Scientific and Practical Cyber Security Journal (SPCSJ) 3(2): 36- 39 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

Cyber security European standards in business

Maksim Iavich[1], Sergiy Gnatyuk[2], Giorgi Iashvili[1] Andriy Fesenko[3]

1.Caucasus University 2. National Aviation University 3. Taras Shevchenko Kyiv National University

ABSTRACT. In the paper we consider the attacks on large and small businesses. We analyze the European standards and legislation. In the paper we also describe the European trainings materials. Using these materials is made the experiment where we have collected the group of 10 people and assessed them using cyber security exercises created using the attacks on Georgia and Ukraine. Afterwards we trained these students for 20 hours using ENISA materials and made them to answer the similar questions once more.We have got rather good results. Based on our research we offer corresponding recommendations for the representatives of small and big businesses.

KEYWORDS: cyber security, European standards, security in business

Nowadays, entrepreneurs clearly know that a cyber attack carries not only potential financial and information losses, but also damages the company's reputation, which threatens to drain customers and reduce investment attractiveness.

The Internet is becoming more and more dangerous every year and continues to be commercialized. This contributes to the fact that the motives of bad hackers, or the so-called "black hats" are becoming more greedy, so businesses should prepare for such possible hacker attacks in a timely manner. Organizations must improve IT security system so that sensitive data does not leak. The must care about security of the company in advance, involving employees and educating them.

Here are three main aspects of information security:

Confidentiality – people out of the organization and employers that are not intended to see sensitive data must not have access to it;

Integrity – existing data in the system must not be changed;

Availability - employees and authorized clients can access the necessary information at any time;

Small businesses are also victims of hacker attacks. If earlier cybercrime was chosen mainly by large companies, now no small firms or even individual entrepreneurs are insured against its “networks”. A loud confirmation of this was the breaking of the OneLogin cloud authorization service, which occurred in June 2017. As a result, attackers gained access to authentication data of more than 2000 companies from almost fifty countries of the world.

According to the opinion cyber security experts, small business is very interesting for modern hackers. Such enterprises have large stocks of finance and other resources than ordinary users. At the same time, the level of their protection is noticeably lower in comparison with large firms and corporations. This combination makes small businesses vulnerable and, at the same time, attractive to cybercriminals of all levels. Hackers are aimed at small companies and individual entrepreneurs due to the fact that the latter do not pay enough

attention to their cyber security. They are confident that the attackers will not waste time on hacking their Internet resources, and therefore underestimate the potential level of risk.

European companies have a very big practice in cyber security. In 2015, almost every 5th European company faced the risk of data loss or theft due to cyber attacks.

The European Network and Information Security Agency (ENISA, European Union Agency for Network and Information Security) has signed a memorandum with the largest companies in the semiconductor industry on the joint development of cybersecurity on the European continent.

The memorandum “General positions on cyber security issues” was signed by Infineon, NXP, STMicroelectronics and ENISA.

Actually, the development of recommendations for priority actions to strengthen cybersecurity, a kind of "road map", is the subject of the memorandum. There is a huge need for a clear identification of the main threats, standardization, the introduction of basic levels of cybersecurity, the development of procedures and measures for the development and implementation of cybersecurity technologies at the software, network and hardware level. The document is rather interesting both for specialists and for ordinary citizens, the safety and well-being of which increasingly depends on the strength of the barrier against invisible threats on the Web.

From the memorandum we can see, that it is very important in cyber security to use the proven solutions and the generally accepted level of security and confidentiality of data attached to the Network and“ smart ”devices - both of these solutions are necessary, and we recommend their implementation, so that Europe takes full advantage of the Internet of Things. As such, standardization and certification are identified as priority areas to accelerate the implementation of a cybersecurity level system that allows citizens, organizations, and institutions to gain trust in the network environment.

As part of the EU Cybersecurity strategy the European Commission proposed the EU Network and Information Security directive. The NIS Directive is the first piece of EU-wide cybersecurity legislation.

NIS Directive has three basic parts:

- National capabilities: EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g. they must have a national CSIRT, perform cyber exercises, etc.
- Cross-border collaboration: Cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc.
- National supervision of critical sectors: EU Member states have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, and finance sector), ex-post supervision for critical digital service providers (internet exchange points, domain name systems, etc).

The most week layer in cyber security in the person. According our research the training of employees greatly decrease the number of successful cyber-attacks on the organization[2].

“ENISA” - The European Union Agency for Cybersecurity is working on making Europe cyber secure since 2004. It cooperates with members states and the private sector to improve the capabilities of defenses against cyber attacks. It also supports the development of a cooperative response to large-scale cross-border cybersecurity incidents or crises. Sinc 2019 the agency works on creating cybersecurity certification schemes[1].

ENISA CSIRT training material was introduced in 2008. In 2012, 2013 and 2014 it was complemented with new exercise scenarios containing essential material for success in the CSIRT community and in the field of information security. In these pages you will find the ENISA CSIRT training material, containing Handbooks for teachers, Toolsets for students and Virtual Images to support hands on training sessions. In order to deliver trainings more efficiently with better and longer lasting results, the following resources can be used.

ENISA introduced cyber security training materials in 2008, and has grown continuously ever since. The ENISA training material are focused on: technical, operational, setting up a CSIRT and legal and cooperation.

We have collected the group of 10 people and assessed them using cyber security exercises created using the attacks on Georgia and Ukraine. Each students had to answer 10 questions. We got the following results:

Student ID	Score
1	4/10
2	2/10
3	4/10
4	5/10
5	6/10
6	2/10
7	3/10
8	4/10
9	5/10
10	2/10

As we can see the average number of correct questions is 3.7.

We trained these students for 20 hours using ENISA materials and made them to answer the similar questions once more. We've got the following results:

Student ID	Score
1	8/10
2	6/10
3	7/10
4	710
5	6/10
6	8/10
7	5/10
8	7/10
9	6/10
10	6/10

As we can see the average number of correct questions is 6.6.

This experiment shows us the European training program give rather good results.

Based on our research we offer global and small business owners to use only proven solutions, to work according EU-wide cybersecurity legislation and to spend recourses on the awareness raising in cyber security fields using European training materials.

REFERENCES:

1. https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2019-2021
2. Kim, BH., Kim, KC., Hong, SE. et al. Multimed Tools Appl (2017) 76: 6051. https://doi.org/10.1007/s11042-016-3495-y