Добран Божич
Махфий маълумотларни ҳимоя қилиш бўйича ҳукумат Офиси маслаҳатчиси.

КИБЕРХАВФСИЗЛИК: ОЛИНГАН САБОҚЛАР

Добран Божич
Советник Офиса правительства по защите конфиденциальных данных

КИБЕРБЕЗОПАСНОСТЬ: ИЗВЛЕЧЕННЫЕ УРОКИ

Dobran Božič
Advisor at the Government Office for the Protection of Classified Information

CYBER SECURITY: LESSONS LEARNED

In 2015-16 we started a cybersecurity strategy in Slovenia. We gathered IT experts from public administration to prepare a Strategy on Cyber Security. It is a readable document that is a compromise of everything: what we want to achieve, how much resources we need and what will be our path. The strategy changes every 2-3 years and now we are going to update it again. The EU has requested us to implement the Directive on network and informational security (NIST) in Slovenian legislation in 2019. Slovenia also was obliged to use the GDPR rules (protection of personal data) and started to work on Law was a compromise between the privacy and security.

In 2018 together with Marko Grobelnik and Mitja Jermol we wrote what cybersecurity includes (informational security and cyber defense). Every country must define cybersecurity for itself and wat will be protected: cyberspace or social networks. In Slovenia, nobody can guarantee that all servers are protected and clean from malware, APT or other bad influential tools.

Areas to address at the very beggining are social part in the area of disinformation – “hacked society” principle. In Serbia they surveyed people on foreign investments. The EU gives 1.8 billion Euros to Serbia, Germany gives 189 million Euros, US 161 million Euros, China promised to invest 56 million Euros and Russia didn’t invest. 40% of Serbs believe China invests the most, others invested 28%, EU invested 17,6% and Russia invested 14,6%.

In a way, information spreads the same way as a virus. If you want to avoid misinformation you must stop it in a proper way. In cybersecurity we treat information as a virus. We can see that AI can help us see how misinformation can influences people and a country. You should react with proper information.

Is cybersecurity a national matter or is it just connected to the IT sphere? We took the IT sphere to cover cybersecurity in Slovenia. We had a big discussion on privacy in security matters. We readily give our information to Signal,

Telegram, WhatsApp, Facebook, but we demand full privacy from the government. To understand these issues you must assemble the whole society (government, state institutions, academia, civil society, media, businesses) and discuss the level of privacy in data security matters.

What areas should be included in the Act on Information Security? We have cybersecurity departments in different ministries and public administration is running an IT system for the whole government, military has their own department as well as the intelligence community has their Intel Security Operational Center. We identified critical areas that require special protection: energy, digital infrastructure, water supply and water distribution, health, transportation, banking, infrastructure of financial markets, food supply, environment.

30 years ago we developed one of the oldest computer security incident response teams (CSIRT) in the world that is monitoring the issues cybersecurity in different areas of the country. As part of the cybersecurity structure, Slovenia has a special inspectorate on security issues that has the power to shut down the nuclear power in case of a danger.

Do we have enough cyber security experts? We educated a lot of experts in cybersecurity. We proposed to them an ecosystem connected to the police, military and businesses. We established a partnership with EU, NATO, Israel and USA.

What areas should be considered in the scope of work of the Cyber Security Entity? Do we need a Cyber Offense Capabilities? Can we prevent an Attack?

We have developed a special EU certified communications security for mobile services. Other EU countries and institutions use this software as a platform. It is self-sustained, and nobody can access it from outside. We also partnered with other organizations and developed points of contact with big technological companies (Facebook–Meta, Twitter, etc.) in order to contact them if we discover fake information or fake pages of politicians or other influential people.

The ecosystem of cybersecurity can’t exist without the government, academia, businesses, NGOs and media. Building cybersecurity is not as expensive as a military, but it lends enormous protection of a country and the people form outside dangers. Comparing the costs of establishing an effective cybersecurity in your country, you will find it is much cheaper than any other national security pillar.