MARCO R. PASSERINI
RES IT srl, Milan, Italy

Cybersecurity and business software control:
do not fear the unknown, face reality!

KEYWORDS: Achema, cybersecurity, cyberattack, RES, safety, software, big data, industry 4.0.

ABSTRACT

Cybersecurity. Can you feel safe? In a world where nobody can really think to be safe from the risk of attacks on their IT systems, where companies are still too slow in realising the risk for their business and their own safety, there is a number of institutional players that offers excellent solutions to limit cyber-attacks to the heart of information systems. However, too often these solutions focus on inhibiting physical attacks, while securing perimeter vs SW applications does not get the attention – and the budget – it should, given that 84% of cyber-attacks are directed to the SW application layer.
Moreover, most security professionals find themselves struggling to mend damage all the time, while it would obviously be better to prevent it. This article suggests taking a more holistic approach to achieveing effective cybersecurity.

CYBERATTACKS ALSO THROUGH THE SW LAYER

"Cybersecurity is the protection of computer systems from the theft and damage to their hardware, software or information […], includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection […]". *(1)*

"Cybersecurity is the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this". *(2)*

I think the two statements above are good enough to describe what cybersecurity is, also to those not yet familiar with the word.

In a world where no one can really feel safe from cyberattacks and where companies still lack awareness of the risk these attacks pose for their business and their own safety – companies are especially not aware of how weak their cybersecurity protocols are - there are many institutional players who offer excellent solutions to limit cyberattacks to the heart of information systems. Unfortunately, too often these solutions concentrate only on inhibiting physical attacks, while they fail to focus on - and allocate budget to - securing perimeter vs SW applications, especially given that 84% of cyberattacks target the SW application layer.
Moreover, most part of security professionals struggle to find solutions to a damage that has already occurred, while it would be desirable to prevent instead of treating.

OT, IT AND IIOT

In an environment where computers and devices have always been characterized primarily as OT, by virtue of their indispensable role for automation, and where IT historically has had a role of service to business and bureaucratic requirements, it is now time for industry 4.0.

In this reality we are witnessing an overwhelming affirmation of IIOT, a close relative of that IoT which permeates our everyday life.
IIoT (and IoT) means explosion of potential in the industries, means greater and better productivity, increased process safety, better "time to market" - in short, it means improving business.
New technological categories such as Machine Learning and Cognitive Services, derived from the A.I. platforms, have favored the progress of the IIoT (a more highly specialized IoT dedicated to specific requirements), whose specific advantages are now appreciated in every industrial sector.

To make the most of the huge potential of these technologies (IIoT, as well as the much better known OT), not only greater device power and greater flexibility are required, but also greater interconnection with IT systems (even "traditional" ones) and with their SW (including the "business software applications"), in order to make the benefits taken by IIoT not only available to the production areas but also to the marketing, planning, sales, management, etc. areas.
This interconnection is creating platforms that are becoming increasingly complex to manage and is posing a cultural problem: not all are prepared to govern the amount of data made available and the related tools for their better management. It is not just a matter of technological platforms, we are actually witnessing the birth of an ecosystem that brings together skills, cultures and platforms.
In the best of hypotheses, "losses of opportunities" can happen, yet that would be just the least of the evils.
In fact, a very dangerous side effect of the difficulty in the management of this complex ecosystem is the exposure to cyberattacks.
Cyber criminals are very experienced in exploiting situations of extreme complexity to their advantage, in which they seem to move easily.

CYBERSECURITY, STATE OF THE ART

Cyberspace is the most complex thing that man has ever built:

- Hundreds of thousands of interconnecting networks and components (HW – SW)

- IoT units will reach 20 billion units installed base in 2020 *(3)*
- 27% of third-party software used in business SW applications is classified "high-risk", 58% is "medium-risk", while only the remaining 15% is considered "low risk" *(4)*
- stratification of programs and protocols developed over decades make SW difficult to manage and control
- complexity generates vulnerabilities (software errors, incorrect configurations and weaknesses in protocols)
- cyber criminals leverage on complexity and bugs to steal data and damage business.

Cyberattacks to companies (industry, telco, utilities, social media, financials, government, …) is a true threat that must be dealt with. In 2017, 29% of companies suffered attacks, and 34% of them experienced a substantial loss of revenue: 4% a total loss, 10% a 60-80% loss, 20% a 20-40% loss, also due to bad outages of service: (10% : > 24 hours, 27% : 9-24 hours, 45%: 1-8 hours) *(5)*.

Every breach lasts for long and is expensive to be identified and fixed. They take, on average, at least 100 days to be detected, and much more to be fixed, depending on the level of their severity.

Many players on the market are ready to help the industrial sector, but it looks as if, while there's strong attention to perimeter safety achieved with technical solutions and dedicated HW, there's not enough attention yet to solutions targeted to the SW application layer, even though cyberattacks through the SW account for about 84% of the total attacks in recent times.

Recent statistics underline that the "culture of cybersecurity" is still too weak in the SMB market, too often the attitude seems to be "we'll cross the bridge when we come to it". 30% of small businesses do not use any protection system at all, while 44% of medium-sized businesses use "advanced" security systems for Intrusion Detection and Id/Access Management only. *(6)*

Despite regulatory authorities have recently tried to drive companies to adopting more efficient systems and protocols, at least in the field of Data Protection, by issuing regulations like the European GDPR (companies were required to be compliant by May 2018), there's still 50% of European SMB that declare they have no idea what GDPR even is.
Almost no one is aware of the CIS RAM recommendations (Center for Internet Security® Risk Assessment Method, a risk assessment method that helps organizations implement and assess their security). *(7)*

PERIMETER SECURING AND SW APPLICATIONS AND DATA SECURING, A HOLISTIC APPROACH

Up to now, as previously mentioned, the focus has been on perimeter safety especially, achieved primarily through technical solutions, dedicated HW, whereas the SW application layer has not been given enough attention, despite the fact that the majority of attacks occur at SW application layer.

Therefore, historically, "perimeter" solutions have been much more developed, thus today a variety of market players offer advanced solutions like: Intrusion Prevention



Services (IPS), Reputation Enabled Defense Services (RED), Gateway, Antivirus (GAV), APT Blocker, Threat Detection & Response, Host Ransomware Prevention (HRP), Data Loss Prevention (DLP), ...

On the other hand, there is much less awareness of and care for securing SW applications through specific tools capable of performing detailed analysis of software components, their interconnections, and the "troian horses" they may allow through.
Securing SW applications so that they do not function as an open door for threats to enter, a full understanding of how the various layers of SW interact with each other is mandatory. To achieve this, it is essential to understand the exact topography of the SW first of all (identify all the SW components, where they reside, how they mutually exchange data, how they call one another), while a second step is assessing whether there are any "at risk" components (often difficult to spot), so to be able to change or replace such dangerous SW objects.

Though running strict testing on SW before this is implemented into a company's production environment (performed by Quality Assurance professionals) is mandatory and useful to avoid the risk of breaches, more comprehensive SW testing could be involving also SW developers in the testing process, thus starting form the very early stages of SW design and development, which could avoid using easy-to-breach SW components and processes.

A comprehensive approach for implementing effective protection systems must leverage the intrinsic capabilities of all these solutions, seek system design through qualified and skilled professionals and include the integration of company-owned platforms and systems with those of suppliers, clients and business partners.

It is mandatory to see all the systems and processes involved as components of one single holistic framework – the idea is that it would make no sense to put bars on the windows if we left the front door unlocked.

ISA IS CONVEYING A MESSAGE TO THE INDUSTRY AND IS STRONGLY COMMITTED TO HELPING ITS ASSOCIATES

Recent analysis of the industry has shown that the attention of enterprises for information security in general is still very low. Financial companies, on average, spend around 0.6% of their revenue for cybersecurity, while energy companies barely spend 0.2%.

As a matter of fact, we hear of an increasing number of breaches into the OT and IT systems of large and important companies, for instance the recent cyberattack to the safety systems of Saudi Aramco (Dec 2017), an important energy supplier.
ISA, the International Society of Automation, which comprises and has advised over 40,000 subscribers worldwide since 1945, has seen its D12 section (EMEA) and especially its Italian section (ISA Italy) do a great job in seriously addressing the issue and has initiated a process of dissemination of cybersecurity culture.

A first important step by ISA Italy has been organising the cybersecurity conference held at ACHEMA 2018 in Frankfurt, with the support of Rockwell Automation , BAGGI and RES IT, where numerous attendees from a number of industries and with varying job responsibilities (CEOs, Department Directors, Marketing Directors, Engineers, IT representatives ...) confirmed their interest in improving the general awareness towards cybersecurity issues.

THE CYBERSECURITY CONFERENCE @ ACHEMA 2018

Various speakers, on behalf of their respective companies (RES IT, Rokwell, Microsoft, CISCO, Panduit, Claroty, Honeywell, Page Europa, GMI), all market beacons of cybersecurity solutions, have been invited and have come together on this intense and interesting day to present their visions (and their solutions).

The interconnection between IT and OT, due to the evolution of the IoT/IIoT, and the cyber-confusion exploitd by cyber-criminals to jeopardize cyber-security, has been the main focus of the day.
Speakers at ACHEMA 2018 agreed on some fundamentals. Making a long story short, they agreed that any device and software can be compromised (threats come from all around) and knowledge of the systems and their interconnections is the mandatory first step to be on the ball (you can't manage what you don't know).

A strong suggestion is to rely on institutional market-proven providers (no do-it-yourself solution would work nor would be safe), and companies need to face the reality with a holistic approach.

REFERENCES AND NOTES

1. https://en.wikipedia.org/wiki/Computer_security
2. https://en.oxforddictionaries.com/definition/cybersecurity
3. GARTNER, Leading the IoT: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf - pag. 2 (last checked on Oct. 15th 2018)
4. CISCO, 2017 Annual Cybersecurity Report: https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf pages 17-18 (last checked on Oct. 15th 2018)
5. CISCO, 2017 Annual Cybersecurity Report: https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf - page 6 (last checked on Oct. 15th 2018)
6. Politecnico di Milano, Osservatori Digital Innovation: https://www.osservatori.net/it_it/osservatori/comunicati-stampa/gdpr-e-security-un-percorso-impervioa-a-trazione-integrale (last checked on Oct. 15th 2018)
7. https://learn.cisecurity.org/cis-ram. ■

ABOUT THE AUTHOR



***Marco Passerini**, VP Channel & WW operations of RES IT and President of RES IT US Inc., has been with RES IT (worldwide leader in IT services and system integration) since the company was founded in 1987. Marco has helped over 100 IT companies around the world to improve their technological and organizational development through IT performance optimization, automation of processes, application management, System-Governance and Quality, SLA control, Cybersecurity, DC mergers and more.*