DIE VORTEILE DES IIOT MIT VOLLER SICHERHEIT NUTZEN

Die klassischen Anwendungsgebiete der Automatisierungssysteme von Copa-Data sind Steuerung und Regelung, Datenerfassung, Visualisierung, Analysen und Berichte. Nicht zuletzt die Verfügbarkeit der hauseigenen Software Zenon in der Microsoft Azure-Cloud ermöglicht Anwendern den Schritt in das industrielle Internet der Dinge und damit eine anlagen- und standortübergreifende Gesamtautomatisierung. Wie Unternehmen die produktiven Potenziale der Smart Factory voll zur Entfaltung bringen können, ohne bei der Sicherheit Kompromisse einzugehen, erfuhr x-technik von Reinhard Mayr, Head of Product Management bei Copa-Data. **Das Gespräch führte Ing. Peter Kemptner, x-technik**

_Herr Mayr, wie sieht die IIoT-Lösung von Copa-Data grundsätzlich aus?

Für unsere seit 2013 kontinuierlich weiterentwickelte IIoT-Lösung haben wir wesentliche Teile unserer Software Zenon als SaaS-Pakete verfügbar gemacht. Im Zusammenspiel mit der Microsoft Azure-Cloud macht Zenon Anlagenbauer fit für die Digitalisierung. Anwender können damit in nur einem System auf sämtliche Daten einzelner Maschinen, Fertigungslinien oder aller Produktionsstätten eines Unternehmens zugreifen. Zusätzlich können sie entweder vollständig cloudbasiert oder in hybriden Szenarien, z. B. vorausschauende Analysen, maschinelles Lernen, standortübergreifendes Reporting, Fernwartung und -steuerung umsetzen.

_Was bedeutet das im Hinblick auf die Sicherheit der Daten vor unbefugtem Zugriff?

Bei Industrie 4.0 – ermöglicht durch das industrielle Internet der Dinge – geht es um mehr als nur die Möglichkeit, dezentrale Produktionsstandorte zusammenzufassen und gemeinsam zu betreiben, ohne sich um die Details der Konnektivität kümmern zu müssen. Es geht um das Vernetzen ganzer Geschäftsprozesse. Mit den Vorteilen der Cloud wie der Möglichkeit mobiler Zugriffe durch – eventuell auch externe – Instandhalter wachsen Datenmengen, Sorgen und Abhängigkeiten. Die steigende Komplexität des integrierten Gesamtsystems vervielfältigt die möglichen Angriffspunkte.

_Welche Strategie empfiehlt Copa-Data seinen Kunden für eine sichere vernetzte Produktion?

Wir empfehlen Defense in Depth. Das ist eine Art Zwiebelschalen-Schichtenmodell, bei dem jeder Systemteil getrennt sicherheitstechnisch betrachtet und behandelt

Die anlagen- und standortübergreifende Analyse, Überwachung und Steuerung der Produktion im **Industrial Internet of Things erfordert Maßnahmen zum Schutz** der Daten und Programme.

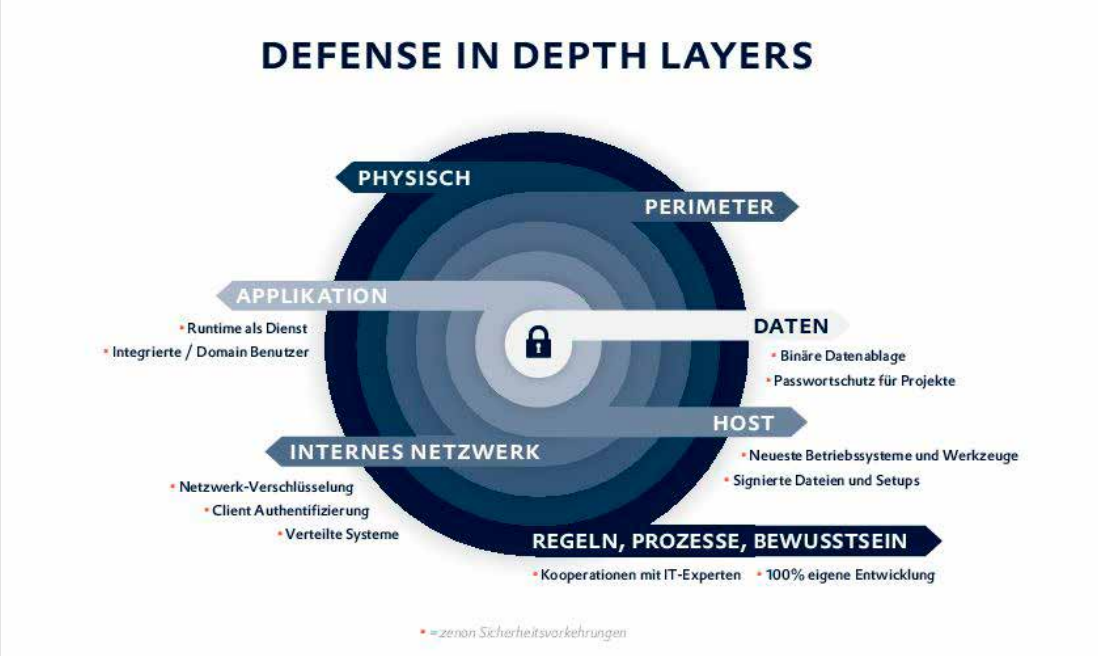
> Wir beraten unsere Kunden ganzheitlich und entwickeln gemeinsam mit unseren Partnern Sicherheitskonzepte, mit denen sie die produktiven Potenziale der Smart Factory voll zur Entfaltung bringen können – und das mit Sicherheit.
>
> **Reinhard Mayr, Head of Product Management, Copa-Data**

wird. Das beginnt beim einzelnen Mitarbeiter und darf sich nicht auf die IT im Unternehmen beschränken, sondern muss sich auch auf externe Datenaustauschpartner wie Kunden oder Lieferanten erstrecken.

Die sicherste Variante – alle Laufwerke ausbauen, USB-Ports sperren und den Produktionsrechner nicht ins Netzwerk hängen – verhindert Konzepte wie Industrie 4.0. Klar ist jedoch: Ein Produktionsrechner oder -server hat nichts im Internet zu suchen. Selbst zwischen der Welt der Automatisierung, der sogenannten Operations Technology (OT), und der Büroumgebung mit ihrer klassischen Information Technology (IT) sollte eine Pufferzone eingerichtet werden, durch die Daten nicht unkontrolliert reisen können. Wir empfehlen, für die Produktionssysteme eine demilitarisierte Zone (DMZ) einzurichten.

_Wie unterstützen Cloud-Installationen von Zenon Kunden bei dieser Abgrenzung?

Der TÜV Süd empfiehlt, zwischen den einzelnen Systeminseln unterschiedliche Technologien für den Datenaustausch zu verwenden. Die einzelnen Teile einer Zenon-Installation einschließlich der Soft-SPS Straton kommunizieren über ein eigenes Netzwerkprotokoll. Der Datenaustausch erfolgt verschlüsselt und durch Authentifizierung abgesichert. >>



Copa-Data geht nach dem **Zwiebelschalen-Schichtenmodell „Defense in Depth“** vor und empfiehlt das auch seinen Kunden. Die Zertifizierung des Unternehmens nach der IT-Sicherheitsnorm IEC 62443 steht unmittelbar bevor.

Da das Protokoll auf dem IP-Layer des TCP-Protokolls aufsetzt, kommen stets dieselben Mechanismen zum Einsatz, ob innerhalb einer Produktionszelle oder über das Internet.

Für die DMZ empfiehlt sich OPC UA mit seinen reichhaltigen Verschlüsselungsalgorithmen, für Webserver HTTPS. Und Microsoft investiert ungeheure Summen und Anstrengungen in relevante Zertifizierungen, Normen, Standards und generell die Sicherheit der Daten in der Azure-Cloud. So profitieren Zenon-Anwender auf den unterschiedlichen Ebenen von Schutzmaßnahmen unterschiedlicher Hersteller. Insgesamt ist die Zugriffssicherheit bei Zenon-Installationen in der Azure-Cloud sehr hoch.

_Noch einmal zurück zu Defense in Depth. Können Sie Beispiele dafür nennen, wie Copa-Data seinen Kunden hilft, dieses Konzept umzusetzen?

Das beginnt mit einer rollenbasierten Nutzerverwaltung, bei der die Rechte für jeden Benutzer individuell eingestellt werden können und jede Aktion protokolliert wird. Wie sämtliche Kommunikation und Datenablage in Zenon erfolgt das selbstverständlich verschlüsselt. Alle Zenon-Programmdateien sind manipulationssicher und lassen sich durch eingebettete Zertifikate von den Anwendern vor dem Installieren auf Echtheit prüfen.

_Deckt das Sicherheitsprogramm von Copa-Data alle Aspekte ab?

Nicht erst seit dem Gang in die Cloud, sondern seit Zenon netzwerkfähig wurde, beschäftigt sich Copa-Data mit der Sicherheit. In langjähriger Zusammenarbeit mit Universitäten und auf Sicherheit spezialisierten Unternehmen haben wir viele weitere Schutzmechanismen geschaffen. Dennoch: Auch bei noch so ausgefeilten Sicherheitsmechanismen bleibt immer ein Stück Risiko. Deshalb bietet Copa-Data ein Patch-Management, mit dem irgendwo auf der Welt entdeckte Gefährdungen rasch behandelt werden. Ein strukturiertes Backup für Programme und Daten nimmt unbeabsichtigten Löschvorgängen den Schrecken.

Der Rahmen dieses Interviews reicht nicht aus, alle Aspekte aufzuzählen, aber wir erwarten noch im ersten Quartal 2018 die Zertifizierung unserer Software nach der IT-Sicherheitsnorm IEC 62443.

_Was können Kunden tun, um den bestmöglichen Schutz zu erzielen?

Das Wichtigste ist, die angebotenen Möglichkeiten auch wirklich zu nutzen, vor allem, um den menschlichen Faktor zu berücksichtigen. Geben Sie jedem Mitarbeiter sein eigenes Nutzerkonto, vom Personalverantwortlichen gewartet, sodass es im Fall eines Abgangs ungültig wird. Steuern Sie die Kommunikationsports und legen Sie solche tot, die vom System nicht benötigt werden. Zusätzlich sollte man angesichts oft millionenschwerer Maschinenparks nicht bei der IT-Ausstattung sparen und kontinuierlich in aktuelle Hard- und Software investieren.

Eine saubere Zenon-Installation sendet nur die nackten Daten in die Cloud, lässt aber die Meta-Daten lokal liegen, sodass entwendete Daten für den unehrlichen „Finder“ wertlos sind. Zenon-Gesamtsysteme können aus lokal, im internen Netzwerk oder in der Cloud installierten Teilsystemen bestehen. Eine weitgehende Vorverarbeitung der Daten am Standort (an der Edge) reduziert Menge und Interpretierbarkeit der Daten. Das erhöht die Sicherheit und senkt gleichzeitig die Cloud-Kosten.

Ab dem zweiten Halbjahr 2018 wird Copa-Data eine umfassende Serie von Trainings zum Thema anbieten. Generell empfehle ich, auf die Dienste unserer erfahrenen und auch im Bereich Datensicherheit bestens geschulten Implementierungspartner zurückzugreifen. Sie bieten unseren Kunden die beste Unterstützung dabei, ihre Konzepte und Projekte im Rahmen von Industrie 4.0 so sicher wie möglich zu machen.

www.copadata.com