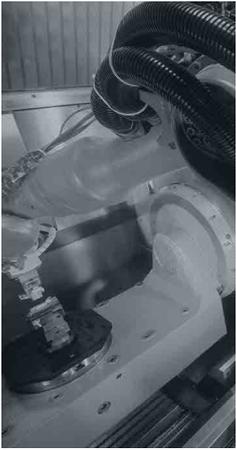




ViPNet 4.0

trifft Industrie

Smarte Systeme brauchen smarte
VPN-Lösungen



Von der Vision zur Realität

Bereits heute arbeiten viele Unternehmen der Fertigungsindustrie mit selbstregelnden Prozessen und greifen via Fernsteuerung auf Firmen- und Maschinendaten zu. Dennoch bestehen viele ungelöste Fragen sowohl technischer als auch strategischer Art. Das Thema Industrie 4.0 befindet sich noch am Anfang der Entwicklung und der Einsatz in der Produktionsindustrie zeigt nur ein Beispiel der vielfältigen Anwendungen der Smart Factories. Starre, unflexible Fertigungsanlagen verwandeln sich zu smarten Systemen mit effizienten und ressourcensparenden Strukturen. Die entscheidende Rolle bei diesen Strukturen spielt die Kommunikation, welche die Welten der Industrie und IT miteinander verschmelzen lässt.

Ein bewährtes VPN...

Für die komplette Neuausrichtung der industriellen Kommunikationswege ist Datensicherheit eine unerlässliche Voraussetzung. Sowohl alle Aspekte rund um Safety als auch der Schutz des wertvollen Unternehmens-Know-hows müssen garantiert sein. Ohne eine flächendeckende Absicherung der Kommunikationsstrecken kann die Vision nicht umgesetzt werden. Doch können klassische VPN-Lösungen mit ihren zu Grunde liegenden Verbindungs- oder Verschlüsselungsmethoden auch im Internet der Dinge bestehen?

...und die neuen Herausforderungen

Die industrielle Topologie der neuen Generation ist äußerst vielfältig und unterschiedlich. Smarte Systeme benötigen für die Kommunikation folglich entsprechend angepasste sichere Infrastrukturen.

In der Zukunft der Industrie 4.0 wird es schwierig, ...

- einen bestimmten LAN-Bereich zu definieren, um für diesen einen Perimeter-Schutz aufzubauen,
- eine Schnittstelle zwischen LAN und Außenwelt zu lokalisieren, um dort einen Zugriffskontrollpunkt zu platzieren und
- zwischen externen und internen Clients bzw. Objekten zu unterscheiden.

Klassische VPN-Technologien geraten unter den Aspekten Topologie und Connectivity schnell an ihre Grenzen. Darüber hinaus können grundlegende Algorithmen des PKI-Kryptosystems, auf welchem alle aktuellen VPN-Lösungen basieren, in Frage gestellt werden. Bei diesen Lösungen kann nur dann von einer vertrauenswürdigen Verbindung gesprochen werden, wenn die Authentizität der Root-Zertifikate garantiert ist. Doch ist dies bei den aktuellen Geschehnissen rund um Prism, Tempora und Co. auch der Fall?



Wie Visionen verwirklicht werden

Bereits vor zwei Jahrzehnten entwickelte Infotecs eine VPN-Technologie, welche keiner festen Server-Client-Abhängigkeit unterliegt und welche keine statische Anbindung an eine konkrete Netzwerktopologie verlangt. Die VPN-Software ViPNet ermöglicht die Verbindung beliebiger Netzwerkobjekte untereinander, unabhängig von deren Standort und IP-Adressierung. Basierend auf symmetrischen Schlüsseln passt sich ViPNet flexibel an die bestehende Topologie an und ist dabei unbegrenzt skalierbar.

Anders als bei der Public-Key-Infrastruktur (PKI) benötigt ViPNet keine Security Association, damit eine Verbindung zwischen zwei Objekten entsteht. Der unmittelbare Aufbau einer verschlüsselten Datenübertragung oder der Wiederaufbau einer abgebrochenen Verbindung ohne Zeitverzögerung sind weitere Vorteile der Technologie von Infotecs. Diese Eigenschaften stellen eine unabdingbare Voraussetzung für die Anwendung im industriellen Bereich dar. Bei einer Absicherung der Kommunikationswege muss zu 100% garantiert sein, dass technologische Prozesse nicht verändert oder gestört werden:

- kein Verlust von Paketen auf Netzwerkebene
- keine Verzögerung von Signalen
- kein Verlust der Gegenstelle beim Ortswechsel von Objekten

ViPNet basiert auf einem symmetrischen Schlüsselmanagement, welches von Grund auf keine Schwachstellen der PKI aufweist. Die Widerstandsfähigkeit der Verschlüsselung ist dementsprechend unabhängig von der Rechenkomplexität mathematischer Funktionen oder Vertrauenswürdigkeit der Zertifikate. Aufgrund dieser Eigenschaften grenzt sich die ViPNet Technologie klar von klassischen VPN-Lösungen ab und stellt sich den Anforderungen der Industrie 4.0.

ViPNet auf einen Blick

- Einfache Integration in beliebige Topologien
- Direkte verschlüsselte Punkt-zu-Punkt-Verbindungen
- Unbegrenzt skalierbar
- Transparent für alle Anwendungen und Dienste
- Soft- und hardwarebasierte Lösungen
- Echte symmetrische Verschlüsselung
- Keine Zertifikatsinfrastruktur notwendig



Industrie 4.0: Vielfalt der Kommunikationswege



Mit ViPNet können beliebige Kommunikationsstrecken zwischen mehreren Endpunkten simultan verschlüsselt werden. Die virtuelle Netzwerkstruktur aus hochsicheren Verbindungen passt sich dynamisch an die erforderlichen Prozesse an.

Kontakt

Infotecs Internet Security
Software GmbH
Oberwallstraße 24
10117 Berlin

Tel +49 30 206 43 66-0
Fax +49 30 206 43 66-66
Web www.infotecs.de
Mail info@infotecs.de