GLOBAL CYBER SECURITY CENTER

Newsletter

2019 February

Cyber Security is our mission

editorial

Skill Shortage, the new threat

The cyber threats continue to grow in modality, intensity and in terms of sophistication, in this scenario the needs of security teams constantly change and require more and more specialized personnel. Increasingly we are witnessing situations where we face the emerging risk with a lack of personnel and a difficulty in attracting and recruiting adequately qualified personnel, a situation that already represents a risk for itself. Capacity and capacity deficits are occurring while major safety incidents damage organizational performance and reputation. Building tomorrow's security workforce is essential to address this challenge and provide solid, long-term security for organizations in the digital age. Filling the skills gap will require organizations to change attitudes and approach to recruitment, training and participation in collaborative pipeline development initiatives. A too rigid and traditional approach to identifying candidates, together with overworked and insufficient working environments, clearly needs new tactics and new ideas. GCSEC is active on EU research programme and awareness campaign. It has developed projects on information sharing, ICS and Smart Grid security, E-crime, Cyber Educational Programme and so on. The last years it has organized events and workshops on ATM security, Advanced Persistent Threat, PSD2 Security and already published studies, such as, “DNS Health and Security” in collaboration with ICANN, “Information Sharing and Public-Private Partnerships: Perspectives and Proposals” in collaboration with UNICRI and “Best Practices in Computer Network Defense: Incident Detection and Response” in collaboration with NATO.

The study on “Mind the Gap: the cyber security skills shortage and public policy interventions” represents the last stone and result of the collaboration with Oxford Centre for Doctoral Training in Cyber Security. We believe that more should be done to prepare our countries to a better and safer digital world. The first step to facilitate the digitalization, in accordance with the Third Pillar “Trust and Security” of European Digital Single Market Strategy is to mind the gap of skills and competencies in cyber security. In this study, we have done an overview of Countries policy and experts opinions on cyber security educational programme, highlighting some recommendations for the future.
Closing the gap between supply and demand is imperative for an enterprise to develop an effective security posture. It is evident that individuals with the required skills, qualifications and experience are either unavailable or demanding compensation that cannot be met with existing budgets. Because they are in high demand, talented security staff regularly move to new employers as they seek out better salaries and projects at more prestigious companies.

Enjoy the lecture…

Nicola Sotira
General Manager GCSEC

events

CYBER SECURITY TECH SUMMIT EUROPE 2019
Location: Bonn, Germany
Date: March 13-14, 2019
https://cyber-security-tech-summit.eu/en/2019.html
The ongoing digitization of our society and economy put an increasing focus on the need to safeguard the associated developments. As cyber attacks continue to get more complex and refined, we are literally forced to spend a lot of time and resources on topics like data/information security and the protection of critical infrastructure. Under the motto “The Cyber Heartbeat of Europe“, the Cyber Security Tech Summit #CSTSE19 aims to set new standards.

CYBERSECURITY SUMMIT ROMA 2019
Location: Rome, Italy
Date: March 19, 2019
https://www.theinnovationgroup.it/events/cybersecurity-summit-roma-2019/?lang=it
CYBERSECURITY SUMMIT 2019 by The Innovation Group, Rome edition, aims to take stock of the current state of security maturity, in the context of Operators providing essential services (OSE), businesses, public administrations. The participation of the Institutions dealing with the national Cyber Defense and the best Italian and international experts, gives a unique opportunity to exchange experiences and networking, to deepen the emerging security needs, the new threat landscape, and to understand how enable a more secure use of Cloud and emerging technologies such as AI, machine learning, blockchain.

Cybersecurity Mediterranean Congress - 2nd Edition
Location: Florence, Italy
Date: May 9-10, 2019
https://gcsec.org/cybersecurity-mediterranean-congress/
The Second Edition of the Cybersecurity Mediterranean Congress will be held in Florence, organized in collaboration with the

in this issue

The Cyber Security Skills Shortage: Facts and Myths

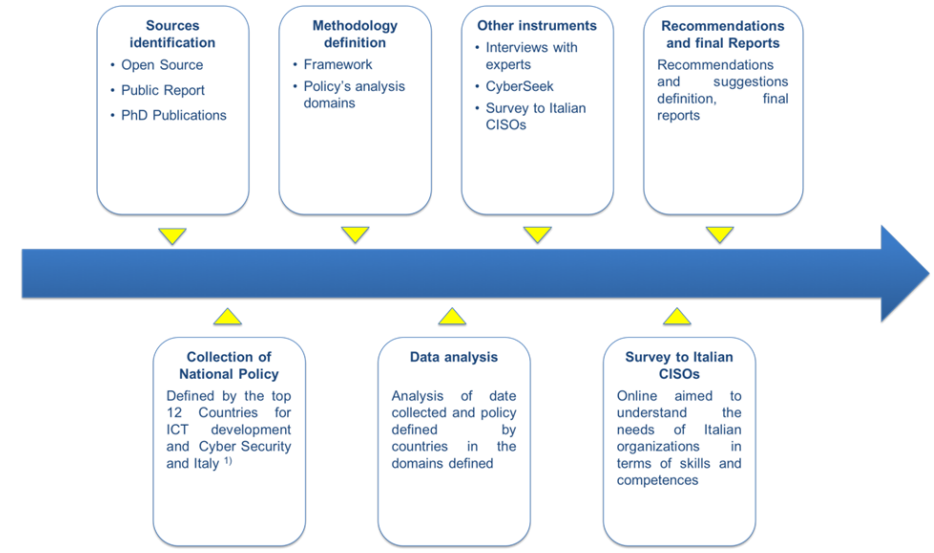
by Tommaso De Zan –PhD Researcher in Cyber Security at the Centre for Doctoral Training in Cyber Security, University of Oxford

The Cyber Security Skills Shortage: Facts and Myths

by Tommaso De Zan – PhD Researcher in Cyber Security at the Centre for Doctoral Training in Cyber Security, University of Oxford

The cyber security skills shortage (CSSS), the lack of cyber security professionals in the labor market, is one of the most pressing challenges in cyber security policy. Various research has reported staggering numbers on the global workforce shortfall and governments of major countries have already voiced their worries. However, not everyone seems on the same page. Rik Ferguson, vice president for security research at Trend Micro, said "*You're being conned. There's no such thing. It doesn't exist.*" Even if a such a shortage existed, it would be hard to deal with as, according to CEDEFOP, we do not really know much about effective policies and practices addressing skills imbalances.

Against this backdrop, last year I have conducted exploratory research, funded and supported by Global Cyber Security Center (GCSEC), to answer two main questions: is there a CSSS and what evidence do we have? If there is one, what are countries doing to increase the pipeline of professionals? I have analyzed approximately 50 reports and interviewed 30 experts in cyber security and skills policy. Findings depict an extremely complex picture.



1) Policy updated to 2013-2018 versions

For sure, there is an evident and a widespread perception of the shortage. But a perception not always equal factual evidence. Indeed, the current empirical knowledge on the CSSS is piecemeal and flawed by several methodological issues, including ambiguous questionnaires, ill-formulated indicators, doubtful quantifications of the global shortage and overall poor generalizability of research findings. It is not by surprise that the account of the characteristics and nature of the CSSS varies greatly depending on data sources. For instance, industry reports almost unanimously consider the education and training system as the main culprit behind the shortage, seen as unable to produce enough graduates ready to take up jobs in cyber security. While agreeing on the need to modernize the current academic offer, national policy documents and interviews provided a more balanced view, underlying that the shortage could be exacerbated by employers themselves, who seem to be

GCSEC Foundation, Thales under the aegis of ITU, and under the patronage of the Swiss Embassy in Italy.

news

60,000 EU data breaches filed under GDPR

https://www.scmagazineuk.com/60000-eu-data-breaches-filed-gdpr/article/1524926

The EU's GDPR regulation and its attached fines appears to be encouraging data breach reports with almost 60,000 such reports being filed since the privacy law went into effect in May, but the number of fines imposed lag far behind. The EU's GDPR regulation and its attached fines appears to be encouraging data breach reports with almost 60,000 such reports being filed since the privacy law went into effect in May, but the number of fines imposed lag far behind.

A report by DLA Piper found 59,000 data breaches have been reported to regulators throughout the EU and all of these breaches are not equal as they range from simple emails being sent to the wrong party to major hacks impacting millions.

However, only 91 fines have been issued so far and not all of them are related to data breaches. Google was fined about US$ 57 million (£44 million) by the French data protection authority – the CNIL – for processing of personal data for advertising purposes without valid authorisation.

New Linux coin miner kills competing malware to maximize profits

https://securityaffairs.co/wordpress/80892/malware/linux-coin-miner.html

Security experts from Trend Micro have discovered a new strain of coin miner that targets the Linux platform and installs the XMR-Stak Cryptonight cryptocurrency miner, researchers observed it killing other Linux malware and coin miners present on the infected machine.

The experts detected a coinminer script on one of their honeypots and, the malicious code shares some parts with the Xbash malware and the KORKERDS cryptocurrency miner that leverages rootkit to avoid detection.

"We found the script capable of deleting a number of known Linux malware, coin miners, and connections to other miner services and ports, and we observed some parts of the script to be reminiscent of Xbash features and KORKERDS." reads the analysis published by Trend Micro.

Better security measures for smartphones, ENISA has created a SMAShiNG new tool

https://www.enisa.europa.eu/news/enisa-news/better-security-measures-for-

rarely providing entry-level opportunities and good quality training. One of the interviewees suggested:

"I think that the CSSS is more due to industry and government than it is to the education system. They need to get much more guidance on how to get people into the system, but then they need methodologies and approaches to nurture these people throughout their careers."

Even though current knowledge on the CSSS does not withstand scientific scrutiny, it would be irresponsible to dismiss it as a prefabricated industry lobby operation, as some shortage critics would do. Abundant national evidence and results from interviews suggest that, at least in certain countries, there are currently numerous issues that impede a correct matching between the cyber security supply and demand. For example, there were almost 314,000 active cybersecurity job openings in the United States between 2017 and 2018; in Australia between 2014 and 2016 cybersecurity salaries increased by 2.7% compared to an average annual wage growth of 1.7 per cent in the wider IT industry, signaling a scarcity of workers which in turn drives wages up. Yet, no measurement has been able to confidently capture the incidence, scale and nature of the problem, especially at the international level.

But if a shortage of some sort exists, how governments have reacted to it?

Overall, policy responses of certain countries have been more elaborate than others, most notably in Japan, the UK and US. More complex policies have attempted to target a wide range of different groups with a multi-stakeholder approach involving the three main actors in the debate, namely the government, private sector and education system. Governments have invested more in higher education, research and the workforce, whereas fewer and vaguer initiatives have been directed towards primary and secondary schools as well as vocational or apprenticeship programs.

However, policy measures implemented by some national authorities suggest that the nature and the characteristics of the shortage are still not well understood. For example, it is not straightforward to distinguish policies that are trying to increase the pipeline of security professionals (under-supply) from those that are seeking to improve the quality of job candidates (under-skilling). However, this is important, as governments might be erroneously thinking to be tackling one aspect of the problem (usually under-supply) when in fact their policies are predominantly addressing another aspect (usually under-skilling).

Moreover, some national policies might need recalibration. For example, one of the causes of the shortage could be the lack of graduates' professional experience and the absence of entry-level opportunities. The analysis found that, with a few exceptions, governments have primarily sought to intervene at the higher education and research level. If data are confirmed, some policies could be reconfigured to ease the transition from school to the workplace, instead of being directed towards other areas.

Finally, from the data collected it is impossible to assess the effectiveness of these policies or, in other words, whether these policies have achieved their intended impact. After a long enumeration of strategies, action plans and policies, one is still left wondering how many individuals targeted by these policies have later joined the cyber security sector. Unfortunately, it seems that not many governments have in place metrics to evaluate programs for reducing the shortage.

Further research on the CSSS is a matter of priority. In an era of increasingly sophisticated cyber-attacks with the potential to have crippling effects on all of our lives, it is wise to educate and train an adequate number of cyber security professionals who are able to fend off cyber-attacks. If data and systems are the essence of the new digitized economy, governments should adopt the necessary measures to guarantee their confidentiality, integrity and availability, including by growing the right people to do it.

The report "Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions" is available here. The Italian case study will be published by March.

Good reading to everyone!

smartphones-enisa-has-created-a-smashing-new-tool

ENISA releases SMAShiNG – SMArtphone Secure developmeNt Guidelines – an online tool that maps security measures for smartphone guidelines. The tool supports developers to build secure mobile applications. The SMAShiNG tool supports developers to build secure mobile applications. It is technologically agnostic, hence can be applied to all mobile applications developed for any operating system on the market nowadays…

SMAShiNG makes it easier for the developers' community to follow guidelines, by selecting only the ones that are relevant to them. The tool allows for selecting security measures associated with a specific domain and export them as a checklist to follow in the design phase, based on the requirements of the developer. The security measures featured by SMAShiNG are defined in the ENISA Smartphone Secure Development Guidelines report, which provides a guide for developing secure mobile applications.

Hackers Wipe VFEmail Servers, May Shut Down After Catastrophic Data Loss

https://www.troyhunt.com/the-773-million-record-collection-1-data-reach

The U.S. servers of privacy-focused e-mail provider VFEmail were hacked into on February 11 and all the data was destroyed, on both the main and the backup systems.

According to VFEmail's owner, the hackers did not leave a ransom note and, given the extent of the destruction, the service will most likely go offline to never return.

In the first tweet following the discovery of the attack, VFEmail said that "This is not looking good. All externally facing systems, of differing OS's and remote authentication, in multiple data centers are down."

Subsequently, after managing to track down the hackers' activities on their servers, VFEmail was able to catch them while they were formatting the e-mail service's backup server…

Malware spam campaign exploits WinRAR flaw to deliver Backdoor

https://securityaffairs.co/wordpress/81669/hacking/winrar-exploit-malspam.html

Experts discovered a malspam campaign that is distributing a malicious RAR archive that could exploit the WinRAR flaw to install deliver malware on a computer. Security experts at CheckPoint software have disclosed a critical 19-years-old vulnerability in the WinRAR that could be exploited by attackers to gain full control over a target computer. Over 500 million users worldwide use the popular software and are potentially affected by the flaw that affects all versions of released in the last 19 years. The flaw is an "Absolute Path Traversal" issue a third-party library, called UNACEV2.DLL, that could be exploited to execute arbitrary code by using a specially-crafted file archive.

“Mind the Gap:
The Cyber Security Skills Shortage and Public Policy Interventions”

GCSEC - Global Cyber Security Center
Viale Europa, 175 - 00144 Rome - Italy
https://www.gcsec.org