In particular in this Directive will play two new type of players in the financial domain, Account Information Service Provider (AISP) and Payment Initiation Service Provider (PISP). These players are quite important in this new scenario, the AISP is a service provider that will have access to the account of the bank customer. This service may use transaction data to analyze customer spending or aggregate this account information from different banks into a single overview. A great benefit for the customers, but a possible great impact on business if not prepared. The same issue analyzing the PISP that will create a software bridge between customer and retailer’s accounts. A PISP is a service provider that will initiate a payment on behalf of the customer directly to bank no payment card details involved. New security requirements, IT infrastructure and API platform are economical challenges for banks, but also an opportunity for finally accelerate the digital transformation, build a banking platform and open to new technologies. Several banks are exploring the blockchain domain and artificial intelligence together with the use of more powerful analytics. Of course there are lots of open questions and together with GDPR and NIS represents a big challenge facing in 2018 and innovation will be a crucial factor. In the CyberSecurity Trends of June GCSEC is preparing a focus with experts talking about PSD2 and analyzing business and technical impact. Good reading....

Nicola Sotira
General Manager GCSEC
A few weeks ago, computers in more than 100 countries were attacked in a cybercrime attack - an attack in which data on a computer is encrypted by an unknown source and can no longer be used without a special encryption key. However, the malware seeks a ransom (usually a small sum, which is within the reach of the victim) for the key. The phenomenon is relatively new (about three years old) and is driven by criminal organizations seeking a small profit. Payment in the virtual currency Bitcoin makes it very easy to extort money because of the difficulty in identifying the payee.

What is special about the attack this time is its breadth, and the fact that it was exploiting a loophole that was visible to all Microsoft windows. The breach was revealed a few months ago, and Microsoft rushed and issued a security patch. Anyone who updated and deployed the patch was not hurt.

In addition to the technological breakthrough in the software, the criminals exploited a human "loophole": People do not rush to update their security software. This is particularly common for large organizations where the process of testing, deploying, and installing the update may take several months. That's exactly what the burglars built: their success attests to the fact transformed from a risk factor to a defense instrument by reinforcing skills and competences through targeted awareness-raising and training. The workshop aims to examine these topics, explain some awareness and training initiatives, analyze behavioral influences, competences and soft skills in the cyber security sector as well.

Russian group delivers the first unhackable quantum-safe blockchain
https://siliconangle.com/blog/2017/05/24/russian-group-delivers-first-unhackable-quantum-safe-blockchain/

Quantum computing and the blockchain both get plenty of attention in 2017, and now researchers in Russia have combined the two to create what they claim is an unhackable distributed-ledger platform. The new technology, described as the "first quantum-safe blockchain," promises to make it secure for organizations to transfer data without the fear of hacking from even the most powerful computers, in this case, the emerging field of quantum computing. Quantum computers make use of the quantum states of subatomic particles to store information, with the potential to do some calculations far faster than current computers.

NSA EsteemAudit exploit could trigger a new WannaCry-like attack
http://securityaffairs.co/wordpress/59450/hacking/nsa-esteemaudit-exploit-patch.html

The WannaCry emergency could not be ended because the NSA dump leaked by the Shadow Brokers team included many other dangerous exploits. Last months the Shadow Brokers group released another batch of data containing exploit codes still unpatched by Microsoft such as the "EnglishmanDentist," "EsteemAudit," and "ExplodingCan." The availability of such exploits and hacking tools represents a serious problem, an attacker with technical knowledge can exploit them to compromise millions of Windows systems across the world. "Of the three remaining exploits, "EnglishmanDentist", "EsteemAudit", and "ExplodingCan" none reproduces on supported platforms, which means that customers running Windows 7 and more recent versions of Windows or Exchange 2010 and newer versions of Exchange are not at risk," continues Microsoft.

Let's start with the EsteemAudit exploit, it is a hacking tool that targets RDP service (port 3389) on machines running no longer supported Microsoft Windows Server 2003 / Windows XP.

Samsung Galaxy S8 Iris Recognition Cracked

Security experts claim to have cracked the
that tens of thousands of victims have not yet installed the security update.

One of the most prominent examples of this is the network of hospitals in the UK, which turned out to be unprotected, and the encryption of files in their computers caused a major disruption to their operations. These are not just information systems essential to the operation of the hospital. There are many computer-controlled systems, which are operated in hospitals, and disabling computers can lead to loss of life. Therefore, these hospitals were forced to take emergency measures, including the transfer of urgent surgeries to other hospitals. The unwillingness of hospitals in Britain is even more serious in view of the fact that such a cybercrime attack was already carried out on a hospital there a few months ago.

And what about us in Israel? As of the writing of this article, there were no ransomware attacks on critical systems. One of the reasons for this is the warnings and instructions issued last week by the National Authority for Cyber Defense. The INCD, together with the cyber headquarters, are part of the national cyber network operating in the Prime Minister's Office. This is a unique system that does not exist in almost any other country, and places Israel at the top of the list of countries that have seriously prepared for cyber threats.

An example of this was given last week by Michael Rogers, head of the National Security Agency (NSA) and head of the cyber network in the US in an unusual open-door hearing in the Senate, the admiral was asked about his links with the cyber network in Israel, Dr. Eviatar Metanya, the head of the INCD, every time he arrives in Israel or when Dr. Metanya arrives in the US. Rogers hinted that Israel is one of the countries from which the United States can study on this subject.

In the last six years, Israel has succeeded in building a national defense system that, as stated, has no parallel in the world. This is why we have become a magnet for cyber sages around the world, and this is why the Israeli cyber week, held in cooperation with the Prime Minister's Office and the Tel Aviv University's Blavatnik Interdisciplinary Cyber Research Center, draws thousands of people from around the world every year. A conference to be held in late June is expected to reach 7,000 people from 50 countries.

Warning Note: The cyber world is very dynamic and its rate of change is very fast. Success today is not a guarantee of success tomorrow. The mechanisms and capabilities established so far do not allow us to be complacent.

---

**Locked Shields 2017**

*by GCSEC*

Let's go back to talks this month of the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE - https://ccdcoe.org/index.html) based in Tallinn. In fact, the 8th edition of the world's largest cyber defense exercise - Locked Shields - has just been ended, which, focusing on the protection of cyberspace, was organized by CCDCOE in cooperation with the Estonian Defence Forces, the Finnish Defence Forces, the Swedish Defence University, the British Joint Army, the United States European Command, Air Operations COE and Tallinn University of Technology. The mission of Locked Shields exercise has always been to enhance the ability to respond,
cooperate and exchange information between different NATO organisational units, member states of NATO and accredited partners in defense, during a cyberwarfare event. That kind of exercise has now become fundamental to the maintenance of geopolitical balance between states, given that cyberspace, as stated in the Warsaw Summit in 2016, is a domain that, in common with other - land, air and sea - must be protected from all possible threats, including cyber threats. Organization of, and participation in this cyber security drill is therefore an important building block in the defense strategy of NATO and all the states that adhere to it. Locked Shields is an exercise belonging to the live-fire or LFX class that reproduces the highest level of realism by providing realistic scenarios and the usage by the attacker and defender of the advanced and innovative attack and defense equipment and techniques. In this context, about 900 cyber security experts from 25 countries have tried to defend and to keep the computer network and the services provided by an Air Base belonging to a “Fictional State” affected by a significant number of cyber attacks (over 2000), that involved about 3000 virtual systems including so-called Unmanned Aerial Vehicles (UAVs), in other words remote controlled aircraft and drones used for military surveillance, power grids and SCADA systems, control systems such as programmable logic controllers used to ensure fuel supply, operational infrastructure and much more. Locked Shields simulation environment made in Tallinn, Estonia, has enabled the Blue Teams, made up of technicians, lawyers, forensic experts and strategists, to participate directly from their country using secure connection; The Italian Blue Team were represented by the Italian Army, the Italian Navy, the Italian AirForce, the Italian military police (Arma dei Carabinieri) and the National Anti-Crime Center for Critical Infrastructure Protection (CNAIPIC), as well as researchers from the academic world and experts of the private sector. Red Teams and Blue Teams are the name used to identify the groups that face during the simulation, in particular, the first, highly specialized and organized, those who lead cyber attacks; the latter are the ones who have to put in security and defend their virtual infrastructure and ensure the proper service delivery. During the exercise, Red Teams will be attacking systems and networks of Blue Teams, exploiting vulnerabilities at people, processes and technologies level, using typical penetration tester techniques. The aims of the cyber attack can be many and varied: theft login credentials in order to steal sensitive information in the computer system (Server, Database, etc.), reduce the capability to perform online delivery services through DDoS attacks, compromising SCADA systems, etc. Blue Teams defend themselves 1) using SIEM platform to analyze security events incoming from vertical security solutions such as AntiVirus, AntiSpam, Data Loss Prevention, Database, Web Filtering, Firewall, Operating System, VPN, Web Server, etc., 2) analyzing network traffic, 3) performing Threat Intelligence activities, 4) using Computation Indicators, 5) performing Computer Forensics, Mobile Forensics, Network Forensics activities and so on. For a regular course of the exercise, there are also other groups that are attending the participants and their correct interpretation of the competition rules, others who are in charge of arranging and maintaining the simulated environment over time. The NATO Cooperative Cyber Defense Center of Excellence, as well as organizing the event, also played the role of the attacker through its Red Teams. The goal of of the Locked Shield exercise was therefore to create the conditions for training participants, and in particular members of the Blue Teams, to respond in the best possible way to complex and articulated large-scale cyber attacks; this by 1) verifying the capabilities of each Blue Team to discover and patching computer system vulnerabilities that could be exploited by Red Teams, 2) managing malicious agents, 3) managing cyber incident, 4) the adoption of cooperation models aimed to exchange information, bearing in mind legal and strategic aspects. Testing competencies in highly competitive and challenging environment like Locked Shield, ultimately improved the ability to respond to a cyber attack by the different Blue Teams, trying to bring them all on the same level, also through the so-called “lesson learned” shared between them. This year, the prestigious challenge was won by the Czech Republic team, followed by the Estonian team and the NATO Computer Incident Response Capability team; in the legal field, the best team was NCIRC, Germany was the best in forensic practices and United Kingdom in strategic communication. Indeed, although the main goal of the Locked Shield exercise is related to more technical aspects, this year, with specific simulations, the strategic, decision-making and legal capabilities of the different teams have also been verified. Beyond the military environment, let us remember that the European Community also considers these kind of exercises very important. Every two years, the European Network and Information Security Agency (ENISA) of the European Community organizes a pan-European exercise; a competition in which are opposed the public and private sector representatives of the European Union (EU) Member States and of the European Free Trade Association (EFTA) to carry out a several exercises (forensic analysis, compromise of fixed and mobile systems through the ’Malware, malicious software, open source intelligent campaigns,
“Public sector could never avoid to put in evidence the defense of network and strategic assets, in order to fit into innovation way. Digital is a so big changing instrument, as already seen in many European countries, but to became a lever for growth we need to improve every day and create an ecosystem in which security is an embedded value that exists in symbiotic relationship with network, systems and organization at all level”.
That's a clear message of Mr. Nicola Sotira, Information Security Manager and General Director of GCSEC, during the interesting seminar Forum PA “ Cybersecurity Priority” moderated by Alessandro Longo Director of Digital Agenda.eu. The session has seen the participation of: Lorenzo Russo cybersecurity senior manager Deloitte, Nunzia Ciardi Director of Postal Police and Communication Dept. of Ministry of the Interior, Andrea Boggio Business Development of Fastweb, Carlo Mauceli National Digital Officer Microsoft Italia, Alessandro Menna Vice President Sales Leonardo; Benito Mirra Cyber Security Officer Huawei Business Group, Federico Santi Security Principal South EMEA DXC Technology, Sabrina Ugolini Central Director of Foreign Affairs and Francesco Vestito, Interforce Manager for Cyber Operation of Ministry of Defense.

Position contest

Data are clear, in accordance with the Clusit Report, Italy is in the top of countries for cyber attacks. Nunzia Ciardi, underline that: “more than 50% of incidents are produced by illegal action no so sophisticated that have success thanks to our inexperience. The meaning is that there is an asymmetric line between the hacker simplicity and poverty and the investments supported by deputy offices in order to monitoring, preventing and management attacks. This “vulnus” should be smooth over and solved; CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche ) indicated that in the last year, hacker attacks have been 900, more than 6000 alerts with 70 investigations opened by Postal Police”. Most likely it is only the tip of the iceberg but it gives an appropriate idea of great loads of work, daily carried out to protect informatics infrastructures and guarantee a universal and inalienable right for everybody: the confidential of communications and privacy. Andrea Boggio, confirmed that privacy is hard to protect; his Fastweb point of view as operator who well knows PA is: “of about 6 million IP address, in 2016 we registered 16 million of security events, for our business is essential to guarantee confidentiality, availability, security and resilience”.

1 https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme
Discussions shown a wide range of problems that will need a prompt replies, not only on the technological side but mostly in skills and awareness of the public opinion. In this contest, CERT will play a very hard role, enforcing information sharing method. Without an adequate sharing of information the country will note be able to contrast the crime challenge that are overtaking threshold of our privacy, stealing know-how, sensitive information and economic resources. It will be important improve standards to redefine internal and external organization processes and create a dialogue way with private sector and PA that will go beyond simply dialectic from customers and companies. From these considerations growth the importance to build a Security by design, that means quality in work organization, management and quality of Service Providers that stands near companies, influencing selections and market penetration.

Training is essential

One of the crucial topic is training. Nicola Sotira said: “it’s necessary to activate a virtuous path of awareness for top management, without this precondition every thought remain abstract. From an extensive awareness could born a risk-oriented organization, able to commit towards security matters”. Communication and disclosure can be essential in this direction. Cybersecurity magazine Cybersecurity Trends edited in Italian language by GCSEC and published in many international editions, engaged the role of virtual agorà, open to all contributes of top expert in the matter, with a special purpose: raising problems and solutions besides to encourage public institutions and companies to deepen in the universe of security culture and all its implications and aspects.

It will be vital to bring up-to-date law and reference standards, in an international contest that continuously faces new threats. Recently the glaring case of “Wannacry” has become an unexpectedly milestone a sort of “ Digital Day after” without any precedent that has shown weaknesses of Digital Society.

Cybersecurity is central for G7

All Europe and not only Italy discovered itself not prepared to an event that has showed customers ingenuity and criticality of public systems that still have not developed a standardized vision of risk. “I want to cry” it’s impossible to find a best name to define a whimsical and untamable virus that has updated the specter of our weaknesses and insecurity; the virus has invested 150 countries, infected 20thousand PC per day since from the first day (occurred as everybody knows last 12th May 2017) bring down U.K. health system. Downstream to so capillary event it must be done a serious consideration on the matter of Global Governance. Cyber crime and terrorism have shot down the border: we know that companies, institutions, hospital, banks are all in the crosshair with any differentiation. It will be consequences on strategic plan starting up from multy-agency cooperation that put together best skills from public, private area of EU countries.

On this matter it’s relevant the engagement of Gentiloni during the Forum PA, on centrality of cyber security for the digitalization process of PA. This strong statement has international effect, in declaration of intent expressed by the Premier closing Bari G7, who has seen for the first time informatics security on top Government Agenda. The die is cast.

It will be crucial from this moment to never let the guard down, drawing conclusion with rational lucidity on consequences that scientific and technologic development involves.