Thema: OT-Security und Corona

Zeichenzahl: ca. 7.800 Zeichen (inkl. Leerzeichen)

Autor: Joe Robertson, EMEA CISO, Fortinet

Status: Final

**Was lehrt uns die Corona-Pandemie in Bezug auf OT-Security?**

*Joe Robertson, EMEA CISO, Fortinet*

Über kaum ein Thema wird derzeit gesprochen, ohne dass früher oder später nicht auf irgendeine Weise die Coronavirus-Pandemie erwähnt wird. Sie beherrscht unser Leben auf vielfältige Weise. Doch natürlich muss das Leben weitergehen, die Wirtschaft weiter funktionieren – jedoch nicht wie gewohnt. So waren etwa Unternehmen gefordert, ihre Geschäftsmodelle zu überprüfen und sich daran zu gewöhnen, dass in naher Zeit weniger Mitarbeiter vom Büro aus arbeiten – diese sind zu „Heimarbeitern“ geworden. Das hat, gepaart mit neuen Sicherheitsbedenken, die IT-Abteilungen unter Druck gesetzt. Zugleich waren die Auswirkungen auf die Absicherung der Operational Technology (OT) enorm.

So wurde es beispielsweise im Lockdown notwendig, Fertigungsstrassen zu verlangsamen oder sogar komplett anzuhalten, weil die Arbeiter nicht ins Werk kommen konnten. Doch anders als in einer IT-Umgebung, wo es vergleichsweise einfach ist, einen Software-Prozess zu verändern oder ein Gerät abzuschalten - auch remote, erlaubt es die Realität von OT nicht, einen chemischen Prozess oder eine Montagelinie einfach zu stoppen. Bestimmte Systeme, Hochöfen oder Dampfkessel etwa, sind für den kontinuierlichen Betrieb ausgelegt und damit ist es praktisch unmöglich, sie abzuschalten. In vielen Fällen muss eine Notschicht vor Ort sein, damit die Maschinen betrieben werden können. In immer mehr Fällen versuchen Anlagenführer die Produktion aus der Ferne zu steuern, obwohl die Systeme hierfür eigentlich nicht ausgelegt sind.

Eine der wichtigsten COVID-19-Lehren ist, dass es jederzeit zu disruptiven Veränderungen kommen kann. Auch wenn wir nicht vorhersagen können, welche Störfälle uns treffen, müssen wir doch davon ausgehen, dass sie uns bevorstehen. Oder so handeln, als wären sie bereits da.

**OT steht im Fokus der Angreifer**

Ursprünglich liefen OT-Prozesse auf nicht Routing-fähigen Protokollen. Dadurch war Security mehr oder weniger auf den physischen Schutz beschränkt. Die Isolierung des OT-Netzwerks von der IT, dem sog. Air Gap, machte es den Betreibern leicht, jene Aspekte der Cybersecurity zu ignorieren, die in Rechenzentren und Unternehmensnetzwerken die grössten Kopfschmerzen bereiteten. Daraus ergab sich, dass zahlreiche Unternehmen der Cybersecurity ihrer Produktionsumgebung nur geringe Priorität einräumten oder diese sogar komplett ignorierten.

**IT und OT wachsen zusammen – die Bedrohung wächst**

In den vergangenen zehn Jahren wurden immer mehr OT-Systeme auf Standard-Ethernet mit IP-Protokoll umgestellt. Doch nicht nur die Protokolle ändern sich. Da industrielle Netzwerke mit dem IT-Netzwerk zusammenwachsen, ist der Air Gap verschwunden. Eine der Hauptarchitekturen für die Automation in Produktion und Fertigung ist das Purdue-Modell. Es teilt funktionale Aspekte eines Prozesses in Zonen ein. Die Prozesssteuerungszone (Process Control Zone) wird durch die Sensoren, Aktoren und deren zugehörige Instrumentierung definiert, die einen Prozess implementieren. Die Betriebs- und Kontrollzone (Operations and Control Zone) ist zuständig für die Verwaltung dieses Prozesses und verschiedener Prozesse am gesamten Standort. Das Purdue-Modell ist sehr hierarchisch: jede Prozesssteuerungszone hat nur einen Kommunikationskanal zur übergeordneten Betriebs- und Kontrollzone. Die Operations & Control Zone hingegen besitzt nur einen einzigen Kommunikationskanal zur IT-Umgebung des Unternehmens, der „Enterprise-Zone“. Diese Verbindung ist normalerweise eine demilitarisierte Zone, die mit einer Firewall abgetrennt ist. Dieses Sicherheitsniveau schien lange Zeit ausreichend.

Jedoch konvergieren IT- und OT-Netzwerken heute zwangsläufig, da immer mehr Informationen zwischen ihnen ausgetauscht werden. In Produktionsumgebungen werden zunehmend Sensoren und SPS-Steuerungen eingesetzt, von denen viele über drahtlose Verbindungen verfügen. Die Angestellten in den Büros nutzen gemeinsam mit den Maschinen in den Produktionshallen sowohl WLAN- als auch LAN-Verbindungen. Zwar können OT- und IT-Netzwerke noch immer logisch getrennt sein, aber physisch sind sie dies nicht mehr. Darüber hinaus erzeugt die Vielzahl an OT-Sensoren eine Flut an Daten, die von den Anwendungen in der Enterprise-Zone analysiert werden muss. Informationen und Anweisungen fliessen auch in die andere Richtung. Und wo Daten ausgetauscht werden, kann es jederzeit zu Bedrohungen kommen.

Das soll nicht heissen, dass das Purdue-Modell nicht mehr gilt. Es heisst jedoch, dass wir die Schutzvorkehrungen, die wir innerhalb und zwischen den OT-Zonen getroffen haben, neu überdenken müssen. Eine für jede Prozesssteuerungszone segmentierte Firewall hat in etwa die Wirkung einer verschlossenen Haustür – sie hält Passanten ab, jedoch kaum einen entschlossenen Dieb. Vor allem dann nicht, wenn gleichzeitig Fenster und Hintertür offenstehen.

**Neue Tools für höheren Schutz**

Viele unabdingbare Werkzeuge zum Schutz von OT-Umgebungen sind bereits verfügbar. Es gibt eine breite Palette an Cybersecurity-Lösungen, die perfekt zu OT-Umgebungen passen. Sie alle bieten umfassende Transparenz und Kontrolle für die Sicherung von IT- und OT-Netzwerken. Im Folgenden einige Beispiele:

* Next-Generation-Firewalls (NGFW) segmentieren nicht nur die Betriebstechnologie logisch, sie können zusätzlich ein Intrusion Detection und Prevention System enthalten, das die Signaturen tausender OT-Malware-Typen erkennen und wenn gewünscht blockieren kann.
* Verdächtiger Datenverkehr, der vom IDS/IPS nicht erkannt wird, kann in eine Sandbox weitergeleitet werden, wo er in einer geschlossenen Umgebung ausgeführt und auf gefährliches Verhalten analysiert wird.
* Ein weiteres Tool ist ein Honeypot, welcher Angreifern vorgibt, ein verlockendes Ziel zu sein. Dieser lockt einen Hacker an, der sich Zugang zum Netzwerk verschafft hat, und ermöglicht die Identifizierung der TTPs (Tactics, Techniques and Procedures) des Angreifers.
* Das explosionsartige Wachstum von IoT- und IIoT-Geräten stellt eine grosse Bedrohung dar. Lösungen für die Netzwerkzugangskontrolle (NAC), stellen sicher, dass sich nur autorisierte Anwender und Geräte mit dem Netzwerk verbinden.
* Software für Endpunktschutz (EPP) und Endpunkt-Detection und -Respone (EDR) kann PC-basierte Controller, Engineering-Stationen, Mensch-Maschine-Schnittstellen (HMIs) oder Archiv-Software abschirmen.

Ein letzter Punkt zur Cyber-Sicherheit für OT-Netzwerke: Es existiert keine Einzellösung, die all diese Probleme löst. Um Ihre OT-Umgebung zu schützen, müssen Sie höchstwahrscheinlich mehrere Anbieter einbinden, die unterschiedliche Arten von Lösungen anbieten: das Industrial Control System selbst, Tools, die Einblick in hochspezialisierte OT-Geräte und PLCs gewähren, Sensoren und Analysegeräte. Dies kann kein Anbieter alleine leisten. Stellen Sie daher sicher, dass die von Ihnen ausgewählten Anbieter in der Lage sind, gut zusammenzuarbeiten. Covid hat uns gewarnt: Wir alle müssen anfangen, uns das Unvorstellbare vorzustellen. Wenn es um den Schutz unserer Produktionsumgebungen geht, ist es jetzt an der Zeit, die Cyber-Sicherheit unserer Operational Technology zu verbessern.

**Bildmaterial:**



BU: Joe Robertson, EMEA CISO, Fortinet