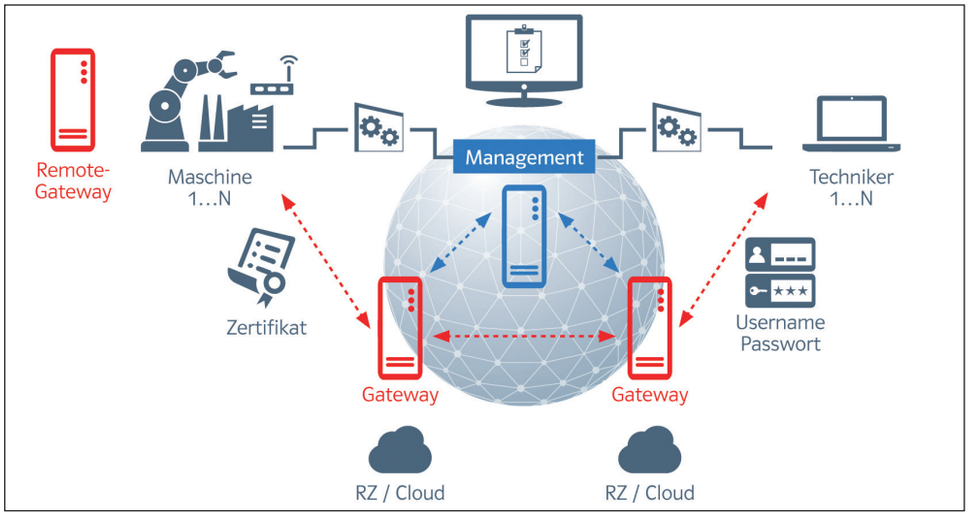
NCP SECURE COMMUNICATIONS

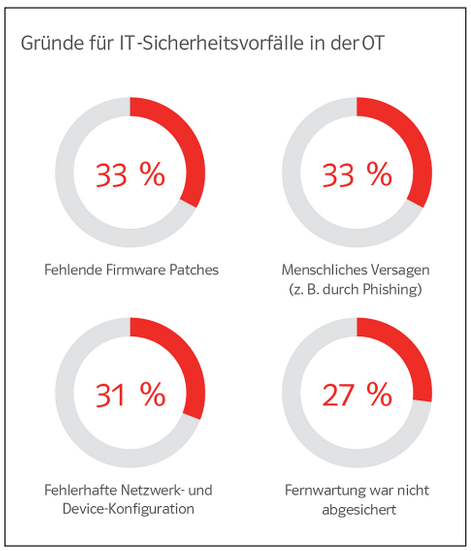
Fernwartung – aber sicher!

Spätestens seit Beginn der Corona-Krise hat der Bedarf an sicheren Fernzugriff-Lösungen nochmals zugenommen. Ist nämlich das Reisen durch pandemisch bedingte Schutzmaßnahmen oder Flutkatastrophen eingeschränkt, ermöglichen solche Remote-Lösungen den Sicherheitsexperten und Technikern einen Zugriff auf die Systeme von außen. Die physische Anwesenheit der Servicetechniker vor Ort erübrigt sich somit: Anlagen können praktisch über weite Strecken und aus dem Homeoffice heraus wieder flott gemacht werden. Wer als Unternehmer den Transformationsprozess versäumt, riskiert einen Maschinenausfall bis hin zum Stillstand der Produktion und den Verlust der Business Continuity.



Cyberattacken treffen alle Unternehmensgrößen

Oft wähnen sich kleine und mittelständische Industrieunternehmen (KMU) vor Cyberangriffen in falscher Sicherheit; sie meinen, weniger bedroht zu sein als Großunternehmen mit Tausenden von Mitarbeitern und ihren zahlreichen, weltweit vernetzten Standorten. Diese Einschätzung ist allerdings ein folgenschwerer Trugschluss. Denn laut der von NCP bei techconsult in Auftrag gegebenen Studie „Absicherung und Fernwartung in der Operational Technology" (OT) konnten keine nennenswerten Unterschiede zwischen den IT-Sicherheitsvorfällen und den verschiedenen Unternehmensgrößen festgestellt werden. Sowohl die kleinsten als auch die größten Unternehmen sind bereits Ziel von Cyberattacken auf ihre OT geworden. Im Gesamtdurchschnitt waren 58% der Unternehmen bereits von mindestens einem Angriff auf ihre OT betroffen! Die laut Umfrage häufigsten Gründe für Sicherheitsvorfälle waren fehlende Firmware-Patches und menschliches Versagen (z.B. durch Phishing). Eine weitere Ursache für Cyberangriffe liegt in einer fehlerhaften Netzwerk- und Device-Konfiguration. Das am meisten alarmierende Ergebnis aber ist, dass eine nicht abgesicherte Fernwartung in mehr als jedem vierten Unternehmen die Schuld an gefährlichen Einfallstoren in die OT trägt! Daher sind – im Hinblick auf die immer relevanter werdende Fernwartung – wirkungsvolle Maßnahmen und Lösungen zum Schutz der OT wichtiger als jemals zuvor.



Sichere Fernzugriffslösungen im Trend

Auch 50% der von techconsult befragten Unternehmen beschäftigen sich bereits mit Lösungen für einen sicheren Fernzugriff oder planen dies zeitnah. Im Zentrum aller Überlegungen steht hierbei eine geschützte Verbindung zwischen Servicetechnikern und Maschinen. Mit Hilfe der NCP Smart Maintenance Lösung wird eine sichere Verbindung aufgebaut, sodass der Techniker im Servicefall binnen weniger Minuten einen sicheren Fernzugriff auf die zu wartende Maschine erhält. Dieser Zugriff ist auf die Dauer der Wartung, die gewünschte Maschine und den definierten Techniker begrenzt. Durch die schnelle Herstellung der Verbindung wird der Produktionsausfall für das Unternehmen auf ein Minimum reduziert.

NCP bedient mit seinen Software-Lösungen viele verschiedene IIoT-Szenarien. Mehrere Komponenten setzen an verschiedenen Stellen der Infrastruktur an und gewährleisten im Verbund als Gesamtlösung die Kontrolle und sichere Datenverschlüsselung. Remote Gateways garantieren die sichere Kommunikation von Anlagen, Maschinen oder Systemen. Ein zentrales Gateway bindet diese sicher an und das zentrale Management System dient der Administration, dem Monitoring und der Integration in vorhandene Infrastrukturen.

Modernste Algorithmen, wie zum Beispiel Suite B Cryptography, stehen für die Verschlüsselung sämtlicher Verbindungen zwischen den Endgeräten und den Gateways. Für eine eindeutige Authentifizierung aller Endgeräte sorgen zentral verwaltete Maschinen-Zertifikate einer Public Key Infrastructure (PKI).

Aufgrund der Mandantenfähigkeit können Provider die NCP Komponenten für zahlreiche voneinander getrennte Kunden gleichzeitig nutzen. Unternehmen haben die Möglichkeit, mehrere Produktionsstandorte oder Unternehmensbereiche über eine gemeinsame Plattform zu administrieren, wobei die einzelnen Bereiche separiert bleiben.