FROST & SULLIVAN

Absicherung des IoT auf Unternehmensebene

Herausforderungen und Lösungen zur Förderung des IoT-Wachstums in Unternehmen

Ein Frost & Sullivan White Paper

von Jason Reed, Senior Industry Analyst, Cybersecurity

EINFÜHRUNG IN DAS INDUSTRIAL INTERNET OF THINGS

Als Bestandteil des ständig größer werdenden Internet of Things (IoT) setzt das Industrial Internet of Things (IIoT) nicht auf Produkte für Konsumenten, wie beispielsweise Wearables und vernetzte Haushaltsgeräte, sondern auch auf vernetzte Geräte, die von Unternehmen zur Verschlankung von Geschäftsprozessen, zur Effizienzmaximierung sowie zur Kostensenkung genutzt werden. Neben Branchen, die traditionell eher mit IIoT verbunden sind, wird IoT zunehmend in sämtlichen vertikalen Industrien eingesetzt, unter anderem im Einzelhandel, im Finanzwesen, im Transportwesen, in der Telekommunikationsbranche und im Gesundheitswesen.

In der mit Herausforderungen verbundenen Welt des IoT herrscht häufig Verwirrung, wenn es um eine klare Abgrenzung zwischen Machine-to-Machine (M2M)-Diensten und dem IIoT geht. M2M wird definiert als der Transfer von Daten, die von einem an einer Anlage angeschlossenen Gerät über drahtgebundene oder drahtlose Kommunikationsnetze an eine Softwareplattform transferiert werden. Die Plattform überträgt diese Daten in für den Endnutzer nützliche Informationen. Während dies auf den ersten Blick sowohl die Beschreibung für M2M als auch für IIoT zu sein scheint, unterscheiden sich die beiden Lösungen in der Art und Weise, wie sie den Fernzugriff auf das Gerät bewerkstelligen. Häufig sind traditionelle M2M-Lösungen auf Point-to-Point-Kommunikation mittels Hardware-Modulen und entweder zellularen oder drahtgebundenen Netzwerken angewiesen. Im Gegensatz dazu verwenden IIoT-Lösungen IP-basierte Netzwerke zum Upload der Gerätedaten in eine Cloud oder auf eine Middleware-Plattform.

> IIoT-Lösungen nutzen IP-basierte Netzwerke für den Upload der Gerätedaten in eine Cloud oder auf eine Middleware-Plattform.

IIoT-Maschinen und Geräte sind unterschiedlich und vielfältig. Zu ihnen gehören Produktionsanlagen in traditionellen Industrieumgebungen, aber unter anderem auch die IT, die sich zunehmend in Kraftfahrzeugen und Sensoren durchsetzt. Diese Sensoren werden zunehmend in kritische Infrastrukturen zwecks vorausschauender Wartung und Überwachung integriert. Jedes Gerät in einer IIoT-Infrastruktur kann darüber hinaus verschiedene Betriebssysteme verwenden, darunter auch eine Linux-basierte Konfiguration, Windows 10 oder ein Betriebssystem, das speziell für das Gerät entwickelt wurde. Die Anzahl der Systeme, die eine einzelne IIoT-Infrastruktur unterstützen, kann die Absicherung des betreffenden Netzwerks zu einer enorm komplexen und zeitintensiven Aufgabe werden lassen.

Dennoch beschleunigt sich die Einführung von IIoT rapide, da Produktivität und Wirtschaftlichkeit im Unternehmen damit verbessert werden können. Tatsächlich prognostiziert eine Frost & Sullivan-Untersuchung, dass die zu erwartende Wertschöpfung durch die globale Umsetzung von IoT in allen öffentlichen und privaten Sektoren im Jahr 2022 bis zu 19 Billionen US-Dollar erreichen werde. Wirtschaftliche Führungskräfte dürfen den derzeitigen Wandel in Richtung IIoT nicht ignorieren, wenn sie in ihren jeweiligen Märkten weiterhin wettbewerbsfähig bleiben wollen. Aufgrund von Sicherheitsbedenken, die nicht unbegründet sind[1], zögern einige jedoch, das IIoT vorbehaltlos einzuführen. Trotz dieser Bedenken zeigen die Untersuchungen von Frost & Sullivan, dass das IIoT heute nicht mehr wegzudenken ist.[2] Welche Möglichkeiten gibt es also, von denen Unternehmen überall in den verschiedenen Bereichen vom IIoT profitieren können?

---

1 Krebs, B. (16. Oktober 2016). IoT Devices as Proxies for Cybercrime. Abgerufen von https://krebsonsecurity.com/2016/10/iot-devices-as-proxies-for-cybercrime/

2 Frost & Sullivan (2. Februar 2016). Internet of Things. Abgerufen von https://www.youtube.com/watch?v=71YV0xF-1Ic

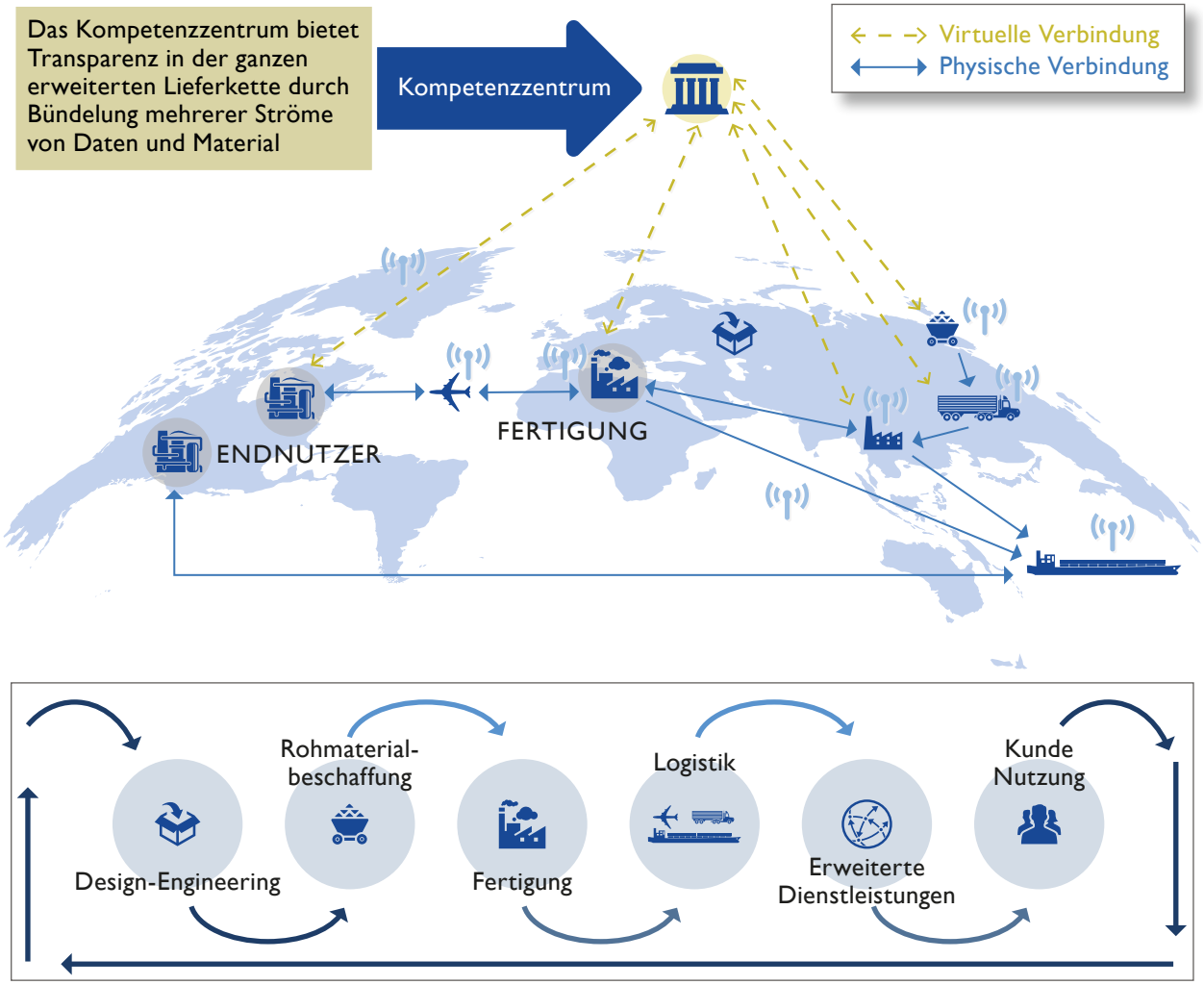
IIOT: PRAKTISCHE ANWENDUNGEN

Vom Fertigungsbereich über die Luft- und Raumfahrt sowie den Automobilbau bis hin zu Stromversorgungsnetzen und zur Gebäudeautomatisierung – die heutige Marktlandschaft ist voll von Beispielen für die IIoT-Nutzung. Nachstehend sind einige der vielen Beispiele für die IIoT-Anwendung in verschiedenen Branchen weltweit aufgeführt.

Connected Logistics: Neudefinition des Supply Chain Management

Durch das IIoT wird die Organisation und Überwachung von Lieferketten neu definiert. Mit vernetzten Kameras und Sensoren, die in den Geräten überall in der Lieferkette eingebettet sind, gewährt das IIoT den Unternehmen einen beispiellosen Einblick in sämtliche logistische Prozesse.

Abbildung 1: Connected Logistics Workflow



Quelle: Frost & Sullivan

In diesem Beispiel bezeichnet das Kompetenzzentrum eine zentralisierte Kommandozentrale, in der sämtliche Prozesse individuell oder als ganzheitliches System überwacht werden können, wobei Tausende von vernetzten Geräten auf jeder Stufe der Supply Chain Rückmeldungen in Echtzeit liefern. Das Feedback

wird durch Überwachung der Daten erzeugt, die zwischen der „virtuellen Verbindung“ der einzelnen Geräte oder der Verbindung zwischen Endpunkten ausgetauscht werden. Der verbesserte Einblick, den die zentrale Steuerung über alle logistischen Prozesse bietet, erhöht die Effizienz und den Output. Gleichzeitig wird es dadurch einfacher, Bereiche zu identifizieren, in denen es zu Problemen oder Verzögerungen in der Lieferkette kommen kann. Häufig wird bei diesem Prozess die Notwendigkeit übersehen, bei jedem Gerät für eine unterbrechungsfreie und sichere virtuelle Verbindung zu sorgen, da eine Störung an irgendeinem Endpunkt einen Welleneffekt auslösen kann, der sich auf die gesamte Lieferkette auswirkt. Die Auswirkungen könnten von geringfügigen Produktivitätsverlusten bis – im Falle einer schwerwiegenden Manipulation der virtuellen Verbindungen – zu einem kompletten Stillstand der Lieferkette führen, der solange andauert, bis die manipulierte virtuelle Verbindung identifiziert und das Problem behoben werden kann.

Kritische Infrastruktur: IIoT ermöglicht vorausschauende Instandhaltung

Mittlerweile ist es in verschiedenen Branchen gängige Praxis, vernetzte Sensoren während der Entwurfsphase in die Infrastruktur einzubetten[3] und nirgendwo ist diese Entwicklung wichtiger als im Zusammenhang mit der Wartung kritischer Infrastruktur, die den globalen Strom von Kapital, Gütern und Dienstleistungen ermöglicht. Versorgungsunternehmen beispielsweise setzen nun seit einiger Zeit Predictive Analytics als Mittel zur Überwachung ihrer Technologien ein.[4] Mit dem voraussichtlich zunehmenden Einsatz von IIoT-fähigen Geräten in den kommenden Jahren werden auch die vernetzten Geräte immer ausgereifter werden. Das Aufkommen von Geräten mit Künstlicher Intelligenz könnte dazu führen, dass routinemäßige Wartungsaufgaben von dem Gerät selbst und ohne menschliche Interaktion durchgeführt werden. Außerdem könnten die Betreiber auf potenzielle Wartungsprobleme aufmerksam gemacht werden. Das Aufkommen von KI-fähigen IIoT-Geräten wird wahrscheinlich tiefgreifende Auswirkungen auf die Betriebsabläufe von Organisationen mit kritischer Infrastruktur haben.

Vorsprung für Einzelhändler: Verbesserung des Kundenerlebnisses mit IIoT-fähigen Geräten

Amazons Bestreben, im Rahmen des Lieferservice unbemannte Fluggeräte (oder besser gesagt Drohnen) einzusetzen, ist bereits Thema vieler Debatten. Die jüngsten Entwicklungen, darunter ein in Großbritannien begonnener geheimer Testlauf [5], deuten jedoch darauf hin, dass diese Technologie kurz vor der Markteinführung steht. Mit angemessener regulatorischer Unterstützung wird Amazon in der Lage sein, einige Waren innerhalb von 30 Minuten nach ihrer Bestellung an Konsumenten auszuliefern.

Für schwerere Produkte hat Embark[6], ein Start-up-Unternehmen für fahrerlose Fahrzeuge, mit Auslieferungen in seinen selbstfahrenden Sattelzügen begonnen.[7] Dies markiert eine neue Phase in der bodengebundenen Logistik, denn diese autonomen Fahrzeuge werden sich voraussichtlich mit der Zeit weiter verbreiten.

---

3 IIoT Viewpoints. (30. Januar 2017). Ambyint CEO on Analytics for Critical Infrastructure. Abgerufen von https://industrial-iot.com/2017/01/ambyint-ceo-on-analytics-for-critical-infrastructure/

4 Custeau, K. (2. Januar 2017). Utilities Squeeze Assets with Predictive Analytics. Abgerufen von https://blog.schneider-electric.com/utilities/2017/01/02/utility-asset-management/

5 Amazon.com. (7. Dezember 2016). First Prime Air Delivery – Fully Autonomous – No Human Pilot. Abgerufen von https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011

6 http://embarktrucks.com/

7 Davies, A. (13. November 2017). Self-Driving Trucks Are Now Delivering Refrigerators. Abgerufen von https://www.wired.com/story/embark-self-driving-truck-deliveries/

Die Gefahr von „Alles vernetzt“

Während Logistik, kritische Infrastrukturen, Einzelhandel und nahezu sämtliche vertikale Industrien von IIoT profitieren können, bringt das Aufkommen von „alles vernetzt“ einige nicht unerhebliche Herausforderungen mit sich. Eine wesentliche Herausforderung dabei ist die Gewährleistung einer sicheren Kommunikation zwischen Geräten und ihren Unternehmen, da ein Datenangriff oder eine Sicherheitslücke katastrophale Folgen für die Sicherheit, die Ertragssituation oder beides haben könnte.

NOTWENDIGKEIT DER IIOT-ABSICHERUNG SEITENS DER UNTERNEHMEN

Die Absicherung des IIoT ist keine einfache Aufgabe, da Angreifer und böswillige Akteure ständig darum bemüht sind, die Sicherheitsmaßnahmen zu umgehen, die von vornherein fest in die Geräte integriert sind, die das IoT bilden. Es wird zunehmend offensichtlich, dass die Sicherheit der Geräte einfach nicht ausreichend ist[8], um massive Datenangriffe zu verhindern. Tatsächlich gab es bereits zahlreiche Vorfälle, die die Unzulänglichkeit der in den unterschiedlichsten Branchen vorhandenen Sicherheitsmaßnahmen demonstrieren.

Intelligente Messgeräte 2009 – 2012

Intelligente Messgeräte wurden entwickelt, um die Effizienz im Zusammenhang mit dem Energieverbrauch zu maximieren und den Energieversorgern die Möglichkeit zu geben, für den Verbrauch zu verschiedenen Tageszeiten unterschiedliche Tarife zu berechnen. Zusätzlich ermöglichen intelligente Messgeräte den Versorgungsunternehmen die Fernüberwachung des Energieverbrauchs. Wie Puerto Rico[9] jedoch im Jahr 2009 entdeckte, gelang es Angreifern mit relativ geringen Fachkenntnissen, intelligente Messgeräte zu hacken, was im Endeffekt einen Energiediebstahl im Wert von über 400 Millionen US-Dollar ermöglichte. Das FBI, das den Angriff entdeckte, war ungewöhnlich offen mit seiner Einschätzung und sagte: „Das FBI stellt mit mittlerer Zuversicht fest, dass sich diese Art von Betrug mit zunehmend verbreiteter Nutzung intelligenter Stromnetze im ganzen Land ebenfalls weiter ausbreiten wird. Grund dafür sind die Leichtigkeit des Eindringens und die wirtschaftlichen Vorteile sowohl für die Hacker als auch für die Stromkunden.“

Kraftfahrzeuge für Verbraucher 2015

Sogar Fahrzeuge, die einen Fahrer brauchen (im Gegensatz zu autonomen Fahrzeugen) sind anfällig für Angriffe, da viele ihrer Systeme und Funktionen zunehmend auf IoT-Verbindungen angewiesen sind. Im Jahr 2015 wurden auf Fahrzeuge von BMW und Jeep erfolgreiche Angriffe ausgeführt, bei denen die Hacker in der Lage waren, BMW-Server zu imitieren und per Fernzugriff die Fahrzeuge zu öffnen und zu schließen. Im Fall von Jeep demonstrierten zwei Sicherheitsforscher einem Reporter, wie sie sämtliche Fahrzeugsysteme aus der Ferne kontrollieren konnten,[10] was zu einem Rückruf von 1,5 Millionen Fahrzeugen führte.

---

8 Accenture. (2015). Security for the Internet of Things: A Call to Action. Abgerufen von https://www.accenture.com/ca-en/insight-security-internet-of-things

9 Krebs, B. (12. April 2012). FBI: Smart Meter Hacks Likely to Spread. Abgerufen von https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

10 Greenburg, A. (21. Juli 2015). Hackers Remotely Kill a Jeep on the Highway—With Me in It. Abgerufen von https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Einzelhandelsunternehmen 2013

Im Jahr 2013 wurde das Unternehmen Target Opfer eines massiven Datenangriffs, bei dem Hacker Malware nutzten, um in das System eines Klimatechnik-Unternehmens einzudringen, das bei dem Einzelhandelsunternehmen unter Vertrag stand. Dies führte zum Diebstahl der persönlichen Daten von über 70 Millionen Kunden. Eine Untersuchung von Sicherheitsexperten bei Verizon offenbarte: Sobald die Cybergegner in Targets Netzwerk waren, konnte sie nichts mehr davon abhalten, sich direkten und vollständigen Zugang zu jeder Registrierkasse in jedem Target-Store in Nordamerika zu verschaffen.[11]

Stromnetz 2016

Während des andauernden Konflikts in der Ukraine verschafften sich Hacker per Remote Access Zugriff auf das Stromnetz in der Ukraine[12] und unterbrachen die Stromversorgung von über 200.000 Kunden. Der Angriff ermöglichte den Hackern die Installation von benutzerdefinierter Firmware, die Löschung von Master Boot Records und die Abschaltung des Telefonverkehrs.

Man-in-the-Middle-Angriffe

Eines der Hauptprobleme bei der Sicherung des IIoT ist die als Man-in-the-Middle-Angriff bezeichnete Angriffsstrategie von Hackern. In diesem Fall fängt der Angreifer die Kommunikation zwischen zwei Systemen ab, indem er sich als ursprünglicher „Absender" ausgibt. Der Angreifer kann den Empfänger anschließend „austricksen", sodass dieser glaubt, er erhalte nach wie vor eine seriöse Nachricht. Innerhalb des IIoT könnte ein solcher Angriff beispielsweise gefälschte Temperaturdaten enthalten, um eine Maschine zur Überhitzung zu zwingen[13] und somit dem Unternehmen schweren Schaden zufügen.

Diese Art Angriff könnte besonders gefährlich im Fall eines autonomen Fahrzeugs sein, wenn sich ein Angreifer als der Server ausgibt, der die Drohne oder das Bodenfahrzeug lenkt. Damit könnte er einen möglicherweise enormen finanziellen Schaden oder Sachschaden verursachen. Klar ist, dass Unternehmen bei der Abstimmung des IIoT-Einsatzes der Absicherung ihrer Netzwerke die gleiche Beachtung schenken müssen.

ABSICHERUNG SÄMTLICHER GERÄTE AUF ALLEN PLATTFORMEN UND AUTHENTIFIZIERUNGSVERFAHREN

Um eine Gefährdung der Geräte oder eine Störung im IIoT zu verhindern, ist es unabdingbar, dass in den Planungsphasen einer Implementierung erweiterte Sicherheitsmaßnahmen fest in die Infrastruktur integriert werden. Die nachträgliche Implementierung erweiterter IIoT-Sicherheitsmaßnahmen ist kostspielig, ineffizient und mühsam.

Die effektivste Methode zur Verhinderung eines Man-in-the-Middle-Angriffs ist beispielsweise die Implementierung eines verschlüsselten Netzwerks als primäres Verbindungsmittel für die Kommunikation zwischen virtuellen Verbindungen in einer IIoT-Infrastruktur. Der verschlüsselte Kommunikationstunnel zwischen zwei oder mehr Geräten dient der Absicherung sämtlicher Daten, die den Tunnel passieren. Wenn

11 Krebs, B. (21. September 2015). Inside Target Corp., Days After 2013 Breach. Abgerufen von https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

12 Zetter, K. (3. März 2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Abgerufen von https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

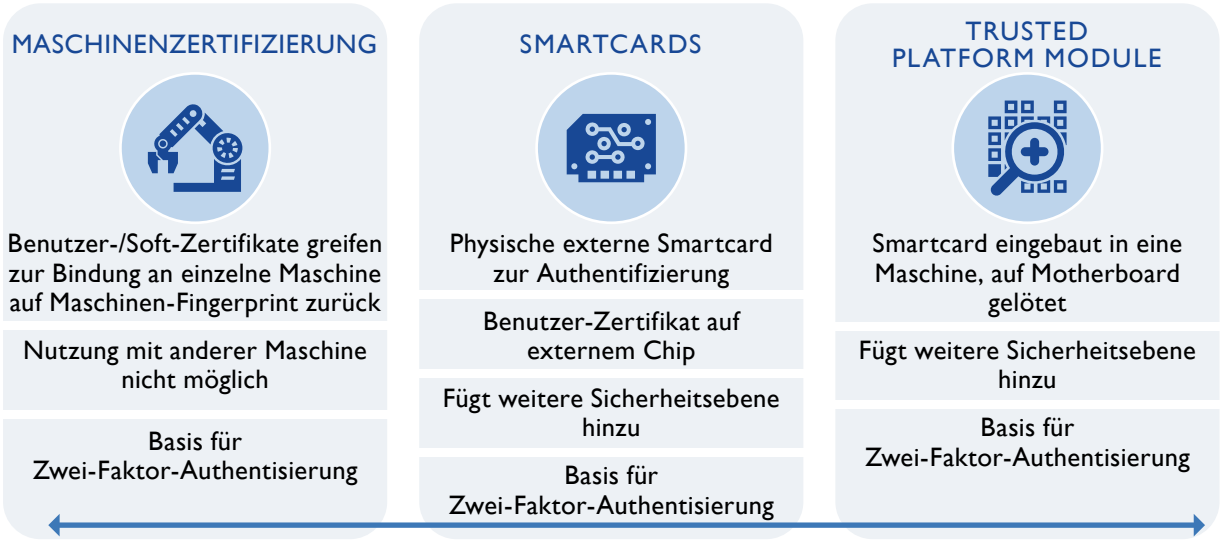
13 Simko, C (26. Februar 2016). Man-in-the-Middle Attacks in the IoT. Abgerufen von https://www.globalsign.com/en/blog/man-in-the-middle-attacks-iot/

die Kommunikation verschlüsselt ist, könnte ein potenzieller Man-in-the-Middle-Angreifer die von ihm beobachteten Daten nicht lesen.

Damit dies erreicht wird, ist ein digitales Zertifikat für die Lösung notwendig. Das Gleiche gilt auch für sämtliche Geräte, mit denen die Lösung kommuniziert. Bei den Datenströmen zwischen den Geräten werden die erforderlichen Schlüssel per Handshake-Prozess ausgetauscht und sämtliche Daten bleiben verschlüsselt bis sie ihre Zieladresse erreicht haben.

In jedem Schritt des Authentifizierungsverfahrens im Rahmen eines VPN-Sicherheitssystems für IIoT werden Zertifikate genutzt. Einige zur IIoT-Absicherung angewendete Authentifizierungsverfahren werden in Abbildung 2 dargestellt.

Abbildung 2: Sicherheitszertifizierung im VPN



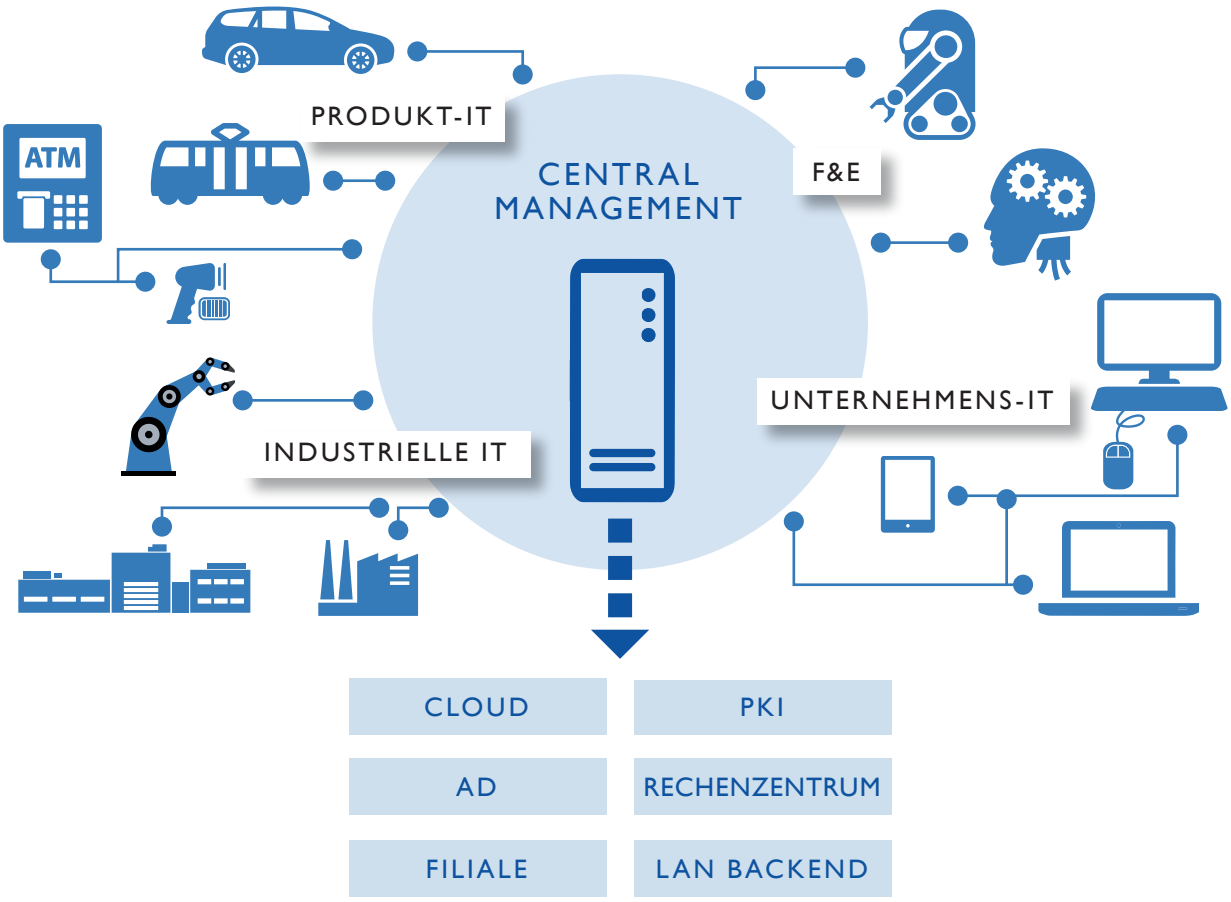
Quelle: Frost & Sullivan

Eine Authentifizierung auf jeder Stufe entlang des verschlüsselten Kommunikationswegs ist unerlässlich. Damit wird sichergestellt, dass das IIoT sicher und resistent gegen die oben skizzierten Arten von IoT-Gefährdungen ist, die die Unternehmensprozesse erheblich beeinträchtigen können. Die meisten Unternehmen verfügen jedoch nicht über hauseigenes Know-how, um eine angemessene Absicherung ihres IIoT zu gewährleisten. Zur Abmilderung der Sicherheitsrisiken im IIoT empfehlen Frost & Sullivan deshalb einen VPN MSSP-Experten.

IIOT-LÖSUNGEN VON NCP ENGINEERING

NCP, ein Anbieter von Secure Communications Software, hat Best-Practice-Lösungen für Kommunikation und Sicherheit in sein Angebot für IIoT integriert. Die NCP-Lösung besteht aus „IIoT-Gateways“ und „IIoT-Clients“, beides Software-Komponenten für verschiedene Betriebssysteme, darunter Linux und Windows 10 sowie spezifische eingebettete Betriebssysteme in IIoT-Geräten. Aufgrund ihres zentralen Management Systems hat sich die Lösung, die sowohl als klassische als auch als IIoT-VPN-Verbindung funktioniert, dahingehend weiterentwickelt, dass sie die Lücke zwischen der Produktions-IT in Geräten und Maschinen und der operativen IT schließt. Traditionell werden diese beiden IT-Systeme häufig nicht unter derselben Management-Plattform betrieben, was die Navigation zwischen den beiden umständlich und schwierig macht.

Abbildung 3: NCP VPN-Lösung für IIoT



Quelle: NCP engineering

Mit Zertifikaten, die in jeder Phase ihrer IIoT-Lösung ausgetauscht werden, dreht sich das System um leichtgewichtige, auf Endgeräten installierte IIoT-Clients, zentrale Gateways und eine zentrale Management-Komponente. Der Prozess beginnt mit Clients, die direkt auf Systemen oder Maschinen installiert werden, während das IIoT-Gateway die Verschlüsselung übernimmt und sicherstellt, dass die Zertifizierungen von jedem Gerät den Standard einer vertrauenswürdigen Zertifizierungsstelle entsprechen. Zusätzlich entspricht die verschlüsselte Kommunikation den Anforderungen der Suite B Cryptographie, um das höchste Verschlüsselungsniveau zu gewährleisten.

Ein maßgeblicher Unterschied bei NCP Secure Communications ist die Management-Komponente, die einen Einblick in sämtliche Komponenten bietet. Dabei handelt es sich um ein zentrales Managementsystem, das für die Verwaltung der Clients und der Gateways in der IIoT-Architektur zur Verfügung steht. Es ermöglicht eine vollständige, zentrale Konfiguration der IIoT-Komponenten, einschließlich der Maschinenzertifikate. Diese Art von ganzheitlicher Lösung, die einen zentralen Einblick in das gesamte IIoT bietet, ermöglicht Administratoren die proaktive Verwaltung ihrer IIoT-Clients und ihrer IIoT-Gateways innerhalb derselben Netzwerkarchitektur.

ZUSAMMENFASSUNG

Während eine Verschlüsselungslösung für IIoT-Netzwerke ein wesentlicher erster Schritt ist, verbessern Unternehmen wie NCP engineering das Nutzererlebnis, indem sie nicht nur als sicherer Kommunikationsanbieter agieren, sondern auch als eine Art Systemintegrator, der die bestehende IIoT-Infrastruktur in eine zentrale Kommandozentrale einbinden kann. Ein solches System, das eine zentrale Management-Komponente beinhaltet, schlägt praktisch eine Brücke zwischen der Corporate-IT, der Produkt-IT und der Industrial-IT. Dies verbessert das Nutzererlebnis, indem es den Integrationsprozess vereinfacht und einen guten Einblick in das gesamte IIoT-System ermöglicht. Diese Art von Technologie sollte denjenigen, die der Sicherheit von IIoT misstrauen, ein sicheres Gefühl geben und außerdem den Übergang von einem traditionellen Organisationsprozess zu einem IIoT-basierten Workflow erleichtern.

FROST & SULLIVAN

NEXT STEPS

Vereinbaren Sie einen Termin mit einem Mitarbeiter unseres globalen Teams, um unseren visionären Führungsstil kennenzulernen und Ihre Ideen, Chancen und Herausforderungen in die Diskussion einzubringen.

Möchten Sie mehr über die Themen erfahren, die in dem vorliegenden Whitepaper erläutert wurden? Rufen Sie uns unter +49 (0)69 77 03 30 an und nennen Sie das Whitepaper, an dem Sie interessiert sind. Ein Analyst wird daraufhin Kontakt mit Ihnen aufnehmen.

Besuchen Sie unsere Webseite **zur digitalen Transformation**.

Nehmen Sie an einer unserer **Growth Innovation & Leadership (GIL)-Veranstaltungen teil** um verborgene Wachstumschancen zu entdecken.

FRANKFURT
Clemensstraße 9
60487 Frankfurt a.M.
Tel. +49 (0)69 7 70 33-0

SILICON VALLEY
3211 Scott Blvd, Suite 203
Santa Clara CA, 95054
Tel: +1 650 475 4500

LONDON
Building 5
566 Chiswick High Road
London W4 5YF
Tel +44 (0)20 8996 8500

+49 (0)69 7 70 33-0
enquiries@frost.com
www.frost.com

Frost & Sullivan, die Growth Partnership Company, arbeitet mit Kunden zusammen, um visionäre Innovationen umzusetzen, mit denen sich globale Herausforderungen bewältigen und damit verbundene Wachstumschancen nutzen lassen, die über den Erfolg oder Misserfolg heutiger Marktteilnehmer entscheiden. Seit über 50 Jahren entwickeln wir Wachstumsstrategien für zukunftsorientierte Global 1000-Unternehmen, öffentliche Behörden und Investoren. Ist Ihr Unternehmen bereit für die nächste Welle an branchenweiter Konvergenz, bahnbrechenden Technologien, erhöhtem Wettbewerbsdruck, Megatrends, neuen Best Practices, veränderter Kundendynamik und aufstrebenden Schwellenländern?

Wenn Sie Informationen zu Genehmigungen wünschen, schreiben Sie an:
Frost & Sullivan
3211 Scott Blvd
Santa Clara, CA 95054