Interview: Said Urban

Martin Haloda

Col. Mgr. Said Urban is the Chief Counsel of the Cyber Security Division of the Ministry of Interior and has more than 32 years of experience in criminalistics. He has worked at the National Narcotics Headquarters, where he led international counter-narcotics operations, and at the Organized Crime Detection Unit. He was also part of the creation of the Cyber Crime Investigation Division and served as Deputy Director of the National Counter Terrorism, Extremism and Cyber Crime Headquarters. In this interview, we ask him to what extent current established processes hinder the fight against cybercrime, how successful we are in this fight, and more.

Cybersecurity of 5G networks

Michal Poupa

The paper discusses the cybersecurity of 5G networks that use modern web technologies such as REST APIs and HTTPS protocols for signalling. It describes key security features such as the separation of user and control plane (CUPS) and the use of technologies such as TLS, OAuth2 and IPsec to protect communications. Emphasis is placed on protecting against zero-day attacks and ensuring API and application security. The paper also introduces modern tools such as the Web Application Firewall (WAF) and techniques to protect against DDoS and DNS attacks.

Interview: Massimo Panzeri

Martin Haloda

Massimo Panzeri is a Security Manager in the European Space Agency Security Office, where he works on space programme accreditation and cyber security engineering. He has more than 20 years of experience in the space sector and has been involved in major projects at national and European level, such as the projects for secure Italian telecommunication satellites (SICRAL), the constellation for Earth observation (COSMO) and the navigation system (Galileo and Galileo 2nd generation). In this interview, we ask how ESA is approaching the supply chain issue, what technological advances they are thinking about in cybersecurity and other.

Industrial cyber security according to NIS2 and the new Czech Cyber Security Act – Part II.

Ilja David

The second part of the article focuses on the importance of the cybersecurity of operational technologies (OT) in the context of the new Czech Cybersecurity Act (nZKB). The Act emphasizes the effective implementation of security measures to strengthen the resilience of industrial enterprises and critical infrastructure. The article presents strategic steps to ensure compliance with the nZKB, emphasising the importance of technical changes in systems and networks.

DORA: Key systems need a proactive approach!

Jan Pich

The Digital Operational Resilience Act (DORA), effective from November 25, 2022, aims to enhance the cybersecurity resilience of the European Union's financial sector. In today's digital world, where data and process protection are critical, financial institutions must strengthen their defenses against increasingly sophisticated cyber threats. DORA introduces a comprehensive framework for managing digital operational risks, with compliance required by January 17, 2025. While the regulation primarily addresses operational and infrastructure resilience, application security remains crucial to an organization's overall resilience. This article explores the link between DORA and secure software development, emphasizing the need to integrate both for lasting cybersecurity resilience.

Safeguarding Healthcare Solutions in the Cyber Era

Marlien Varnfield, Samuel Romanov

Cybersecurity in healthcare is essential to protect sensitive patient data and ensure the integrity of healthcare systems. As digital technologies become increasingly interconnected, the vulnerability of these systems to cyber threats is also increasing. AEHRC, with the assistance of the research capabilities of five different groups, is contributing to the digital transformation of healthcare in Australia. From remote monitoring of newborns to analysing medical images using artificial intelligence, AEHRC is innovating and improving health services. Yet it faces challenges associated with the vast amounts of data and complex regulatory requirements that place a premium on security across the healthcare ecosystem.

MANAGEMENT SUMMARY

Issues of financial support from public funds and inter-ministerial cooperation in research, development and innovation across new technologies – Part I.

Nikola Chvátalová, Adam Janovec

Research, development and innovation are key to the economic development and technological progress of the Czech Republic. However, state support in these areas is often insufficient and unsystematic, especially in the context of a rapidly changing geopolitical and national security situation. Cybersecurity is one of the key areas where it is important to develop and produce self-certified solutions. Without an improved mechanism for providing public funding in this area, the state's ability to respond to sophisticated threats risks being weakened. National Coordination Centres could provide inspiration for more effective support for scientific and innovative activities in cybersecurity.

The ZeroTrust security model is always tailored, with success in the attitude of the individual – Part I.

Tomáš Masný

The location of corporate assets, especially data, has changed significantly over the past decade. The mobility of users, employees and suppliers is no longer limited by geography when it comes to the IT and Telecoms sectors. The dynamics of the digital world in recent years have eroded the effectiveness of the classicalperimeter model, which is still prevalent in many organizations today. In response to this trend, there is a growing interest in the ZeroTrust model, which emphasizes identity and data protection and assumes perimeter penetration.

Generative artificial intelligence and cybersecurity

Jan Pilař

The article discusses the increasing impact of generative artificial intelligence (genAI) on cybersecurity. It highlights how tools like ChatGPT and Microsoft Copilot present both challenges and opportunities, particularly regarding data protection. The article emphasizes the need for effective security measures and explores how AI assistants can help experts boost efficiency and automate repetitive tasks.

PR – BlackBerry AtHoc: the ultimate solution for crisis communications

Philip Svoboda

BlackBerry AtHoc is a comprehensive crisis communications platform that enables the immediate dissemination of key information across the organisation. With a robust infrastructure and intuitive controls, it ensures that the right instructions get to the right people at the right time. Key benefits of BlackBerry AtHoc include multi-channel communications, crisis response automation, scalability, seamless integration into existing corporate infrastructure and industry-leading data protection. The distributor of BlackBerry AtHoc for the Czech Republic is TD SYNNEX.