WIE SICHER IST IHR SCADA-SYSTEM?

Security für die Smart Factory

OB MAN NUN über das Internet der Dinge spricht, über die Smart Factory oder über Big (Smart) Data – bei all diesen Trends der Industrie 4.0 geht es um gesteigerte Konnektivität, Optimierung, Effizienz und Datenaggregation. Es ergeben sich jedoch auch neue Anforderungen an die Sicherheit, und Produktionsunternehmen müssen ihre SCADA-Systeme für potenzielle Cyberbedrohungen und externe Angriffsszenarien vorbereiten.

Wir haben vor kurzem mit Marco Ramilli gesprochen, einem Informationswissenschaftler aus Italien mit umfassenden Erfahrungen im Bereich der Erkennung und des Schutzes vor Hacker-Angriffen, und haben ihn über die neuesten Entwicklungen im Bereich Security in der Industrie befragt. Erste Einblicke erhalten Sie in dieser Ausgabe der *IU*. In dem Folgeartikel in der nächsten Ausgabe wird Herr Ramilli detailliert auf das Thema Cyber Security eingehen und Ihre Fragen dazu beantworten.

Herr Ramilli, was sind Ihre Gedanken zum Internet der Dinge? Wie wird es Ihrer Meinung nach das Geschäfts- und Privatleben beeinflussen?

MARCO RAMILLI: Die Möglichkeit, sich mit einer unglaublichen Anzahl vernetzter, automatisierter Geräte über das Internet zu verbinden, mit ihnen zu kommunizieren und sie fernzusteuern, wird allgegenwärtig sein: von der Fertigungshalle über den Operationssaal im Krankenhaus bis hin zum Keller in Ihrem Wohngebäude.

Der Übergang von geschlossenen Netzwerken über Firmennetzwerke bis hin zum öffentlichen Internet setzt sich mit alarmierender Geschwindigkeit fort und erweckt gerechtfertigte Bedenken, was die Sicherheit betrifft. Betrachten wir zum Beispiel einen simplen intelligenten Zähler (Smart Meter), der Daten über den Energieverbrauch an den Betreiber schickt, um eine dynamische Abrechnung oder eine Netzoptimierung in Echtzeit zu ermöglichen. Das System muss imstande sein, diese Informationen vor unberechtigtem Zugriff zu schützen. Ein Sicherheitsvorfall, der diese Daten betrifft, kann weitreichende Folgen für das Alltagsleben haben: von der fälschlichen Erhöhung einzelner Stromrechnungen bis hin zum Ausfall der öffentlichen Stromversorgung.

Es stellt sich zum Beispiel auch die Frage, wie man Millionen von mobilen, tragbaren und weitverzweigten Anwendungen mit Sicherheitsupdates versorgen soll. Wie sieht es mit dem Thema Datenschutz aus? Wo werden die Daten zu meiner Herzfrequenz gespeichert, wenn ich meine Pulsmesser-App schließe? Gibt es irgendwelche Patentrezepte, um Cyberbedrohungen im Internet der Dinge zu verhindern? Wie leicht ist es für Nutzer, sich selbst zu schützen? Sind dafür besondere Tools oder Vorgehensweisen nötig?

Die Antwort lautet: Nein, es gibt keine Patentlösung, um sich vor allen Bedrohungen zu schützen. Aber Nutzer können die bekanntesten Bedrohungen abwenden, indem sie sich spezielle Verhaltensweisen aneignen und gewissen Sicherheitsregeln folgen.

Wie hat sich das Thema Security in der Industrie über die Jahre gewandelt und was sind die Auswirkungen auf SCADA-Systeme?

MARCO RAMILLI: Vor einigen Jahren noch waren Cyberangriffe kostspielig und aufwändig. Die durchschnittliche Erfolgsrate von Cyberangriffen wurde auf etwa 20 % eingeschätzt. Aus diesen Gründen waren Cyberangriffe kein wirklich großes Thema und nur wenige Unternehmen davon betroffen. MarketsandMarkets[1] schätzt, dass Cyberangriffe heutzutage zu den fünf gefährlichsten Bedrohungen in der Geschäftswelt zählen. Dank sogenannter „Exploit Kits" und einer neuen Untergrundwirtschaft namens „Exploit as a Service" sind die Kosten von Cyberangriffen gesunken und ihre Erfolgsrate von 20 % auf etwa 80 % gestiegen.

Normalerweise werden Daten auf Servern, Netzwerken und auch beim Endnutzer geschützt, aber wie sieht es mit den Daten auf SCADA-Systemen aus? Sind diese ausreichend abgesichert? Da SCADA-Systeme meist weniger stark abgesichert sind als andere Systeme eines Unternehmens, werden diese meist direkt angegriffen, anstatt die „traditionelle Route" über Malware oder System Exploitation zu wählen. Angriffe auf SCADA-Systeme sind inzwischen weitaus billiger und erfolgreicher geworden. Darum ist es absolut wichtig, solche Angriffe zu blockieren und Bewusstsein dafür zu schaffen, wie diese entdeckt und identifiziert werden können.

Herr Ramilli, vielen Dank, dass Sie Ihre Erfahrungen mit uns geteilt haben.

DAS INTERVIEW FÜHRTE GIUSEPPE MENIN
INDUSTRY MANAGER BEI COPA-DATA ITALIEN

[1] www.marketsandmarkets.com

IU
Erschienen in
INFORMATION UNLIMITED
DAS MAGAZIN VON COPA-DATA
Nr. 26, November 2014

www.copadata.com/iu

FOTOGRAFIE: CHRISTOPHER CURRIE, GILLIAN LAWTIE

FRAGEN SIE DEN EXPERTEN

Herr Ramilli beantwortet gerne Ihre Fragen zu den Themen Datensicherheit und Schutz vor Cyberangriffen. Wenn Sie eine Frage stellen möchten, schicken Sie einfach ein E-Mail an **IU@copadata.com.**

Die Fragen und Antworten werden in der nächsten Ausgabe des *IU-Magazins* im Jahr 2015 veröffentlicht.

Bis jetzt haben wir in allen Unternehmen, die uns um Hilfe gebeten haben, Sicherheitslücken gefunden. Unsere Kunden wissen meistens gar nichts von diesen Informationslecks, aus denen laufend Informationen aus ihren Unternehmen nach außen fließen, und sind sich nicht bewusst, welchen neuen Bedrohungsszenarien ihre Unternehmen ausgesetzt sind.

MARCO RAMILLI, YOROI

ÜBER MARCO RAMILLI

Marco Ramilli hat einen PhD in Computer Security und an der University of California in Davis (USA) sowie der Universität Bologna (Italien) studiert. Er hat im Bereich Computer Security gearbeitet, zuerst an der UC Davis und später für die Regierung der USA (National Institute of Standards and Technology [NIST], Abteilung Security), im Speziellen an Techniken der Malware-Umgehung sowie im Bereich Reverse Engineerung von Wahlcomputern. Danach hat er bei Palantir Technologies im Bereich Cyber Security Intelligence gearbeitet und ist nun einer der Gründer von YOROI, einem vielversprechenden Startup, das Industriedaten vor Cyberangriffen schützt. Laut Herrn Ramilli spielen SCADA und ICS-Security eine wichtige Rolle bei Angriffen auf Industriedaten. Mehr Informationen über Herrn Ramilli und seine Aktivitäten im Bereich Cyber Security finden Sie unter **www.marcoramilli.com**.

ÜBER YOROI

Der Name YOROI leitet sich von der alten Bezeichnung für die Rüstung eines Samurais ab. Heute schützt YOROI seine Kunden, so wie ein YOROI früher den Samurai schützte. Unser Ziel ist es, mithilfe unserer Erfahrung und Ausbildung ein „Unternehmen zu kartographieren", also seine Geschäftsprozesse zu verstehen, die Geschäftsrisiken zu bewerten und so wie ein Angreifer zu denken, um Sicherheitsmaßnahmen zum Schutze des Unternehmens umsetzen zu können. Für jeden Kunden gibt es bei uns eine aktive Karte *(siehe Abbildung 1)*, über die wir Callbacks zu Bedrohungen geolokalisieren, mit Active Directory kommunizieren, um eine Attacke zu lokalisieren, Malware und Bedrohungen analysieren und E-Mail-Metadaten überwachen, um verdeckte Informationsübertragungen oder Angriffe zu entdecken. Diese „Landkarte" ist rund um die Uhr aktiv und kann auf den Bildschirmen der IT-Abteilung des Unternehmens angezeigt werden. Unser System überprüft strategisch die verwundbaren Stellen des Unternehmens, überwacht dynamisch den Status der Malwareverbreitung und garantiert unseren Kunden eine schnelle und tiefgehende Analyse. Wir bieten einen permanenten Cyber Security-Service, über den unsere Security-Samurais die Netzwerkaktivitäten unserer Kunden mit unserer Technologie überwachen, um Angriffe zu erkennen und Bedrohungen auszumachen, die von Angreifern ausgenutzt werden könnten, wie z.B. verwundbare Stellen, E-Mail-Ströme, Datenfluss zwischen verschiedenen Einheiten etc. Wir reagieren schnell und blockieren bösartige Aktivitäten entsprechend der Prozessrichtlinien des Kunden und arbeiten proaktiv an der Sicherung der SCADA-Netzwerke sowie der privaten und öffentlichen Netzwerke der Kunden. Weiterführende Informationen finden Sie unter **www.yoroi.ninja**.

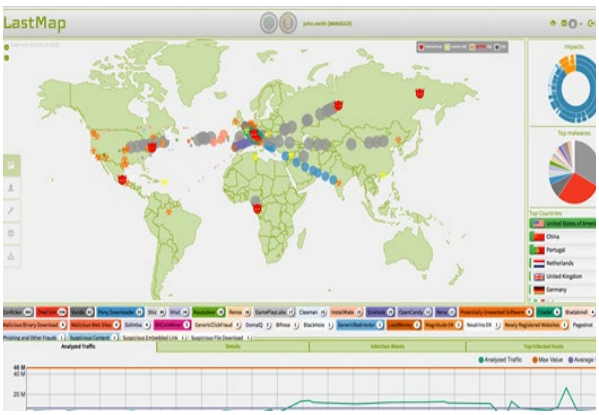

Abbildung 1: Umfassende Bedrohungsanalyse für optimale Sicherheit und Kontrolle. Die Karte zeigt dynamische Abläufe aus einem anonymisierten Kundennetzwerk. *Quelle: http://www.lastmap.net.*