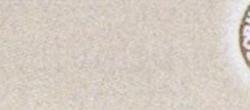## Interview: Adam Kučínský

Daniela Vacíková

He has been working in the field of cyber security since 2014, focusing on information security management, crisis management, protection of key information and communication systems of the state and related regulatory issues. While still under the National Security Office, he worked on the creation of the first law on cyber security and participated in the creation of the National Office for Cyber and Information Security. In this interview, we ask him about the current status of the upcoming law, the procedure for possible amendments, and more.

Concept of zones and conduits for securing operational technologies (OT) – Part II.

Ilja David, Roman Jašek

The article discusses the concept of security zones and conduits, which is the basis of the defense-in-depth of Operational Technologies (OT). This concept is important for the protection of critical infrastructure and industrial enterprises, as it allows to design a secure and effective segmentation of the organization's systems. When used in conjunction with the PERA model, it allows systems to be segmented based on both security and functional profiles simultaneously. This paper describes the concept of zones and conduits, the definition of zone and conduit, and discusses the relationship between the zone and conduit concept and the PERA model.

Zero trust and network security

Michal Čížek

This article presents an introduction to the topic of zero trust in the context of organizational security. In addition to the theoretical underpinnings of the concept, it also presents the technologies that are typically implemented to fulfill zero trust principles, the typical threats they protect against, and the advantages over the traditional concept of the cybersecurity perimeter.

Electronic Evidence in the context of International Law – Part II.

Veronika Hloušková

The article deals with the international legal regulation of electronic evidence. In the context of the unification and efficiency of the seizure and other handling of electronic evidence in criminal proceedings, legal instruments are being negotiated at the international level to assist in their cross-border obtaining. Attention is drawn to the much-discussed US CLOUD Act, whose executive international agreement is being negotiated by the United States and the European Union.

Ensuring digital resilience: a New Era of Standardisation and Certification in the EU
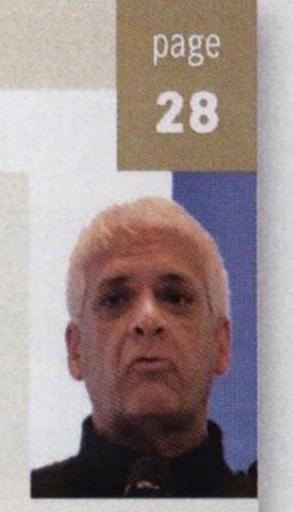
Václav Stupka, Jakub Vostoupal

The importance of cybersecurity standardization and certification of information and communication technologies is significantly strengthened with the reincarnation of the certification framework under the Cybersecurity Act and the upcoming Cyber Resilience Act, even in the context of the Czech cybersecurity environment. This trend is further confirmed by other regulatory developments, including the inclusion of certification mechanisms in the NIS2 Directive. The coming changes should therefore not be underestimated, which is why this article focuses on presenting relevant news from the world of EU cybersecurity certification and potentially problematic overlaps between the two Acts.

Interview: Ira Winkler

Martin Haloda

CISO of CYE Security and Director of the Security Engineering Consortium. He is the author of „You Can Stop Stupid" and „Security Awareness for Dummies" and is considered one of the world's most influential security experts. He has designed, implemented and supported security awareness programs in organizations in all industries around the world. In this interview, we ask him about what budget a company should have for cybersecurity, what are the top cybersecurity challenges, and more.

MANAGEMENT SUMMARY

Communication systems and their properties

Jan Dušátko

The Internet has become the nerve network of the global economy, banks, industrial companies depend on the services provided, politics, marketing, media, but also cyber-terrorism, cyber-crime, state and industrial espionage. The cables connecting the various cities across continents is easy to imagine. Their operation and interconnection is more or less similar to conventional telephone lines or power lines. But what about connecting the continents? At present, only two basic methods can be used – submarine cables and satellite links.

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

Ilja David

The first part of this article focuses on introducing what industrial cybersecurity is, what OT technologies are, what are the basic differences between IT and OT, what standards are used to address OT cybersecurity, the relationship between NIS2 and OT, and how OT systems are addressed in § 28 of the Decree on Security Measures of Regulated Service Providers in the Higher Obligations Regime, which is part of the draft of the new Czech Cybersecurity Act. All this is done in order to provide a suitable theoretical basis for the next part of the article, which will deal with the implementation steps of OT security in the enterprise.

Electronic Evidence in Criminal Proceedings – The legal tools used for obtaining them – Part II.

Veronika Hloušková

The article analyses the procedural tools which are entrusted to the law enforcement authorities on the basis of Act No. 141/1961 Coll., on Criminal Procedure (Criminal Procedure Code), and which are used in the current practice in relation to obtain electronic evidence. The main aim of the article is to evaluate whether the current legislation is sufficient to effectively secure electronic evidence and at the same time protects constitutionally guaranteed rights of persons without disproportionately interfering with these rights. The seizure of electronic evidence from cloud storage and mobile phones is discussed.

AI from the perspective of a medical device – Part II.

Antonín Hlavinka

The article explores the evolving role of Artificial Intelligence (AI) in healthcare. It discusses how AI transcends traditional medical boundaries, offering new diagnostic and treatment tools and significantly altering healthcare delivery. The article covers the latest research, the significant contributions of AI in diagnosis and treatment, and the ethical and legal challenges associated with its integration into healthcare. It also outlines the current applications of AI in medicine and future directions in this rapidly developing field.

SECTIONS

„It is no longer determined through impacts, but determined through size and the fact that the company or organization provides regulated service..."