BE CERT

In these days, the Italian Government has published the decree "Urgent measures on the cybernetic national security perimeter". With this disposition, a true cyber security perimeter is created, moreover, the Government adopts regulatory instruments that allow it to take action promptly and in an effective manner in case of threat events and dangers to national security. The decree complements the European Directive NIS (Network and Information Security) by directing companies that supply essential services and OTTs in the digital world. Furthermore, another decree will be adopted that will define the core companies for national security that will be included in the perimeter and added to the 465 already identified by the NIS directive. Additionally, in the decree it is envisaged that the Prime Minister, on the instructions provided by the Interministerial Committee for the Security of the Republic (CISR), will have the power, in time of crisis, to intervene and provide for the removal of threats both in a defensive and offensive manner.

In this context, which focuses on the cyber security issue of the country and its infrastructures, the role of the Computer Emergency Response Team (CERT) assumes its centrality. This unit has its roots in the 90s when, following Morris’s malware, there was a loss of money for about 100 million dollars and the blocking of a substantial part of computers connected to the Internet. Following this event, the American Government decided to create the Computer Emergency Response Team (CERT) in history located at Carnegie Mellon University.

CERTs are crucial for protecting critical infrastructures and organizations that operate in essential services; they have structures that have the ability to respond to computer security incidents in an effective manner. Precisely, in the word "CERT" is shown the core of the CERT’s activity, namely the response in case of an accident. Thanks to the capacities of these structures, these actors must perform as promoters, more and more, security awareness issues and act in this area as educators.

The CERT, comparable in some respects to the emergency rooms in the HealthCare must, has not only to provide for the management of accidents, but also take on all the activities concerning the safety of assets and processes that must be protected. It must be an active actor in the prevention, also promoting users and all its stakeholder awareness.

The role of these centers, as underlined by National and European directives, has become fundamental in this increasingly interconnected digital ecosystem. The CERT is the reference point on the collaboration, sharing and exchanging information, essential issues to guarantee the resilience of the digital system.

Nicola Sotira
General Manager GCSEC

30th ISF Annual World Congress
Location: Dublin, Ireland
Date: 26-29 October 2019

The Congress offers attendees an opportunity to discuss and find solutions to current security challenges, and gain practical advice from peers and leading industry experts from around the world. Join over 1,000 global senior executives and business leaders for 3-days of keynote presentations, workshops and networking sessions where you can share knowledge, best practice and thought leadership in a confidential peer-group environment.

Cyber Security & Data Protection Summit 2019
Location: London, UK
Date: 20th November 2019
https://cybersecuritysummit.co.uk/
About you. After years of dedication to projecting, developing, ensuring the good functionality of IT&C systems – you reached the position of deputy head of the central IT&C department of the SRI – you passed "to the other side of the line", i.e. to defend and protect IT&C systems. What motivated you to take the decision to make this "switch", quite rare within IT specialists?

It is true that work in Romanian Intelligence Service (SRI) for over 20 years and until the beginning of 2017 I worked in an area with several and diverse technical tasks. I did not choose to "change sides" in the vast digital area, but the SRI management considered that, at that time, I represented a good option for taking over the management of the National CYBERINT Center, the position being then free after the retirement of my predecessor. Although I felt that my profile, based on development and creativity is not compatible with the specific work to achieve in cybersecurity, in reality it turned out that I quickly succeeded a very good assimilation and integration within the team, and therefore, I can say I enjoyed a "wild card" from the SRI, which I tried to valorise giving my best.

Pay-per-service. In the contrary to most of the EU states, your services defend the whole country as a duty without any compensation for your job. To be more precise, if the Romanian Central State has still few e-services, municipalities like Sibiu provide to citizens a total access for to many delicate documents (taxation, cadaster, familiar situation, etc.) and propose online payment for taxes, services, fines a.s.o. In France, such a city could opt between paying the ANSSI (National Agency for the Security of Information Systems) or a private company for its security. In Romania, we already do find the same situation for the transport of important artefacts within different museums: to pay the escort of the transport to the Jandarmeria or to choose one of the state-agreed private security companies. What do you think about this situation and its applicability in Romania, with its pluses and minuses?

Indeed, in Romania not all life events do enjoy a good online implementation - birth, marriage, etc. - this implementation being an ongoing process, but the payment of taxes is done online in several cities in Romania, not only in Sibiu, this group including obviously the capital, Bucharest. Regarding the comparison with the French model, I consider that each EU Member State defines its own legislation. In Romania, there is a single point for payment of taxes, www.ghiseul.ro. The site is managed by the Romanian Agency for Digital Agenda and supported by the Electronic Payments Association of Romania. The most important aspect in this case is that eventual fees and commission are not charged to the taxpayers opting for the site www.ghiseul.ro. As a consequence, this new service gathers about half a million active users who can pay their taxes with no commission fees in real time.

Real attributions vs. political attributions: in recent congresses, you have shown successful and proof-solid attributions of attacks, on the contrary of all the mostly political attributions we can read on mainstream media worldwide. Do you think that serious EU media will once be mature enough to diffuse only examples like yours or will they continue to be neglected under the tons of "immediate attributions" providing excellent "breaking news"?
Both attribution types are equally important: the technical as well as the political one, the second being built on the first. The National CYBERINT Center is the main actor in the realization of technical attributions concerning cyber attacks supported by state actors. In our country, a special mechanism has been created, under the signature of the President of Romania, to allow us at take part of international initiatives of the “blame and shame» type, which do have a major media impact. As an example, in 2018, I was part of such an international endeavour when facing the wave of attacks of the APT28 campaign, together with the initiator states - the UK and the US followed by other member states of the European Union. In my opinion, it is important to ensure a media coverage to political attributions based on technical expertise because only in this case, a huge impact can be expected. Once these cyber attacks are discovered and attributed to the author by most State victims, in a joint and conjugate effort will certainly become the object of a substantial international media coverage.

Until five years ago, most of EU State agencies like yours were regularly speaking of the successful use of “honeypots”. This term fell now into oblivion. Is it because it is a general basic practice to try to distract at least ad minimam the “bad guys” attention or, on the contrary, because technologies allow attackers to recognize them too easily?

Within the evolution of the cybersecurity phenomena, “honeypots” played and play their role, but can not be considered solutions fitting every type of cyber attacks. When discussing state attacks, the malware used is extremely complex and able in many cases to detect such “honeypots”. An area in which this solution produces results is the classic cybercrime aimed at obtaining financial benefits by cyber-fraud means.

Retaliation and proactivity: last year, Swiss citizens voted massively in favour of letting the cantonal polices and your homologue, the FedPol, to create, under a prosecutor's control, fake business profiles on social media and any other useful tools to watch and intervene at the early stages of fraud, economic espionage or sabotage operations. Since years, your colleagues in Netherlands and India have the legal right to watch and intervene at the early stages of fraud, economic espionage or sabotage operations. Since years, your colleagues in Netherlands and India have the legal right to retaliate in case of attacks. Major powers do it systematically, through their agencies or via privateers. What do you think about this situation? Should it be an asset for a more cyber-secure Romania to have those rights or would it just increase the amount of men and techniques needed to perform those tasks without a justified result?

I believe that such instruments can support proactively and very efficiently threat prevention in cyberspace and can be of help in the investigation of some incidents that have already occurred. Unfortunately, in Romania, we do not have a law to regulate mounting a side-channel attack over the network.

The weakness, tracked as CVE-2019-11184, renders a performance optimization feature called Intel's DDIO (Data-Direct I/O) that was implemented to grant network devices and other peripherals access to the CPU cache.

Warning: Researcher Drops phpMyAdmin Zero-Day Affecting All Versions

A cybersecurity researcher recently published details and proof-of-concept for an unpatched zero-day vulnerability in phpMyAdmin—one of the most popular applications for managing the MySQL and MariaDB databases.

phpMyAdmin is a free and open source administration tool for MySQL and MariaDB that's widely used to manage the database for websites created with WordPress, Joomla, and many other content management platforms.

Discovered by security researcher and pentester Manuel Garcia Cardenas, the vulnerability claims to be a cross-site request forgery (CSRF) flaw, also known as XSRF, a well-known attack wherein attackers trick authenticated users into executing an unwanted action.

Over 1 million Google Chrome users affected by Cookie Stuffing from two popular adblockers

AdBlock and uBlock, two popular Ad Blockers, were found stuffing cookies to generate revenue.

Last year, AdGuard pointed out five similar fraud ad blockers with over 20 million active users.

An overview: Google Chrome on Monday booted two pretentious Ad Blockers ‘AdBlock’ and uBlock’ that were home to extensive ongoing ad fraud.

AdGuard, a maker of an ad-blocking software (Russia) discovered the extensions accused of redirecting users to malicious or compromised websites hosting malware or phishing scam.

“AdBlock” was published by “AdBlock, Inc” and “uBlock” by “Charlie Lee.”

The two extensions used names that are confusingly similar to two better-established ad blockers, AdBlock Plus and uBlock Origin, and that this alone should deter people from using them,” said Andrey Meshkov, co-founder and CTO of AdGuard.

Shoddy Code Is Behind Many Of The Biggest Recent Data Breaches

It’s an unfortunate side effect of our current tech landscape that we’ve become desensitized to news of another major corporation suffering a massive data breach.
cyber security and defense, which could allow players to use such highly useful tools. However, international law, applied also in Romania, allows the use of progressive retaliatory measures in case of cyber attacks. In this frame, proving the link between a cybernetic actor and a state actor holds a special importance because only the achievement of these conditions can allow the provisions of international law to be applied.

In a public-private collaboration perspective, which are your projects and wishes for the years to come, for a more secure Romania. What has been recently achieved and what remains to be done?

Among the main perspectives that the National CYBERINT Center plans to carry out as public-private partnership, I would like to mention the strengthening of university programs in the 21 universities that agreed to start Postgraduate in-depth study programs on cyber security (of short duration or even masters) and the continuation of our pilot project devoted to introducing concepts of cyber security and cyber hygiene in the national high school curriculum in the Colleges with IT specializations. Also, another goal is to increase the quality of national exercises by providing a constant number of players and observers – an example being the national cybersecurity exercise, CyDEX – but also to consolidate national conferences on cyber security, as for instance the international conference "Strategic Partnership Romania-US cyber security" and the «cybersecurity dialogues - Romania» congress organized in Sibiu. On the legislative level, it is extremely important to implement in a more accelerated pace the provisions of NIS Directive, which will increase the safety of IT services and essential services operators; it is also vital to create a solid market for cyber security in Romania. Last but not least, at an institutional level, I think we should create a hub for the exchange of information between the main actors responsible for cybersecurity within the diverse Romanian public institutions, which can be built following and adopting the models established in other countries, such as USA, UK or Israel.

They happen all too often, for far too avoidable reasons, and companies refuse to learn their lessons. Although there are a variety of factors that lead to these hacks, at their core they usually revolve around human error. More concerning is that many of these breaches are happening at the application level, and not through more well-known vectors such as phishing, ransomware, and malware. A 2018 study found that nearly 46% of all data breaches occurring that year were application layer attacks. This is concerning, as it reveals that a large problem with today's cyber security isn't necessarily a more dangerous ecosystem (although that undoubtedly plays a part) but rather shoddy development practices.

Cybercrime, Smominru botnet is spreading and it’s stronger

Guardicore Labs: Smominru cryptomining botnet is still spreading and it’s stronger. Only in August the worm infected over 90,000 machines worldwide, Italy included, targeting Windows 7 and Server 2008 systems. Smominru cryptomining botnet is still spreading and it’s stronger. Only in August the worm infected over 90,000 machines worldwide. It has been revealed by Guardicore Labs cyber security experts. Countries hit include Italy, China, Taiwan, Russia, Brazil, and the US. Infected networks include US-based higher-education institutions, medical firms and even cyber security companies. As the attacks were untargeted and did not discriminate against industries or targets, they reached victims in various sectors. The malware, once it gains a foothold, attempts to move laterally and infect as many machines as possible inside the organization.

European Cybersecurity Month 2019 is launched

October marks the kick-off of the European Cybersecurity Month (ECSM), coordinated by the European Union Agency for Cybersecurity (ENISA), the European Commission and supported by the Member States. This campaign will focus on expanding awareness about cybersecurity to citizens across Europe. The 2019 campaign focuses on different themes addressing the need for behavioural change and identifying opportunities to help users recognise the risks of new technologies.
**Question 1)** The cyber scenario is continually growing and organizations should be more and more prepared to face new threats. In this context, which is the role of a modern CERT and in particular in the financial sector? What are the priorities?

In Israel, we have a National Financial CERT that is part of Israel's National CERT. The National Financial CERT's responsibility is to support the cybersecurity protection of the financial ecosystem – with national and international threat intelligence, recommendations on how to mitigate the threats, and incident response teams with boots on the ground that can support an organization in a case of a need.

The focus of the National Financial CERT is on end to end financial processes which are identified as critical to the financial ecosystem to function, such as cash flow, credit card transaction, and more. The financial processes status and resilience determine the prioritization and status of the financial ecosystem.

**Question 2)** Preventive activities plays an important role. Could the sharing of information improve resiliency of Financial Services? Are you working in this direction?

Being prepared to any hazard that may occur is key. Therefore, on top of cybersecurity drills to the professional teams that the cyber directorate is running, the Ministry of Finance is running cyber resilience drills to the financial leadership. Just half a year ago, we executed a drill in which participated the Minister of Finance, the Central Bank Manager, all of the financial regulators and representatives from the private market, working together on answers to scenarios in which dramatic cyber attacks occurred, impacting the financial ecosystem, resulting in financial decision making that are required due to cyber-attacks.

On top of that, the Financial CERT is providing various recommendations to the financial institutions on how to protect themselves. The recommendations vary from a specific vulnerability, domain or IP address to block, to identification of new attack methods, vectors, etc.

It is up to the financial institutions themselves to decide whether to follow a specific recommendation or not. The interesting thing with the Israeli National Financial CERT, is that we're not a regulator. Therefore the connection of the financial institutions to us is fully voluntary. Still, 100% of the banks, 100% of the credit card companies, and all of the big and medium insurance companies are all connected to the Financial CERT to consume its services and report incidents to it.

**Question 3)** The human is becoming from vulnerable point to the first line of defense against cyber-attacks. Your CERT is investing in awareness and training?

It is true that one of the weakest links in cybersecurity protection is the human factor. Whether it is since they are deceived to follow a link, open a malicious email, connect an unscanned USB, or whether it is the risk of an unhappy employee that becomes the threat from within.

Israel's National CERT is working directly with the public, creating awareness. The financial CERT is working directly with the CISOs and SOC managers. It is the CISOs’ responsibility to educate and even test the employees.

We mitigate the weakest link from another angle. Since we focus on end to end financial processes, we want to make sure that each one of the links in them is protected, and it means that not only the financial institutions should be protected but
also the 3rd party suppliers that are part of these processes. This is why we have a unique unit in the ministry of finance that is focused on cybersecurity guidance to the financial supply chain, and that is working with the most critical suppliers that influence the critical end to end financial processes, running cybersecurity surveys for them, providing recommendation for them to follow, in order to make sure that they become more resilient.

**Question 4)** What is the role of new technologies like artificial intelligence, machine learning, blockchain, 5G? Can these really help a CERT in its strategic operational tactical activities?

The National CERT and the financial CERT are utilizing new technologies such as blockchain, AI and so on in order to protect the financial ecosystem and the Israeli cyber sphere in general, whether it is through self-developed products or through usage of new released products.

**Question 5)** Innovation is everywhere. Do you see yourself as a contributor to it?

Indeed, innovation is everywhere, and as a country that invest in it on a regular basis, we wanted to leverage the unique data and expertise that we have at the Financial CERT in order to promote fintech and cyber startups, and to help Israel in becoming a fintech-nation on top it already being known as a cyber-nation. This is why we launched the fintech—cyber innovation lab program. In this lab that will be owned by the private sector, we are leveraging cyber-financial government data to fintech and cyber startups in order for them to be able to develop, test and demo their products with a stronger connection to security and to live events. We are the first country in the world that is leveraging such data to the industry and we see it as a natural evolution of the expertise that we gained.

We want the private sector to own it in order to bring their own needs and requirements. This is why we've released a tender that will be closed by mid-November. The lab should be up and running in 2020.

**Question 6)** How to improve real collaboration among the financial institutions? GCSEC have set up the CERT STAR initiative, a program of technical and operational meeting dedicated to CERT’s analysts and operators to improve their collaboration and competences. Do you have similar initiatives?

We believe that information sharing is one of the key tools in becoming more resilient. This is why the Israeli National Financial CERT is actively investing in this – besides ongoing forum meeting with its members, we are sharing information not only with the local financial ecosystem (which are our customers), but also with international financial institutions, such as Poste Italiane. Such collaboration can make a difference – we are much weaker as silo islands, each one taking care of its own territory, the cyber attacks are like tsunami waves, harming what ever comes in their way. If we'll stand together, each one of us will be better protected.
The mission of GCSEC is to develop and disseminate knowledge and awareness on Cyber Security, creating the conditions for improving capabilities, skills, cooperation and communication between the different stakeholders involved in the use and protection of internet. During the last years, GCSEC has focused the efforts in spreading around the Cyber Security culture and awareness. The Foundation aims to create and share cyber security knowledge, with no-profit intentions, in the enlarged community of experts and layperson.

In particular has established specific projects to enhance CERT competences. GCSEC has carried out **CERT STAR Program**, an educational program of closed meetings dedicated to Italian CERTs and SOCs aimed to enhance competences, improve cooperation and experiences exchange.

During the meetings, core security topics like threat hunting, incident prevention and response, intelligence and digital forensics are analyzed at technical operational level. Meetings include practical exercises and use of virtual laboratories, tools and instruments.

The program is dedicated to CERT's and SOC's analysts and operators of Big Companies, Public Administration and Low Enforcement. Meetings on a bimonthly basis started on February 2019. Topics of 2019 program are APT and cyber range, Dark Web Intelligence, Cyber Threat Intelligence, Application Security, End Point Security, Cyber Strategies for executive.

To help CERTs to enhance their competences, GCSEC are developing **CERTrating**, an online platform that helps organization to measure maturity level of its CERT and each services provided to constituency, to identify areas for improvement and the strategies best suited to its needs. CERTrating provides also a dashboard and specific reports to present to the Top Management the current status of CERT and its services.

CERTrating offers also a simple and immediate view of the maturity of CERT and its Services and of positioning with respect to other Italian CERTs through a graphical representation of the level of maturity of CERT and its services, the maturity trend over time, the history of all the evaluations carried out for CERT and its services and the distance from the average maturity level of the other Italian CERTs.

The tool is developed according to the Capabilities Maturity Model defined by ENISA (SIM3), which is based on, consist in three tier measurement of CERT capabilities across 4 parameters: Organization, Human, Tools and Processes. All parameters are evaluated in order to determine level of maturity (Basic, Intermediate or Advanced).

Answering simple multiple choice questions CERTrating provides the maturity of the CERT by applying the SIM3 model defined by ENISA and the applied maturity of CERT, that is not related to the CERT as a whole but taking into account the maturity of each single service and the role played by each of them for the achievement of the company objectives.

The platform provides a self-assessment survey for the whole CERT (based on SIM3 Model) and others 14 self-assessment surveys for CERT’s services. The self-assessment surveys for Services are based on the model implemented by ENISA but customized for each service.

All surveys are composed by 44 detailed questions. Answers available are set on specific maturity levels:

- **Answer 0** = not available / undefined / unaware
- **Answer 1** = implicit (known/considered but not written down, “between the ears”)
- **Answer 2** = explicit, internal (written down but not formalised in any way)
- **Answer 3** = explicit, formalised on authority of CSIRT head (“rubberstamped” or published)
- **Answer 4** = explicit, actively assessed on authority of governance levels above the CSIRT management on a regular basis (subject to control process/review).

Once the user complete to self-assessment surveys, the Tool provides specific actions to improve the level of maturity of CERTs (ex: minimal actions to pass from Basic level to Intermediate maturity level).

The CERTrating Tool is developed in Italian and English to help CERT to define its maturity in the complex world of Cybersecurity. The platform will be available by the end of the year on [www.certrating.com](http://www.certrating.com).

For many information, please send an e-mail to info@gcsec.org.
Il primo Tool per valutare il livello di maturità del tuo CERT e dei suoi Servizi

Available Soon

www.certrating.it

Per maggiori dettagli
Info@gcsec.org