Prevenire

è (molto) meglio che curare

L'evoluzione delle tecnologie di produzione mostra chiaramente quanto siano centrali i sistemi informatici nel mondo manifatturiero. Questo rende le aziende ancora più vulnerabili ai cosiddetti cyber attacchi, in grande aumento a livello mondiale e anche in Italia. Con conseguenze molto serie per chi li subisce. ASSIOT e ASSOFLUID hanno organizzato un interessante momento di confronto sul tema.

di Fabrizio Dalle Nogare

● Da sinistra, Francesco Di Prisco, Omar El Hamdani, Simone Scanavini e Abdel Adim Oisfi.

● *From the left, Francesco Di Prisco, Omar El Hamdani, Simone Scanavini and Abdel Adim Oisfi.*

Solo nei primi 6 mesi del 2017, quasi 2 miliardi di dati sono stati violati nel mondo, in aumento del 164% rispetto al semestre precedente (fonte: Gemalto). Al momento, secondo Cybersecurity Ventures, i costi del cybercrime sono stimati in circa 4.000 miliardi di dollari, ma si pensa che la cifra possa raggiungere i 6.000 miliardi nel 2021.
Bastano queste poche cifre per rendere l'idea della dimensione di un fenomeno, quello legato ai cyber attacchi e alla sicurezza delle informazioni, che interessa inevitabilmente anche il mondo industriale e produttivo, sempre più attento alla raccolta e all'analisi dei dati di produzione. "Stando ai dati diffusi di recente, l'industria manifatturiera italiana deve crescere in termini di consapevolezza della portata del fenomeno", ha detto il direttore di ASSOFLUID Marco Ferrara. Della stessa idea è anche Fabrizio Cattaneo, segretario di ASSIOT, che ha sottolineato come sia importante "fare cultura su temi di cui, forse, si parla ancora poco".

Special report

Prevention Is (Much) Better than Cure

The evolution of production technologies clearly shows how important IT systems are in manufacturing. This makes companies even more vulnerable to the so-called cyberattacks, which are increasing worldwide and even in Italy. With very heavy consequences for those who have to cope with them. ASSIOT and ASSOFLUID organized an interesting event to discuss the subject.

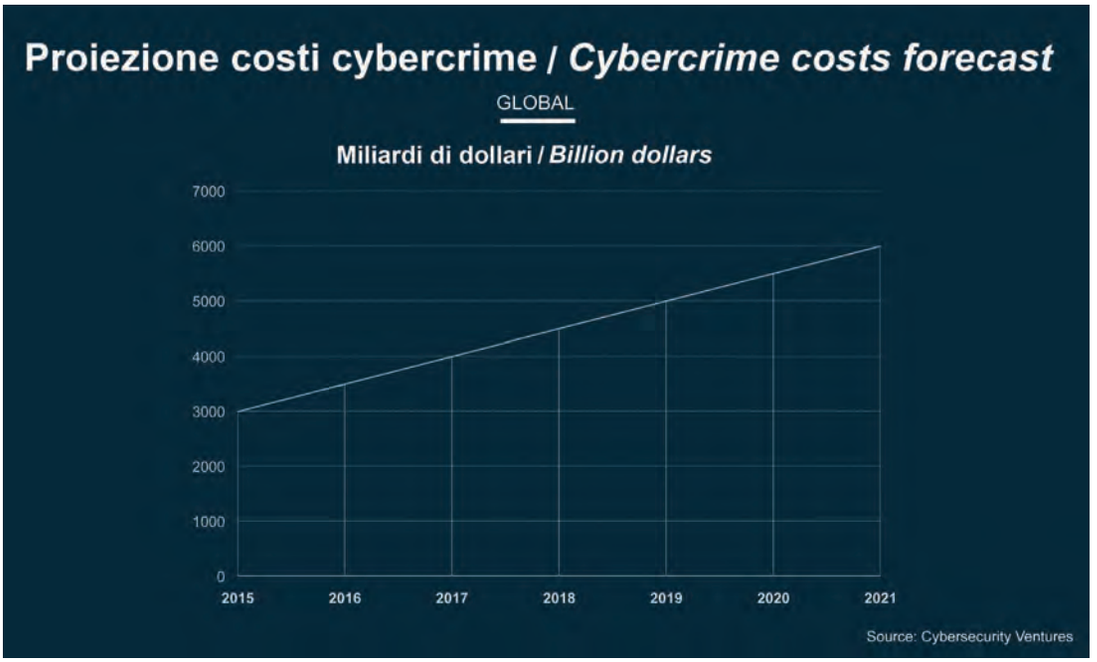
Only in the first six months of 2017, almost 2 billion data were violated worldwide, up 164% over the previous six months (Source: Gemalto). According to Cybersecurity Ventures, cybercrime costs are currently estimated at about $4,000 billion, but this figure is expected to reach $6,000 billion in 2021.
These few figures are enough to make the idea of the relevance of a phenomenon, the one related to cyberattacks and information security, which inevitably affects the industrial and manufacturing world, which is increasingly focused on collecting and analyzing production data.
"According to the latest statistics, the Italian manufacturing industry needs to become more aware of such a phenomenon", said ASSOFLUID Director, Marco Ferrara. This view is also shared by Fabrizio Cattaneo, ASSIOT Secretary, who stressed how important it is to "promote culture on topics that perhaps are not widespread yet".

An actual underground war

Simone Scanavini, eForHum Cisco Instructor, in the introduction to his speech used an expression borrowed from the world of computer science: World Wide War. "It is an actual underground war. Every 40 seconds a company in the world is under attack - he said -. The major danger is having to stop production for an undefined amount of time, with very significant damage. In addition, attacks can last for months, even years, and companies may also jeopardize their reputation, which is then very difficult to rebuild".
Also, the source of the attack can come from outside, but also from inside the company: according to data for the first half of 2017, against 73% of attacks coming from outside, 18% is attributable to so-called "malicious insiders", or rather people working for a given company. "According to a research conducted by Cisco Systems, only 56% of security alerts are being investigated, while it is possible to remedy no more than 13% of these", added Mr Scanavini.

The evolution of regulations

Omar El Hamdani from Shielder, a company working in IT security, web development and



● I costi del cybercrime sono oggi stimati in circa 4.000 miliardi di dollari, ma si pensa che la cifra possa raggiungere i 6.000 miliardi nel 2021.

● *Cybercrime costs are currently estimated in around 4.000 billion dollars. They are expected to reach 6.000 billion in 2021.*

Una vera guerra sotterranea

Ha usato un'espressione mutuata dal mondo dell'informatica Simone Scanavini, eForHum Cisco Instructor, nell'introduzione al suo intervento: World Wide War. "Si tratta di una vera e propria guerra sotterranea, se pensiamo che ogni 40 secondi un'azienda nel mondo subisce un attacco - ha detto -. Il grande pericolo è quello di dover interrompere la produzione per un tempo difficile da definire, con danni molto rilevanti. Inoltre, gli attacchi possono anche durare mesi, addirittura anni e le aziende mettono a rischio anche la loro reputazione, che poi è molto difficile ricostruire".

La fonte dell'attacco, poi, può essere esterna, ma anche interna all'azienda: secondo i dati relativi alla prima metà del 2017, a fronte del 73% degli attacchi provenienti dall'esterno, il 18% è imputabile ai cosiddetti *malicious insider*, cioè persone che lavorano in azienda.

"Secondo una ricerca condotta da Cisco Systems, soltan-

design, provided an overview on both national and international standards concerning the issue of information security. "The new data protection regulations, and in particular the European General Data Protection Regulation (GDPR), which will enter into force from May 2018, are expected to change deeply the world of IT security - he said - giving more rights to the users. Among other things, it will become mandatory to communicate any cyberattack".

On a national scale, the framework for cybersecurity is provided by CIS-Sapienza and is strongly SME-oriented.

Francesco Di Prisco, Responsible for D.A.S. Training, focused his speech on the practical consequences of cyberattacks, defined as "actual criminal acts of great significance.

A company that has to face an attack is uncomfortable with three subjects: employees, customers and suppliers, with relevant consequences. A defense is mandatory and can be very expensive".

Searching for vulnerabilities

But how does a cyberattack take place? Abdel Adim Oisfi from Shielder described five case scenarios that actually happened. These tests simulate an attack to verify the reliability of prevention and defense strategies implemented by companies.

"The first step is always identifying vulnerabilities - explained Mr Oisfi - through what is called penetration test or by means of an OSINT, an acronym for Open Source INTelligence, which consists of searching for information on platforms or public access sources - social networks, for example - to find possible access points to an organization's IT system. Generally speaking, only a few information are enough to understand how a company is vulnerable". Among the five scenarios described, referred to companies with different sizes, the simplest was that of a company with employees in several locations around the world and capable to handle remote instrumentation. The resources were exposed on the Internet and it was quite easy to decript credentials, become network administrators, and "turn off" the company.

The difficulty of access in the various examples described grew up to the case of a very large company in the energy sector, highly protected both on a virtual and physical level. In this case, the vulnerability was found in the employees access badges, which were cloned by means of a device that was approached to the badges during their journey on the subway. Relying on these badges, the attackers were able to enter the company and act on the IT system. More complicated, not at all impossible. ●

Suddivisione per tipologia dei dati violati nelle aziende.

The categories of violated company data.

PMI e grandi aziende uguali davanti al pericolo

Abbiamo rivolto qualche domanda a Simone Scanavini, eForHum Cisco Instructor ed esperto di sicurezza informatica.

Sono le aziende più grandi e strutturate a essere più appetibili per i cyber attacchi, oppure le PMI corrono pericoli simili?
Oggi sta cambiando lo scenario: aziende con fatturato e dimensioni importanti si stano attrezzando per contrastare il fenomeno e il target si sposta verso quelle più piccole, che hanno spesso rapporti commerciali con quelle più strutturate e non sempre dispongono di budget da investire in sicurezza. È un modo per colpire le grandi aziende in maniera indiretta.

Cosa può fare un'azienda per una gestione attenta dei social network?
L'azienda può fare poco dal punto di vista pratico per evitare che i dipendenti abusino dei social network. Può tuttavia stabilire delle regole chiare per scaricare la propria responsabilità nei confronti di danni reputazionali o iniziative prese a nome dell'azienda, con policy ben definite al momento della consegna degli strumenti. Ovviamente occorre poi fare dei controlli, gli unici strumenti efficaci di prevenzione.

Le aziende del settore manifatturiero producono e produrranno sempre più dati. È giustificato il timore di non saper gestire al meglio questi dati? E come ci si pone oggi davanti alla questione dello storage in cloud o in locale?
Lo storage in cloud sta diventando più sicuro che in locale. Nel cloud operano grossi player con livelli di sicurezza molto elevati. Scegliendo la strada del cloud si scongiura il rischio dell'attacco dall'interno, da parte dei cosiddetti malicious insider. I dati saranno sempre di più, aumenterà il bisogno di protezione e sarà importante affidarsi ai professionisti giusti per minimizzare il rischio. In più, con le nuove normative tale esigenza diventerà un obbligo.

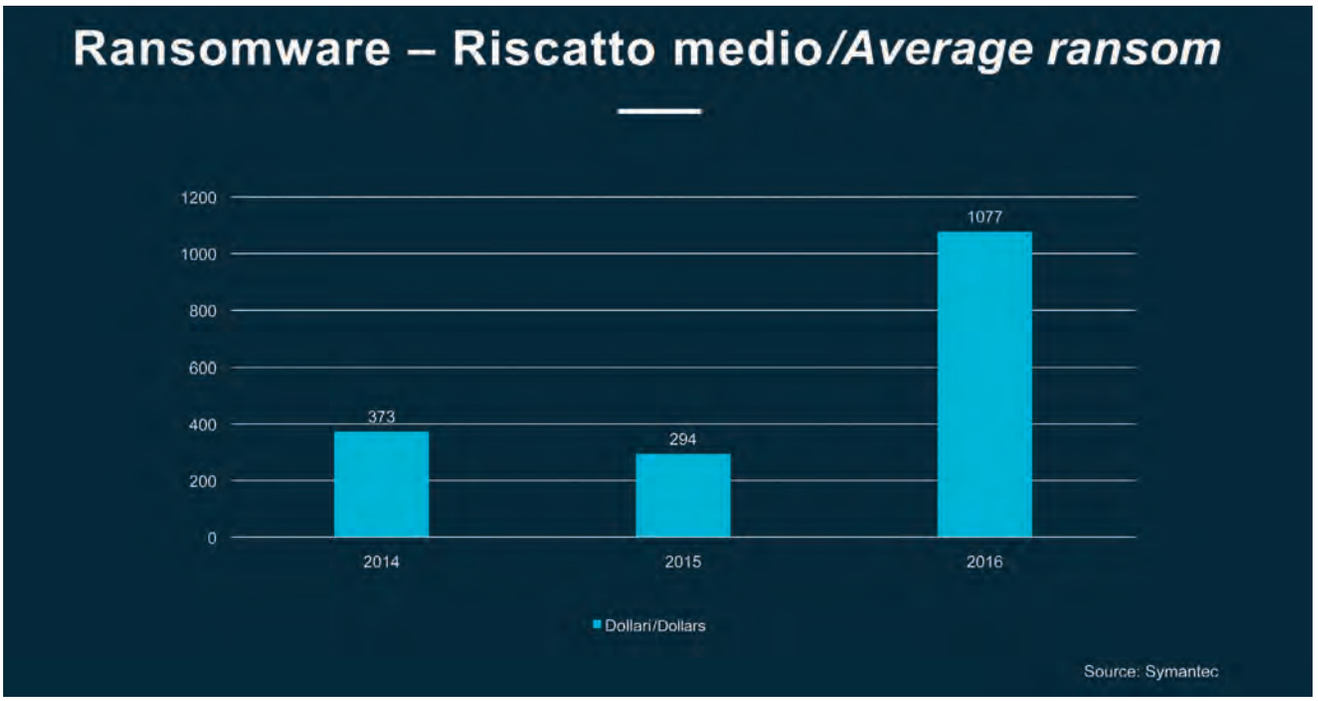
SMEs and big companies are equally in danger

We asked a few questions to Simone Scanavini, eForHum Cisco Instructor and IT security expert.

Are bigger companies more attractive than SMEs to cyberattacks?
Today, the scenario is changing: companies with significant turnover and size are gearing up to fight back and the target is moving to smaller ones, which often have commercial relationships with bigger companies and do not always have the budget to invest in security. It's a way to attack big companies indirectly.

What can a company do for a careful management of social networks?
Companies can do little to prevent employees from abusing social networks. However, they can set clear rules to discharge their responsibility for reputable damages or initiatives taken on behalf of the company, by means of well-defined policies. Obviously, controls are needed, as they are the only effective prevention tools.

Manufacturing companies will produce more and more data. Should they be worried of not being able to handle this data properly? And what do you think of the issue of Cloud or local data storage?
Data storage on Cloud platforms is becoming more secure than storing them in local. Big players manage Cloud platforms, with a very high security degree. By choosing the Cloud, the risk of attacks coming from the so-called "malicious insiders" is wiped out. The amount of data will increase more and more, as well as the need for protection. It will be important to turn to the right professionals to minimize the risk. In addition, such a requirement will become mandatory with the next regulations.



● Il crescente impatto economico dei ransomware.

● *The growing economic impact of ransomwares.*

to il 56% degli allarmi di sicurezza viene investigato, mentre si riesce a porre rimedio a non più del 13% di questi", ha aggiunto Scanavini.

L'evoluzione delle normative

Omar El Hamdani di Shielder, azienda che si occupa di sicurezza informatica, sviluppo web e design, ha quindi fatto una panoramica sugli strumenti legislativi, sia internazionali che nazionali, che regolano il tema della sicurezza delle informazioni. "Le nuove normative sulla protezione dei dati, e in particolare la General Data Protection Regulation (GDPR) europea, che avrà efficacia dal maggio 2018, rivoluzioneranno il mondo della sicurezza informatica - ha detto - garantendo più diritti all'utente. Ci sarà, tra l'altro, l'obbligo di comunicare qualsiasi eventuale attacco informatico". A livello nazionale, le linee guida di riferimento in tema di cyber security sono quelle del CIS-Sapienza, fortemente orientate sulle PMI.

Francesco Di Prisco, Responsible for D.A.S. Training, si è soffermato sulle conseguenze concrete dei cyber attacchi, definiti come "atti criminosi penalmente rilevanti. Un'azienda sotto attacco si trova a disagio nei confronti di tre soggetti: dipendenti, clienti e fornitori, con conseguenze immaginabili. Difendersi è obbligatorio e può essere molto costoso".

Alla ricerca delle vulnerabilità

Ma come si mette in atto un cyber attacco? Abdel Adim Oisfi di Shielder ha illustrato cinque scenari su casi effettivamente affrontati.

Si tratta di test che simulano un attacco per verificare l'affidabilità delle strategie di prevenzione e difesa implementate dalle aziende.

"Si parte sempre dall'identificazione delle vulnerabilità - ha spiegato Oisfi - attraverso quelli che sono chiamati *penetration test* oppure per mezzo di un OSINT, acronimo di Open Source INTelligence, che consiste nella ricerca di informazioni su piattaforme o fonti di pubblico accesso - per esempio i social network - per trovare dei possibili punti di accesso al sistema informatico di un'organizzazione. In linea di massima, non servono molte informazioni per capire quanto un'azienda sia vulnerabile".

Dei cinque scenari descritti, che prendevano in esame realtà di dimensioni diverse tra loro, il più semplice era quello di un'azienda con dipendenti dislocati in varie sedi nel mondo e in grado di gestire la strumentazione da remoto. Le risorse erano esposte su Internet ed è stato facile decifrare le credenziali, diventare amministratori della rete e "spegnere" l'azienda.

La difficoltà di accesso nei vari esempi descritti cresceva fino al caso di un'azienda molto grande nel settore dell'energia, molto ben protetta sia a livello virtuale che fisicamente. In questo caso, la vulnerabilità è stata rintracciata nei badge di accesso dei dipendenti, che sono stati clonati grazie a un dispositivo che poteva essere avvicinato alle tessere durante gli spostamenti in metropolitana dei dipendenti stessi.

Gli attaccanti, dotati di badge, sono quindi potuti entrare all'interno dell'azienda e agire sul sistema IT. Ben più complicato, ma per nulla impossibile. ●