Cybersecurity: A Holistic Approach

by  **Pavol Jurčo**, Head of Infrastructure Department, Data System Soft, spol. s r.o.

DataSystemSoft spol. s r.o.

Cybersecurity has lately been much debated in Slovakia as cyber attacks on organizations operating critical infrastructure could have fatal consequences for the whole of society. The number of cyberattacks has been growing every year, due to the increased professionalism of attackers.

Cyberspace

"Cyberspace" means all the information contained in electronic networks, i.e. the internet or an internal organizational network. The results of cyberattacks can be theft of know-how or sensitive information, long-term outage of product or service supplies, reputation damage, supplier fines or even forced closure of the business. In addition, the increasing expansion of IoT technologies has caused an unprecedented interconnection of the physical and digital worlds which in addition to the undeniable benefits may also expose critical physical state assets to vulnerabilities.

Therefore, the aim of cybersecurity measures should be to protect the interests of the asset owners by securing the ICT ecosystem. From states or state blocs, this means the creation of effective legislative policies, which in turn creates a burden on individual organizations.

Legislation

To improve cybersecurity in the EU, "The Directive on Security of Network and Information Systems" was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. Member States have 21 months to transpose the Directive into their national laws and an additional six months to identify operators of essential services.

In Slovakia, "The Concept of Cybersecurity of the Slovak Republic for 2015-2020" proposed the National Security Authority as the responsible institution for cybersecurity matters. Currently, the National Security Agency is preparing a Law on Cybersecurity that will govern cyber and information security comprehensively and will introduce basic security requirements and measures for the coordinated protection of information and communication in cyberspace. Non-compliance with these regulatory frameworks will result in significant fines for organizations.

Coping with cybersecurity

At most organizations, current cybersecurity practices are focused on technical aspects and meeting the minimum legislative requirements, which are "static", i.e. they do not reflect the latest developments in cyberattacks. The implementation of security measures are primarily in the hands of IT departments, without the active participation and involvement of managers from other departments. In addition, existing inflexible security policies may be a hindrance to the realization of innovative ideas within organizations. Since attackers are aware of known vulnerabilities, it is worth implementing relatively simple technical measures in an organization's existing infrastructure to protect from the most common types of cyberattacks. These measures include:

- Application whitelisting: as many attacks attempt to run a malicious third-party script or program, creating a list of legitimate applications permitted to run on certain servers or user machines can be an effective method of protection.
- Up-to-date security updates: as attackers routinely monitor published patches (i.e. vulnerabilities), it is imperative that you run only vendor-supported software versions and apply the latest patches regularly.
- Attachments and hyperlinks in e-mails: attacks can be prevented by using a correct setup on the e-mail server that allows automatically filtering of suspicious e-mails.
- User accounts with limited rights: user accounts with administrators rights can facilitate easy and complete control of devices, but also misuse by attackers.
- Passwords and password hashes in memory: implementation of special tools can restrict storage of sensitive information in the memory of user devices and limit their misuse by unauthorized applications.

Having antivirus as the only cyber protection method is not a good idea and dealing with cybersecurity requires more than the implementation of a few technical features by the IT department. Instead, a holistic approach should be taken leading to a correct balance of human, organizational, legislative, technical and other factors leading to an organization's ability to deal with cyber threats as a single flexible and effective organism.

Having said that, the goal of cybersecurity is not the complete avoidance of attacks (which is not possible due to the complexity and size of the protected space), but rather to adopt principles of cyber-resilience so an organization can effectively foresee, prevent and mitigate changing types of attacks and eliminate financial, physical and reputation damage. This can be done via the improvement of employee and team ability to recognize and counter cyberattack techniques and strategies.

The goal of these efforts should be the following abilities:

- Identification and understanding of an organization's weak points
- Ability to keep up with current legislative requirements
- Integration of "cyber-resilience philosophy" into everyday activities
- Deep integration of security principles into technological infrastructure, so they are not a hindrance to innovation and further development
- Implementation of active defense policies allowing for proactive attack detection
- Continuous testing to update and improve reactions to security incidents
- Key employees understand the information value of assets

Conclusion

Cybersecurity is not an isolated problem for IT departments; it requires complex cooperation within individual organizations and between commercial and state subjects. The key factor in these efforts is effective communication across the whole organization and the human factor to allow the identification and management of ever-changing security threats.

As it is unlikely that all the required skills will be available within one subject, the affected bodies must coordinate their efforts with subject-matter experts to create a cost-effective and efficient cybersecurity strategy allowing organizations to operate seamlessly in cyberspace.