Online Sicherheit für Maschinen und Anlagen

Gesicherte Punkt-zu-Punkt Verbindungen bei der Datenkommunikation

© *pixabay/geralt*

Virtual Private Networks - VPNs - sind für die IT-Sicherheit von Unternehmensnetzwerken nicht mehr wegzudenken. Fernzugriffe unterschiedlichster Couleur bestimmen in weiten Teilen die heutige Datenkommunikation im Netz – sei es die sichere, weltweite Vernetzung von Fachabteilung oder der Zugriff des Außendienstmitarbeiters auf das Unternehmensnetzwerk, um Maschineneinstellungen zu ändern. Remote Zugriff via VPN ist ein gesetzter Standard.

Bei einer VPN-Verbindung werden die Daten zwischen zwei oder mehreren Computern im Internet über einen abgesicherten Tunnel übertragen. Über die gesicherte/getunnelte Verbindung können die Rechner aufeinander zugreifen, dabei entsteht der Eindruck, als ob sie sich in einem lokalen Netzwerk befänden.

Unterschiedliche VPN-Technologien

Grundsätzlich gilt, dass es verschiedene VPN-Technologien mit unterschiedlichen Verschlüsselungs-Typen gibt. Das Point-to-Point Tunneling Protocol (PPTP) ist beispielsweise sehr schnell, aber weist im Vergleich zu Protokollen, die auf SSL/TLS setzen wie IPSec und OpenVPN, Sicherheitsschwachstellen auf. Bei TLS-basierten VPNs kommt es auf die Art des Verschlüsselungsalgorithmus und die Schlüssellänge an. Und OpenVPN unterstützt viele Ziffern-Kombinationen, Key-Exchange-Protokolle und Hashing-Algorithmen. In der Regel verwendet OpenVPN die AES-Verschlüsselung mit RSA Key Exchange und SHA Signaturen. Dabei wird empfohlen eine AES-256 Encryption zu verwenden und einen RSA-Key mit einer Länge von mindestens 2048 Bits zu verwenden. In Bezug auf die SHA Signatur gilt die SHA-2 cryptograpic hash function besser, als die SHA-1.

Verschlüsselung und Geschwindigkeit

Vor diesem Hintergrund ist es wichtig zu berücksichtigen, dass je stärker eine Verschlüsselung ist, desto massiver wirkt sich dies auf die Verbindungsgeschwindigkeit aus. Daher ist die Wahl der VPN-Technologie wesentlich abhängig davon, welche Daten über die Verbindung in welcher Geschwindigkeit und mit was für einem Sicherheitsstandard ausgetauscht werden sollen.

Die Sicherheitsbedürfnisse von Anwendern, gerade in Zusammenhang mit kritischen Daten, wie z. B. bei Energieversorgern, großen Industrieunternehmen oder Gesundheitseinrichtungen sind dementsprechend hoch. Daher wird deutlich, dass VPNs nicht nur die Daten zwischen LAN und Rechner schützen, sondern auch eine erhebliche Rolle für das Industrial Internet of Things (IIoT) spielen.

Schwachstelle IIoT

Im IIoT müssen verschiedenste Komponenten miteinander kommunizieren, klingt erst einmal nicht aufregend, aber oft handelt es sich bei IIoT Produkten um kleine, nicht sehr leistungsstarke „Dinge“, die leider eher mäßig mit Sicherheitsfunktionen ausgestattet sind. Und gerade da wird es spannend – Sensoren, TAGs oder andere Datensammler mit TCP/IP Netzwerkstack sehen im Internet genauso aus wie andere Geräte und ein offener Port, ist immer eine einladende Schwachstelle. Zahlreiche Programme machen den ganzen Tag nichts anders, als das weltweite Netz nach solchen Schwachstellen abzusuchen, um sich dann der Daten zu bemächtigen oder gar schlimmeres in Gang zu bringen.

Schutz ist notwendig

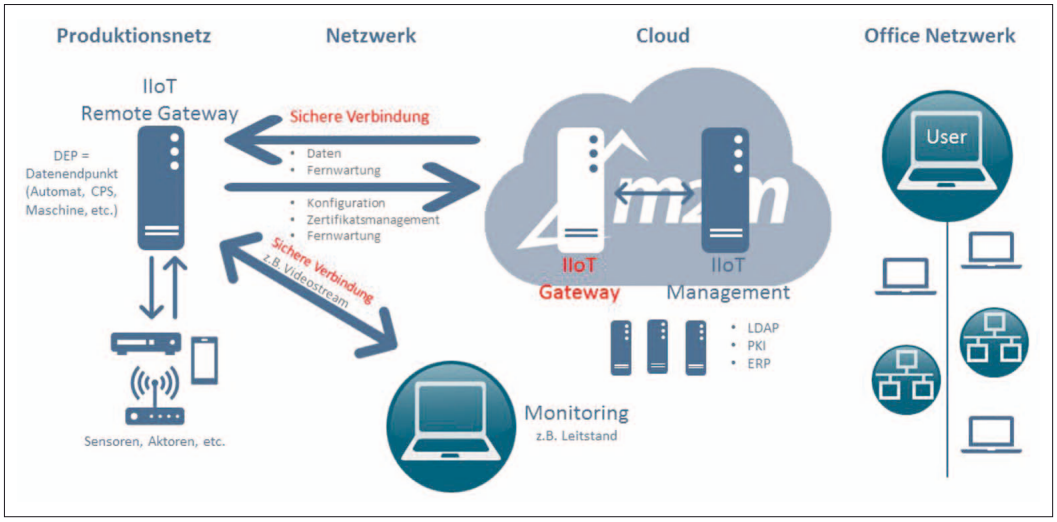
Starke Passwörter oder andere Möglichkeiten der Authentifizierung sind das Mindeste, was gewerbliche Anwender einsetzen sollten. Effizienter und vor allem sicherer ist dagegen ein Internetzugang via Virtual Private Network (VPN) – sie sind derzeit die sicherste Lösung. Der VPN-Client baut eine verschlüsselte Verbindung mit der Gegenstelle auf und gewährleistet eine sichere Datenübertragung, die von außen nicht mitgelesen werden kann. Verschlüsselte VPN-Clients sind in der Lage unterschiedliche Topologien, Architekturen und Betriebssysteme aus dem industriellen Umfeld sicher miteinander zu verbinden und passende Schnittstellen zur traditionellen IT-Umgebung zu offerieren. Der Einsatz von VPN-Verbindungen im industriellen Umfeld sind mittlerweile in Standards zur Informationssicherheit fest definiert (NIST 800-82/ ISO-27000). VPNs gelten als unerlässliche Sicherheitsmaßnahme, um Kontrollzugänge/Ports zu schützen. Dies gilt im Besonderen für Endgeräte beim Kunden, die vom Hersteller aus der Ferne gewartet und überwacht werden.

Vielfalt der VPN-Protokolle

VPN-Verbindungen verwenden immer eine verschlüsselte Tunnel-Verbindung. Es gibt verschiedene Protokolle, wie eine solche VPN-Verbindung aufgebaut werden kann. Diese Protokolle stellen sicher, dass die übermittelten Daten sicher bleiben und nicht von anderen gelesen werden können. Dabei haben sich mittlerweile einige Verbindungsprotokolle etabliert.

PPTP (Point to Point Tunneling Protocol) ist eines der ersten Pro-

Autor:
Karin Reinke-Denker M.A.
m2m Germany GmbH
info@m2mgermany.de
www.m2mgermany.de



Gesicherte Punkt-zu-Punkt Verbindungen via VPN (© m2m Germany)

tokolle, das weitverbreitet genutzt wurde. Eingesetzt wird es in der Regel, wenn Geschwindigkeit wichtiger ist als Sicherheit, da PPTP einige, kleinere Sicherheitslücken aufweist. Wer dagegen auf Sicherheit setzt, nutzt in erster Linie OpenVPN. Es ist eines der am häufigsten verwendeten Protokolle. Es handelt sich um ein Open-Source-Protokoll, das Verschlüsselung auf der Grundlage der Protokolle OpenSSl und SSLv3/TLSv1 verwendet. Die meisten VPN-Anbieter unterstützen OpenVPN und es ist für viele verschiedene Plattformen verfügbar (z. B. Windows, Mac (OSx), Android, iOS, Linux, Router).

IPSec/L2TP

Alternativ dazu bietet sich das IPSec/L2TP Protokoll an, es kombiniert IPsec für die Verschlüsselung von Daten mit L2TP für die sichere Verbindung. Die meisten Betriebssysteme beinhalten IPsec/L2TP und sind eine akzeptable Alternative, wenn OpenVPN nicht verfügbar ist. Im Fokus für Anwendungen via Smartphone, die regelmäßig zwischen Wifi-Netzen und öffentlichen Netzen wechseln, bietet sich IKEv2 an. IKEv2 ist ein auf IPSec basierendes Protokoll. Dieses Protokoll kann sich schnell mit Netzwerken verbinden und zwischen Netzwerken umschalten. Dies macht es zu einer idealen Wahl für Smartphones.

Newcomer unter den VPN-Protokollen ist das WireGuard Protokoll, das sich noch ganz am Anfang befindet. WireGuard ist noch in der Entwicklungsphase und ist daher eher als ein experimentelles Protokoll anzusehen. Es läuft auf einem Linux-Kernel und zielt darauf ab, noch bessere Leistungen als OpenVPN und IPsec zu erreichen. Laut den Entwicklern von WireGuard soll der effiziente und kompakte Code, kombiniert mit der Tatsache, dass WireGuard sich in den Kern des Linux-Betriebssystems einfügt, bedeuten, dass das Protokoll zu hohen Geschwindigkeiten führen wird. Klar ist, dass sichere Verbindungen im IoT und IIoT gefragter sind als je zuvor.

Client oder Gateway – das ist hier die Frage

Allerdings ist der VPN-Client nur dann die Lösung, wenn das IoT- bzw. IIoT-Gerät die notwendigen Mindestanforderungen auf der Hardwareseite für eine VPN-Verbindung erfüllt. Ein VPN-Client benötigt ein Linux oder Windows-Betriebssystem und ausreichende Ressourcen – teilweise benötigen VPN-Clients bis zu einigen MByte RAM und den entsprechenden Linux-Kernel. Aufgrund der Tatsache, dass es gerade bei IIoT Geräten darum geht, möglichst klein und stromsparend zu agieren, geht dies oft zulasten der CPU-Leistung und aufwendige Sicherheitsfunktionen bleiben auf der Strecke. Können die Ansprüche des VPN-Clients auf Hard- oder Softwareseite nicht erfüllt werden, können IIoT-Gatways die Alternative sein.

VPN-Clients via IIoT Gateways – von LTE bis LoRa

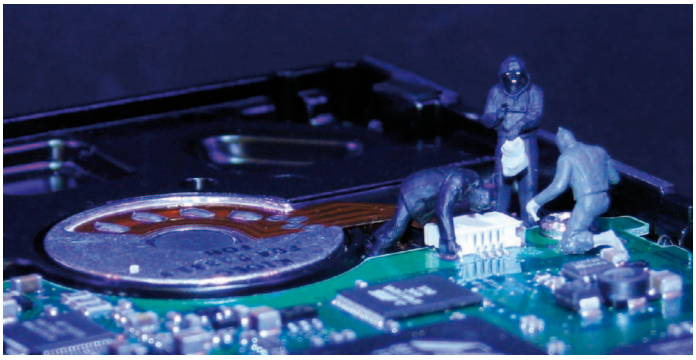
Bislang spielten IIoT-Gateways in Bezug auf die Anbindung von älterer Hardware ohne Netzschnittstelle eine Rolle, um sie an Modbus oder TCP/IP anzubinden, Signal- und Medien-Konvertierungen vorzunehmen oder einfache Logikverknüpfungen zu erstellen. IIoT-Gateways können aber auch als VPN-Client eingesetzt werden, um die zu geringe Rechenleistung des eigentlichen IIoT-Gerätes auszugleichen. Denn die Gateways selbst haben ausreichend Rechenleistung und sind eher eine komplette Computing-Plattform, als nur ein schlichtes Gateway. Auf einem IIoT Gateway kann problemlos eine für industrielle Anwendungen taugliche VPN-Software installiert werden, die wiederum alle gesammelten Daten von Sensoren und Aktoren ab dem Ausgang des IIoT-Gateways sicher verschlüsselt – so ist es möglich, fehlende Sicherheitsfunktion oder andere Beschränkungen der „kleinen“ IIoT-Devices zu umgehen und trotzdem eine sichere VPN-Verbindung aufzubauen.

Oft verfügen IIoT-Gateways über eine Cloud-Ready Funktion, d. h. sie sind bereits mit Clients für diverse Cloud-Dienste ausgestattet und können drahtgebunden oder drahtlose Netze anbinden; nebst Firewall und anderer Sicherheitsmechanismen.

VPN-Management für mehr Sicherheit

VPN-Services für Industrieumgebungen gibt es von verschiedenen Anbietern und sie sind in der Regel einfach zu konfigurieren. Die Grundfunktionen bei einem Virtual Private Network sind relativ einfach, komplex ist nur deren Management. Bei stationären IIoT-Geräten spielen Faktoren wie wechselnde Verbindungsmedien und diverse Betriebssysteme keine große Rolle, aber die Erstkonfiguration, Zertifikate, Rechtevergabe und Passwörter stellen Herausforderungen an die Verwaltungsoberfläche.

Profis unterstützen

Stehen im Anwender-Unternehmen die notwendigen Kenntnisse nicht zur Verfügung, um komplexe Strukturen und/oder erhöhte Sicherheitsanforderungen abzudecken, empfiehlt es sich mit einem Lösungspartner zusammen zu arbeiten. Dieser bietet in der Regel entsprechende Hard- und Software an, sowie den passenden VPN-Service. Dabei kann es sich um Einzelzugänge oder Bundle-Pakete für bis zu 100 Zugängen handeln oder aber auch bis zur High-end Lösung reichen, mit beliebig vielen VPN-Verbindungen.

Eine solche High-end Lösung stellt eine eigene Instanz da, die beim Kunden selbst betrieben wird, sie läuft entweder im Rechenzentrum des Kunden oder bei einem Internet-Serviceprovider. Wenn Sicherheit an erster Stelle steht, ist es sinnvoll kompetente Partner mit einem Full-Service Angebot zu involvieren – so können eine sichere Anbindung von Maschinen und Anlagen mit allen Remotemanagement Features, sowie IIoT Szenarien wie „vom Sensor bis in die Cloud“ abgedeckt werden. ◄