THE CHALLENGE OF CYBERSECURITY FOR ITALIAN COMPANIES

© Cifotrt

CYBERSECURITY IS A VERY CURRENT TOPIC. NOT A DAY PASSES WITHOUT NEWS OF ATTACKS CARRIED OUT AGAINST COMPANIES OR GOVERNMENT ORGANIZATIONS. NO ORGANIZATION, LARGE OR SMALL, CAN BE CONSIDERED IMMUNE FROM THE POSSIBILITY OF ATTACKS. IT IS THEREFORE NECESSARY TO BECOME AWARE OF THIS PHENOMENON AND TO PUT IN PLACE THE INFRASTRUCTURE AND PROCEDURES THAT MINIMIZE AND, IF POSSIBLE, AVOID THESE RISKS, KNOWING FULLY WELL THAT ANY POLICY MUST BE MONITORED AND UPDATED TO ADAPT TO THE RISKS THAT CONSTANTLY EVOLVE AND CHANGE.

by STEFANO SALVADEO
CEO, Grant Thornton Financial Advisory Services Srl

and by NICOLA SEGUINO
IT Partner, Grant Thornton Financial Advisory Services Srl

In recent months, we have seen an increase of news about cyberattacks toward companies and public bodies and even toward sovereign states.

A number of analyses, some interesting, some not, have appeared on various specialist sites about the reason for the increase of the vulnerability and the inability of affected organizations to react immediately by decreasing the negative consequences of an attack. Even in the recent American presidential campaign, cybersecurity was in the spotlight in the debate between the two candidates, among cross-accusations at a global level. In this article we want to address the issue of cybersecurity from the point of view of companies that need to manage this risk, attempting to concretely contribute to the debate and to provide some ideas for further reflection.

Cybersecurity*: what is it?*

Let's begin by defining what cybersecurity is. Cybersecurity is the set of technologies, processes and practices used to protect networks, computers, programs and data from attacks, damage or unauthorized access. In IT, the term security implies cybersecurity. Ensuring IT security requires coordinated efforts throughout the information system. Elements of IT security are:

- application security;
- information security;
- network security;
- disaster recovery/business continuity;
- training for end users.

One of the most problematic elements of IT security is the rapid and continued evolution of risks. The traditional approach was to concentrate most of the resources on the most critical system components and on the protection against the greatest known threats, leaving without protection those components and risks that were apparently less dangerous. This approach is insufficient in the current context. Threats change more quickly than our perception of risk does.

Risk assessment

The National Institute of Standards and Technology (NIST), i.e. the American organization in charge of technology management, recently published updated guidelines in its framework for risk assessment, recommending a migration of strategies toward assessments of continuous, real-time monitoring.

In the first place, given the breadth of its scope, cybersecurity can only be based on the logic of preventing, reducing and transferring risk, and on Risk Governance processes, although applied to a chaotic domain, the borders and dynamics of which are always changing. This domain must therefore be monitored 24/7 by trained personnel equipped with Risk Management methodologies and appropriate means (e.g. behavioral analysis tools, big data analytics, artificial intelligence, etc.), that are capable of operating in real time.

In the second place, to precisely define the external component of risk, i.e. the probability that an external threat could succeed, it is necessary to use Cyber Intelligence methods and tools capable of observing, via continuous monitoring, the outside and the inside with the same level of attention, and to correlate the two domains.

Again, in this case, it is a matter of developing sophisticated skills and building new processes, that are different from the consolidated practice, taking into account that currently – in the best of cases – organizations are structured only to observe what happens within their own pre-set borders (which are now becoming increasingly less defined, due to new technologies).

In the third place, it becomes necessary to define and constantly update a threat model, i.e. to identify which risks must be mitigated and what are the vulnerability of one's company to try to systematize the most likely intrusion methods that could be used by hackers, in order to identify the most suitable mitigation policies.

This threat modelling activity must also be continuous and must integrate with both Risk Management and Cyber Intelligence processes.

The requirements of reliability include, for example, security, accuracy, performance, resilience and survivability to a number of potential adverse situations. Adopting effective policies that support reliability is important only to the extent that the requirements are sufficiently complete and defined, and can be precisely assessed.

In recent years, in Italy and in Europe, lawmakers and operators have been implementing the cybersecurity provisions that have been adopted also in other countries, firstly in the United States, where every year a specially created organization, NIST, publishes security-oriented guidelines on systems engineering.

These include the protection of intellectual property in the form of data, information, methods, techniques and technologies used to create an adequate system.

Systems security engineering measures are based on the combination of consolidated infrastructure engineering and security principles, concepts and techniques to promote, adapt and integrate their principles and practices in systems engineering. These activities are carried out using a systematic and coherent approach to achieve a range of results at each stage of the life cycle of the system, including its design, development, production, use, support, and dismissal.

In Italy, these principles are incorporated in the National Cybersecurity Framework drawn up by the Research Center of Cyber Intelligence and Information Security (CIS). That document has many points in common with NIST's Cybersecurity Framework but has been well adapted to the Italian business situation, which is made up, in particular, of small and medium-sized companies. It should be kept in mind that the National Cybersecurity Framework is not a security standard, but rather a framework in which existing and future standards and rules for the sector can be classified.

Who is at risk of being attacked?

Over the last ten years we have continued to connect all kinds of devices to the Internet and have begun to base all our business on computers and interconnected networks, almost always without taking care to make them safe, because of a distorted perception of the risk involved, driven by two main thoughts:

"Why should they specifically attack me?" and *"It has never happened, anyway"*.

The first question is easy to answer: cyber criminals attack everybody, indiscriminately, with completely automated scripts. A target is not attacked only if it has "precious" information. For attackers, any information is precious, any computing resource can be exploited to generate income in the form of bitcoins, to perform DDoS attacks([1]), to send spam or to steal credentials, identity and information that only later will be screened or simply resold.

The second objection is even easier to answer since not only all of us are continually attacked, but our companies are also routinely threatened.

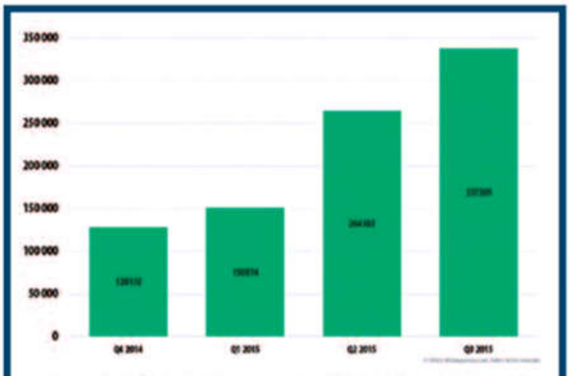
Who can say they have never had a computer infected with malware in their company's network? What was once called a virus and made more or less strange popups appear, is now called malware and, while hiding in any possible way, it steals our data even more effectively.

Thus, during 2015, the Italian scenario reflects what has also been seen in the rest of the world: the exponential growth of malware, especially of the ransomware type, such as *Cryptolocker* and similar.

These events have sparked major debates on the importance of information security and on how necessary it is now that all companies invest specific resources in this field. In addition, DDoS attack threats are also always present, targeted to interrupt online services (recently Dyndns and of all the east coast of the United States was blocked); all companies offering these services may be potential victims of these attacks.

Overall, during 2015, Trojan-Ransoms were detected on 753,684 users (see chart below). Ransomware, therefore, is becoming an increasingly serious and alarming problem.

At a global level, during the third quarter of 2016, a substantial portion of Internet users (20.2%) was attacked at least once by cyber attacks coming from the web and attributable to malware.



Number of users attacked by Trojan-Ransom malwares

(overview of the period 4th quarter 2014 – 3rd quarter 2015)

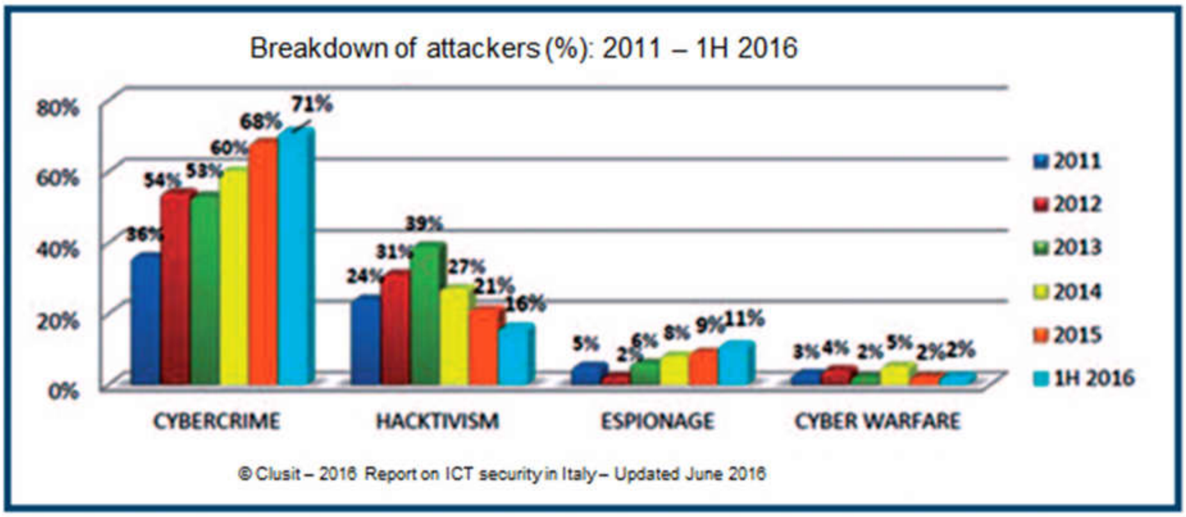
It should be borne in mind that this data is only a fraction – albeit a significant one – of the total of serious attacks that were presumably successful during the third quarter of this year. This survey, in fact, reasonably has some shortcomings, due to the fact that some fields are particularly effective in minimizing public exposure of information on attacks they suffer, and are therefore under-estimated. Moreover, while in the United States under current laws the victims must disclose breaches, the requirement does not apply to most of the other countries (Italy included); as a result, attacks against American targets appear to be the majority. Lastly, some types of attacks (the more subtle and silent, for example those related to industrial espionage or Information Warfare) are carried out over relatively long periods and therefore, if they ever become public knowledge, they only surface years later.

Undoubtedly, public awareness of the problem of IT security is growing significantly, but it is very clear that private users and the organizations themselves do not yet do enough to fight such a threat. According to the CLUSIT 2016 report, in Italy, in the first half of the year alone, there were 521 serious attacks in the public domain. This is only the tip of the iceberg, both because most of these attacks do not become publicly known, and because often the most serious consequences only surface years later (as occurs in case of intellectual property thefts for economic espionage or preventive impairment of critical systems for geopolitical purposes).

How to deal with the risk

Some practical and basic rules can limit the likelihood of our systems and of our users' credentials being affected, reducing the impact of potential fraudulent actions:

- regularly back up your data ([2]);
- be wary of unexpected emails, or those from unknown senders or senders that are not credible, especially if they invite you to open an attachment or to click on a link;
- turn on the safe navigation and link verification function of your antivirus;
- activate the safe navigation and link verification features on all browsers;
- be very careful when opening attachments, always wait for the antivirus to complete scanning them;
- keep your operating system and all your applications up to date, enabling automatic updating and periodically checking that they work properly;
- check that your antivirus works properly, in particular that it updates signatures on a daily basis and that the updates are successful because some malware tries to interfere with antivirus' updating operation;



© Clusit – 2016 Report on ICT security in Italy – Updated June 2016

- if you see clear signs of phishing attempts, report the circumstance using the features of your browser.

Large organizations should also implement more structured strategies to avoid or limit corporate-level attacks, such as:
- raise awareness among employees on the existence of attacks targeted at specific organizations, that are particularly convincing and carried out using spear phishing or watering-hole methods;
- use IP address reputation services that make it possible to selectively block IP addresses, websites and URLs considered dangerous;
- in the cases allowed by the perimeter firewalls, block traffic toward anonymization networks since this limits the communication mechanism used by some malware;
- train staff to recognize phishing attempts, also by using simulations.

Under the General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, adopted in April last year by the European Commission and which will enter into force in May 2018, companies will be required to notify the appropriate regulatory authority of any data leaks suffered; this measure includes, among other things, the application of significant fines if personal data is not adequately protected.

The GDPR is a regulation with which the European Commission intends to strengthen and unify the protection of personal data within the borders of the European Union (EU). It also deals with the issue of exporting personal data outside the EU.

These are some of the main changes for businesses, required by the GDPR:
- all public and private firms with over 250 employees must appoint an internal Data Protection Officer (DPO), who is responsible for data protection and is tasked with ensuring full compliance with the regulation;
- the fines for companies that infringe the provisions of the GDPR will be increased: without prejudice to the minimum fines set by law, they can reach 4% of the company's annual turnover;
- in the event of personal data breaches within the company, for example unauthorized access, the company must notify the authorities and its own users within a set period from the time the security breach is discovered;
- companies will have to respond to the privacy impact assessment requirement, assessing the overall impact of the legislation within the company;
- the general principle of privacy by design will have to be implemented, i.e. the need to set up specific technical and organizational measures to protect data, starting from the time a product or a service is designed;
- the right to be forgotten must be provided to interested parties, i.e. the possibility of deciding what personal information can be disclosed (especially on line), after a certain period of time, except for specific requirements (e.g. legal obligations);
- concerned parties must have the right to data portability: the possibility to transfer, for example, their data from one legal entity to another.

Conclusions

The main task of cybersecurity is to protect and safeguard the organizations/companies' mission against the risks posed by cyberspace and IT systems. All organizations are exposed to many risks of various kinds.

Increased connectivity has multiplied the risk of attacks by hackers.

It is, therefore, essential that companies adopt best practices within their organizations, and that they monitor their IT systems also from the external security perspective. Only a proactive and continuous approach can minimize the negative effects of this phenomenon. It is a phenomenon that can be controlled and managed, but not completely eliminated.

[1] A variant of DoS attack. A DoS is an attack that tries to use all of the resources of a computer system (whether local or on a network).

[2] Since it is not possible, at present, to decrypt the data, restoring it from a backup is currently the only possible solution for crypto-ransomware victims.