STORMSHIELD

MEINUNGEN

EFFIZIENZ UND SICHERHEIT: VORTEILE DER SEGMENTIERUNG VON INFORMATIONSSYS-TEMEN

Khobeib Ben Boubaker
Head of Industrial Security Business Line,

Mit der digitalen Transformation, der zunehmenden Öffnung nach außen und der Vernetzung verschiedener Informationssysteme werden Unternehmen anfälliger für Cyberangriffe. Es gibt jedoch wirksame Möglichkeiten, sich selbst zu schützen, wie z.B. die Segmentierung des Informationssystems. Eine Technik, die dazu beiträgt, Bedrohungen einzudämmen, indem sie verhindert, dass sie sich auf andere Gebiete ausbreiten. Damit optimiert sie die Leistung der Ausrüstung. Aber wie segmentiert man ein Netzwerk? Im Zeitalter von Industry 4.0, zwischen betrieblichen Anforderungen, Business Continuity und veralteten Systemen: Ist es in der industriellen Welt wirklich so einfach? Einige Antworten.

NETZWERKEFFIZIENZ UND -SICHERHEIT

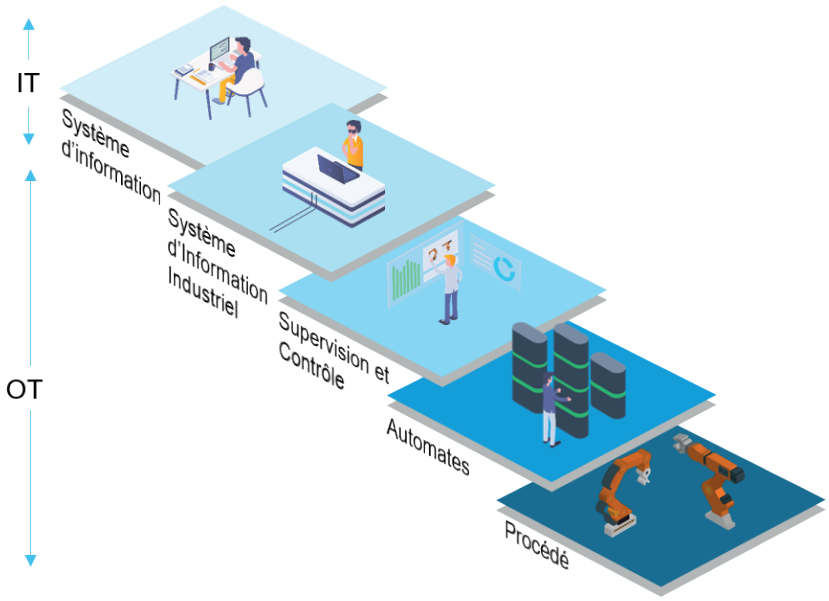
Die Netzwerksegmentierung ist zunächst sehr wichtig für rein funktionale Fragen: Verfügbarkeit und Effizienz der Anlagen. Wenn zu viele Anlagen an dasselbe Netzwerk angeschlossen sind und Kommunikationsflüsse und privater Austausch einfließen, entsteht ein „Hintergrundrauschen". In einem Industriebereich zum Beispiel wird der Automat nicht in der Lage sein, es zu ignorieren: Selbst wenn er nicht alle Anfragen bearbeitet, analysiert er sie systematisch. Dies steht im Widerspruch zum Erfordernis der operativen Effizienz dieses Geschäftsbereichs. „*Dieses Hintergrundrauschen lenkt die SPS von ihrer primären Funktion ab, eine Situation, die schnell zu Sättigung und damit zu Fehlfunktionen führen kann. Ein Werk kann seine Netzwerkarchitektur nicht kontinuierlich erweitern, ohne sie zu segmentieren*", sagt **Vincent Riondet**, Manager Delivery Schneider Electric.

Den **größten Nutzen bringt die Segmentierung allerdings bei der Cybersicherheit**. Die Segmentierung der Bereiche nach den spezifischen Nutzungsbedürfnissen der einzelnen Personen ermöglicht es uns, den Mitarbeitern nur die Ressourcen und den Zugang anzubieten, die sie benötigen. Daten, die sich auf die Organisation, den Betrieb und die Automatisierung beziehen, sind daher in Zonen enthalten, die ihrerseits Unterzonen enthalten können: so segmentiert, ist die Wahrscheinlichkeit geringer, dass sie verloren gehen oder kompromittiert werden. „*Um diese Einteilung in homogene Netzwerke zu erreichen, ist es notwendig, eine genaue Bestandsaufnahme ihrer Ausrüstung und ihrer Typen vorzunehmen und zu wissen, wie sie physisch miteinander verbunden sind. All diese Informationen werden es uns ermöglichen, auf eine Kommunikationsmatrix zuzugreifen und eine Risikoanalyse durchzuführen: Dies ist unerlässlich, um zu wissen, welche Prioritäten zu setzen sind und wie man segmentiert*", erklärt Vincent Riondet.

IT/OT: MEHRERE EBENEN DER SEGMENTIERUNG

Am Anfang war die IT. Bezüglich der Informationssysteme von Unternehmen sind daher erste Segmentierungsebenen notwendig, um bestimmte Gruppen von Diensten oder Computern entsprechend ihrer Gefährdung durch Cyber-Bedrohungen - hauptsächlich im Zusammenhang mit der Internetverbindung - zu trennen. In größeren Unternehmen ist eine interne Segmentierung vorstellbar, um die dem Internet ausgesetzten Dienste, die Computer der Mitarbeiter, die internen Dienste, aber auch mobile Mitarbeiter und Besucher zu isolieren.

Parallel dazu haben sich unter dem Einfluss der digitalen Transformation von Unternehmen und dem Aufkommen von Industry 4.0 industrielle Netzwerke im Laufe der Zeit unter dem Dogma der IT/OT-Konvergenz entwickelt. *„Ursprünglich war das Industrienetzwerk nicht mit dem IT-System verbunden*“, erklärt **Tarik Zeroual**, Named Account Manager Stormshield. *„Derzeit gibt es auf Seiten der Unternehmen aus Führungs- und Geschäftsgründen eine echte Bereitschaft, Informationen aus der Praxis automatisch zu sammeln: Daten zum operativen Betrieb, Nutzung und Wartung reichen nicht mehr aus. Die Hersteller ihrerseits wollen nun Informationen zur Nutzungshäufigkeit der Geräte sowie alle Informationen über Ausfälle und Ausfallzeiten dieser Geräte erfahren*“. **Die Errichtung einer Barriere zwischen der Welt der IT und der OT stellt daher eine grundlegende Sicherheitsstufe dar,** um den Cyber-Schutz industrieller Netzwerke zu gewährleisten.



Diese Konvergenz stellt für die meisten Hersteller eine große Herausforderung dar, sagt Vincent Riondet. *„Die überwiegende Mehrheit unserer industriellen Netzwerke ist sehr schlecht strukturiert. Sie wurden von Automatisierungsspezialisten installiert und eingerichtet, die nicht darauf spezialisiert waren: Sie berücksichtigten z.B. nicht die Themen IP-Adressierungsplan, Broadcast, Flow-Management. Ihr einziges Ziel bestand darin, die Geräte miteinander kommunizieren zu lassen.*“ Eine Herausforderung, die umso größer ist, als die Bedrohung nicht unbedingt von sehr weit her kommt. Werksmitarbeiter und Außenstehende verwenden immer noch häufig USB-Sticks, sei es zur Datenerfassung auf der Überwachungsstation oder zur Aktualisierung von PLCs. Dennoch passiert es häufig, dass diese infiziert werden. Eine einfache Verbindung könnte ein ganzes Informationssystem beschädigen. *„Diese Segmentierung ermöglicht es, sich vor allen internen und externen Bedrohungen zu schützen, egal ob sie aus dem Internet oder von außen kommen*“, sagt **Vincent Nicaise**, Industrial Partnership Manager bei Stormshield.

SEGMENTIERUNG: MEHR ALS EINE EMPFEHLUNG?

Die Netzwerksegmentierung ist daher die wirksamste Maßnahme, um Cyber-Bedrohungen einzudämmen und die Verbreitung von Malware innerhalb einer IT- oder Betriebsinfrastruktur zu verhindern.

Sie ist auch eine der Schlüsselempfehlungen der Norm IEC 62443. Diese Norm der industriellen Cybersicherheit hat das Konzept der Verteilung von „Zonen" und „Leitungen" entsprechend der Kritikalitätsstufen der dedizierten Anlagen aufgestellt. Eine Tiefenverteidigungslogik, die dank der Integration von Firewalls die autorisierten und nicht autorisierten Kommunikationsflüsse zwischen vorgegebenen Segmenten oder Blöcken streng und unveränderlich bestimmt. Das in Blöcke unterteilte Netzwerk ist dadurch als Ganzes besser gegen Angriffe durch Cyberkriminelle geschützt.

Die Segmentierung, die in den Texten der Norm der Norm IEC 62443 empfohlen wird, **erweist sich als ein wichtiger Schutzwall, um ein Eindringen von außen und Cyber-Angriffe zu begrenzen**. Wie das Anlegen eines Sicherheitsgurtes im Auto ist diese Technik ein Muss - unabhängig von der Art des betreffenden Netzwerkes.

EINE PHYSISCHE ODER VIRTUELLE TRENNUNG

Es gibt zwei Methoden der Segmentierung: physische Segmentierung und virtuelle Segmentierung. Die physische Segmentierung besteht darin, parallele Netzwerke so zu erstellen, dass sie völlig getrennt sind. Für jede Maschinenkategorie - SPS, PC, Drucker usw. - wird ein Schalter (Switch) installiert. Die virtuelle Segmentierung hingegen bietet den gleichen Material-Schalter für die verschiedenen Geräte: Diese sind an verschiedene Ports des Schalters angeschlossen und werden virtuell durch virtuelle Netzwerke (VLANs) getrennt, die verschiedene Switches simulieren und so die logische Segmentierung eines physischen Netzwerks ermöglichen. Sie können nicht miteinander kommunizieren, es sei denn, sie sind mit einer Firewall verbunden, die ihnen dies erlaubt.

„Beide Methoden haben sich in Bezug auf die Segmentierung bewährt, beide bieten bei richtiger Anwendung den gleichen Schutz gegen Cyber-Angriffe. Der einzige Unterschied besteht meiner Meinung nach in den Kosten. Die physische Segmentierung erfordert die Anschaffung zahlreicher neuer Geräte. Nur sehr wenige Unternehmen können sich diesen Luxus leisten. Die virtuelle Segmentierung ist die wirtschaftlich sinnvollste", sagt Tarik Zeroual.

NAT, EIN PROTOKOLL, DAS SICH ALS NÜTZLICH ERWEISEN KANN

Die Umsetzung der Netzwerksegmentierung, ob virtuell oder physisch, erfordert in einigen Fällen eine Änderung der Organisation der Adressen, die von den Geräten

zur Kommunikation miteinander verwendet werden. Tatsächlich wurden die Anlagen anfänglich entsprechend den betrieblichen Erfordernissen eingerichtet, ohne die Zuweisung von IP-Adressen zu berücksichtigen. Bei einem „leeren" Netzwerk konnten alle Geräte problemlos miteinander kommunizieren. *„Doch durch die Zonensegmentierung können Geräte nur noch mit Geräten kommunizieren, die sich in der gleichen Zone, im gleichen Teilnetz befinden. Es ist unmöglich, von einem Werk, das seine Industriesysteme seit etwa 15 Jahren aufgebaut hat, zu verlangen, dass es diese Anlagen einer nach der anderen neu konfiguriert und erneut testet, um zu sehen, ob sie funktionieren. Es wäre für sie ein finanzielles Desaster"*, sagt Vincent Riondet.

Um das Problem kurzfristig zu lösen, ist es auch möglich, die NAT-Funktion (Network Address Translation) verwenden: Dieses System erlaubt es, Adressen „umzuwandeln", um IP-Adressen an andere IP-Adressen anzupassen. *„Diese Funktion besteht darin, eine Adresse in einem Teilnetz in eine Adresse in einem anderen Teilnetz zu übersetzen, um eine Verbindung zu gewährleisten. Sie ermöglicht es, keine Änderungen an den Anwendungen vornehmen und diese nicht neu konfigurieren zu müssen. NAT kann eine vorübergehende Lösung sein, bei der Informationen durchgelassen werden, während man darauf wartet, dass industrielle Systeme modernisiert oder ersetzt werden"*, fährt Vincent Riondet fort. *„Wir haben Kunden, bei denen sich dieser Wechsel über zwei Jahre erstreckt. Wir haben jedoch bereits die Grundlagen für diese zukünftigen Neukonfigurationen gelegt, unsere Ziele und unsere Segmentierungsstrategie definiert. Dies bedeutet allerdings, dass jeder Wartungsstillstand viel Zeit in Anspruch nimmt. Der Industriesektor ist komplex, wir müssen Schritt für Schritt voranschreiten. Ohne NAT wären die meisten Branchen nicht in der Lage, ihre Systeme zu sichern."* Durch die Netzwerkadressübersetzung ist es auch möglich, ein industrielles Subsystem in die gesamte betriebliche Infrastruktur zu integrieren, ohne die Zertifizierung des Herstellers oder Dienstleisters zu verlieren.

Wie wir gesehen haben, **ist die Segmentierung des Informationssystems ein komplexer Vorgang,** der Zeit braucht. Aus der Perspektive einer tiefgreifenden Verteidigung ist es daher zwingend notwendig, ohne weitere Verzögerung zur Sache zu kommen!

STORMSHIELD

Weltweit müssen Unternehmen, Regierungsinstitutionen und Verteidigungsbehörden die Cybersicherheit ihrer kritischen Infrastrukturen, sensiblen Daten und Betriebsumgebungen gewährleisten. Die auf höchster europäischer Ebene zertifizierten Stormshield-Technologien sind die richtige Antwort auf IT- und OT-Risiken und erlauben den Schutz der Geschäftstätigkeit. Unsere Mission: Cybersorglosigkeit für unsere Kunden, damit diese sich auf ihre Kerntätigkeiten konzentrieren können, die für das reibungslose Funktionieren von Institutionen, Wirtschaft und Dienstleistungen für die Bevölkerung so wichtig sind. Die Entscheidung für Stormshield ist eine Entscheidung für eine vertrauenswürdige Cybersicherheit in Europa. Weitere Informationen finden Sie unter www.stormshield.com.