Auf die Schnelle

Das Wesentliche in 20 Sekunden

- Cloud-Projekte werden häufig nicht mit der nötigen Sorgfalt vorbereitet.
- ‚Junge' Automatisierer scheren sich nicht mehr um Datensicherheit.
- Wer in die Cloud geht, muss seine Anlagen als kritische Infrastrukturen betrachten - und entsprechende Maßnahmen umsetzen.
- VPN und Firewall allein, schützen nicht wirklich.
- Wer Daten in Clouds transferieren will, muss auf den Standort aller Beteiligten achten.

später lesen/ weiter empfehlen

INTERVIEW mit Dieter Barelmann, Videc

Die Mär von sicheren Daten

Mit Industrie 4.0 verbunden ist stets eine zentrale Datenhaltung möglichst aller verfügbaren Informationen, natürlich vorzugsweise in einer Cloud. Schließlich sollen abhängig von der Aufgabenstellung, authentifizierte Lieferanten, Fremdsoftware und eigene Mitarbeiter nach Belieben darauf zugreifen können. „Unter heutigen Security-Gesichtspunkten ein Horror-Szenario," meint Dieter Barelmann, Geschäftsführer der Firma Videc.

Herr Barelmann, warum sind Sie kein Freund der Cloud und damit auch nicht des Industrie 4.0-Gedankens?

Dieter Barelmann: Ich bin schon ein Freund dieser Entwicklungen beziehungsweise solcher Konzepte. Ich nehme nur zur Kenntnis, dass bei der Umsetzung solcher Projekte häufig nicht mit der nötigen Sorgfalt gearbeitet wird. Wir haben eine Menge Anbieter von Komponenten und Lösungen, die – wenn man zurück blickt – bei der Entwicklung das Thema Security scheinbar als zweitrangig angesehen haben. Oder nehmen Sie nur den Kenntnisstand zum Thema IT-Security bei den Automatisierern: Bei vielen besteht nach wie vor noch viel Nachholbedarf. Wie können also sichere Anlagen gebaut werden, wenn diese Rahmenpunkte gar nicht erfüllt sind?

Zudem, die Zusammenarbeit zwischen IT-Mitarbeitern und Automatisierern ist nach wie vor nicht immer die Beste. Die häufigsten Ursachen sind Kompetenzüberschneidungen, ein unterschiedliches Vokabular sowie abweichende Prioritäten in den Sichtweisen.

Die ‚jungen' Automatisierer scheren sich nicht mehr um Datensicherheit.

Wieso sind die Daten in einer Cloud per se nicht sicher?

Dieter Barelmann: Das kann man so nicht pauschalieren. Wir müssen unterscheiden zwischen einer privaten Cloud und den öffentlichen Clouds. Und wo sollen eigentlich welche Daten liegen und können das die Anwender nach Bedarf umschichten. Das alles hat großen Einfluss darauf, wie abhängig meine Industrieanlage von der Verbindung zur Cloud ist.

Die Frage ist, wie will ich eine Cloud nutzen? In vielen Bereichen kann eine Cloud-Lösung einen großen Innovationssprung für das Unternehmen bewirken. Eine Cloud erfordert allerdings ein enormes Umdenken in der Umsetzung von Lösungen – und natürlich der Sicherheitsmechanismen. Schließlich bin ich als Entscheidungsträger die Verantwortung nicht los, wenn die Daten einfach woanders gespeichert und ausgewertet werden.

Clouds gelten doch als sicher und der Zugriff auf die Daten ist übers Internet doch stets gegeben.

Dieter Barelmann: Sie wollen provozieren. Der Zugriff auf Daten ist niemals stets gegeben, da die Verfüg-

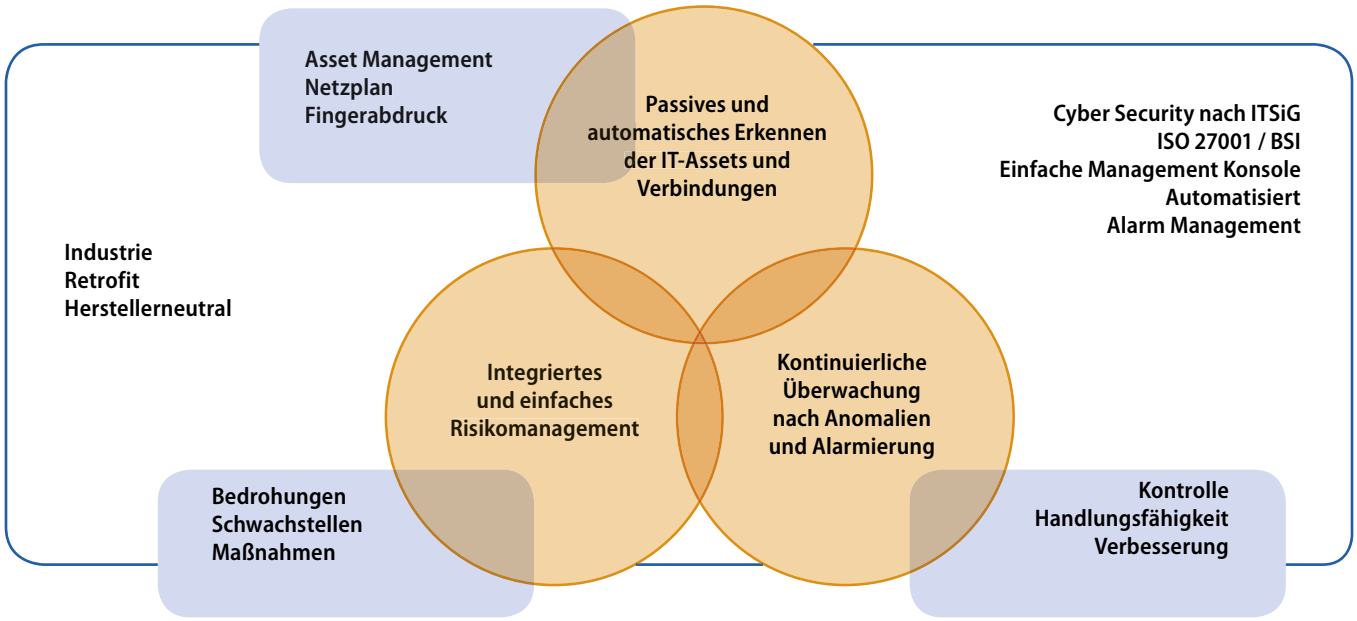
barkeit des Internets nirgends zu 100 Prozent gewährleistet ist. Denken Sie zum Beispiel an den Angriffsversuch letzten November auf die Telekom. Glücklicherweise war Angriff nicht erfolgreich. Sonst hätte eine große Zahl Telekom-Router zur gleichen Zeit unkontrolliert auf die Server der Telekom einwirken können. Dadurch wäre das Netz zusammengebrochen und alle Security-Maßnahmen zum Schutz der Produktion wirkungslos. Die zentrale Frage lautet: Läuft bei so einer Störung die Cloud beziehungsweise die daran angebundene Produktion dann noch mit der gleichen Qualität und Produktivität weiter?

> *Wer in die Cloud geht, muss seine Anlagen als kritische Infrastrukturen betrachten.*

Warum denken nicht alle so wie Sie und sind gegenüber Cloud-Lösungen so skeptisch?

Dieter Barelmann: Wir sind die ‚letzte Generation' Automatisierer, die das noch so sieht und sich um das Thema Security und private Daten Gedanken macht. Schauen Sie doch, wie unbedenklich viele jüngere User mit ihren privaten Daten umgehen. Gelingt es nicht die Sensibilität bezüglich der Daten an die nächste Generation der Verantwortlichen weiter zu geben, wird es in Zukunft schwer, noch sichere Produktions- und Versorgungsanlagen zu erstellen. Und die Qualität und Quantität der Cyberangriffe nimmt zu.

Das IT-Sicherheitsgesetz sollten auch Unternehmen der nicht-kritischen Infrastrukturen aufgreifen und bei ihren Cloud-Strategien berücksichtigen.



Die Kernfunktionen der Security-Lösung IRMA (Industrie Risiko Management Automatisierung) erleichtern die Umsetzung des IT-Sicherheitsgesetzes.

Was empfehlen Sie ihren Anwendern? Wo und wie würden Sie denn die Daten speichern?

Das hängt vom Unternehmen ab. Generell sollten sich Anwender über die Konzeption ihrer Cloud-Strategie Gedanken machen – und zwar im Vorfeld. Dafür bringen wir das entsprechende Know-how aus dem Bereich Security wie auch aus der Automatisierung mit. Wie Sie wissen, haben wir selbst Produkte für Cloud-Lösungen im Portfolio. Und ich bin überzeugt, dass diese Lösungen gute Chancen am Markt haben.

Was sollte man der Auswahl eines Cloud-Anbieters beziehungsweise einer Lösung beachten?

Dieter Barelmann: Das sind aus meiner Sicht die Kernpunkte, die es zu klären gilt, bevor man an eine Umsetzung herangeht.

- Wo liegen meine Daten und wer ist der Eigner der Cloud?
- Ist das Rechenzentrum ISO 27xxx zertifiziert?
- Sind alle Beteiligten Unternehmen und Personen in Deutschland? beziehungsweise in der EU ansässig und zertifiziert?
- Wie geht das Rechenzentrum mit Lastspitzen um?
- Wie authentifiziert das Rechenzentrum die Zugriffe – der eigenen wie auch diejenigen der notwendigen Sub-Unternehmen?
- Wie ist das Desaster-Recovery in dem RZ geplant?

VPN und Firewall allein, schützen nicht mehr wirklich.

Worin bestehen für Sie denn die größten Bedrohungen, kurz: Warum ist Industrial Security wichtig?

Dieter Barelmann: Täglich werden IT- und Automatisierung angegriffen und meist erwischt es das Unternehmen, wo einfach ‚die Lücke' gefunden wurde. Die Motivation der Hacker ist dabei unterschiedlich Die Angreifer suchen entweder gezielt nach solchen Angriffsvektoren - um Geld damit zu erpressen - oder aber es besteht Interesse an der Technik/Information und der Herausforderung in das System reinzukommen.

Und es kann jeden treffen. Denn heute haben die überwiegende Zahl an Schadsoftware oder die Advanced Persistent Threats keine konkrete Branche oder kein Unternehmen im Fokus. Diese Hacks suchen nach fehlerhaften Konfigurationen oder fehlender Security. Und wo gibt es wohl die meisten Security-Lücken?

Somit ist die Bedrohung sehr real, dass Schadsoftware auf Leitständen beziehungsweise Scada-Systemen der Industrie landet, kritische Infrastrukturen nicht mehr funktionieren oder Unternehmen tagelang nicht liefern können. Und das dann flächendeckend, weil die gleichen Automatisierungssysteme mitunter massenhaft im Einsatz sind.

Was macht denn ein gutes Security-Konzept aus?

Dieter Barelmann: Ein Security-Konzept besteht immer aus Organisation und Technik. Leider werden zu oft die bereits vorhandenen Security-Funktionen nicht in der ganzen Breite genutzt oder nicht fortlaufend angepasst. Dazu braucht es ein Information Security Management, wie es beispielsweise das IT-Sicherheitsgesetzt für kritische Infrastrukturen fordert. Die darin definierten Maßnahmen sollten generell auch in den produzierenden Unternehmen Einzug halten. Des Weiteren sind die aktuellen Security-Lösungen wie Firewalls und VPN zu statisch. Viele Angriffsmethoden umgehen inzwischen gezielt die vermeintliche Sicherheit von Firewalls und VPNs, beispielsweise durch so genanntes ‚drive by'. Dabei wird der Schadcode quasi huckepack über zugelassenen Ver-

> *Cloud-Projekte werden häufig nicht mit der nötigen Sorgfalt vorbereitet.*

bindungen mittransportiert und passiert ungehindert die vermeintlich sicheren Grenzen. Keine Frage, Firewalls und VPN sind wichtig. Wenn das aber die einzigsten Security-Komponenten sein sollten, ist das in meinen Augen schon grob fahrlässig.

Ein gutes Security Konzept basiert auch immer auf einer sich automatisch aktualisierenden Übersicht, beispielsweise in Form eines Netzstrukturplans oder Asset-Registers. Da diese Funktionen automatisiert sein müssen, ist die fortlaufende Erkennung von Anomalien der nächste konsequente Schritt im Security Konzept. Um den vollen Nutzen von Industrie 4.0 oder Cloud Service zu nutzen, muss das sich gegebenenfalls ständig ändernde Risiko Anomalie gemanaged werden.

Bei Industrie 4.0 propagieren Sie einerseits Security by Design. Andererseits haben wir die breite Basis an Maschinen und Anlagen, die auch Bestandteil einer I40-Installation sind. Wie passt das zusammen?

Dieter Barelmann: Viele Anlagen haben Automatisierungsgeräte, die keine Security bieten und auch in Zukunft nicht bieten werden. Dennoch sind auch diese Komponenten in ein Gesamtkonzept zu integrieren. Hierfür haben wir mit IRMA eine Lösung geschaffen, die passiv die Kommunikation der Anlage mithört. Die Software validiert das Kommunikationsverhalten aller Teilnehmer und kann in ein internes Risikomanagement integriert werden. Treten Unregelmäßigkeiten in der Kommunikation auf, alarmiert unser Produkt die zuständigen Mitarbeiter. Unterschiedliche Darstellungen in einem – selbstverständlich immer aktuellen und automatisch erstellten – Netzplan erleichtern die Analyse. Übrigens: IRMA steht für Industrie Risiko Management Automatisierung.

Wichtig war bei dem Design der Software, dass wir die Bedienung einfach halten und der Pflegeaufwand möglichst gering bleibt. Denn Industrie 4.0 wird die Vernetzung und Kommunikation der Geräte und Anlagen stark erhöhen. Umso größer wird der Druck, den Überblick über das Kommunikationsverhalten und die Kommunikationsteilnehmer zu behalten.

Das Interview führte Chefredakteur Stefan Kuppinger.

all-electronics.de
infoDIREKT 788iee0317