News

6 Wege, um pharmazeutische Produktionsstätten auf die kommenden Cyber-Bedrohungen im Jahr 2021 vorzubereiten

In der pharmazeutischen Industrie erfordert jede Produktionsanlage und jeder Herstellungsprozess ein besonderes Maß an Sorgfalt. In der letzten Zeit ist dies sogar noch mehr der Fall als sonst, da Angreifer immer schneller aggressive Malware entwickeln, die auf sensible, wichtige Branchen wie die pharmazeutische Industrie und ihre Produktion abzielt. Gerade angesichts der Corona-Pandemie und ihrer noch immer nicht absehbaren politischen, finanziellen und sozialen Folgen, versuchen selbst staatliche Organisationen sich durch illegales Erlangen von Forschungsergebnissen oder Wirkstoffformeln Vorteile zu verschaffen.

So haben etwa laut dem südkoreanischen Geheimdienst sowie dem russischen Sicherheitssoftware-Hersteller Kaspersky nordkoreanische Hacker versucht, illegal an Informationen über den Coronavirus-Impfstoff des US-Pharma-Unternehmens Pfizer zu gelangen und hatten es dabei auch auf Daten zur Behandlung einer Corona-Infektion abgesehen.(i) Cyberangriffe durch kriminelle oder terroristische Organisationen stellen gerade für sensible Schlüsseltechnologien wie pharmazeutische Unternehmen ernste Bedrohungen dar. Betriebsunterbrechungen, Ausfallzeiten, verunreinigte Produkte, die Notwendigkeit monatelanger Neu-Evaluierungen, das Auslaufen von Gefahrenstoffen und Datenschutzverletzungen (die zur unfreiwilligen Bekanntgabe von Rezeptur- oder Wirkstoffdaten führen) sind die drohenden Folgen dieser Unsicherheitsfaktoren. Die Stakeholder können und sollten vor den potenziell tödlichen Folgen solcher Vorfälle geschützt werden.

Hauptbedrohungen in der OT

Die zwei größten Sicherheitsherausforderungen in pharmazeutischen OT (Operational Technology)-Umgebungen sind zum einen die Überprüfung der Sicherheit von Endgeräten, die per Air-Gap (Luftspalt)-Methode abgeschottet sind. Bei dieser Methode werden zwei IT-Systeme voneinander physisch und logisch getrennt, die Übertragung von Nutzdaten aber dennoch zugelassen. Zum anderen gilt es, Bedrohungen einzudämmen, die durch Techniker von Drittanbietern verursacht werden, die ihre eigenen Endgeräte in das Netzwerk eines Unternehmens einbringen. Denn wenn Partner, Lieferanten oder Berater zur Wartung der IT vor Ort sind, müssen sie ihre potenziell infizierten Laptops oder USB-Sticks mit dem Netzwerk des Industrial Control Systems (ICS) oder den Produktionsanlagen verbinden. Laut einer aktuellen Umfrage haben 60 % der befragten Unternehmen im Jahr 2020 "Malware-Aktivitäten verzeichnet, die sich von einem Mitarbeiter zum anderen verbreitet haben".(ii)

Konventionelle Endpoint Security Lösungen können diese Probleme nicht lösen, da sie für On-Premise IT-Umgebungen entwickelt wurden und für Anwendungsfälle in der Pharmaindustrie nicht geeignet sind. Um die OT-Netzwerke der Pharmaindustrie vor Sicherheitsbedrohungen zu schützen, stellt TXOne Networks, ein führender Anbieter von OT-Sicherheitslösungen, einige Erkenntnisse aus erster Hand vor, was große pharmazeutische Produktionsunternehmen tun können, um die Sicherheit ihrer Produktionsanlagen zu stärken.

6 Tipps zur Verbesserung der OT Sicherheit

Mit diesen sechs Praktiken können die betriebliche Sicherheit verbessert und Produktionsstätten vor möglichen Beeinträchtigungen geschützt werden:

1. Mobil-taugliches Scansystem installieren

Um den aktuellen Zustand der eingesetzten IT besser erfassen zu können, wird eine mobile IT-Sicherheitslösung zum Scannen von Malware benötigt, die zur routinemäßigen Wartung der IT-Systeme von Gerät zu Gerät mitgenommen werden kann, um Bedrohungen so früh wie möglich zu erkennen und zu verhindern, dass sie sich in lokalen Dateien verstecken.

2. Routinemäßige "Log-Only"-Cybersecurity-Checks

Bei sensiblen Produktionsanlagen sollten Unternehmen eine Scan-Lösung einsetzen, die sogenannte "Log-Only"-Scans durchführen kann, bei denen die Ergebnisse lediglich protokolliert und dokumentiert werden. Sicherheitsexperten und IT-Administratoren bevorzugen in der Regel Scanner, die ein Scan-Protokoll erstellen, ohne bei erkannten Bedrohungen sofort Maßnahmen zu ergreifen. Auf diese Weise können sie vermeiden, dass geschäftskritische Programme oder Dateien entfernt werden, und die Unternehmen können bei Bedarf einen maßvolleren Ansatz wählen, um die Bedrohung zu beseitigen.

3. Prüfen auf „Endpunkt-Schwachstellen“

Die bei der Überprüfung der Produktionsanlagen gesammelten Daten können verwendet werden, um zu verstehen, welche Patches und Anwendungen auf jedem einzelnen Endgerät in der Produktion installiert sind, und um nicht gepatchte Geräte, Ressourcen oder Betriebssysteme zu erkennen, deren Produktlebenszyklus abgelaufen ist (sogenannte „End-of-Life Operating Systems“). Dies verbessert die transparente Ermittlung des jeweiligen Status, insbesondere bei eigenständigen IT-Geräten, und vereinfacht den Prozess der Verwaltung eines industriellen Steuerungssystems (Industrial Control System - ICS).

4. Gründliche Plug-and-Scan-Sicherheitsinspektionen

Jedes digitale Endgerät, das vor Ort am Produktionsstandort eingesetzt wird, muss einen Kontrollpunkt durchlaufen, an dem es auf Bedrohungen für die IT-Sicherheit gescannt wird, die sich in seinem Inneren verstecken können. Eine mobile Scanning-Lösung, die einfach und schnell zwischen den jeweiligen Endgeräten ausgetauscht werden kann, ist dafür unerlässlich.

5. Zentrales Protokollieren von Asset-Informationen und Scan-Ergebnisse

Eine werksweite oder sogar unternehmensweite Perspektive macht das Sammeln von Informationen über die Unternehmens-IT zu einem Kinderspiel. Um den Audit-Prozess zu straffen, sollten Pharmaunternehmen ein festes Prüfverfahren („Audit-Trail“) zur Einhaltung der Compliance erstellen. Auf diese Weise können sie allen Beteiligten in der Lieferkette (einschließlich Krankenhäusern, Apotheken und anderen Gesundheitsdienstleistern) auf einfache Weise Sicherheitszeitpläne oder Dokumentationen zum Status der IT zukommen lassen.

6. Nutzen von Security Operation Zentren optimieren

Ein ideales SIEM-System (SIEM - Security Information and Event Management) sollte in der Anwendung so bequem wie möglich sein, indem es zentral organisierte Protokolle und Ereigniserfassung ermöglicht, unabhängig vom Fabrikat der Produktionsgeräte, die ein Unternehmen in Bezug auf IT-Sicherheit untersucht. Die Protokolle sollten sich zum Beispiel

leicht in SIEM-Systeme wie etwa QRadar oder Splunk exportieren lassen. Im Idealfall wahrt ein Unternehmen die Datenintegrität und speichert die Daten so, dass sie beispielsweise den Anforderungen der Patientensicherheit bei klinischen Studien und anderen rechtlichen Vorgaben genügen.

Wenn ungesicherte mobile Geräte an einen Produktionsstandort gebracht werden und den IT-Kontrollpunkt eines Unternehmens erreichen, müssen die Sicherheits-Scans schnell und gründlich erfolgen. Aufzeichnungssysteme zum Nachweis der Compliance und zur Überwachung von Produktionsgeräten sollten bequem und so gestaltet sein, dass sie sich gut in die täglichen Arbeitsroutinen einfügen. Jeder Prozess im Sicherheitskonzept eines Unternehmens sollte so einfach und intuitiv wie möglich sein. Ein vielversprechender Weg, diese komplexen und vielfältigen Sicherheitsherausforderungen zu bewältigen, ist der Einsatz von portablen Endpunkt-Sicherheitslösungen zum Schutz der OT-Netzwerke der Pharmaindustrie. Dieser Ansatz funktioniert am besten, wenn die jeweilige mobile Lösung genau auf die Bedürfnisse des Unternehmens zugeschnitten ist.

Fazit

Mobile Sicherheitslösungen, sogenannte Portable Security Lösungen, helfen den Eigentümern und Betreibern von Industrial Control Systems („ICS“) bei der Durchführung von Malware-Scans sowie bei der Erfassung sicherheitsrelevanter Informationen auf Standalone-Computern und in Air-Gapped-Systemen. Diese USB-basierten Lösungen enthalten bereits die benötigte Scan-Software und können so das Erkennen und Entfernen von Malware wesentlich erleichtern, da keine Sicherheits-Software auf den Zielsystemen selber installiert werden muss. So können Pharmaunternehmen bei Bedarf Malware-Scans durchführen, wann und wo immer sie benötigt werden, und müssen sich keine Sorgen über Leistungseinbußen auf den gescannten Geräten machen. So vereinfachen mobile Sicherheitslösungen den Prozess der Sicherheitsüberprüfung und ermöglichen es den Anwendern, ihre Compliance nachzuweisen.

(i) Geheimdienst: Hacker aus Nordkorea wollten an Pfizers Impfstoff-Daten - channelpartner.de

(ii) “*The State of Email Security 2020*” Mimecast, letzter Zugriff 4 Dezember, 2020

Autor: Dr. Terence Liu, CEO von TXOne Networks, einem Joint Venture von TrendMicro und Moxa.