© CAIA IMAGE / SCIENCE PHOTO LIBRARY / PICTUREDESK.COM

Cyberohnmacht: Die Absicherung von Produktionsanlagen gegen Cyberangriffe, interne Manipulationen oder fehlerhafte Konfigurationen stellt eine zunehmende Herausforderung für Produktionsunternehmen dar.

DIE STRENGE IRMA

WEIL HERKÖMMLICHE SICHERHEITSSYSTEME WIE VPN UND FIREWALLS PRODUKTIONSANLAGEN VOR MODERNEN HACKERANGRIFFEN NICHT MEHR AUSREICHEND SCHÜTZEN, SETZT SYSTEMINTEGRATOR SYS.CO AUF DIE SICHERHEITSLÖSUNG IRMA. WIE DIESE IN ECHTZEIT PRÄVENTIV NOCH UNBEKANNTEN BEDROHUNGEN BEGEGNET, ZEIGTE JÜNGST EIN BIOMASSEHEIZWERK.

Mit der zunehmenden Vernetzung der produzierenden Unternehmen mit Partnern, Lieferanten und Kunden steigen die Anforderungen — und damit auch die Bedrohungen. Dieser Tatsache müssen sich vor allem auch Fernwärmekraftwerke stellen. Die meisten Industrial Firewalls sind nicht in der Lage, die dazu im Einsatz stehenden dynamischen Verbindungen mit ihren verschiedensten Ports oder auch den Standard Web-Port (80) zuverlässig zu kontrollieren. So entstehen potenzielle Einfallstore, die Cyberangriffen viele Möglichkeiten der Verbreitung und der unbemerkten Beschaffung von Informationen eröffnen. Dazu zählen auch die Advanced Persistent Threats (APT), so genannte Bedrohungen, die mit hohem Aufwand und zielgerichtet die Standard-Schutzeinrichtungen umgehen und dabei häufig bislang unbekannte Schwachstellen (Zero-Day Exploits) ausnutzen. Solche Manipulationen und Angriffe können nur durch eine nachhaltige Überwachung der Produktionsanlagen-IT identifiziert und mögliche Schäden mittels einer intelligenten Echtzeitanalyse neutralisiert werden. „Neben den klassischen Einfallstoren bieten sich noch viel einfachere Angriffsflächen“, unterstreicht Holger Frank Dunke, Geschäftsführer von sys.co in Salzburg. „Zum Beispiel wenn ein Servicetechniker sein Notebook für eine Reparatur mit einer Anlage verbindet, kann sich Malware sehr leicht und völlig unabsichtlich Zugang verschaffen.“ Gerade Steuersysteme sind höchst anfällig für unbekannte oder sonst eher harmlose Vehikel. Als Ursache kommen also nicht immer nur Programme infrage. Dann ist ein beträchtlicher Schaden buchstäblich vorprogrammiert: Die Produktionsanlage wird wie von Geisterhand manipuliert, es entstehen mysteriöse Fehlfunktionen oder sie bleibt einfach stehen. Deshalb stellt die effiziente Absicherung von Produktionsanlagen gegen Cyberangriffe, interne Manipulationen oder fehlerhafte Konfigurationen eine zunehmende Herausforderung dar.

Firewalls und VPN können leicht umgangen werden

Trotzdem finden IT-Sicherheitsvorkehrungen in Produktionsanlagen immer noch überwiegend nach dem Prinzip der Perimeter-Sicherheit mit Firewalls und VPNs statt. Dies bedeutet, einzelne Bereiche werden voneinander abgetrennt, die untereinander nur zulässige Kommunikationsverbindungen erlauben. Solche Sicherheitselemente, die Datenverbindungen analysieren, sie präventiv zulassen oder gegebenenfalls blockieren, sind bei weitem nicht mehr ausreichend. Diese scheinbare Sicherheit wird heute spielend leicht durch simple „drive by“-Angriffsmethoden umgangen. Dafür wird der Schadcode quasi „huckepack“ in zugelassenen Verbindungen mittransportiert und kann so die vermeintlichen Barrieren ungehindert passieren. „Es gibt heute auch viele so genannte ‚getriggerte‘ Bedrohungen, wo zuerst gar nichts passiert“, betont Klaus Lussnig, Geschäftsführer der Industrial Automation GmbH in Innsbruck. „Erst nach etwa 200 Tagen wird der Schädling aktiv. Meist ist der Ursprung dann gar nicht mehr nachvollziehbar.“ Darum ist es angezeigt, dass die Spuren, die ein Trojaner hinterlässt, rechtzeitig erkannt werden.

Vorgaben und Assets definieren

Alle diese Schwachstellen sollten für die Implementierung eines neuen Sicherheitskonzepts für ein Biomasse-Heizkraftwerk restlos ausgeräumt werden. Denn für ein Heizkraftwerk mit knapp 10 MW thermischer Leistung und über 400 Fernwärmekunden unterschiedlichster Leistungsstufen stehen Zuverlässigkeit und Sicherheit an erster Stelle. „Sicherheit für den Kunden heißt in der Regel, die Anlage läuft reibungslos und im Schadensfall muss sie wieder zeitnah in Betrieb zu stellen sein“, erklärt Dunke. „Doch wie soll mit der Vielzahl an möglichen Bedrohungen umgegangen werden?“ Daher entschied sich der Betreiber für die Sicherheitslösung IRMA (Industrie Risiko Management Automatisierung) der Industrial Automation GmbH, die als zusätzliches Konzept implementiert wurde, um präventiv bzw. den noch nicht bekannten Bedrohungen effektiv begegnen zu können. Um eine solide Ausgangslage zu schaffen, wurde zu Projektbeginn die komplette Anlage analysiert. Denn bis dato wusste der Betreiber noch nicht, wie komplex und anspruchsvoll das Projekt werden wird. Das bedeutet für viele eine große Herausforderung. „Wir finden hier selten eine perfekte Welt vor, in der alles penibel genau dokumentiert ist, sondern leben in einer realen Welt“, räsoniert Dunke. „Gerade im Automatisierungsbereich hat man sehr viel mit gewachsenen Strukturen zu tun. Die Anlagen sind daher

„ES GIBT HEUTE AUCH SO GENANNTE ‚GETRIGGERTE‘ BEDROHUNGEN, WO ZUERST GAR NICHTS PASSIERT. ERST NACH 200 TAGEN WIRD DER SCHÄDLING AKTIV.“

Klaus Lussnig, Geschäftsführer Industrial Automation

Die Anwendung auf einen Blick:

IRMA

Was: **Industrie-Computersystem zur Identifikation und Abwehr von Cyberangriffen in Produktionsnetzwerken**

Besonders weil: **Absicherung von „zertifizierten“ Produktionsanlagen und Prozessen ohne Re-Zertifizierung**

Auch interessant: **Absicherung von „nicht patchbaren“ Systemen, z. B. Windows NT, Windows 2000, Windows XP, alte SPS, OPC-Classic**

Könnte interessieren: **Maschinen- und Anlagenbetreiber, IT-Leiter**

Plug & Safe: IRMA benötigt für die Konfiguration nur einen einzigen Port, an dem dann der gesamte Netzwerkverkehr vorbeiläuft. Auf diese Weise identifiziert IRMA automatisch, welche Geräte angeschlossen sind und wer mit wem kommuniziert.

© INDUSTRIAL AUTOMATION

meist nur zum Teil dokumentiert.“ Erst nach einer profunden Analyse konnte das Projektteam nun beginnen, Vorgaben zielführend zu definieren und für den Betreiber die Dimension des Projekts zu umreißen.

Ein Port und los gehts

Der große Vorteil: IRMA benötigt für die Konfiguration nur einen einzigen Port. An diesem so genannten Mirror-Port läuft der gesamte Netzwerkverkehr vorbei. Auf diese Weise sieht sich IRMA im vorgegebenen Netz um und identifiziert automatisch, welche Geräte angeschlossen sind und wer mit wem kommuniziert. „Da IRMA komplett passiv ausgelegt ist, übt es selbst keine problematischen Zugriffe im Netzwerk aus“, erklärt Lussnig. „Und letztlich kann ich nur schützen, was ich auch kenne.“ Diesen Prozess ließ das Projektteam eine Woche laufen. Viele Kunden erkennen dann häufig zum ersten Mal, welche Assets tatsächlich in ihrem Netz vorhanden sind und welche Verbindungen diese Geräte untereinander eingehen. „Man kann sagen, IRMA liefert nicht nur einen Fingerabdruck der gesamten Anlage ab, sondern schafft Transparenz für den gesamten Datenverkehr“, sagt Lussnig. „Das ist im Grunde der USP des Systems.“ In einem nächsten Schritt musste IRMA erklärt werden, welche Funktionen die einzelnen Assets im Netzwerk übernehmen. Im Zuge dessen erstellt IRMA automatisch einen kompletten Netzplan. Für diesen Schritt war die Kooperation und Mitarbeit der Inhouse-EDV-Mitarbeiter unabdingbar. „Als Externer kann ich nicht automatisch alles wissen“, so Dunke. „Damit die Herausforderungen im Projektverlauf immer geringer wurden, musste das Wissen des Kunden in das Projekt eingebracht werden.“ Ab dem Moment, wo der Kunde mithalf, die Assets zu definieren, zu kategorisieren und zu validieren und in ein Risikomanagement einzuarbeiten, war der Berater in der Lage, genau den Umfang und monetären Aufwand des Projekts zu greifen. Ein weiterer großer Vorteil: Im Grunde musste der Kunde nur während dieser bestimmten Phase aktiv mitarbeiten. Danach konnte der Kunde Aufgaben wahlweise an die Berater abgeben oder auch selber übernehmen. „In einem folgenden Schritt brachten wir für den Bereich Risikomanagement unser Know-how ein“, so Dunke. „Das heißt, Assets wurden bestimmten Bedrohungskategorien und Sicherheitsmaßnahmen zugewiesen.“ In einem RISK-Managementprozess erhielten somit Assets Wichtigkeitsstufen und es wurde genau festgelegt, was im Falle einer Bedrohung passieren soll. Damit wird das qualifizierte RISK-Management zum zentralen Punkt von IRMA.

Sicherheit, die in Echtzeit mitdenkt

„IRMA ist das erste Überwachungssystem, das sich störungsfrei in den Produktionsprozess implementiert“, betont Dunke. Es lernt das kontinuierliche Überwachen und steuert die Alarmierung angepasst an die Schutzklassen in ihrem Risikomanagement-Prozess. Denn eine penible Überwachung und ein ebenso genaues Reporting in Echtzeit sind die notwendigen Voraussetzungen für das Erkennen von Cyberangriffen, die eine Produktionsanlage bereits erreicht haben. Dafür ist es erforderlich, dass die von den Angreifern eingesetzten Werkzeuge und Datenverbindungen kontinuierlich beobachtet, kontrolliert und analysiert werden, um die Ausbreitung und damit auch den Cyberangriff selbst zu stoppen. Die verschiedenen Alarmmeldungen werden mit IRMA priorisiert, angezeigt und verteilt und können auch online in einem Alarmmanagement dargestellt werden. Mit IRMA erfolgt die Priorisierung von Alarmmeldungen wahlweise automatisch oder in effizienter Weise über das Risikomanagement. Die Alarmhäufigkeiten sind auf ein handhabbares Maß beschränkt und die Aussagekraft der Alarme ist sehr hoch.

Trotz dieser zur Verfügung stehenden Lösungen und Technologien sind Endkunden wie zum Beispiel Ferien- und Krankenhäuser oder Kasernen in Fernwärmeanlagen immer noch ohne Verschlüsselung vernetzt. „Tragisch ist, dass somit auch außerhalb der Unternehmensnetze – wider besseren Wissens – fahrlässig auf Sicherheitsmaßnahmen in der BUS-Kommunikation verzichtet wird“, mahnt Dunke. „Das ist wirklich ein ganz heißes Spiel …“

ZUM AUFTRAGGEBER:

Der Systemintegrator sys.co bietet für das industrielle Umfeld von der Zustandsanalyse bis hin zur aktiven Durchführung der Optimierung von Leit-, Datenverarbeitungs- und Kommunikationssystemen ein breites und flexibles Leistungsspektrum. sys.co integriert mittels VPN z. B. verschiedenste SCADA-, HMI- und BUS-Systeme vom abgelegenen Fernwärmekunden am Schlechtpunkt des Leitungsnetzes bis zum Großabnehmer mit professioneller Inhouse-IT.

ZUM AUFTRAGNEHMER:

Industrial Automation ist ein Anbieter für Softwaresysteme für Automatisierungs- und Informationstechnik. Dazu gehören ein ganzheitlicher Schutz vor Cyberangriffen in Produktionsanlagen, die Identifikation aller IT-Systeme in den Anlagen, die zentrale Analyse der Netzwerke und IT-Komponenten in MES, SCADA, SPS und PLC sowie ein kontinuierlicher Überwachungsprozess.