Mit der Security Appliance Irma zu mehr Sicherheit im OT-Bereich

Sechs Basisschritte zur OT-Security

Dem Aufruf, die Projekte im Bereich Digitalisierung zu beschleunigen, wurde in den letzten beiden Jahren verstärkt nachgekommen. Situationsbedingt war das durchaus nachvollziehbar. Unter diesem Druck wurde allerdings häufig ein wichtiger Aspekt aus den Augen verloren: die Cyber-Sicherheit.

Dieter Barelmann, Jens Bussjäger

Aus seinen Erfahrungen aus Kundenprojekten sowie solchen von Partnern der Systemintegration hat Videc sechs wichtige Handlungsempfehlungen zusammengestellt. Sie bilden die Basis für eine wirksame Risikominimierung und Cyber-Sicherheit für OT-Umgebungen. Dabei sind diese Punkte nicht vollumfänglich zu betrachten, aber sie beschreiben die Basics – und damit geht es meistens los.

Schritt 1: Bewusstsein bei den Mitarbeitern für die Gefährdungen schärfen

Es ist nicht richtig sichtbar. Es ist raffiniert und komplex. Es ist vorhanden. Laut BSI-Lagebericht werden täglich mehr als 320 000 Varianten von Schadsoftware in Phishing-Mails verteilt, um Passwörter auszuspionieren und ungesicherte Systeme zu finden. Deswegen ergibt es Sinn, die Mitarbeiter für diese Gefahren zu sensibilisieren. Denn, je besser die Mitarbeiter geschult sind, desto besser funktioniert die Abwehr.

Es können infizierte Geräte oder Management-Laptops mit den Produktionsanlagen verbunden sein. Das Hauptaugenmerk der Betriebsverantwortlichen liegt darauf, die Verfügbarkeit der Produktion zu gewährleisten. Es ist notwendig, diese Gefährdungen kennenzulernen, zu beurteilen und Vorbereitungen zu treffen, wenn sie eintreten.

Schritt 2: Für die Produktion kritische Systeme kennen

Was man nicht kennt, lässt sich nicht schützen! Daher beginnen alle Security-Management-Programme und -Standards mit dem Asset-Register oder vollständigen logischen Netzstrukturplan.

Im Security-Management sind Assets die Werte der Unternehmen, also beispielsweise Gebäude, Personal, Lager und die Produktionsanlagen. Geht es um die Absicherung der Produktionsanlage, sind die Geräte und Systeme der vernetzten Automatisierung die Assets.

Doch während Türen, Tore, Zäune, Brandmelder, Helme oder Kleidung sichtbar sind, sind Steuerungen, HMI, Sensoren, Motoren usw. „in" den Maschinen und Anlagen verbaut. Des Weiteren sind auch die Personal Computer im Leitstand oder beispielsweise die der Arbeitsvorbereitung im Office verbunden. Nicht zu vergessen, die Remote-Zugänge von Integratoren und Herstellern. Das Erkennen dieser „riskanten und offenen" Assets ist möglicherweise der wesentlichste Schritt zur OT-Sicherheit.

Schritt 3: Netzwerksegmentierung der OT-Umgebung für mehr Kontrolle

Wir kennen die Schotten im Schiffbau und Brandmauern bei Gebäuden. Für vernetzte Produktionsanlagen ist es das Air-Gap-Modell, von dem viele Anlagen als primäres Sicherheitselement abhängig sind. Allerdings ist die Trennung des Internets, der Office-IT und der Produktionsanlage kaum noch vorhanden. Auch werden immer mehr IT-Systeme im Zuge von Industrie 4.0 bzw. der Digitalisierung mit der Produktion verbunden.

Um ein sicheres Zusammenspiel von IT- und OT-Infrastruktur zu ermöglichen und die Digitalisierung zu beschleunigen, ist es wichtig, die Anforderungen an die Netzwerksegmentierung zu durchdenken. Im Notfall ist es besser, eine System-zu-System-Konnektivität in einem Purdue-Modell umgesetzt zu haben.

Ziel muss es sein, diese getrennten, kontrollierbaren Bereiche, die sich schützen lassen, wieder bestmöglich zu errichten.

Die Lösung ist der Einsatz von Managed-Switches und Firewalls. Zusätzlich sind Kontrollen der ordnungsgemäßen Funktion (vgl. Schritt 4) einzurichten. So entstehen Segmente (Zonen) und Übergänge (Conduits), die die detaillierte Absicherung im Netzwerk ermöglichen.

Schritt 4: konsequente Bedrohungsüberwachung und Vorfallmanagement

Transparenz ist der entscheidende erste Schritt für ein wirksames Echtzeit-Monitoring von Cyber-Bedrohungen. Für Unternehmen ist es unverzichtbar zu wissen, welche Geräte und Systeme sich in ihrer Umgebung befinden, wie die Anlagen miteinander verbunden sind und wie die Netzwerksegmentierung eingerichtet ist.

Sobald Sichtbarkeit hergestellt ist, gilt es zu klären, wie das Netzwerk rund um die Uhr lückenlos überwacht werden soll. Hinweis: Für Kritische Infrastrukturen (Kritis) ist mit dem ITSiG 2.0 der Einsatz von Angriffserkennungssystemen in der Automatisierung Pflicht. Informationsfluss und Alarmierungsszenarien sind wichtige Bausteine in einer Gesamtstrategie.

Schritt 5: Konnektivität und Zugangskontrollen

Während es für IT-Umgebungen etablierte Praktiken für das Identitäts- und Zugriffsmanagement gibt, besteht im OT-Bereich vielfach Nachholbedarf. Berechtigungsnachweise werden oft gemeinsam intern und extern genutzt, und der Zugriff ist nicht auf bestimmte Netzwerkgeräte oder -segmente beschränkt.

Schritt 6: Schwachstellen- und Patch-Management

Altsysteme, geschäftskritische Rahmenbedingungen und die begrenzten Patch-Fenster von OT-Umgebungen erschweren typischerweise die Entwicklung einer ganzheitlichen Strategie für das Gefahrenabwehr- und Patch-Management.

Anstatt sich durch hunderte von Schwachstellen zu patchen, müssen Anwender verstehen, welche potenziell gefährdeten Systeme für die Produktion am wichtigsten sind. Idealerweise werden Sicherheitslücken im Zuge der nächsten regelmäßigen Wartung geschlossen – mit dem Wissen im Hinterkopf, dass für viele OT-Schwachstellen überhaupt kein Patch oder Firmware-Update verfügbar ist.

Hinweis: Viele der bekannten Software-Schwachstellen der eingesetzten Systeme müssen nicht zwingend gepatcht werden: Die in den Schritten 1 bis 5 beschriebenen Maßnahmen sind oft ausreichend.

www.videc.de

↗ SPS: Halle 6, Stand 308

Jens Bussjäger

Geschäftsführer und Leiter Entwicklung bei der Achtwerk GmbH & Co KG.

Dieter Barelmann

CEO der Videc Data Engineering GmbH in Bremen.