Human factor and security

We know that attackers will focus on the weakest link and the majority of the security professionals agree that people are the weakest link. But, as we know, in this scenario we have information security manufacturers that like to sell expensive hardware and software solutions that are addressing threats. Moreover IT people love so much technology that suppliers may satisfy this need and maintain this process alive.

This summer KPMG and BT delivered an interesting report “Go on the offensive - Working together to shut down the Digital Crime”. Here you may see that 94% of the IT key decision makers are aware about the new threats and know that cyber attacks can really hurt their organizations. But in the same research, we see also that 47% of the interviewed admit that they do not have any strategy to face cybercrime. Is this factor a technology issue? In this case we are addressing again human factor, we are facing a management issue that is not addressing properly this matter. Executive need to address cyber security and generate the commitment in the whole company. Cyber security must be part of the executive agenda together with the others financials and business issue.

So, again we are talking of human factor that are crucial for effectively fight the cybercrime.

In the mentioned report there is another interesting topic, 97% of the companies were the objects of cyber attacks, but more than 40% admit to have big difficulties in managing and counterering those attacks; the reason is lack of people with skill and knowledge. Here again we are facing human factor, we need to increase internal training in the company, increasing the knowledge level in security and also University needs to contribute preparing people with the right profile and skillset.

Regarding development there are many discussions about security functions, where also the marketing is pushing.

Security needs to be understandable all the jargon and technical terminology will confuse non-technical minded users and may cause errors. So, options and descriptions need to be meaningful to users, security features need to be easy to locate. Moreover where the user is responsible for security it should be visible, in this case user must be informed. Ensuring usability generates less pressure on the user and less accidental mistakes.

Are we talking again of human factor? End users awareness campaigns are instruments to increase the security culture and may contribute to change behaviour. But campaigns conducted in a generic way, aimed to recognizing threats like phishing or social in a broad sense are less effective. If we want to be effective we have to run awareness campaigns that are aimed to change behaviour in a specific situation. So as we may see human factor is key in different areas and we have to address this culture all over. When it comes to defence, focus only in technology is a mistake. We are humans and the problems are merely human before being technologic.

We need to address human security in the same way as we are addressing security for web server or infrastructure. Develop a thorough understanding of human vulnerabilities, building an appropriate balance between systemic improvements to avoid human weaknesses.

GCSEC starts already this journey at Maker Fair, where we presented a campaign that is going to address the human factor in different area. Stay tuned and have a look to our website where you may find all the initiatives and our fantastic journey.

Nicola Sotira
General Manager GCSEC
"If you know the enemy and know yourself, you need not fear the result of a hundred battles." Art of War, Book III, Sun Tzu.

As already in the VI century B.C., even today the role of knowledge and information is essential to make choices at functional and strategic level. In the era of IoT (Internet of Things) and digital communication, which is the value of your information and how secure is it?

Actually, the power of information is well known by modern companies, which have in place analysts to evaluate the competitors (Business Intelligence), specialists for physical security to prevent unauthorized access to the corporation, and advanced technological software to prevent the intrusion of cybercriminals. But unfortunately, it is not enough to protect the company and to prevent unwanted access.

Clearly all countermeasures are useless when attacking with methodologies that can bypass any procedure in place to defend the assets. Indeed, even the most sophisticated lock in the world is easily overcome if the owner provides you the key unknowingly. For this reason, the best hackers combine technological "brute force" attacks with social engineering attacks designed to facilitate access in a system with the art of deception.

The famous hacker and social engineer Kevin Mitnick, describes social practices, certification and education. The Cloud Security Alliance is defining leading edge best practices for assuring trust and resilience of all next generation information technology platforms, including Cloud Computing, Big Data, Mobile and Internet of Things.

"NATO – EU Cooperation" International Conference at European Parliament
googl/p/K9Kf
Date: 16 November, 2016
Location: Brussels
The current international security environment contains new threats and challenges for both NATO and EU member countries, stresses the need for greater partnership and cooperation between these organizations. Seen in the light of the recent NATO Summit in Warsaw and with particular reference to the first joint NATO-EU declaration, along with their standing agreements on cyber security, this conference will focus on how the international organizations can develop a cooperative security strategy. This conference aims to bring together experts, policy makers, officials, and industry representatives to analyze the nature of the recent NATO-EU Joint Declaration and how the Warsaw Summit has enhanced NATO-EU cooperation. The event is free of charge.

Advanced Persistent Threats: real cases
Date: 22 November, 2016
Location: Rome
The event will focus on one of the most sophisticated forms of attack on organizations network, the "Advanced Persistent Threats" - APT - with the study of real cases. The APTs are real strategies of multilevel and multi-channel attack, unleashed on organization networks in different ways and on many fronts. The overall goal of this meeting is to share helpful views on real cases, foster collaboration, promote new forms of communication and enhance mutual trust and awareness among all stakeholders within the European cyber-crime community.

Survey European General Data Protection Regulation
googl/uzgBm8
GCSEC and Europrivacy have published a survey on how the organizations are preparing themselves for the adoption of the new European General Data Protection Regulation (GDPR) and the impacts that it will determine on the public sector, the big Italian companies and SMEs. The survey is completely anonymous. The new European GDPR entered into force on 24 May 2016, is posing a number of questions to the European organizations that must comply by 25 May 2018. GDPR is directly applicable and binding to all European Member States, without a National Law Review, and is applicable also to foreign companies that provide services or
engineering as the "use of influence and persuasiveness to deceive and manipulate others by convincing them that the social engineer is one that is not". Other authors, define social engineering as "the art or science of the human manipulation in order to get of sensitive or confidential information".

According to Clusit¹ and Verizon² Report 2016, the so called “elicitation methods”, a number of data collection techniques used to gather knowledge or information from people exploiting common weaknesses of human behaviour, were one of the most critical information security aspects in 2015. Among the best-known techniques, there is phishing, basically harmless mail that contains fraud scope, leading to install with a simple "click" malware on your computer or steal private credentials. Do not underestimate the phone calls of suspected colleagues (for big companies it is difficult to know everyone) to steal confidential information. More complicated, but not less used, is the "Dumpster diving" (rummaging through garbage looking for information), the "Baiting" (leaving in locations such as elevators, bathroom or hall, infected devices, like USB derivers, which once plugged in to a hardware, install malicious programs), the "Tailgating" (following at short distance someone who has permission and the ability to access private areas in order to get illegal intrusion), and finally the "Shoulder surfing" (spying the victim from behind in order to steal his credentials to access a system, often the victim is observed when uses a smartphone or digit Pin at ATM or POS terminal).

These techniques are just the prelude to real cyber attacks in order to violate the confidentiality, integrity and availability of information.³

Therefore, the essential thing to understand is that the acquisition of seemingly unimportant information often allows cyber criminals to bypass the systemic countermeasures; Kevin Mitnick says: "why waste time on elaborate strategies when you just make a call to capture information from absolutely unaware harmless people and use them to open the door." ⁴

Even the most trained people can fall into the trap of social engineering, because the exploited weakness are mostly based on behavioural and cognitive Bias (shortcuts and heuristics) hat lead to an incorrect evaluation taking advantage of misinterpretation of information owned by use. Human is infallible and human emotions can often be exploited against user or an organization.

Therefore, even well trained users can become victims: renowned is the case of the CIA director, John Brennan, who has seen his email account compromised. In fact, in October 2015, a group of hackers called CWA (Crackas With Attitude), through social engineering techniques and talking to some employees of the well-known American provider Verizon, has broker into the victim’s account AOL (American Online), taking administration of the account and its relevant sensitive documents.

Social engineering attacks cannot only causes direct economic losses but also reputational damage with associated impact in many cases far greater that can seriously affect the stability of the organization.

This phenomenon can be contained with the culture of security, training and awareness of employees on existing threats, risky behaviour and best practices. All this without neglecting technical countermeasures such as email scanning, software updates, background check on their employees, use of encryption, the adoption of firewall and "intrusion detection systems". To properly reduce the risk of such attacks, you should adopt an interactive teaching methodology for your employees: case "Analysis", "Role Playing", simulations, always supervised by a well-defined monitoring body authority, where employees can make reports and ask questions about dubious cases in the course of their work. The techniques used by attackers are well researched and exploit psychological persuasion schemes⁵, which without the necessary training can fool anyone.

⁵ "Dumpster diving" (rummaging through garbage looking for information), the "Baiting" (leaving in locations such as elevators, bathroom or hall, infected devices, like USB derivers, which once plugged in to a hardware, install malicious programs), the "Tailgating" (following at short distance someone who has permission and the ability to access private areas in order to get illegal intrusion), and finally the "Shoulder surfing" (spying the victim from behind in order to steal his credentials to access a system, often the victim is observed when uses a smartphone or digit Pin at ATM or POS terminal).

Massive ATM Hack Hits 3.2 Million Indian Debit Cards — Change Your PIN Now!
goo.gl/gTf4jL

India is undergoing the biggest data breaches to date with as many as 3.2 Million debit card details reportedly stolen from multiple banks and financial platforms. The massive financial breach has hit India's biggest banks including State Bank of India (SBI), HDFC Bank, Yes Bank, ICICI Bank and Axis, and customers are advised to change their ATM PIN immediately. Hackers allegedly used malware to compromise the Hitachi Payment Services platform — which is used to power country's ATM, point-of-sale (PoS) machines and other financial transactions — and stole details of 3.2 Million debit cards, reports The Economic Times.

Oracle fixes 253 vulnerabilities in last cpus of 2016
goo.gl/bGx2zI

Oracle fixed 253 vulnerabilities across 76 product lines on Tuesday as part of its quarterly Critical Patch Update. Many of the fixes addressed by Oracle tackled vulnerabilities tied to securing critical enterprise data. Vulnerabilities in Oracle Fusion Middleware, a family of infrastructure products the company develops, are some of the most pressing. The update addresses 29 vulnerabilities in the software, 19 of which can be exploited remotely without authentication. Five of those vulnerabilities fetch a CVSS score of 9.8, the highest rating any vulnerabilities fixed this time around garnered. Each of these vulnerabilities could lead to the takeover of components in the affected software, in this case Oracle Big Data Discovery and Oracle WebLogic Server. In addition to Fusion Middleware, three other vulnerabilities, in Oracle’s Commerce Platform, and two retail apps – its Retail Customer Insights, and Retail Merchandising Insights – also contained critical, remotely exploitable vulnerabilities.

Euro Bank Robbers Blow Up 492 ATMs
goo.gl/4UjVS

Some 492 ATMs across Europe were blown up by thieves in the first half of 2016, as criminals looked to supplement their attempts at infiltrating machines via cyber-attacks. The non-profit European ATM Security Team (EAST) claimed physical attacks soared 80% from the 273 reported in the same period in 2015, costing over €16,000 (£14,450) each, not including damage to equipment and buildings. Total physical attacks jumped 30% from the first half of 2015 to reach 1,604 incidents in the first six months of the year, with losses rising 3% to hit €27m (£24m). The news comes as cybercriminals increasingly target ATMs with virtual or 'logical' attacks.
"We do not learn from experience ... we learn from reflection on experience", John Dewey.

Some 28 incidents were reported in the first half of 2016, up from just five the same period last year, at a total loss of €400,000 (£361,000). These "cash out" or "jackpotting" attacks typically involve malware which takes control of the ATM’s cash dispensing function to fill the pockets of the cybercriminals.

Citizen awareness about cyber risks in the context of Maker Faire

by Alessandra Zaccaria and Claudia Ruggeri, GCSEC

In digital innovation era, during which the key-word is interconnection, all devices are connected to Internet in everyday life and are potentially exposed to attacks by malicious users or users that accidentally make errors, due to a weak comprehension of new technologies or use of Internet. The correct use of Internet and digital services has been the focus of the awareness campaign organized by GCSEC, Poste Italiane and Italian Postal and Telecommunications Police, during the fourth edition of the Maker Faire, the European innovation exhibition held in Rome 14-16 October 2016.

In order to enhance the awareness of the risks that we are exposed online, the visitors have carried out a CyberQuest, an app designed and developed by Poste Italiane for raising awareness about safer use of the Internet. Through a questionnaire consisting of 15 multiple-choice questions, with different degrees of difficulty, on 5 thematic areas (Social networks, Online payment systems, smartphones, Internet and e-mail) the user can discover your knowledge and learn, through simple explanations, how to improve your security.

CyberQuest adopts an adaptive approach; the question’s complexity grows with the ability of the respondent. A smart algorithm assigns the questions on the base of the user’s answers, choosing three difficulty levels, low, intermediate and high.

For each question, there are four answers, two wrong, one correct and the other ideal. In the correct answer case, the difficulty of following question remains unchanged, whereas it decreases if the answer is wrong and it increased if the answer is ideal. In general, the analysis of results shows that the percentage of correct responses is greater than the percentage of wrong answers, and there isn’t a remarkable difference between one category and another, as you can see on figure.
In detail, the percentage of wrong answers in the Internet category is 27.93%. The results of this category show that Italian citizens don’t know enough the risk and countermeasures related to malicious software, privacy and cloud independently of user level of Internet knowledge. This trend is the same for all three levels of difficulty. In fact, the participants have not shown a lot of confidence in settings for the safe navigation in a Local Area Network, in the meaning of false positive of an antivirus system and in the Web Application Firewall. There is not full evidence of all the differences between different types of malicious software. About the privacy, there is not full knowledge of regulations about copyrights and cookies. Italian citizens already don’t correctly use the digital signature and cloud. So for this category, most of the wrong answers are associated to complex questions, addressed only by "more expert" respondents.

Regarding the e-mail use, the percentage of wrong answers is 27.34%. Despite the spamming is a widespread phenomenon from long time, users still shows difficulty in junk and advertising e-mail management and they don’t know how to prevent this phenomenon. In the same way, it is still hard to spread the full awareness about Social Engineering risks: a e-mail sent by the company administration office to request the credentials employee is a good trap, the users have a low threshold of attention! At last, the use of certified e-mail, either for commercial purposes or between Public Administration and citizen, it seems partially influenced by low Knowledge, such as of the compatibility with simple e-mail. Even in this case, we can say that the percentage of errors has increased with the increase of difficulty of the questions.

The Online Payment Systems, with 31.73% wrong answers and Social Network with 22.03% are respectively two categories wit the highest and lowest percentage of wrong answers. From these two areas we can observe the existence of a significant delta of around 10%.

A plausible reason for this difference can be the degree of complexity of the questions posed in the field of Online Payment Systems, related to more specific knowledge such as the Europyap Mastercard Visa or Tokenization service. Moreover, a weak knowledge of online payment system could be a symptom of users' preferences for traditional payment methods. Furthermore, the most common mistakes are associated to difficult questions; also experienced users make mistakes on questions concerning biometrics, authentication and EMV standard.

The questions of Social Networks area are related to user behaviour. In this case, the most common errors are related to low-level difficulty questions like cyberbullying, a worrying rise phenomenon, or personal data protection, reflecting less attention of the user in daily online operations. Privacy is a weak point for even the most experienced.

Finally, the participants answered questions regarding the use of the Smartphone, one of the most widespread technological devices connected to the Internet. Even if citizens use smartphone everyday to access to a lot of digital services, they don’t correctly use it and don’t know how to protect their digital identity and information. A portion of the respondents does not usually perform system and application update or data backup, both useful to guarantee an adequate level of security. The users are not enough able to distinguish the official apps from fake ones and don’t pay attention to the conditions of use.(i.e. the permissions required to use the app independently if these are essential or not to their operations). It is also reported that often the user connects its devices without security controls to free wireless networks, ignoring related risks.

In the end, the respondents who fulfilled voluntarily CyberQuest proved aware to the issue of information security, demonstrating a good knowledge of the risks related to a non-conscious use of the Internet. This outcome is encouraging but needs to be improved, because even the most experienced users have committed several errors. Security is an on-going process, not a result achieved once and for all, and requires different times from technological innovation.

It's possible to view awareness campaign materials and try your secure navigation with CyberQuest on GCSEC web site https://gcsec.org/activities/awareness
"We have organized an exhibition that, with suggestive and linear simplicity, could speak to children and adults by helping them to open their eyes on the dangers of the network. Without a moralistic intent, drawing up a rigid list of prohibitions would be counterproductive, especially when we communicate with children. What we need is the awareness about risks to which we are exposed using our "spyphone" and its correct use. Laurent Chrzanowski, you are an archaeologist, a member of the Board Cybersecurity for Romania, and from many years you study the social and cultural impacts related to the development of new media. "Spyphone" is a your neologism, as you explained me while leading me down the Heroes and Social Media Victims exhibition "we can call iPhone but it is misleading, what we have in our hand is a spyphone, it follows us, knows all about us and informs the ecosystem on our tastes, habits and even movements". This exhibition already exposed in Geneva within ITU (International Telecommunication Union) and translated into six languages, have been revived by GCSEC of Poste Italiane at the Maker Faire, the biggest innovation showcase in the world with 40,000 visitors (many schools) only on the opening day.

Professor, the exhibition has met great and transversal interest. What are the reasons for this exploit?

IT security and communications has become one of the great issues of our time. The public response is due to this important evidence. A matter for everyone: Today 91% of the CV of young people seeking work is often rejected by HR managers because the social reputation of candidates is often spotted. We are ourselves today that we become suppliers to our enemies of the most terrible weapons. For this reason it's important to raise attention and competence when we handle tablets, PCs and mobile phones.

I would like to start from the exhibition, impressive architecture and setting. It starts from antiquity, kings, emperors, demigods masters in the rhetoric of the image. What reason has prevailed this editorial choice?

The image has a symbiotic relationship with the power, always. A short circuit that is not born in the post-modernity as we often believe. Kings, emperors, monarchs and more recently dictators and statesmen, have suffered the charm of the images that have stoked the cult of personality. It remained the same until eras and distant and very different contexts. Today we have to record the speed with which the private citizen is involved, launched in the network as in a big stage, where he remains hopelessly naked and defenceless.

The dimension of the ego in the universe of personal communication, emerges overwhelmingly. Which are the consequences?

The consequences are certainly overexposure and an accentuation of fragility. Usually in the digital world, the user is inclined to overexpose himself, doesn't afraid to be judged and immediately trust in other users supposing that its digital life is completely separated by real life and that it can not impact in the daily life. An important countermeasure cloud be to strength the knowledge of technological instruments and digital services like social network which should be used with great skill and foresight.

What's the lesson that the past can give us?

The past can teach us a lot. The exhibition starts from the Egyptian civilization, crossing the classical world underlines some emblematic facts. We think for example the figure of Dracula, the first victim of a revolutionary new media: the press. The prince had excluded the saxon merchants from the richest Southern Romania countries. They decided to take revenge publishing prints, which depict him while was drinking the blood in front of the victims horribly impaled. The fictional hero figure opens the question of the image in relation to defamation. The same happens on the Web, what do you think?

Everything we do in the network has a continuous echo, difficult to regulate and control as demonstrated by so many tragic news stories. Everyone have many friends on social, the selfie game gives a good idea of this on-going exhibition of ourselves, an ego projection. The problem is that we do not realize that the web is the largest archive ever existed in the world. It do not forget anything. That's the risk with which we must learn to live with.

Can the Big Date dimension effectively illustrate his concern?

This is another great chapter, which requires a dedicated infrastructure that only a few states or major private player can afford. In ancient times this size was particularly present. The rulers after death were praised or damned, with the digital revolution we are ourselves that we use the web to exalt or condemn. We live, in fact, in a virtual ecosystem in which a potential enemy can fake photos, playing on the relationship between reality and appearance, in diabolic and
From wall to wall is a special section of the exhibition. What is intended to evoke?
The exhibition intends to evoke the historical characters that wanted to ensure their image to gain eternity. The first kings were proclaimed by the will of God, when you are not identified with the divinity. To the ancient Egyptians writing a name on a statue, and then breaking meant hell condemn the enemy. We think of the role of the image in dictatorships. Stalin has retouched photos to erase his political opponents, but also Caracalla, the Roman emperor of Century III is no exception. Geta disappears from any incision because killed by his brother Caracalla, who took power and does not intend to share it with no antagonist. Christianity in the Middle Ages intervenes by changing the names of cities, for reasons of control and power. From Gutenberg onwards it will also be the subject of attention bourgeoisie and image policies. As, moreover, it was also important to the image in the history of religions is demonstrated by events such as the Eastern Emperor Leo III Isaurian that those with a specific decree decided to ban the cult of sacred images. This attitude "iconoclastic" triggered the reaction of the Church, and with the Council of Nicea, we are in the eighth century, was able to re-establish the right balance, distinguishing between devotion and idolatry of sacred images.

The issue is complex and would lead us away. We try to go back to current events: how you can educate to a correct use of the media?
Avoiding alarmism and working gradually. We must think not only of children but also adults, who are not familiar with digital, as evidenced by many facts gory and other crime that fill the pages of newspapers. The school can do much if it does not rely only on volunteers, but also the University, who often forgets this specific task.

One last question on the role of the Poste Italiane that hosts this interesting exhibition space. What is your feeling about this?
The crucial role of businesses that they are equidistant from the executive and the investigative forces, can promote a security culture, open for all. Poste Italiane have deciding with his Foundation to participate in this great innovation event gave an important witness of social responsibility, declined on the major issues of the changing frontier. Cyber security among these issues is the principal.