REDUCING RISK

THE CZECH REPUBLIC RESPONDS TO GROWING THREATS

By Veronika Netolická and Martin Konečný

PHOTOS BY REUTERS

Damage to the Czech Republic's critical information infrastructure (CII) has the potential to impact national security by affecting basic living conditions, people's health or the state's economy. The country's National Cyber Security Strategy for 2015-2020, its Security Information Service's 2015 Annual Report, and the National Security Audit all identify fundamental threats in this area. As revealed in these documents, cyber espionage is a serious CII threat. However, it is not the only threat. Unverified and unsecured hardware and software supply chains, ransomware and cyber terrorism also pose significant dangers.

CYBER ESPIONAGE

Cyber espionage seeks to obtain strategically sensitive or important information from individuals or organizations by using or targeting a means of communication. Cyber spies can gain political, economic or military advantage, posing a considerable threat to national security.

According to the Czech Republic's Security Information Service's 2015 report, the country faced major cyber espionage threats from Russia and China. That year a Russian cyber espionage campaign targeted two Czech ministries. Those two countries are not new to cyber espionage and their campaigns also target CII. In this area, for example, advanced nanotechnology research in the Czech Republic — a field for which the country is recognized — could become a target. The allure of obtaining crucial information, whether technological or political, makes such research a valuable target.

What makes cyber espionage especially dangerous is the low detection risk. In many cases, ongoing campaigns are detected months or even years after being launched. States must actively defend themselves against such campaigns. Also, the data obtained may be used not only for espionage purposes, but sometimes for extortion or further dissemination. Cyber espionage can also function as the backbone of more sophisticated cyber attacks. Retrieval of classified information can be targeted via the login details and personal data of prominent people who can be exploited. As digitalization increases and the volume of CII entities grows, cyber espionage campaigns are becoming more common and intense.

SUPPLY CHAIN SECURITY

According to the Security Information Service's annual report from 2014, supply chain security breaches can be used to threaten national security. For example, by using vulnerable hardware devices, the computer systems in CII could be penetrated. In this case, security risks arise from states' heavy dependence on hardware and software purchased from external suppliers, which might in turn be a source of cyber espionage.

As a case example, in 2010 the U.S. Navy purchased thousands of microchips from China for use in everything from missiles to transponders to rocket launchers. These microchips, however, contained a "back door" that allowed for remote shutdown of systems using them. In 2013, the U.S. Congress officially identified China's activities as a cyber threat. The U.S. banned the purchase of government supplies from Chinese companies, and it was also recommended that American private companies limit purchases of Chinese software. Because microchips can be programmed to actively interfere with a system, it is important to verify the hardware and software being used. In the Czech Republic, as in many other countries, suspicions revolve around Chinese vendors such as Huawei or ZTE.

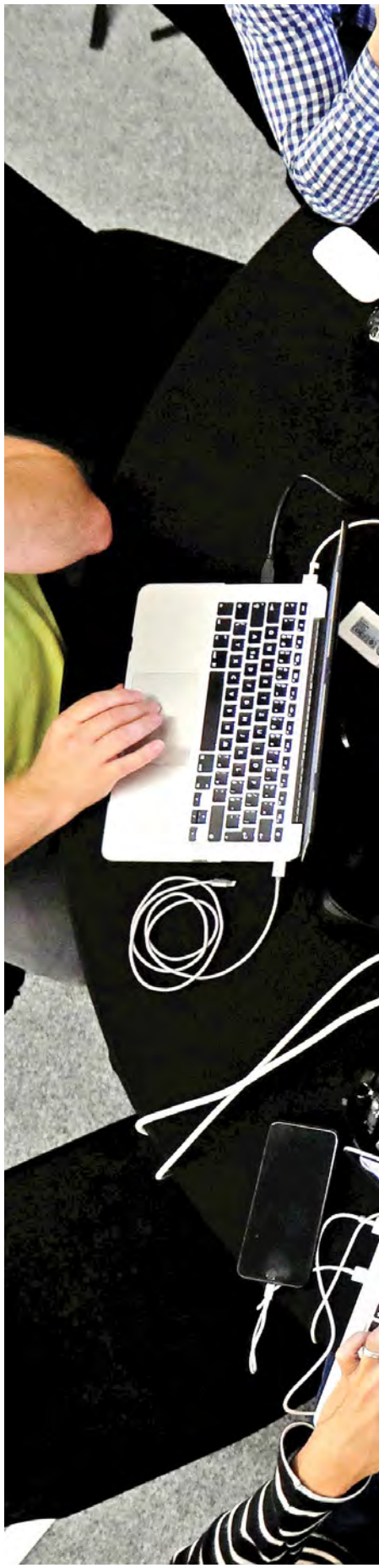
RANSOMWARE

But the damage may not be restricted to hardware. It may also involve the use of malicious programs such as ransomware, which blocks computer systems or encrypts recorded data and keeps it locked until a ransom is paid. Such attacks also pose a significant threat to CII.

The biggest ransomwares (WannaCry, Petya) targeting the infrastructure of states didn't directly affect the Czech Republic. But there is no guarantee that won't change because the criminal use of ransomware is so profitable. The best protection against ransomware is, at a minimum, regular backup of important documents to a device independent of the computer on which the data resides. After a ransomware attack, in most cases — even when the ransom is paid — the data is not returned. Even if it were, the confidentiality of the data is compromised.

CYBER TERRORISM

Cyber terrorism is a relatively recent phenomenon, and there is no consensus within the security community on defining the term. Recent attacks do not match the characteristics of conventional terrorism. According to the Czech National Security Audit from 2015, security is less threatened by a cyber terrorist attack than by a cyber espionage campaign. Though the Czech Republic might not currently be at a high risk for cyber terrorism, the risks can be expected to rise in the future. However, a discussion about this phenomenon should not be neglected now because the potential impact on CII could be catastrophic.



Photographers work on computers at an election headquarters in Prague, Czech Republic, in 2017. A solid legal foundation is key to cyber security.

LEGISLATION

A comprehensive legal framework provides a solid foundation for the protection of CII. The Act on Cyber Security, a cornerstone of Czech cyber legislation, became law on January 1, 2015, and was amended two years later.

The amended act regulates the following entities:

- Critical information infrastructure
- Operators of essential services (OES) (per the network and information security (NIS) directive)
- Important information systems (IIS) of public authorities
- Digital service providers (DSP) (per the NIS directive)
- Internet service providers (ISP)
- Significant network (or significant ISP) with secure network connection abroad or to CII

Implementing legal regulations related to the act cover:

- Cyber security requirements
- Determination criteria of OES
- Determination criteria of IIS
- Governmental cloud security (defining security requirements for public authorities)

The government institution responsible for cyber security is the National Cyber and Information Security

A man monitors a protest rally in front of Prague Castle in the Czech Republic in 2017. Attacks on critical information and communications systems threaten national security.

Agency, which operates the National Cyber Security Centre (NCSC). The NCSC has two integral parts — the government CERT (computer emergency readiness team) and Cyber Security Policies Department. According to the Act on Cyber Security, an additional CERT is responsible for cyber security for the rest of the country — the national CERT. The government CERT protects CII, OES and IIS and handles cyber security incidents; the remaining regulated entities (ISPs, significant networks and DSPs) fall under the national CERT.

Another legislative piece related to CII is the Crisis Act, which defines the determination process for CII elements. The Crisis Act is within the competency of the Ministry of Interior. The NCSC cooperates with the Ministry of Interior on determination of CIIs. Therefore, the role of the NCSC, alongside incident handling support, is to provide support with cyber security controls implementation, penetration testing, the conduct of cyber security exercises and support for cyber security education.

The NCSC is also responsible for performing inspections (cyber security audits) of all involved entities.

REDUCING RISKS

Considering the possible impact of cyber security incidents on national security, CII protection and OES efforts are top priorities for the Czech Republic. Accordingly, requirements on cyber security controls for these types of regulated entities are relevant to their importance.

The Czech approach to mitigating cyber risks is built upon a risk-based approach. In other words, it is based on the ability of companies/institutions to manage potential risks against their own systems. The aim is to decrease risks that could cause an unfavorable impact at the state level as well. The CII and OES must fulfill security requirements, defined by law, to mitigate risks. These are described in the Order on Cyber Security Requirements, which covers the following organizational and technical areas:

- Information security management systems
- Asset and risk management
- Organizational security
- Security policy and documentation
- Supply chain management
- Personal security
- Operation and communication management
- Change management
- Access management
- System acquisition, development and maintenance
- Cyber security event and incident management
- Continuity management
- Physical security
- Network security
- Identity management
- Malicious code protection
- Log management
- IDS/IPS
- Security information and event management
- Application security
- Cryptography
- Industrial cyber security and supervisory control and data acquisition
- Security
- Digital services security
- Audit

The current amended version of the Order on Cyber Security Requirements was drafted in cooperation with a team of cyber security experts from the private and public sectors. The team was composed of representatives of regulated entities and cyber security experts. Recommendations from the European Union and the European Union Agency for Network and Information Security were included.

As was already mentioned, the NCSC provides support for practical application of security requirements defined by this order. In 2017, the NCSC started a project of security audits for the most important government institutions. The aim is to recommend risk mitigation and to improve cyber security and cyber defense. This project is carried out annually.

LESSONS LEARNED

Although the legislative framework and safeguards of the Czech Republic have created a solid foundation for CII protection, cyber security cannot be maximized without a willingness on the part of CII entities to protect their own systems. Therefore, the Czech Republic aims to create an environment in which CII operators must implement basic safeguards to strengthen the security of their systems.

The state plays an important role here, acting more as a partner than a sanctioning authority. Building trust between CII operators and the state is the starting point. For example, consultations are now held between state experts and CII entities about upcoming laws. In 2017, a nontraditional stand was taken on the drafting of the Order on Cyber Security Requirements, and professionals from the public can provide content feedback and suggestions before the legislative process begins.

An approach based on trust opens up possibilities for sharing information. Effective information sharing will allow an understanding of incoming threats in greater detail and will contribute to introducing adequate measures, which, if implemented, can prevent future cyber incidents. Each state must realize that reducing risks in cyberspace is a never-ending, comprehensive process, and that the state should become involved and remain dynamic in cyber activities. □