WRITTEN BY

BIBIÁNA ŽIGOVÁ
Senior Manager for Information Security
TPA SLOVAKIA

LEARNING FROM CYBER-ATTACKS

Cyber threats are any potential dangers in the digital space that threaten information systems, data or infrastructure. These threats can range from individual hackers, organized groups, to state-sponsored cyberattacks. With digitalization, the need to secure IT infrastructure is growing. Cyberattacks cause significant financial losses, disruption to organizations' operations, and compromised personal information.

THE MOST FAMOUS CYBERATTACKS

WannaCry - Computer ransomware targeting Microsoft Windows systems, which began on May 12, 2017, is regarded as one of the most destructive and aggressive attacks of its kind to date. After infecting the computer, it encrypts the data on the hard drive and asks for a payment of $300 (€270) in Bitcoin to unlock the files (after the deadline ends, the price increases up to $2000 / €1800). The virus has been spreading since Friday, May 12, 2017. So far, the virus has infected more than 250,000 computers in more than 150 countries around the world. It is most widespread in Russia, Ukraine, India and Taiwan.

SolarWinds - SolarWinds, a major supplier in the software sphere, suffered an attack that began in September 2019. As a result of this attack, more than 18,000 SolarWinds customers installed updates containing malicious code. Hackers used it to steal customer data and then spy on other organizations. The SolarWinds cyberattack was a typical example of an attack on the supply chain.

Colonial Pipeline - On May 7, 2021, the ransomware attack on Colonial Pipeline, a U.S. critical infrastructure company, captured media around the world with images of long lines of cars at gas stations on the East Coast. Americans occupied gas stations in panic and refueled for fear of not being able to get to work or drive their children to school. This was the moment when the vulnerability of critical infrastructure, as such, became a national reality and topic.

And we don't have to go far. The ransomware attack on the Slovak cadastre, more precisely the Bureau of Geodesy, Cartography and Cadastre, in January 2025 pointed to the unflattering state of cyber security of Slovak state institutions.

WHAT AWAITS US?

In the digital age, where technological advancements are advancing at an exponential pace, cyber threats are constantly evolving. Attackers are abusing modern technology, artificial intelligence, and automation to create more sophisticated and destructive cyberattacks. The future of cyber threats will bring several key trends and challenges that organizations and individuals must prepare for.

Artificial intelligence (AI) is a double-edged sword. On the one hand, it helps organizations detect and eliminate cyber threats more effectively, but on the other hand, it can also be abused by cybercriminals. AI can generate realistic deepfake videos, automate phishing attacks, and bypass security measures using machine learning.

Ransomware remains one of the biggest cyber threats, and it is expected to increase further in the future. The attackers use the so-called double extortion, where they not only encrypt the victim's data, but also threaten to publish it if the ransom is not paid. With increasing automation, ransomware attacks will become even more sophisticated and targeted.

> **In the digital age, where technological advancements are advancing at an exponential pace, cyber threats are constantly evolving.**

With the increasing number of devices connected to the Internet (IoT), the area of possible cyberattacks is also increasing. Many IoT devices do not contain sufficient security measures, allowing hackers to exploit their vulnerability to botnets, distributed denial-of-service (DDoS) attacks, or unauthorized access to private information.

With the development of quantum computers, new threats are also emerging. Current encryption algorithms may be breached in the future, putting sensitive data of governments, corporations, and individuals at risk. Organizations will need to prepare for the transition to so-called post-quantum cryptography to maintain the security of their information.

With the rise of the metaverse and virtual reality come new cyber risks. Digital identity fraud, theft of virtual assets, misuse of personal data and the spread of disinformation will be key challenges in this evolving environment.

In response to the growing number of cyber threats, both global and local regulatory measures will be strengthened. New regulations, such as NIS2 in the European Union, will require organizations to better secure their IT infrastructures, including regular audits and improved response strategies to cyber incidents.

WILL WE LEARN FROM THE ATTACKS?

Cyberattacks are already a common part of the digital world. Every year, we encounter new, more sophisticated threats that affect organizations, states, and individuals.

After every major cyber incident, we see a wave of responses – organizations strengthen their security measures, update systems, and invest in employee training. In many cases, stricter regulations and standards are implemented, such as GDPR or NIS2. But the effectiveness of these measures is often limited – not only because threats are constantly evolving, but also because of resistance to change and a lack of prevention.

The history of cyberattacks shows that many incidents are repeated for the same reasons – weak passwords, outdated systems, inadequate access control, or underestimation of social engineering. Although these errors are relatively easy to eliminate, organizations often respond only after an incident, instead of taking a proactive approach to security.

Learning from cyberattacks requires more than just responding to incidents. Organizations should regularly conduct risk analyses, test the resilience of their IT infrastructures, and implement zero-trust principles. Cooperation between state institutions, companies and academia on the exchange of information on threats and best practices is also important.

If we want to minimize the impact of cyberattacks, we need to change not only technology, but also thinking. Security is not a one-time project, but a continuous process that requires a strategic and long-term approach and finances. True learning begins with instilling responsibility at all levels of the organization.