GLOBAL CYBER SECURITY CENTER

Newsletter

2017 September

Cyber Security is our mission

editorial

Too much cyber will kill you…

I changed a little bit the title of the famous song “Too Much Love Will Kill You”; song released in 1992 by Brian May as the second single extract from his first solo album Back to the Light of the same year. Often when we are talking and writing on Cybercrime we talk about data, breach, leakage so the main subject are data 1 and 0. Information war is more and more aggressive as the data increase their value for companies, organizations and government. This year, in collaboration of Polizia Postale and Poste Italiane, we were involved in an awareness campaign toward schools and we received many questions about the Blue Whale, a twisted suicide challenge which appears to goad vulnerable teens into killing themselves. This sort of social media group is encouraging people to kill themselves; it started in Russia where they estimated 130 suicides of children before the game start spreading in Europe. In this case we cannot talk about data leakage, we are dealing human life. This summer I was reading some article related to Kenya elections, as reported from Guardian and NYT, the country was in a tough period and elections was a challenge in order to change. As you know elections toked place in August, but the Supreme Court found that the control had failed by Independent Electoral and Boundaries Commission (IEBC) in accordance with the law, and that irregularities impacted the outcome of the poll to such an extent that a new election is required. In order to be clear we have to explain that in Kenya was under development a new electronic ballot and a voter registration systems and IEBC had the ownership of this task.

Maybe you may foresee the election result reading a small news published by the Guardian July 31th; in this article, they were talking about the death of Mr. Chris Msando tortured and murdered. This man was the head of Information, Communication and Technology at the Independent Electoral and Boundaries Commission (IEBC) working to the new vote platform. Controlling the IT platform maybe you may control or change results and maybe, in order to control the IT, you have to torture and kill the IT guy. So we start to see more and more real consequences to human life coming from digital. Auto, hospital, DNA research are others recent examples of what we may start to define human breach, we are not talking of data but real danger for our life. In this scenario, we can smile about some funny news of these days reported on a UK newspaper that is publishing a warning coming from Noel Sharkey, professor of artificial intelligence and robotics at the University of Sheffield, about the possible hack of sex android; having the full control of the connections, arms, legs and other attached tools like in some cases knives or welding devices this android may kill. So even in this case, and for this personal aspect of our life, we are dealing with an operating system, much like computers or smartphones and an always connected object.
Enjoy your reading

Nicola Sotira
General Manager GCSEC

events

La tutela della privacy digitale alla luce del General Data Protection Regulation UE 679/2016
Location: Milan
Date: October 17, 2017
http://www.unimib.it/open/eventi/European-Cyber-Security-Month-La-tutela-della-privacy-digitale-alla-luce-del-Gene-ral-Data-Protection-Regulation-UE-6792016/7956981055633095230
In the context of the European Cyber Security Month (ECSM) organized by the ENISA Agency, it will take place a seminar on Personal Data Protection in the Digital Single Market (DSM) organized by Prof. Emilio Tosi, Professor of Private Law at the Department of Business Economics and Law on Economics (Di.SEA.DE) University of Milan Bicocca.

CS4CA Europe
Location: London
Date: October 4-5, 2017
http://www.cs4ca.com/europe/
This innovative Summit comes at a critical juncture for European security leaders facing increasingly complex threats from multiple different attackers. The conference will be bringing together operational technology/process control and corporate IT departments from the chemical, power, energy & utilities sectors to share best practice, discuss policy implications and face threats together.

ATM & Cyber Security 2017
Location: London
Date: October 10-11, 2017
https://www.rbrlondon.com/events/atmsec
ATM & Cyber Security 2017 (formerly 'ATM Security') is the world's leading conference focused on physical and logical ATM security. The event attracts over 340 delegates, representing more than 140 organisations from over 40 countries worldwide. The event comprises a speaker programme containing important contributions from retail banks, law enforcement agencies, hardware and

in this number

PSD2 change the rules of the game

by Nicola Sotira General Manager GCSEC

Several compliance and regulations in 2018 will have impacts on companies and will require a second thought on the IT infrastructure as well as a redesign of processes and organization.
NIS and GDPR have filled the spaces of pages and conferences emphasizing deadlines, penalties and concepts to be applied on the Companies for good implementation in their respective deadlines. The 2018 will also be the year when PSD2 (Revised Payment Service Directive) will change the rules for banks, this EU directive breaks the monopoly that today the banks hold on payment services, opening up to competition of interested companies and in fact leaving customers the ability to decide when and whether to allow access to account to third party, following an open Bank model. The customer, in this new scenario, may decide autonomously which platform to use to manage its funds and provide payments. For sure, the policies that will guide the choice will be innovation and customer experience. In this regulatory environment, financial market is pretty humming moved by startups strongly focused on technological innovation that offer services in many areas, including the crowdfunding, peer-to-peer loans in addition to services based on crypto currencies. Obviously to this offer from the start up world, it's necessary to add the services coming from big corporations like Amazon, Apple, Google and Facebook.
The new players enter the market thanks to this directive that will oblige banks to facilitate the access to customer accounts to third party applications, obviously with the agreement of the holders; in this case, when we're talking of applications we talking significantly about applications. It means that banks will have to allow a secure access to the accounts of their customers by implementing the Application Programming Interfaces (APIs). It is more and more obvious that the approach that users have with banks switch from using smartphones where the speed, simplicity and user experience are challenging.

Two new players in the market PISP and AISP

In accordance with this directive, new players will enter the market of payment services, including PISP and AISP. The acronyms stand for: Payment Initiation Service Provider (PSIP) and Account Information Services Provider (AISP). These new subjects, if authorized by customer, may have access to and operate the bank account. This will allow, through access interfaces (APIs) that banks should make available, the development of new services; services that will be more integrated and harmonized with other

software providers and a range of industry bodies. The event focuses both on physical ATM security and newer cyber and logical security threats.

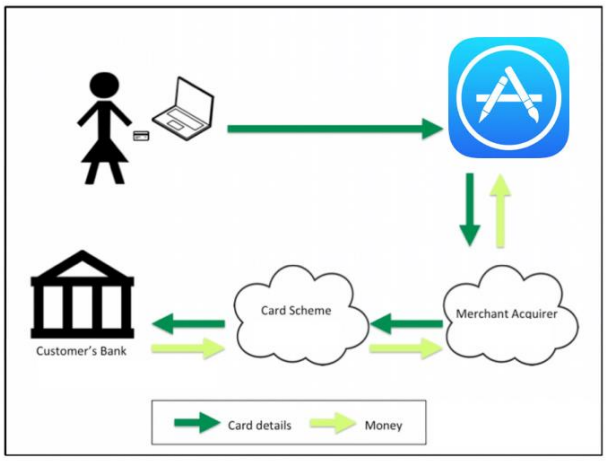
IT Security Industry Collaboration Event - EU Regulation: Business opportunities for SMEs
Location: Bruxelles
Data: October 3, 2017
https://www.enisa.europa.eu/events/enisa-industry-event-2017/it-security-industry-collaboration-event-eu-regulation-business-opportunities-for-smes
The objective of this second Industry event in 2017 is twofold:
to follow up and finalize the common position on funding mechanisms (theme of the previous Industry meeting) and to introduce a pragmatic discussion on business opportunities of EU regulation.

news

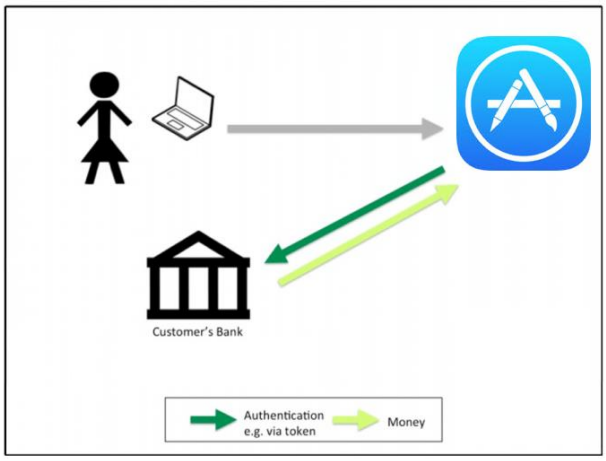
Hackers Exploit PowerPoint Files to Deliver Malware
http://virusguides.com/hackers-exploit-powerpoint-files-deliver-malware/#
Fortinet security experts warn that hackers are exploiting malicious PowerPoint files alongside recently patched Microsoft Office vulnerability to attack foreign ministries, international organizations, UN agencies, and entities interacting with international governments. The attackers use a file called ADVANCED DIPLOMATIC PROTOCOL AND ETIQUETTE SUMMIT.ppsx and exploit the CVE-2017-0199 vulnerability which Microsoft addressed in April. During that time, cyber criminals had been abusing CVE-2017-0199 for delivering various type of malware like Dridex, Latentbot, Godzilla, and WingBird. Despite being patched recently, the exploit continues to be used in cyber attacks. The first PowerPoint attacks which exploited CVE-2017-0199 for malware delivery were registered a month ago. They were associated with the distribution of a Trojanized version of the REMCOS legitimate and customizable remote access tool (RAT).

Equifax hack could affect half the population of the US
https://www.welivesecurity.com/2017/09/08/equifax-hack-half-us-population-affected/
The credit reporting agency, Equifax, has revealed that they suffered a huge cyberattack that could affect up 143 million Americans. The hackers gained access to sensitive personal data, including social security numbers, birth dates and addresses of nearly half the population of the US. The company released a statement on their website saying: "Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017." On September 7 Equifax publicly confirmed that a breach occurred, but has so far refused to disclose why it waited six weeks before disclosing the cyberattack. In addition to gaining

players in the new ecosystem. In the current scenario, if an online user decides to buy a service from Apple will complete the transaction using a credit card. Apple (merchant in PSD terminology) will use an acquirer (financial institution that handles payments to certain brands of credit cards and debit cards). The acquirer will contact the customer's credit card circuit, charging on his account (FIG. 1)



Let's jump forward and review the scenario described above, in the light of PSD2. Our client is again making purchases from Apple, but instead to enter its credit card details, it is asked if accepts the charges on the account. Where the charges is permitted will be given to Apple permission to make payment, on our behalf, using the account (FIG. 2).



The directive, therefore, allows a company to manage the initial phase of payment, Payment Service Provider Initiatiation (PISP) that in this example is Apple. At that point the PSIP is a payment service provider that acts as an intermediary between the client and his account by providing the incentive to charge.

Technically the PISP fits into the payment transactions processed online and cannot in any way access funds deposited in the account of client. The customer in this scenario creates a transaction on line connected directly to the bank account and charging himself through the services offered by the PSIP.

In PSD2 is then provided another type of services represented by the AISP, with these services the customer may aggregate information from multiple accounts by making them available through a single interface. The AISP can then connect to accounts and retrieve the information need to give customers an overview of their financial situation, i.e. a detailed analysis of their spending habits on, everything so easy and interactive. These services will also be useful to provide services such as monitoring of investments or to support financial planning. Legally the AISP can act only under a specific

access to personal data, the cybersecurity breach also exposed 209,000 credit card numbers that also includes customers from Canada and the UK.

Malicious plugin installed backdoor on 200,000 WordPress websites

https://www.scmagazine.com/malicious-plugin-installed-backdoor-on-200000-wordpress-websites/article/688878/

A very persistent malicious actor added a backdoor to a WordPress plugin called Display Widgets that installed backdoors on possibly 200,000 websites since June 21. The hacker used the open-source Display Widgets plugin, which lets users control how their WordPress plugins appear on their sites, as the delivery mechanism for the backdoor. Although the number of potentially infected sites is large, what is almost as impressive is the hacker's persistence. The infected plugin was repeatedly removed from the site by Wordpress.org between June 22 and September 8 with the hacker dutifully replaced it. It was finally removed for good on September 8.

While it has not appeared again, Wordfence, a private company with its own security plugin for WordPress, issued a warning to WordPress users.

Red alert 2.0: New android banking Trojan for sale on hacking forums

https://thehackernews.com/2017/09/android-banking-trojan.html

The Recent discoveries of dangerous variants of the Android banking Trojan families, including Faketoken, Svpeng, and BankBot, present a significant threat to online users who may have their login credentials and valuable personal data stolen. Security researchers from SfyLabs have now discovered a new Android banking Trojan that is being rented on many dark websites for $500 per month, SfyLabs' researcher Han Sahin told The Hacker News. Dubbed Red Alert 2.0, the Android banking malware has been fully written from scratch, unlike other banking trojans, such as BankBot and ExoBot, which were evolved from the leaked source code of older trojans.

Malware-Infected CCleaner Installer Distributed to Users Via Official Servers for a Month

https://motherboard.vice.com/en_us/article/a3kgpa/ccleaner-backdoor-malware-hack

Hackers have managed to embed malware into the installer of CCleaner, a popular Windows system optimization tool with over 2 billion downloads to date. The rogue package was distributed through official channels for almost a month.

CCleaner is a utilities program that is used to delete temporary internet files such as cookies, empty the Recycling Bin, correct problems with the Windows Registry, among other tasks. First released in 2003, it has become hugely popular; up to 20 million people download it per month.

Users who downloaded and installed CCleaner or CCleaner Cloud between Aug. 15 and Sept. 12 should scan their computers for malware and update their apps. The 32-bit versions of CCleaner

agreement of the client, authenticate with the PSP communicating with everyone involved in the transaction, access only to authorized accounts involved in the transaction and cannot make access for purposes different from those provided by the service. Clearly it is central the issue of security and the need to harmonize Strong Customer Authentication policy for all banks.

PSD2 Strong Customer Authentication (SCA)

In the context of PSD2 all payment service providers (PISP) must adopt strong authentication tools (SCA) every time is launched an electronic payment transaction.

The costs for infrastructure design and implementation, as well as to verifying the effectiveness of SCA, falls on Account Servicing Payment Service Providers (ASPSP), the banks. While regarding PSIP AISP they should ensure that the SCA is correctly applied; they will rely on an authentication procedure provided by ASPSP.

In the SCA, a valid combination of the elements of authentication will generate an authentication code on the PSP of the customer, specific for the amount agreed by the spender and the beneficiary at the start of the transaction. This is referred to as "dynamic linking. This security mechanism applied to operations protects from man in the browser and man in the middle attacks. Terminals for parking or tolls fee are exempt from SCA mechanisms to don't create unnecessary inconveniences or tails, the same for the remote payment up to 30 euros. It should be noted that the directive introduces a derogation to the use of SCA if level of risk of payment is up to 500 euros. The exoneration can be applied in the case in which the service provider has an overall fraud rate lower than the total fraud rate specified by the directive. These simplifications improve business and competition if will be introduced innovative technologic instruments that guarantee in online transactions fraud rate compatible with as required in different applications. Another consideration is the decision of EBA to use eIDAS certificate for authentication of ASPSP, AISP and PISP; a brave decision because is not clear if there will be also eIDAS certification authority in time for the implementation date of October 2018.

Distributed Ledger and block chain

The Distributed Ledger Transaction (DLT) proposes a new paradigm that could revolutionize the economic system on the base of the concepts of transaction and confidence. Generally, Banking and financial processes require approval processes in which you must get high levels of assurance; in this context, DLT and Blockchain can be a field for experimentation, alternative at traditional logic.

Technology Blockchain can manage authorization processes through infrastructure in which to the public keys are associated assets with the relative private key that validates the transaction.

A process that is similar to that of the digital signature, but without the obligation to have an accredited Certification Authority (CA).

Based on these concepts is clear how this technology eliminate the single point of failure and increases security; themes which today threaten the payment systems. This will also make transactions transparent and manageable without a central authority. Scenario on which the World Bank is expressed by saying that the elimination of these costs could result in significant savings.

Conclusions

One of the key points of this directive is to have allowed the entry of new actors within the value chain of electronic payments, which will result in a greater competitive pressure in the market and certainly a real advantage for the consumer and for banks that seize the innovative aspects expanding their portfolios of services and revising traditional models.

v5.33.6162 and CCleaner Cloud v1.07.3191 were affected.

46,000 new phishing sites are created every day

http://www.securitymagazine.com/articles/88172-cisco-2017-midyear-cybersecurity-report-predicts-new-destruction-of-service-attacks

An average of 1.385 million new, unique phishing sites are created each month, with a high of 2.3 million sites created in May. The data collected by Webroot shows today's phishing attacks are highly targeted, sophisticated, hard to detect, and difficult for users to avoid. The latest phishing sites employ realistic web pages that are hard to find using web crawlers, and they trick victims into providing personal and business information.

Phishing attacks have grown at an unprecedented rate in 2017

Phishing continues to be one of the most common, widespread security threats faced by both businesses and consumers. Phishing is the number 1 cause of breaches in the world, with an average of more than 46,000 new phishing sites created per day. The sheer volume of new sites makes phishing attacks difficult to defend against for businesses.

European Commission proposes more powers for EU's infosec agency

https://www.theregister.co.uk/2017/09/19/enisa_revamp/

The European Commission has proposed an expansion in the role of ENISA, the EU's cybersecurity agency.

During his State of the Union speech on Wednesday, Jean-Claude Juncker outlined plans to widen ENISA's remit through a Cybersecurity Act. Under a revised mandate, ENISA would be tasked with introducing an EU-wide cybersecurity certification scheme. The thinking is that the agency would be able to counter threats more actively by becoming a centre of expertise for cybersecurity certification and standardisation of ICT products and services. The agency would also support member states in implementing the Network and Information Security (NIS) Directive and be take a role in reviewing the EU Cybersecurity Strategy, an upcoming blueprint for cyber-crisis cooperation.

ZNIU: First Android Malware to Exploit Dirty COW Vulnerability

http://blog.trendmicro.com/trendlabs-security-intelligence/zniu-first-android-malware-exploit-dirty-cow-vulnerability/

The Linux vulnerability called Dirty COW (CVE-2016-5195) was first disclosed to the public in 2016. The vulnerability was discovered in upstream Linux platforms such as Redhat, and Android, which kernel is based on Linux.

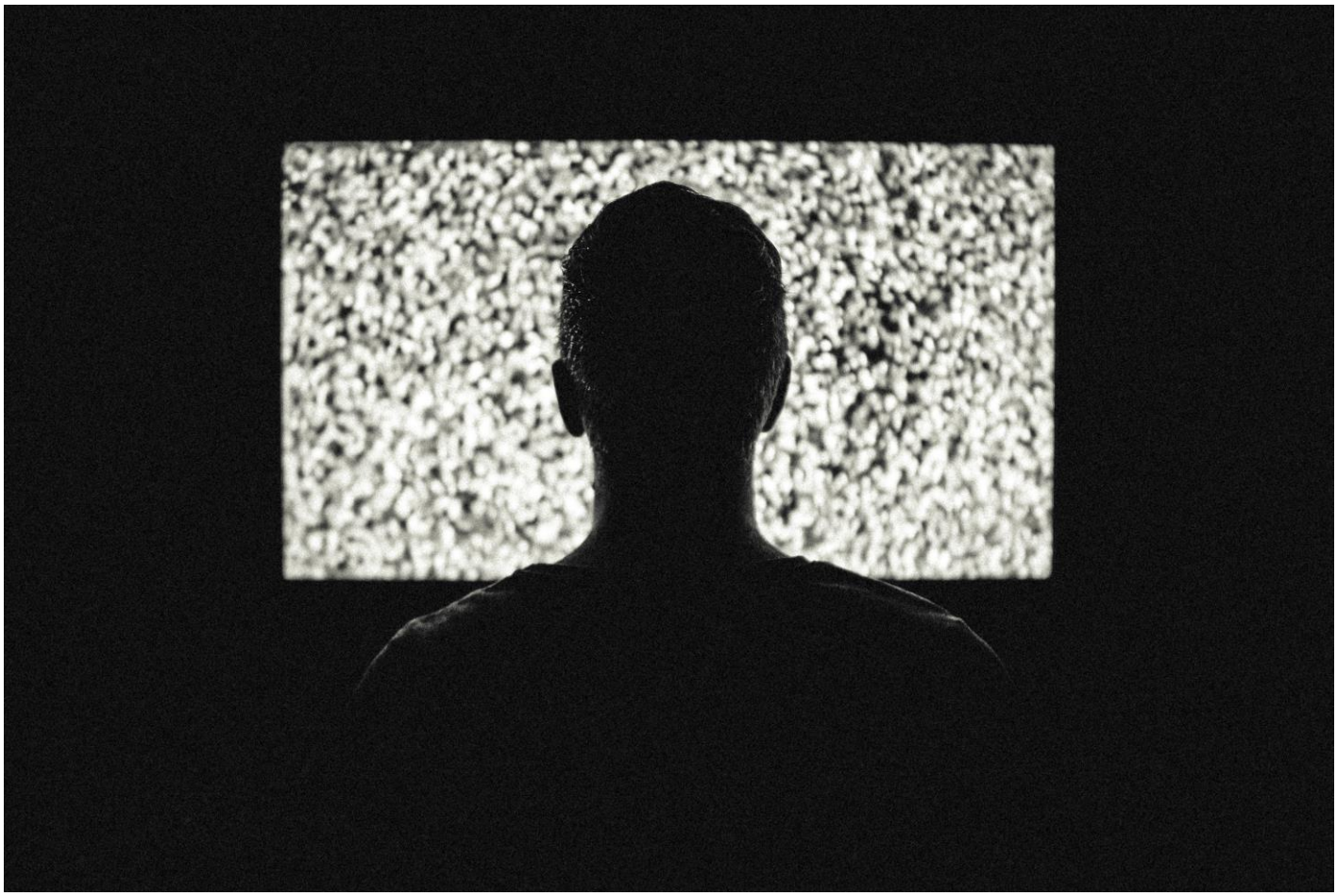
It was categorized as a serious privilege escalation flaw that allows an attacker to gain root access on the targeted system.

The phenomenon of the deep web

by Massimiliano Cannata - Technology innovation, training and security culture Reporter

THE DIGITAL REVOLUTION AND THE NEW SECURITY CHALLENGES

"The network is the world redesigned with communication materials. With the advent of digital media, nothing will be the same as before. A new category of being will mingle with the traditional dimension, modifying interpersonal relationships, habits, individual attitudes, and collective behaviors. We still do not know the consequences that will arise from the enormous potentialities that multimedia brings with it. " The citation from the French philosopher Pierre Levy, quoted by Gian Maria Fara, President of Eurispes, author of the preface to the essay by Livio Varriale (La Prigione dell'umanità, Minerva Edizioni), is about to go out to library, it may be helpful to trigger a reflection on the pervasiveness of Internet that has now overcome the original communicative purposes, radically modeling the universe of work and the rhythms of everyday life. We all live in the web as in a homeopathic dimension. From industry to digital, companies and industries on a global scale, they are experimenting with a deep paradigm shift: intangible capital and know-how deposits thanks to the new Instruments of the ICT are, in fact, available for the first time on potentially open to everyone. Widespread connectivity, Big Data, Internet of Things, Cloud Computing are all instruments that in addition to changing organizational and production processes are deeply affecting the equilibrium of contemporary society. Suffice it to think that 90% of the available data has been created over the last two years, which social networks already allow billions of people to express and communicate their ideas around the globe at a click rate and in 2020 the number of devices connected to the networks are expected to reach 80 billion.

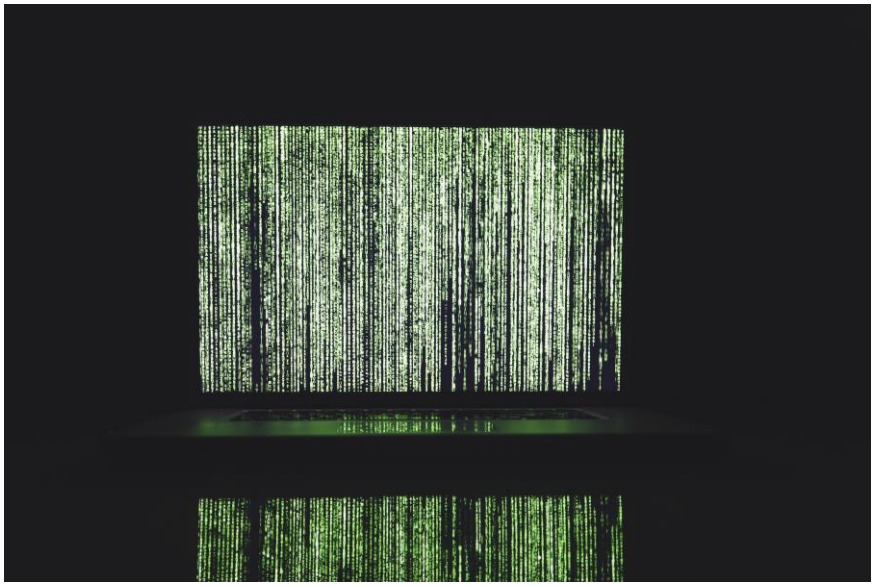


The Dark Side of the Net

There is, in fact, a dark side of the network that goes under the definition of "deep web", the "sewer of the parallel universe" that hides illegal and terrible disadvantages, which warns security specialists. "This other face of the moon has the left profile of a black region of the unleashed, where weapons are traded, narcotic drugs are dispersed, cyberspionage is made, outlaw medicine circulates, pedophile pornography and all forms of physical prostitution and what is worse intellectual. " The so-called "clear" network is just the tip of the iceberg, an infinitesimal crumb, as opposed to a growing submerged, populated by sites that refer to banks, governments, multinational corporations, terrorist cells, scrupulous hackers. An organized army, a criminal machine that feeds itself with scientific and diabolical speed. The latest news have shown the urgency of this phenomenon. The recent and striking case of "Wannacry" as it

is known has unexpectedly marked a sort of unprecedented "Day after Digital" that has bare the vulnerabilities of the digital society. Europe and not only Italy has found itself unprepared with respect to an event that has highlighted the naive and unpreparedness of users, showing the fragility of public systems that have not yet matured a homogenous risk vision. "Even the latest recent alert about obsolete software capable of risking the secrets of the army by making the defense apparatus vulnerable can give the idea of the game in play. We all walk on a silk earthquake, suspended on a abyss where technological power and fragility go hand in hand. The dangerous expansion of the deep web is making the picture outlined here even worse by understanding the importance of multilevel risk governance, designed to counter the increasingly sophisticated threats. All this will result in increasing investments in the formation of new professional figures. The security manager will have the difficult task of "protecting" the transmission of a growing amount of data and information. A systematic capacity to handle particularly complex schedules, policies, and processes must be set up. Big Data will be increasingly relevant, which will require special security expertise from Data Analysis.

Between immunization and adaptation



Varriale's study shows, finally, with plenty of data, such as governance of the security and governance of complex systems, are now terms that intertwine. In a world characterized by instability where the culture of control has fallen, the governing class will have to quickly understand that traditional government strategies for the evolutionary processes of science and technology will be less and less effective. It will be crucial to put in place strategic skills and intuition in intercepting the signals of change. The latest experience teaches that cybercriminal action will not be able to solve a mechanical response to external attacks, but rather to implement policies that can interpret the "karstic" processes of the infection, which lie in the "subsoil" of the deep web. In conclusion, it does not seem appropriate to adopt the biological metaphor used by linguist and anthropologist Gian Paolo Caprettini: "Tomorrow's security will be based on the delicate balance between two processes: immunization and adaptation. The attacks come from the outside world, and the subject - an individual, state or business - will only have to set antibodies to ensure survival. But antibodies are nothing but a re-elaboration of genetic information. " It will be decisive to find a balance between two antagonistic forces that shake homo-tecnologicus: a centrifugal thrust that brought him and leads him to overcome the space by leaving himself and a centripetal force that causes him to fall back to close the bridges with the 'outside, to live in the' voluntary slavery 'of device that continually restrict their freedom. Can the network be a compensation mechanism, the powerful valve that can allow him to recover lost contacts with the lives of contemporary cities or become a suffocating and subdued prison? Meanwhile, real and virtual, they continue to blend in the web flow, amplifying the circularity of an existential and psychological process that makes every attempt at orientation difficult. We will probably have to add a further meaning to the term security, which can be identified in the need to balance the relationship between the I and the world, between the "electronic body" and the creative resources of which each is original bearer.