THE CYBERSECURITY QUALIFICATIONS AS THE PREREQUISITE FOR THE CYBERSECURITY CERTIFICATION OF ENTITIES

Jakub Vostoupal

Mgr. Jakub Vostoupal, PhD student, Masaryk University, Faculty of Law – Institute of Law and Technology.
Veveří 158/70, 611 80 Brno, CZ
Email: Jakvost@gmail.com

Keywords: ***Compliance, Certification, Cybersecurity, The Cybersecurity Act, Conformance assessment, Qualification Frameworks***

Abstract: *Cybersecurity is one of the key aspects of cyber-governance. There is no way of maintaining an effective state administration without proper cybersecurity measures. A relatively new way of strengthening overall cybersecurity of the Union is the widespread use of the cybersecurity certification. The certification procedures are now primarily focused on products, but that will probably shift in the future. Instead of ever-evolving products, there shall be certification procedures for services, processes and maybe even for the entities themselves. Even though there are no foundations for this idea to evolve yet, the qualification frameworks could possibly present a solution to this predicament, a first step of defining the future schematic requirements. In this article, I present the possible future for the certification systems and emphasize the importance of the qualification frameworks as the prerequisite for the entities-stage of cybersecurity certification.*

1. Introduction

The COVID-19 pandemic forced many of so far offline-based subjects into the cyberspace. Many of these subjects had little to no knowledge of cybersecurity and were severely unprepared for the challenges of the online environment. To make things even more challenging, the lockdowns issued by the governments cut many of the monetary streams of these subjects down. They had no cybersecurity to speak of and almost no funds to spare, many of these subjects were literally fighting for their future. In this environment, it is not surprising that cybercrime flourished (which can be demonstrated on the warning of the Czech National Cybersecurity Agency, see National Cyber and Information Security Agency, 2020). With no intention of diminishing the horrors of the cybercrime against these subjects, the real danger during the pandemic lies with the cyberattacks against the critical information infrastructure. Since the end of the year 2019, we have witnessed an unprecedented number of cyberattacks against hospitals and other parts of the critical infrastructure not only in the Czech Republic but all over the European Union (which led even to a call out against China, see Cerulus, 2020).

In the Czech Republic, one of the most serious cyberattacks was mounted against the Rudolph and Stephanie Regional Hospital in Benešov on December 11, 2019, so even before the COVID lockdown (National Cyber and Information Security Agency, 2020). The situation worsened since then, there was even a successful attack against the University Hospital Brno, one of the greatest hospitals in the republic, and the NCSA issued a warning for all hospitals (National Cyber and Information Security Agency, 2020).

The Benešov attack began with the spear-phishing campaign mounted via the botnet Emotet, proceeded by an infection of the network by malware Trickbot, which was possibly leaching personal medical data out of the hospital, and ended with the use of ransomware Ryuk. That encrypted almost all of the hospital data and effectively froze the entire hospital, the central medical point for almost 400 000 people (National Cyber and Information Security Agency, 2020). The infrastructure of the attacked hospital was recovering for three weeks and the hospital reported a loss of more than 2 million EUR (*Annual Report for Business Year 2019*, 2020).

The attack vector of this particular aggression showed several great weaknesses of the existing system, at least in the Czech Republic. Firstly – the Benešov Hospital was not an obliged entity (it was too small to pass the criteria) under the Czech Act on Cybersecurity[1] and therefore was not obliged to implement any cybersecurity precautions, so the technologies used were not as resilient as they should have been according to the risks the hospital faced. That is mostly by a grotesque lack of finances for cybersecurity (all over the state administration) and a sad lack of understanding of how important the cybersecurity is and how to implement sufficient precautions. And secondly – there is an astounding lack of cybersecurity experts on the market (Muncaster, 2019). This is a serious risk, not only for hospitals and the obliged entities but for the state administration as well, because these subjects cannot offer such sweet deals to the cybersecurity experts as a private sector can.

The failure of the cybersecurity in Benešov and many others had three parts. First – the technologies, the products. The products used in the hospital were in many cases nowhere near cyber secure, they were not updated, they were not separated, etc. That can be in future remedied by extending the reach of the Czech Act on Cybersecurity/NIS directive[2] and by using certified cybersecurity technologies. Many of the attacks all over the Union might be partly caused by the fragmented approach to the NIS obligations, specifically the identification of the obliged entities.[3] This is about to change as the NIS directive 2.0 approaches (Boratynski, 2020). The NIS 2.0 should remake the baseline for the obliged entities as well as the obligations (e.g., the supply chain security), especially for some of the smaller bodies (Haid & Schneider, 2020). The Commission clearly fights for even more united and more complex cybersecurity approach and there are several areas (e.g., said supply chain security) in an overlay with the matter of Cybersecurity Act[4], i.e., the certification activities. This makes for a more holistic and feasible framework for the obliged entities once it is all up and running because they shall have an obligation as well as the means to fulfil this obligation. All of this shall greatly improve the cybersecurity in the Union. But it is not enough. Extending the reach of the NIS and other compliance obligations as well as using certified products is commendable, but the cybersecurity is not only about the products, about the "building blocks". Even a certified product can be undone by the unsecured network, lack of security processes or by people. Especially people (Malatji et al., 2020).

Products, processes (and services), and people. These three aspects are the parts of the most cybersecurity failures, the Benešov incident included (Sivasankaran, 2017). These three are the core of the cybersecurity focus or at least should be (Sivasankaran, 2017). As Sivasankaran aptly states, the omnipresent preference of product-focus and trust in technologies in cybersecurity is often its own undoing (Sivasankaran, 2017). By the way of example – even if I have the unpickable lock, it would all be for nought if the doors could be easily broken or the person operating the lock could not lock it. And the perpetrators always choose the easiest way. If the doors are impenetrable, they may be getting in through the wall. But why bother when there are always people who can let them in?

There is a sad but often simple truth in the cybersecurity field – the flesh is weaker than the machine. It is confirmed by the prevalent popularity of the social engineering techniques, spear phishing and phishing campaigns as well as e.g., the report of Kaspersky lab (*Understanding Security of the Cloud*, 2019), where

[1] The (Czech) Act no. 181/2014 Coll., the Cybersecurity Act.

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[3] Even though this may not be the case in Czechia as the Czech Act on Cybersecurity is even stricter and reaches further than the NIS directive dictates.

[4] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

an alarming number of corporate breaches in the cloud is caused by the social engineering techniques. It is therefore obvious, that the product-focus can never be enough.

2. The Cybersecurity Act and the Certification Framework

The cybersecurity certification is a relatively unknown form of compliance procedure (at least in some member states, the Czechia included), during which a third, unbiased party – certification body – assesses fulfilment of cybersecurity criteria, usually formulated in a standard or a certification scheme, of the assessed object/technology of the manufacturer. In case of passing the assessment, the certification body issues a certificate, proving to anybody that this technology was subjected to and passed the tests, increasing trust in relevant technology in turn (generally speaking). For a long time, the certification legislation and procedures were fragmented all over the Union, some states (e.g., France) using developed certification systems and capacities, other almost ignorant of the fact these procedures exist at all (e.g., the Czech Republic). Not only was this a higgledy-piggledy chaos for anyone who wanted to navigate their way in the legal requirements, but there was also a matter of a cross-border non-recognition of the certificates. If a manufacturer got a certificate in France according to the French rules, it meant nothing in the (e.g.) Great Britain and vice versa. In this case, the manufacturer who wanted to sell his products in multiple member states had to undergo several of the certification procedures (which are usually really demanding, both in time and finances required). That excluded many of the SMEs from enjoying the benefits of the single market.

A rather new piece of legislation called the Cybersecurity Act (Regulation of the EU) is the new hope for the cybersecurity market of the Union. It introduces a revolutionary unitary framework for cybersecurity certification of products, services and processes with certificates universally recognized all over the EU. The Commission in close cooperation with ENISA and other stakeholder groups are working on filling this framework up with schemes for specific technologies (e.g., as of January 2021, there are preparatory works on a scheme based on the Common Criteria system and another focusing on the cloud technologies underway).[5]

3. Winds of change

The Cybersecurity Act is not fully operational yet. The Framework shall enter into force in June 2021[6] and a lot is going on right now. The first of the key documents of the Framework, the Union Rolling Work Programme for Cybersecurity Certification, which should draw up the image of the certification system, capabilities and even of the cybersecurity certification market itself, is being prepared and Masaryk University due to the membership in SCCG, an advisory body to the ENISA, has access to the draft of the Programme.

The Programme itself indicates several areas of interest for future certification activities. The first one and the corresponding candidate scheme is now entirely sure – the so-called EUCC. The Common Criteria system "takeover", it should serve as a basis for the substantial and high assurance level-certification of cybersecurity in products, such as in the Common Criteria system and under the rules of CC (although changed a bit). It shall not be used as a certification scheme for standard users and consumers as it does not allow for the conformity self-assessment procedure nor the certification on the basic assurance level. For these purposes, the Commission plans to use the Lightweight Evaluation Scheme (also for products). Also, the IoT products are to be excluded from this and shall have their own certification scheme (in my opinion because there will not be only product-based certifications in the IoT scheme but also the certification of some of the processes or services connected to the IoT).

[5] The Union Rolling Work Programme is still not published, but you can see the candidate scheme EUCC here:

[6] According to Article 69 of the Cybersecurity Act, but I partially expect the COVID-19 pandemic made such a huge impact, there shall be a delay. E.g., the Union Rolling Work Programme should have been issued in June 2020 and to this day (4.1.2021) it still was not.

The Common Criteria system is a stable and relatively old certification system (Preneel, 2014). As such, it has a lot of problems. For once it does not allow for certification of anything else but products. Then the certification procedure is costly and lengthy. Only higher assurance levels really matter, and these are costly and not internationally fully recognized (Preneel, 2014). The protection profiles are sometimes defined using ad hoc criteria, not specified enough, not secure either, so there is a valid question if these are really trustworthy. There are errors in the implementation of security mechanisms, there are national security interests in play (Preneel, 2014). But probably the biggest problem of them all is the maintenance problem. There are problems with the context changes, with new-vulnerabilities management, with patch management, with keeping the pace with the ever-evolving world of technologies and it is not a race that can be won in the long run (Preneel, 2014). There shall be an ever-growing gap between the standardization and the technology level itself due to the lengthy and bureaucratic procedures of standards and schemes approval. The standards and schemes shall be more and more obsolete and the certification according to them more and more futile. The Cybersecurity Act and the EUCC aim to counter some of these problems, but ultimately, even they are going to fail (the approval of the first two schemes under the Framework began after the approval of the Cybersecurity Act – 2019 – and as of January 2021, there is only the first version of the EUCC published).

Not only because of this but also because of the above-mentioned need for the further-than-products approach, the oncoming candidate schemes of the Framework are going to shift the focus from the products to the services and processes, which shall be more resilient to the maintenance problem, more holistic and more complex. The obliged entities shall not be obliged to certify each new cybersecurity product, to wait several months for a new certificate, to solve (somehow) obsolete schemes etc. This shift presents a possible change from many separate certifications to a few complex and holistic ones. It might be possible to even certify the cybersecurity of entire "ecosystems" and not just a few solutions.

The first example is the cloud services candidate scheme[7]. There is also a talk of supply chain candidate scheme which will probably be among the processes-certification schemes together with the ISMS (Information Security Management System) scheme.

From the point of view of the obliged entity, the certifications of services and processes are a much better solution for they need to undergo fewer certification procedures and it shall be probably easier to manage the certificates and keep them updated (the patch management included). It shall be probably even more secure. But even this solution is not resistant to the problems mentioned above (*Understanding Security of the Cloud*, 2019). We might try to change the bureaucracy behind the certification schemes for it to be much faster, much more flexible, but I doubt that we could fully counter the effects of the delay-gap as well as the over-complexity of the certification market, even if we were successful (Preneel, 2014). ENISA, Commission and other stakeholders are doing their best, but as I watch the preparatory works of the certification framework, this outcome might be eventually unavoidable.[8] Also, there is a danger in making the schemes more abstract and more easily manageable for the certification apparatus – the certification procedures itself would become more uncertain and implementation complex for the obliged entities. It essentially shifts the costs, does not eradicate them.

3.1. One step more?

Hypothetically, there is one more step on this certification staircase, one that would require the entities to undergo even fewer procedures. One that could bundle up the separate procedures and services together (e.g., secure manufacturing, ISMS, secure R&D or secure supply chain) and would offer probably much more ho-

[7] As of January 2021, it is yet to be published.

[8] We shall see how the implementation of the Framework processes and services schemes goes after all the Commission and ENISA are trying to do something that was never done on this scale before.

listic approach. Not to certify "the building blocks", nor the process of "building", but to certify the "builders" themselves. This idea is a music of a distant future and no silver bullet, nevertheless, could be the one outcome the certification Framework will ultimately produce.

It is not possible to evaluate people and entities in the same way as one can technologies as of yet. The whole system would have to evolve, the whole thinking would have to become much more flexible then now. But in my point of view, because of the problems with the upkeep of the standards systems, with the schemes, this might counter the problem and at the same time evaluate the cybersecurity in even more complex and holistic way. The certificate would essentially prove, that the entity itself is trustworthy, that they uphold some level of security in their activities, that they have implemented reasonable precautions, they have the necessary knowledge, codes of conduct, their products, services and processes in use are secure up to the level of certification.

4. The Confusion

There exist some certification services for people, e.g., the cybersecurity experts (K. M. Martin, 2015). The state of affairs brings to mind the situation of cybersecurity certification of products only a short while ago. Fragmented, numerous initiatives made by mostly a private sector with an unclear terminology, different requirements, different approaches and different goals (K. M. Martin, 2015). The methodologies of the certification systems similar to products, services and processes are almost non-existent (K. M. Martin, 2015). If there is to be a certification of entities one day, it should stem from the united terminology, united requirements, united methodology and all of that can start by clarification and unification of understanding who cybersecurity professionals are and what they do (Furnell, 2021). This is but a fragment of the market potentially interested by the certification of entities, but it may prove to be a good starting point because solving the confusion in the matter of cyber-qualifications could provide united foundations for the scheme-level requirements for these experts (Ryerse, 2020). Yes, it might not be always specific, always clear, but we could start there and move forward. Now? There is nothing. Even the term "cybersecurity" shifts its meaning according to who we are talking to – lawyer, programmer, cybersecurity manager, high-level business manager etc. (Ryerse, 2020).

If we want to make a certification scheme for any of the cybersecurity professionals, it is unacceptable to not know who the professional is, what he is supposed to do and what he is supposed to know. And there is no united framework for this in the whole Union. In Czechia, the obliged entities often have no idea who they are looking for (especially the state administration) and how to assess if the professional is worthy. They just want to be secure often oblivious to the meaning of the term itself.

The lack of the so-called qualification framework causes difficulties with education because the schools do not know how to produce said experts.[9] (Newhouse et al., 2017). How can one define a scheme when no one can say, what should be the abilities, knowledge, and skills of the ideal cybersecurity graduate (Rowe et al., 2011)? E.g., in Czechia, there is only a handful of higher education possibilities concerning the cybersecurity topic (*Cybersecurity Higher Education Database*, 2020). There is a severe communication failure of the market itself (Ryerse, 2020).

4.1. Qualification Frameworks

The situation is not so hopeless as it might seem. There are no universal qualification frameworks in Europe as of yet, but there are several national attempts for a framework (Czechia included) and of course SPARTA (González-Sancho, 2019; *SPARTA*, 2019). The qualification frameworks are applicable throughout the sys-

[9] The qualification frameworks are described as a "*taxonomy and a common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed*" (Newhouse et al., 2017) for a reason.

tem (both public and private sphere, CERT teams of nuclear plants as well as the private contractors), for they simply state which work role should have what abilities, knowledge and skills (Newhouse et al., 2017). This makes it a lot easier for the demand-side of the market (e.g. the governments) to formulate their requirements and evaluate the candidates through the references to the specific roles of cybersecurity qualifications and to formulate it realistically on top of that. That, in turn, allows the education institutions to react, to create the educational plans, study programs and academic qualifications and training courses that correspond with the needs of the market and are attractive for the potential students in turn (De Paoli et al., 2014; Joint Task Force on Cybersecurity Education, 2018; K. M. Martin, 2015; Rowe et al., 2011). It adds a certain degree of clarity to the mix and might cause the influx of students into the cybersecurity, if only because of the great demand and rather good financial state of affairs. All of that should lead to strengthening the overall state of cybersecurity in the Union (Muncaster, 2019).

As I mentioned above, there are several promising projects (e.g., SPARTA – González-Sancho, 2019; *SPARTA*, 2019) striving to create a functioning framework. Even Czechia is working on its national cybersecurity qualifications framework, which would essentially be the implementation of the ENISA‘s SPARTA-activities. This framework is based on the NIST‘s NICE (National Initiative for Cybersecurity Education) framework (Newhouse et al., 2017), which defines individual skills, abilities, knowledge, and tasks (e.g., the knowledge of cryptography) and connects them into the “Competencies” group. These “competencies” are then used to describe the relevant work roles, which are also hierarchically organized into categories and speciality areas (Newhouse et al., 2017). The level of detail and robustness makes the NICE framework almost an ideal source of inspiration for the European frameworks and also, for the idea of the certification of entities. The ENISA qualification activities as well as e.g., the Czech national qualification framework could in the future easily serve as the basis of relevant certification schemes, as the sets of security requirements.

5. Conclusion

The cybersecurity certification is a fascinating way of evaluating compliance and strengthening the overall cybersecurity level of the Union. But there are inevitable and serious problems with the standards and schemes creation and upkeep, which may seriously affect the obliged entities all over the Union and the certification framework as a whole. The resulting shift from the products-based certification to services and processes might eventually progress even further – to the certification of entities. That might create an even more complex and more holistic approach to the cybersecurity certification and minimize the related burdens of the obliged entities.

The cyber-qualifications might prove to be an ideal starting point for creating the methodology and united terminology for this system, but first, it is needed to unite/create the cyber-qualification frameworks themselves and to clarify the confusion.

Acknowledgements

This article was created on the basis of the project support of the Ministry of the Interior, Czech Republic within the project “*Národní kvalifikační rámec v kyberbezpečnosti*” [National Qualifications Framework in Cybersecurity] with the identification code VI20192022161.

6. References

Annual Report for Business Year 2019. (2020). Nemocnice Rudolfa a Stefanie Benešov, a.s. https://www.hospital-bn.cz/wp-content/uploads/2020/05/V%c3%bdro%c4%8dn%c3%ad-zpr%c3%a1va-rok-2019.pdf

Boratynski, J. (2020, December 16). *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient*. Shaping Europe's Digital Future - European Commission. https://ec.europa.eu/digital-single-market/en/news/new-eu-cybersecurity-strategy-and-new-rules-make-physical-and-digital-critical-entities-more

Cerulus, L. (2020, June 22). *Von der Leyen calls out China for hitting hospitals with cyberattacks*. Politico. https://www.politico.eu/article/eu-calls-out-china-for-hitting-hospitals-with-cyberattacks/

Cybersecurity Higher Education Database. (2020). ENISA. https://www.enisa.europa.eu/topics/cybersecurity-education/education-map

De Paoli, S., Berendt, B., Laing, C., Tirtea, R., Catalui, D., Fischer-Hübner, S., & ENISA. (2014). *Roadmap for NIS education programmes in Europe: Education.* European Network and Information Security Agency. https://data.europa.eu/doi/10.2824/32639

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security*, *100*, 1–7. https://doi.org/10/ghgqjc

González-Sancho, M. (2019, February 26). *Four EU pilot projects launched to prepare the European Cybersecurity Competence Network*. Shaping Europe's Digital Future - European Commission. https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network

Haid, C., & Schneider, F. (2020, December 28). *European Union: Cybersecurity On The Rise: The NIS Directive 2.0*. Mondaq. https://www.mondaq.com/austria/security/1020144/cybersecurity-on-the-rise-the-nis-directive-20

Joint Task Force on Cybersecurity Education. (2018). *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. Association for Computing Machinery. https://doi.org/10.1145/3422808

Malatji, M., Marnewick, A., & von Solms, S. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. *Computers & Security*, *95*. https://doi.org/10/ghqzm3

Martin, K. M. (2015). Cyber Security Education, Qualifications and Training. *Engineering & Technology Reference*, 8–19. https://doi.org/10.1049/etr.2014.0029

Muncaster, P. (2019, November 7). *Cybersecurity Skills Shortage Tops Four Million*. Infosecurity Magazine. https://www.infosecurity-magazine.com:443/news/cybersecurity-skills-shortage-tops/

National Cyber and Information Security Agency. (2020). *Annual Report about the state of Cybersecurity in Czech republic for the year 2019 (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019)*. NCISA. https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

National Cyber and Information Security Agency. (2020, April 7). *Cyber attack warning against attacks at hospitals and other significant targets in the Czech Republic (Varování před hrozbou kybernetických útoků na nemocnice a jiné významné cíle ČR)*. NCISA. https://www.nukib.cz/cs/infoservis/hrozby/1428-upozorneni-na-hrozbu-ransomware-utoku/

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (NIST SP 800-181). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181

Preneel, B. (2014). Strengths and Weaknesses of Cybersecurity Standards. *Trust in The Digital World*, *3*, 18. https://trustindigitallife.eu/wp-content/uploads/2016/06/presentation-bart-preneel-2014.pdf

Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011). The Role of Cyber-security in Information Technology Education. *Proceedings of the 2011 Conference on Information Technology Education - SIGITE '11*, 113–121. https://doi.org/10/cmwfqm

Ryerse, J. (2020, October 5). *The Importance of a Cybersecurity Framework*. Security Magazine. https://www.securitymagazine.com/articles/93509-the-importance-of-a-cybersecurity-framework?v=preview

Sivasankaran, G. (2017, February 20). *In Technology We Trust? Three Reasons Why That's Not Enough*. Secureworks. https://www.secureworks.com/blog/in-technology-we-trust-three-reasons-why-thats-not-enough

Strategic Programs for Advanced Research and Technology in Europe—SPARTA. (2019). European Union and L3CE. https://cordis.europa.eu/project/id/830892

Understanding Security of the Cloud: From Adoption Benefits to Threats and Concerns. (2019, May 7). Kaspersky Daily. https://www.kaspersky.com/blog/understanding-security-of-the-cloud/