Digitalisierung an vorderster Front

Corona hat der Digitalisierung einen immensen Schub verliehen – sei es beim Thema Homeoffice oder bei Fernwartungen im Rahmen von Industrie 4.0. Einer sicheren Datenkommunikation kommt daher in vielen Bereichen eine neue Bedeutung zu.

Vom Privileg zum neuen Normal: Corona hat das Homeoffice in den meisten deutschen Unternehmen zum Standard werden lassen – und das in einer immensen Geschwindigkeit. Was vor der globalen Pandemie einige Wochen, teilweise sogar Monate an Vorlauf bedeutet hat, war plötzlich binnen weniger Tage möglich. An dieser Stelle sei jedoch betont: Die bisher langen Vorlaufzeiten für die Einrichtung umfassender Homeoffice-Lösungen waren keinesfalls einer Verweigerungshaltung seitens der IT- oder Geschäftsführung geschuldet, wie es manchmal gerne dargestellt wird. Vielmehr ging es darum, die Sicherheit der Arbeitsprozesse auch außerhalb des Unternehmens zu gewährleisten. Dass dennoch so viele Mitarbeiter innerhalb kürzester Zeit von zu Hause arbeiten konnten, unterstreicht deshalb noch einmal, welche Leistungen die IT-Abteilungen der Unternehmen in den letzten Monaten vollbracht haben.

PATRICK OLIVER GRAF
CEO & Managing Director, NCP engineering GmbH

SEBASTIAN OELMANN
Product Manager Industrie 4.0 | IIoT, NCP engineering GmbH

Nun gilt es allerdings, die IT-Sicherheit auch als strategische Anforderung neu zu überdenken, die das Fortlaufen der zum Überleben einer Organisation notwendigen Prozesse garantiert, glaubt Patrick Oliver Graf, Geschäftsführer beim Nürnberger Softwareentwickler NCP:„Unzureichende Sicherheit bedeutet das mögliche Ende einer Organisation. Deshalb werden Arbeitsprozesse nicht mehr von der technischen Ausstattung abhängig gemacht, sondern die technische Ausstattung von den Vorgaben der Arbeitsabläufe.“ Für Graf bedeutet das, die Ablösung der alten „Vor-Corona-Infrastruktur“ und den Aufbau einer neuen und vor allem sicheren sowie zukunftsfähigen Infrastruktur.

REMOTE WORK VIA VPN

Dass Mitarbeiter überhaupt von außen auf Dateien und Software zugreifen können, verdanken sie den sogenannten Virtual Private Networks, kurz VPNs. Vorstellen muss man sich diese wie einen gesicherten Tunnel, durch den man „in“ das Büronetzwerk gelangt.

Vernetzte Welt – allgegenwärtige Datenkommunikation

Allerdings sind die Kapazitäten meist begrenzt und lassen sich nicht ohne weiteres schnell hochfahren, um eine große Anzahl an Mitarbeitern gezielt über Nacht vom Homeoffice aus arbeiten zu lassen. Unabhängig davon, ob Unternehmen VPN-Services von einem Dienstleister (MSP) beziehen oder eine entsprechende Architektur selbst vorhalten und betreuen muss sichergestellt sein, dass eine Erweiterung flexibel möglich ist, um auf Gegebenheiten reagieren zu können. Hier sind softwarebasierte VPN-Zentralkomponenten deutlich besser geeignet, da die Anzahl der Tunnel schnell erweiterbar ist. Die Abrechnung erfolgt bei uns ganz unkompliziert anhand des tatsächlichen Nutzens, also Pay per Use.

Bei NCP hat man während der ersten akuten Phase der Corona-Pandemie auch sofort reagiert und Kunden eine unkomplizierte Erweiterung ihrer Lizenzpakete ermöglicht, die umfassend genutzt wurden, wie Graf bestätigt.

ZENTRAL GESTEUERT

Ein weiteres Highlight der NCP-Lösungen ist das zentrale VPN-Management. Denn mit zunehmender Anzahl an Nutzern und Endgeräten steigt automatisch auch die Komplexität. Genau hier steuert ein zentrales VPN-Management gegen: Mit einem „Single Point of Administration“ wird ein sicherer und effizienter Betrieb gewährleistet. Entscheidend dafür sei die automatische Skalierbarkeit in Abhängigkeit von den Bedürfnissen des Unternehmens, betont Graf.

So lasse sich der Remote Access übrigens auch auf das Industrial Internet of Things erweitern, wie Sebastian Oelmann, Product Manager Industrie 4.0 und IIoT bei NCP, ergänzt. Zwar seien Maschinen gegen das Coronavirus immun, das Wiederhochfahren der Anlagen nach dem Lockdown erfordere oftmals jedoch die Anwesenheit von Technikern und Mitarbeitern des Wartungsservices. „Solange Reisen auch innerhalb Europas je nach Land und Region eingeschränkt sind, kommt der Fernwartung eine wichtige Rolle zu“, unterstreicht Oelmann.

BUSINESS CONTINUITY

Im Vorteil sind in der aktuellen Phase damit natürlich jene Unternehmen, die bei den Themen Industrie 4.0 und IIoT schon besonders weit sind. Sie verfügen über die Datenleitungen, die Servicetechniker benötigen, um sich remote Zugriff auf die Anlagen zu verschaffen. Dann allerdings gilt es immer noch, die größte Herausforderung zu adressieren, wie Oelmann weiß: „An der IT-Sicherheit hängt vielerorts die Wiederaufnahme der Produktion.“

Genau hier kommt VPN ins Spiel. Es ermöglicht im Servicefall den Technikern innerhalb weniger Minuten Zugriff auf die Maschinen. Die Experten von NCP haben dafür eine Lösung entwickelt, die über den VPN-Tunnel eine sichere Datenkommunikation ermöglicht: NCP Smart Maintenance Solution. Dank der Smart Maintenance Solution erhält ein Techniker im Servicefall binnen Minuten sicheren Fernzugriff auf die zu wartende Maschine. Dieser Zugriff kann zeitlich auf die Dauer der Wartung begrenzt werden. Außerdem ist sichergestellt, dass sowohl die Maschine als auch der Techniker exklusiv verbunden werden.

„Erfahrungsgemäß ist gerade die Zeit zwischen der Aktivierung des Servicetechnikers und der Möglichkeit der Verbindung essenziell für Industrieunternehmen. Je weniger Zeit dazwischen liegt, desto besser geeignet ist die Lösung, da weniger Produktionsausfall zu erwarten ist“, berichtet Oelmann aus der Praxis. Sicherheit wird aber auch an anderen Stellen der NCP Smart Maintenance Solution großgeschrieben. So sind beispielsweise sämtliche Verbindungen zwischen den Endgeräten und den beiden Gateways mit modernsten Algorithmen, wie Suite B Cryptography verschlüsselt. Ein weiteres Security-Feature stellen zentral verwaltete Maschinenzertifikate in einer Public Key Infrastructure (PKI) dar. Hierdurch wird eine eindeutige Authentifizierung aller Endgeräte gewährleistet. Bei NCP weiß man, dass eine IT-/OT-Infrastruktur nur so stark ist wie das schwächste System. Deshalb sei eine sichere Datenkommunikation auch in allen Bereichen unerlässlich, schließt Oelmann ab.

www.ncp-e.com