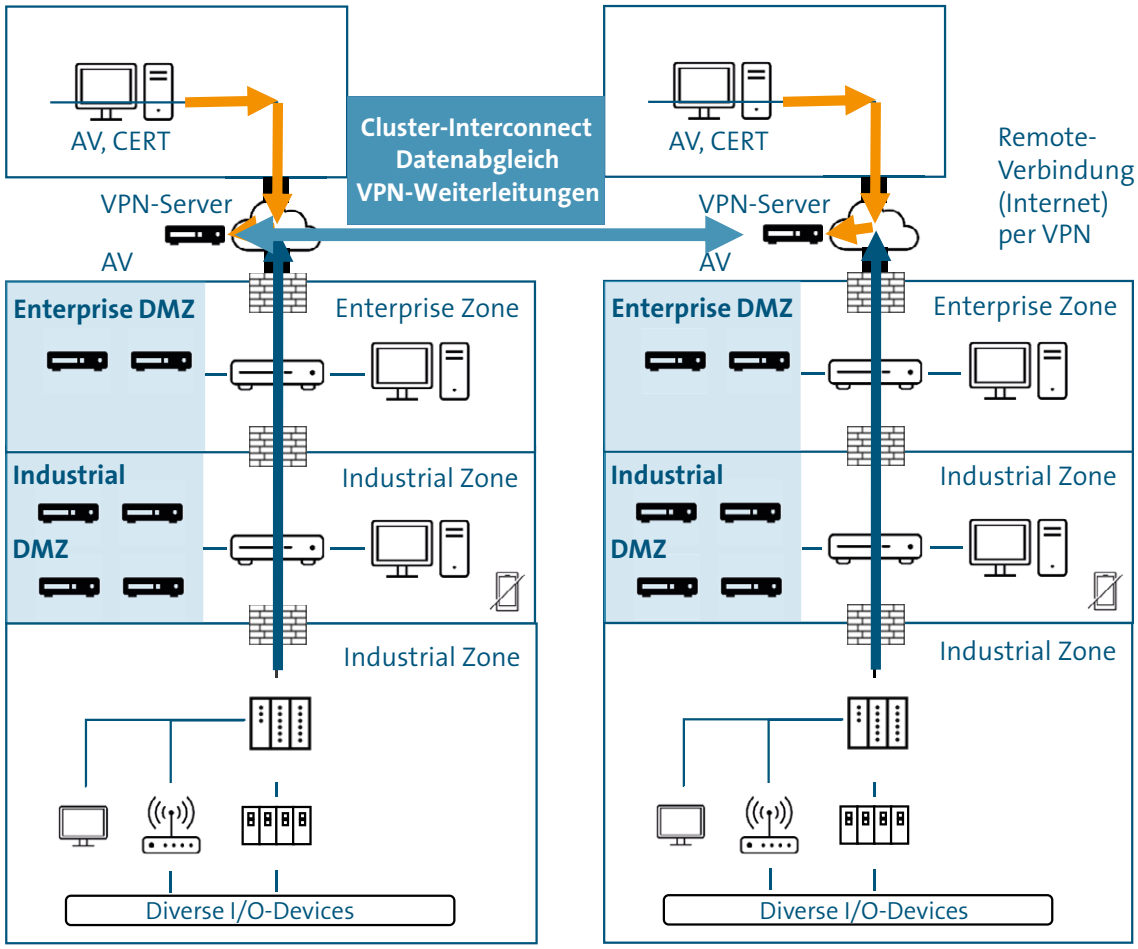
Bewertung des AK

- Pro:
  - Stand der Technik
  - Sehr gut skalierbar
  - Zentrale Wartung
  - Zentral Verwaltung von Benutzer und Maschinen
  - Temporäre Benutzer einfach

- Kontra:
  - Kontrolle über Dateitransfers?
  - Abhängigkeit vom Cloud-Anbieter (Verfügbarkeit)
  - Wie sehe die SLAs aus?
  - Datenschutzfolgeabschätzungen (Cyber-Gesetzte)

Abbildung 9

Rendezvous-System Softwarebasiert (Cloud)



Legende
AD: Active Directory, PKI: Public Key Infrastruktur
AV: Virenscanner, CERT: PKI-Zertifikat, DMZ: De-Militarized Zone

Mitarbeitende im Arbeitskreis „Sichere Fernwartung“

Dr.-Ing. Hans-Peter Bock	TRUMPF GmbH + Co. KG
Nils Bücker	Pilz GmbH & Co. KG
Dr. Walter Hafner	HighConsulting GmbH & Co. KG
Alexander Heckl	genua GmbH
Martin Holtmannspötter	Robert Bosch GmbH
Sören Jäckel	Phoenix Contact GmbH & Co. KG
Dr.-Ing. Lutz Jänicke	Phoenix Contact GmbH & Co. KG
Peer Ketterle	HAVER & BOECKER OHG
Maximilian Korff	SIEMENS AG
Markus Maier	genua GmbH
Marc Meyer	BSI
Sebastian Oudes	KRONES AG
Thomas Pilz	Pilz GmbH & Co. KG
Thomas Riegler	VDMA
Peter Teichrib	BEUMER GmbH & Co. KG
Daniel Tigges	BEUMER GmbH & Co. KG
Steffen Zimmermann	VDMA

Quellen und Verweise

[1] IEC 62443 Industrial communication networks – Network and system security
[2] [http://pera.net/]

Impressum

VDMA
Software und Digitalisierung

Lyoner Straße 18
60528 Frankfurt am Main

Kontakt
Thomas Riegler
Telefon +49 69 6603-1669
E-Mail thomas.riegler@vdma.org
Internet vdma.org/software-digitalisierung

Layout und Satz
VDMA DesignStudio

Bildquellen
Titelbild shutterstock

Stand
Dezember 2021

© Copyright by VDMA Software und Digitalisierung

VDMA
Software und Digitalisierung

Lyoner Straße 18
60528 Frankfurt am Main

Kontakt
Thomas Riegler
Telefon +49 69 6603-1669
E-Mail thomas.riegler@vdma.org
Internet vdma.org/software-digitalisierung

vdma.org/software-digitalisierung

Titelbild: shutterstock