CYBER SECURITY

PRIVACY? SECURITY?

Today's society is literally dependent on information and communication technologies. Imagine the collapse of these technologies and services out of nowhere. For a large part of the population it would have catastrophic consequences. About vulnerability and addiction of modern world on information technology, we are convinced every time a cyber attack occurs. So the question aries.. Are we really modern society? Maybe a better definition would last today - an online company. We are constantly connected, whether we like it or not, in front of a mobile phone, computer, internet etc. You don't hide, we are just used to it. Technologies are constantly being modified, improved, researched from one and the other side.. But let's face it, in a lot cases, we find out that we don't even need to yet.

Information and data represent considerable potential, and in a way can decide whether or not a company exists. Is there any privacy at all? We need to realize that the more we eagerly devour every IT news, the more data these technologies will collect and share about us. Perhaps a bold statement, but privacy is a thing of the past, we have ubiquitous freedom, but we pay for it with our data and become more vulnerable. It's definitely not an instruction to disconnect from all the "Internet", nor do you have to succumb to digital hysteria, but you need to think about it at least a little. You don't let thieves into your house either, but do you let your computer do it?

Cyberspace has no end or beginning, but it depends on the real world. Cybersecurity is an area that is crucial for many organizations, and therefore this area must be approached responsibly and, above all, systematically with a long-term plan. The general definition of cybersecurity says that it is the protection of computer systems and networks against theft or damage to their HW, SW or electronic data. It must be added that there is no absolute security, there will always be a risk or threat of attack. The primary goal of cybersecurity is to minimize potential risks or threats. There are three elements that are able to establish cybersecurity, their mutual integrity can do it. People - Technology - Processes. People are an essential element in cybersecurity because we can fit ourselves into the role of the creator of this security, the recipient (security rules), the entity that needs to be protected or we can even pose that risk or threat in the creation of cybersecurity. Technology alone cannot solve all our problems, but we are able to spend considerable funds for them. To ensure cybersecurity, it is essential to update technologies to be able to respond to changes associated with IT developments. We may think that technology

plays a vital role in cybersecurity, but appearances are deceptive. Much more important is the area of well-set processes and users who can apply processes or adapt to the situation and, most importantly (and this is very important) follow the pre-set rules. Setting up such processes and their subsequent maintenance is the most challenging part of building cybersecurity. It is entirely appropriate to simulate cyber-attacks, precisely because of the possible impacts. Penetration testing makes possible to find errors in the set processes (eg detection of infrastructure weaknesses) and thus prevent these undesirable impacts. The undeniable benefits of penetration tests include the protection of customers, business partners and third parties, protection of the company's reputation, asset mapping and, of course, compliance with various standards (OWASP, NIST, FIPS). There are different types and strategies of penetration tests, such as the "Black Box" Test, a test where the attacker has no information about the system, and this test is best able to simulate a real attack. "Gray Box" Test, the attacker has partial rights and system information or "White" Box "Test, where the attacker has all complete rights (admin rights).

We have a lot of experience in the field of cybersecurity, so we keep up with the times in this direction and follow the latest trends. We help large and small companies, including prestigious banks, increase their security. We are always ready to cooperate, evaluate potential risks and propose adequate solutions.

Building and maintaining cybersecurity could be compared to a never-ending cycle of risks or threats that need to be extended to support processes, such as educating people in this area. People should understand at least the basic rules and principles that apply to this topic, they should understand the basic functions of the computer systems they use on a daily basis, and they should also understand the applications they use.