HOW SECURE IS YOUR SCADA?

Security for the Smart Factory

REGARDLESS OF WHETHER we are talking about the Internet of Things, the Smart Factory or Big (Smart) Data, all these trends which characterize Industry 4.0 involve increasing connectivity, optimization, efficiency and data aggregation. However, they also have significant implications for security and production companies need to prepare their SCADA systems for potential cyber threats and external vulnerabilities.

We recently met with Marco Ramilli, a computer science researcher from Italy with an extensive background in identifying and protecting against hacking, and asked him about the evolution of industrial security. Get first insights in this *IU* interview: In the next issue's follow-up article, Mr. Ramilli will discuss the topic of cyber-security in detail and answer your questions.

Mr. Ramilli, what are your thoughts on the Internet of Things (IoT)? How will it affect businesses and private life in your opinion?
MARCO RAMILLI: The ability to connect, to communicate with, and to remotely manage an incalculable number of networked, automated devices via the internet will become pervasive: from the factory floor to the hospital operating room to the residential basement.

The transition from closed networks to enterprise IT networks to the public internet is accelerating at an alarming pace and justly raising alarms about security. For example, let's think about a simple smart meter able to send energy usage data to the utility operator for dynamic billing or real-time power grid optimization. The system must be able to protect that information from unauthorized use or disclosure. A security breach involving that data might have deep impacts on daily life: from increasing the cost of energy bills right through to shutting down the public power service.

It also raises more questions: how to deliver security updates to millions of mobile, wearable and wide-ranging systems? What about privacy? Where is my heart rate data stored after leaving my mobile cardio app? Are there any patterns or any silver bullets to limit cyber threats on the IoT? How easy is it for users to protect themselves? Do they need specific tools or procedures?

The short answer is: no. There isn't a silver bullet for these threats. But users could do a lot of things to avoid well-known threats by adopting specific behaviors and security approaches.

How has industrial security changed over the years and what are the implications for SCADA systems?
MARCO RAMILLI: Years ago, cyber-attacks were expensive and hard to realize. The average cyber-attack success rate was estimated to be around 20% of all attempted cyberwarfare. For these specific reasons, cyber-attacks were not so common and only a few companies were affected by such a threat. MarketsandMarkets[1] estimates that nowadays cyber-attack is one of the top five threats to business. Thanks to exploit kits and to a new underground economy called "exploit as a service", the cyber-attack price dropped and the success rate swelled from 20% to around 80%.

Usually data is protected on servers, networks and even at the end-user access point, but what about data on SCADA systems? Are they sufficiently secure? Since SCADA systems are frequently less secure than other business systems, attackers often decide to directly attack the company's SCADA system rather than trying to implement a more "traditional attack path" such as malware propagation or system exploitation. Nowadays, attacking SCADA systems is much less expensive and carries a higher success rate. Therefore, it is essential to block those attacks and to increase the awareness about how to discover and identify such attacks.

Mr. Ramilli, many thanks for sharing your experience with us.

GIUSEPPE MENIN
INDUSTRY MANAGER, COPA-DATA ITALY

[1] Source: www.marketsandmarkets.com

IU
Published in
INFORMATION UNLIMITED
THE COPA-DATA MAGAZINE
No. 26, November 2014
© Ing. Punzenberger COPA-DATA GmbH
www.copadata.com/iu

PHOTOGRAPHY CHRISTOPHER CURRIE, GILLIAN LAWTIE

ASK THE EXPERT

Mr. Ramilli is happy to answer your specific questions on data security and cyber-attack protection. If you are interested in asking a question, drop an e-mail to **IU@copadata.com.**

The Q&As will be published in the next *IU Magazine* which will be published in 2015.

ABOUT MARCO RAMILLI

Marco Ramilli received his PhD in Computer Security following study at the University of California at Davis (USA) and the University of Bologna (Italy). He worked on computer security, in particular on malware evasion techniques and voting machine reverse engineering at UC Davis and, later, with the US Federal Government (National Institute of Standards and Technology (NIST), Security Division). He then worked in cyber security intelligence at Palantir Technologies and is now one of the founders of YOROI, a very promising start-up which protects industrial data from cyber-attack. According to Mr. Ramilli, SCADA and ICS security plays a key role in today's attacks on industrial data. To find out more about Mr. Ramilli and his activities in the field of cyber security, visit **www.marcoramilli.com**.

ABOUT YOROI

YOROI gets its name from the ancient name of the Samurai's armor. Today, YOROI protects its customers as the YOROI protected the ancient Samurai. The goal is to use our experience and education to "map a company": understanding the business processes, assessing the business risks and thinking as an attacker would do in order to apply security measures to protect the company. For each customer we have an active map (see Figure 1) which is able to geo-localize the threat callbacks, to interact with Active Directory in order to localize an attack, to analyze malware and threats, and to monitor email metadata in order to discover covert channel information leakage or attack. The "map" is active 24/7 and is even available on monitors in the company's IT offices. Our system strategically checks the company's vulnerabilities, dynamically checks the malware propagation status, and guarantees fast and deep analysis for our customers. We offer a 24/7 cybersecurity service, where our security samurais analyze the customer network flows using our technology in order to find intrusions and threats, such as vulnerabilities, email flows, data moving between entities, and so on, which might be exploited by attackers. We promptly act to block that specific flow, according to the customer's process policy, and proactively work to secure the customer's private, SCADA and public networks. For further information visit **www.yoroi.ninja**.

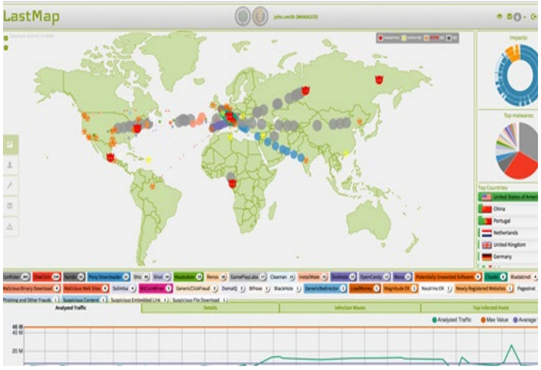

Figure 1: Complete threats analysis for optimal safety and control. The map shows dynamic flows from an anonymized customer network.

Source: http://www.lastmap.net.

> *So far, we have always found security breaches in any company that has asked for our help. Often our customers have no idea about the information leakage and the information that is constantly flowing out of their companies and they are not aware of the new threat paradigms that might affect their business.*
>
> **MARCO RAMILLI,** YOROI