NATIONAL UNIVERSITY OF PUBLIC SERVICE
Doctoral School of Military Engineering

Ferenc Koczka

Protection issues of higher education systems

Doctoral (PhD) thesis

Thesis Booklet

Supervisor:

Dr. Krasznay Csaba

BUDAPEST, 2023

Content

1. Summary

Hungarian higher education institutions present a rather heterogeneous picture of the field of IT security in that their operations are not uniform, their security systems are unique and different, and their policies treat system elements performing the same task differently. These are ultimately rooted in a enabling and permissive environment for the sector.

In addition to the fact that the Hungarian legislation does not directly provide for an IT security environment for higher education, the way in which universities operate and the attitudes of their staff differ from those of the business sector. The university environment is characterised by openness and freedom of teaching and research, which creates a situation of conflict between IT operations staff and teaching and research staff. Dadkah makes reference to this in the context of investigating cyber-attacks on researchers, but my personal experience is also consistent with this [1]. The FireEye white paper [2] highlights the restrictive effect of security tools that impede access to information. Academics and researchers are pressuring university management to relax security measures, and the aim of the administration is to implement and enforce the strictest possible security procedures, creating a difficult situation in higher education. This phenomenon is described by Adams as early as 2003 as a clash of cultures [1].

Academic institutions use a wide range of IT systems in their operations, whose primary functions are to support teaching and research activities, as well as economic, operational and administrative processes. Although in recent years the government has partially centralised the systems that support the economic operations of universities and has taken significant steps towards the unification of academic systems, the majority of the infrastructure that supports the operations of higher education institutions is still operated by the institutions themselves. In Hungary, universities and research groups have undergone significant organisational changes in recent years, and some research institutions continue to operate under changed conditions, which their IT systems must follow. My personal experience is that these changes, like the rapid changes forced by the Covid19 situation, have a general negative impact on overall IT security.

The primary objective of my research is to scientifically investigate the state of IT in higher education, to explore its data assets and to demonstrate that the security classification of their IT systems is performed in a heterogeneous way. Based on various databases, I have shown that they are not only victims of internal IT incidents but also targets of cyber-attackers, and I have analysed the motivations and methods of these attacks based on the available data. Using vulnerability analysis, I built a database on the vulnerabilities of the IT system of a Hungarian

university and analysed it to show some of its characteristics. Contingent on the measurement results, I developed a methodology based on the systems used and the data relationships between them, which can be used to strengthen the protection of higher education institutions and to provide an immediate response to environmental changes.

2. The Subject of the Research

Only general legislation applies to IT systems and data management processes in Hungarian higher education institutions. The operation of this sector is not governed by laws and regulations that set the framework for the operation of state bodies, nor are they subject to Act L of 2013 or BM Decree 41/2015. The design, architecture, development, operation and implementation of their IT systems are not subject to the obligations imposed by sector-specific legislation. As a consequence, in practice, the triple combination of existing preferences, expertise and financial background of the departments responsible for IT operations - in many cases taking into account standards and best practices - determines the strategy used in the design of systems and the decisions taken in their construction and operation.

In addition to the permissive nature of legal regulation, these institutions handle large volumes of sensitive data, the identification of the values stored in IT systems, which are stored and operated in different environments, some of which are the same software, is an essential prerequisite for the proportionate and cost-effective protection of this data. In Hungary, these are subject to an unknown number of attacks, and there are no measurements or research on trends in their changes.

The knowledge of the vulnerabilities of the systems is a crucial element of effective protection, but there is no data available describing the state of the educational institutions, which would allow to define and apply proportionate protection measures for the given systems, taking into account the already identified data assets. A vulnerability assessment on university IT systems adapted to their architecture could be used to verify the problem.

Considering the answers to the problems presented, the development of a methodology to improve the effectiveness of the protection of higher education institutions, taking into account the specificities of the sector, could be an ideal solution to define the transitive protection tasks of interconnected systems.

The topicality of the subject is due to the following factors:

- Expected changes in the legislative background. The European Union's NIS2 Recommendation proposes a number of new requirements to improve IT security, while tightening up existing requirements and significantly broadening the scope of institutions covered. As the previous recommendations targeted critical infrastructures and digital service providers, NIS2 covers a much broader scope, while remaining coherent with existing legislation in the sector. These changes are likely to bring significant changes at the legislative level for higher education institutions.
- Only partial knowledge of the higher education data estate. There is currently no academic research available to assess the data assets of the sector.
- IT security has been negatively affected in the recent past not only by Covid19 and restructuring, but also by the war situation and changing economic and labour market conditions.
- In the absence of adequate studies, there is a lack of data on the extent of vulnerabilities, exploitability and age of higher education systems.

Overall, the situation in higher education is unique in several aspects that have not been studied in the domestic context, and there is no significant amount of research or data on them internationally.

To achieve this aim, my thesis follows the following logic:

1. Topicality of the subject, choice of topic and context. In this chapter, I describe the legislative background and institutions related to IT systems in higher education institutions and identify the main areas of their data assets based on relevant literature. The chapter details the research questions, hypotheses and research methods.
2. Based on this, I will analyse their policies, identify the IT systems they use and provide evidence of differences in their security classifications. Through researching, organising and analysing multiple data sources, I will show the volume, nature, temporal variation and proportion of attacks and incidents on higher education systems compared to other sectors. Based on data collected through a public interest request, I provide evidence of the low reporting rate of IT incidents in Hungarian higher education institutions.

3. After exploring the human aspects that influence the protection of university IT systems, I present the known methods for measuring vulnerabilities, the databases and measurement tools that underpin their operation. Prior to a general multi-university vulnerability assessment, I will examine its legitimacy aspects and test the provability of my hypotheses on the basis of a case study that allows for the analysis of a university. If the case study is justifiable, I will use further measurements to prove their generality and thus prove my hypotheses.

4. The results of the tests justify the need for a recommendation applicable to the sector as a whole, the structure of which demonstrates that by extending the classification under the ibtv. it is possible to create a methodology that, in addition to the general classification rules, takes into account the specific institutional activities, the specificities of the software used, their data content and the processes of data exchange between them. The basic element of the methodology is a matrix describing the persistent or regular data relationships of each system, with changes reflected by vulnerabilities or configuration errors detected during a periodic vulnerability scan review. By applying the methodology, the defined security classifications become more accurate, and the definition of ideal protection procedures can be adapted at short notice based on changes in the modified confidentiality, integrity and availability classification of the system.

3. Research Questions and Methods

I conducted my research in the field of IT systems in Hungarian higher education institutions, and I defined my research questions and hypotheses in the following way:

Problem statement 1: the IT security policies of higher education institutions are not uniform and apply incorrect security classifications.

a. RQ1: what IT systems are in place in Hungarian higher education?

b. RQ2: what kind of data is stored in these systems?

c. RQ3: what security classification do institutions apply to each of their systems?

Hypothesis: the administrative arrangements of Hungarian higher education systems are heterogeneous in content and systems with the same functions are classified differently.

Problem statement 2: is there a higher level of vulnerability in Hungarian higher education institutions' peripheral sites than in their centre?

a. RQ1: what is the amount and type of vulnerabilities in IT devices at the peripheral sites?
b. RQ2: what is the variation in the number of vulnerabilities?

Hypothesis: in Hungarian higher education IT systems, the number of vulnerabilities is lower in centrally located IT systems than in peripheral ones.

Problem statement 3: are vulnerabilities in IT systems typically caused by the software that runs the IT tools, or by configuration errors caused by operations?

a. RQ1: what is the proportion of vulnerabilities in Hungarian higher education institutions according to the CVSS five-stage classification?
b. RQ2: is the number of vulnerabilities detected as a result of faulty configuration settings higher?

Hypothesis: there is a significant amount of technical information on vulnerabilities in Hungarian higher education information systems known for more than one year, which is predominantly the result of faulty configuration settings.

Problem statement 4: can the classification and protection of IT systems be improved by continuous vulnerability assessment analysis and extension to the systems concerned based on the interrelationships of each system?

a. RQ1: what is the appropriate security classification for each system according to the ibtv?
b. RQ2: what factors might influence the difference in classification for each system?
c. RQ3: what relationship matrix describes the possible data relationships between each system and what is their nature?

Hypothesis: a specialised risk-based classification methodology can be defined for IT systems in higher education in Hungary.

In my research I used primary and secondary research methods. In my literature search, I studied a wide range of legislation, standards, recommendations and good practices, comparing them with the higher education environment and my own experience as a manager, operator,

developer and teacher, in order to examine their validity in higher education systems and to identify their differences.

I have used document analysis of the IT security policies of each institution to take stock of their IT systems and compare their security ratings, and comparative critical analysis to identify discrepancies. For the sake of objectivity, I have sought, as far as possible, to collect quantitative data, which I have processed using statistical methods.

Using various measurement tools, I carried out measurements to detect vulnerability scans, security events and configuration errors, which were used to perform statistical calculations to establish correlations. The method used to measure information security was experimental rather than interviews in order to establish a realistic picture of the situation. The computer processing of my measurement results was carried out by converting spreadsheets, using SQL queries based on a database management system, creating my own databases, and using mostly my own programs. Some of the diagrams in this thesis were produced using in-house developed programs.

I have identified the measurements carried out in one institution as case studies [3, pp. 129-156], and their general validity has been verified by induction on a representative sample of IT systems from other universities under the same environmental conditions.

To collect research data, I used public data requests and a search of statistics available on the Internet. Using my existing development experience, I processed the Hackmageddon data files after converting them into a MySql database, and created Python programs and Unix shell scripts to evaluate the data.

Considering that my data and their relationships were unknown at the beginning of the research, I used grounded theory to collect and analyse them and to create a possible data relationship map of each IT system [3, pp. 83-128].

I have identified the measurements carried out in one institution as case studies [3, pp. 129-156], and their general validity has been verified by induction on a representative sample of IT systems from other universities under the same environmental conditions.

To collect research data, I used public data requests and a search of statistics available on the Internet. Using my existing development experience, I processed the Hackmageddon data files after converting them into a MySql database, and created Python programs and Unix shell scripts to evaluate the data.

Considering that my data and it's relationships were unknown at the beginning of the research, I used grounded theory to collect and analyse it and to create a possible data relationship map of each IT system [3, pp. 83-128].

To achieve these goals, I participated in academic and professional conferences, where I processed, analysed and evaluated the experience of other institutions' IT systems, environments and solutions. I gathered information from colleagues and professionals working in the same areas of higher education. In order to get a more accurate picture of incidents affecting IT systems in higher education, I have continuously collected updates on cyber-attacks on higher education IT systems, articles from journals, authoritative journals and academic publications, as well as peer-reviewed articles from open and closed Internet communities, mainly from secondary sources.

4. Summary of the Research

By analysing regulations, I have shown that Hungarian higher education institutions have a significant amount of data and have mapped the nature of the systems that manage them and the approximate amount of personal data they manage. By analysing mainly international data, I have shown that approximately 6-9% of incidents or attacks on IT systems are directed against educational institutions. I have also shown that, in the domestic context, there are no relevant databases or registers describing IT incidents affecting the sector and that the willingness of higher education institutions to report is low. By analysing the Hungarian legal environment, I have demonstrated that the education sector lacks specific regulation in contrast to other state-owned or maintained organisations, which handle significantly smaller amounts of sensitive data and have to comply with a strict legal framework in the design and operation of their IT systems. In order to classify the security of the universities' IT systems and to demonstrate the homogeneity of their policies, I analysed a representative sample of their policies through a document analysis survey and found that their level of protection against OSINT data collection is low, with significant variations, some of them outdated, and in the case of small universities, low and sometimes even non-existent levels of sophistication.

After proving that the university IT systems contain a large amount of sensitive data, and that the methods of protection are determined solely by the IT management of the institution, I examined the state of protection of these systems against internal and external attacks. As a result, I have demonstrated that the level of vulnerability of IT system components does not

differ between central and peripheral campuses, while they are affected by a number of vulnerabilities known for many years. I have also demonstrated that a significant proportion of the vulnerabilities identified are configuration errors that can be corrected by the operating staff over several years, and that can be eliminated by replacing outdated software and, in some cases, hardware, in addition to stricter control of system configurations.

Having shown that higher education IT systems contain data in approximately the same environment and of approximately the same nature, while their security classification, and thus presumably the procedures used to protect them, differ, and that their systems contain a large number of known vulnerabilities and are subject to IT incidents and cyber attacks, I have developed a recommendation for their uniform classification. I based this on Act L of 2013 and BM Decree 41/2015, but I also extended it to tracking the chain of impact based on a map of general and potential data links between systems. By analysing the results of continuous vulnerability assessment procedures, based on the mapped interconnections per system, the components that determine the security classification, and consequently the protection procedures applied, can be reviewed in rapid response to changes in the risks to each system. Based on the relationship matrix, the systems concerned can then be clearly identified and security measures can be extended to them.

5. New Scientific Results

In proving my hypotheses, I have achieved the following new scientific results:

R1. I have proven the inhomogeneity in the security classification of IT systems in Hungarian higher education, which I have supported by analysing data from international databases, and in connection with this I have listed the IT systems of higher education institutions, their partially obsolete state and the possibility of collecting OSINT information.

R2. I disproved that the peripheral IT systems of Hungarian HEIs contain a small number of vulnerabilities accessible from the Internet.

R3. Using a representative sample, I demonstrated the high number and age of existing vulnerabilities in Hungarian higher education information systems and showed that the vulnerabilities are predominantly the result of configuration errors.

R4. I developed a methodology based on data linkages between systems and continuous vulnerability analysis for the classification of Hungarian university IT systems using dynamic risk analysis.

6. Deriving Hypotheses

I organised my research along four hypotheses based on the following ideas: assessment of data assets - permissiveness of legal regulation - occurrence of IT incidents and attacks - vulnerabilities and misconfiguration in IT systems - development of a protection methodology.

H1. The administrative regulations of the Hungarian higher education systems are heterogeneous in content and treat systems with the same tasks differently.

Document analysis of IT policies is one of the possible methods to identify the data assets and IT systems of higher education institutions and to classify them according to the IT Act. After defining a representative sample of universities to be studied, I collected their policies and requested their availability for research purposes for those that were not public. I aligned the structural differences between the individual regulations with those in general use, harmonised the scales used by them and finally listed their systems and their classification.

Hypothesis H1 was confirmed: although there was a small variation in the key schemes, overall the classification of many schemes differed, with a difference of two points being observed.

H2. In Hungarian higher education IT systems, the number of vulnerabilities is lower in the centrally located components than in the peripheral ones.

To prove this hypothesis, I examined the prevalent methods of IT security analysis based on data collected through vulnerability testing. Following a case study of a vulnerability assessment at a Hungarian university, I explored further conclusions that could be drawn from its results. I presented two practical applications of vulnerability measurement and some types of software that perform it. To evaluate the results, I have partly built my own database, supplemented with data from other sources to extend the functionality of the software that performs the measurement. In the first phase of the measurement, I described some local outliers and negative examples and then analysed the measured data.

Hypothesis H2 cannot be confirmed. For the case study university, there was no significant difference in the proportion of vulnerabilities measured in the central infrastructure and peripheral areas.

H3. There is a significant amount of technical information on vulnerabilities in Hungarian higher education information systems known for more than a year, mostly the result of faulty configuration settings.

As an extension of the measurements, I have developed the technical requirements for the analysis of the internal system, I have developed a detailed analysis of the universities' subject areas in order to identify their differences and I have presented the background on which this can be transferred to a measurement software. I have analysed in detail the number and nature of vulnerabilities in each area, with findings for vulnerabilities that can be detected from the direction of the public internet and from the internal network, without the protection of border protection devices, separately. I have shown that the vulnerabilities detected are largely the result of configuration errors, and that a significant number of them were already known at least one year before the measurement. I have shown that some elements of the IT systems contain very old flaws that were known in 1999. Finally, I examined the outliers in the number of vulnerabilities by sector and analysed them by looking at specific vulnerabilities.

I confirmed hypothesis H3: the systems under investigation had a significant number of configuration faults and most of them were more than one year old.

H4. A specialised risk-based classification methodology can be provided for IT systems in higher education in Hungary.

The discrepancies in the IT regulations have shown that Hungarian universities apply the principles of the ibtv. only superficially in the security classification of their IT systems. As a consequence, systems with the same functions are classified at different levels and their security procedures are likely to differ. By applying the methodology developed to verify this hypothesis, the accuracy of the classification can be significantly improved, tailored to higher education systems and able to provide immediate responses to the secondary effects of vulnerabilities in individual systems. The first level of the methodology is to map the IT systems used in higher education, define their functions and approximate the data content they handle. Based on the specificities of higher education and the nature of the systems used, I tailored the classification criteria of the ibtv. and then using tht information, I defined the confidentiality, integrity and availability classifications or their intervals for each system. In developing the second level, I mapped the existing data relationships between the IT systems of a university and then generalised them to identify possible additional ones, which I captured in a relationship matrix. The validation of the matrix was carried out in several steps during the detailed description of each system. The third level is the detailed description of each system,

with a detailed exploration of the possible incoming and outgoing data connections, including the following differences in the variating ways each system operates. In developing this level, I have demonstrated that there are sometimes significant differences between the recommended classifications and the classifications considered in the analysis of the rules.

Hypothesis H4 was proven: a risk-based classification methodology applicable to higher education IT systems was defined.

7. Practical Use of the Research Results and Recommendations

The results of my PhD thesis are primarily of interest to educational and research institutions, especially to university IT managers and IT security staff. The results of the research carried out during the preparation of the thesis, the methodology of the measurements and the methods of processing the data collected may help to adapt and further develop the results in other institutions. I would also recommend the consideration of the application of the software and methodologies used in this thesis to all those professionals who would like to develop and maintain a protection system in other sectors based on the measurement of IT security and the continuous measurement of its vulnerability status. I also recommend its review to researchers who aim to carry out further scientific studies related to the topic and to exploit their results, especially in Hungarian higher education institutions. My results and findings may serve as a basis for forthcoming legislative amendments.

I recommend for further research the data on system vulnerabilities, from which I believe further findings of scientific value can be drawn using grounded theory.

In addition, my recommendation includes the establishment of a common forum of higher education managers and a 'hotline' between them to ensure that IT incidents affecting the sector can be dealt with swiftly. A number of recent incidents demonstrate that without this, higher education institutions are unable to take immediate protective measures in the event of a sector-wide attack. And I recommend that legislators tighten the regulation of the operation of IT systems in higher education and bring it under the scope of Act L of 2013.

Finally, I recommend the use of the classification system developed in my thesis in the advancement of regulations for higher education institutions and in the determination of security classifications for their systems.

8. Future Directions

During the preparation of my thesis, I collected a large amount of data. By analysing Hackmageddon's data on the education sector, it is possible to continuously track the amount

of cyber-attacks on the sector, its proportion in relation to other sectors and the direction of change. Analysis of additional databases can produce up-to-date information on non-attack IT incidents in educational institutions. Further analysis of the vulnerability assessment data may reveal new correlations, and analysis of additional institutions may confirm their generality.
The practical application of the protection methodology developed by proving H4 can improve its functionality and modify its possible flaws. By developing an appropriate software background, its application can be automated, and by conducting vulnerability assessments of universities themselves, a common higher education protection system can be developed, which can be used to extend the scope of the presented methodology to other universities.

9. Bibliography

[1] A. Adams, A. Blandford: Security and Online Learning: to Protect or Prohibit, in Usability Evaluation of Online Learning Programs, UK, Information Science Publishing, 2003, pp. 331-359.

[2] FireEye Inc.: Why Cyber Attackers Are Targeting Higher Education, and What Universities Can Do about It. White paper, Fireeye Inc., 2015.

[3] Horváth D., A. Mitev: Alternatív Kvalitatív Kutatási Kézikönyv, Budapest, Alinea Kiadó, 2015.

10. List of Publications

Journal articles

[M1] Koczka Ferenc, Négyesi Imre: Az információbiztonság fejlesztésének lehetőségei az akadémiai szférában. Hadtudományi Szemle, Ludovika Egyetemi Kiadó, Budapest, 13. évf. (2020) 1. sz. 113–130. oldal. DOI: 10.32563/hsz.2020.1.9

[M2] Koczka Ferenc: A felsőoktatási intézmények informatikai védelmének szektorspecifikus kérdései. Hadmérnök, Ludovika Egyetemi Kiadó, Budapest

[M3] Koczka Ferenc: Egy egyetemi informatikai rendszeren végzett sérülékenységvizsgálat módszere és néhány tapasztalata. KNBSZ. (During publication.)

[M4] Koczka Ferenc: Szemelvények egy felsőoktatási rendszer informatikai védelmének tapasztalataiból. Networkshop 2023 konferenciakötet. (During publication.)

Articles published in foreign language publications

[K1] Koczka, F. (2020) “Opportunities of Darknet Operations in Cyber Warfare: Examining its Functions and Presence in the University Environment”, AARMS –

Academic and Applied Research in Military and Public Management Science. Budapest, 19(1), pp. 65–81. doi: 10.32565/aarms.2020.1.6.

[K2] Koczka, F. (2021) “Security of Encryption Procedures and Practical Implications of Building a Quantum Computer”, AARMS – Academic and Applied Research in Military and Public Management Science. Budapest, 19(3), pp. 5–22. doi: 10.32565/aarms.2020.3.1.

Presentation in a conference publication

[O1] Koczka Ferenc: Információbiztonsági teszt az Eszterházy Károly Egyetemen. Networkshop 2018, Hungarnet, 2018.04.04-06. Doi: 10.31915/NWS.2018.1

[O2] Koczka Ferenc: Issues of Legal Regulation of Hungarian Higher Education IT Systems, Austrian Computer Society (OCG), Budapest, 2021.05.10-11. DOI: 10.24989/ocg.v341.22

[O3] Koczka Ferenc: OSINT technológiák és alkalmazási lehetőségeik a felsőoktatási rendszerek ellen, Online térben az online térért: Networkshop 30 országos online konferencia, 2021. április 6-9. Doi: 10.31915/NWS.2021.21

Book chapters

[F1] Krasznay Csaba, Koczka Ferenc: A távolléti oktatás jelentette kiberbiztonsági és adatvédelmi kihívások, Járvány sújtotta társadalom: A koronavírus a társadalomtudományok szemüvegén keresztül (tanulmánykötet), Budapest, 2021.

[F2] Koczka Ferenc: Az ellátási láncok támadása, azaz mi történik, ha már a nyomtatott áramkör sem megbízható? Taktikák és stratégiák a kiberhadviselésben, NKE, Budapest, 2021.

Conferences

[N1] Koczka Ferenc: Hiding illegal contents on the net: is it possible or even necessary? In Service of The Nation Conference, Budapest, 2019.11.22.

[N2] Koczka Ferenc: Felsőoktatási rendszerek védelmi problémái. XXIII. Tavaszi Szél Konferencia, Budapest, NKE, 2020.

[N3] Koczka Ferenc: Kinek a felelőssége? Networkshop 2020 online konferencia, 2020. 09.03.

[N4] Protection Issues in Higher Education Systems, CASPA Seminar and Workshop in Tallinn, 2021.10.04-08.

[N5] Egy új kockázat az informatikai védelemben: a kvantumszámítógép. Információvédelem menedzselése XCIX. Szakmai fórum, Budapest, 2022.01.19.

[N6] IDS bevezetésének tapasztalatai az Eszterházy Károly Egyetemen. Networkshop

2022 Konferencia, Debrecen, 2022.04.21.

[N8] IDS bevezetésének tapasztalatai az Eszterházy Károly Egyetemen. Networkshop 2022 Konferencia, Debrecen, 2022.04.21.

[N9] Koczka Ferenc – Prantner Csilla – Biró Csaba: A posztkvantum kriptográfia aktuális kérdései. Networkshop 2023 konferencia.

University textbook

[E1] Koczka Ferenc: A Unix operációs rendszer. https://www.koczka.com.

11. Curriculum Vitae

Ferenc Koczka is a graduate student of the Military Engineering Doctoral School of the National University of Public Service (NKE), graduated on 8 July 2022. He is currently an Assistant Professor in the Department of Computer Science at Eszterházy Károly Catholic University and in the Department of Cyber Security at the National University of Public Service.

After completing his studies in music at the Primary School No. 1 in Eger, he graduated from Gárdonyi Géza High School. He then spent a year of conscript service with the 1st Rifle Squadron in Baja, and obtained a degree in mathematics and physics from the Ho Chi Minh Teacher Training College in Eger. Already during his military service, his attention turned to computer science, which he focused on during his college studies. He medaled in several computer science competitions, and his thesis was a computer language teaching program, which medaled at the OTDK. He is a holder of the MTS Pro Scientiis gold medal.

After graduating from college in 1990, he was offered a teaching assistant position at the college, teaching general computer science. In the meantime, he completed a degree in computer science at Eötvös Loránd University and subsequently obtained a teaching diploma in pedagogy at the University of Debrecen. During his studies, he continuously improved his knowledge, and in 1994 he turned his attention to Unix systems, which has determined his professional career until the end. He has attended several courses on the operation of IT systems.

From 1999, he worked for 9 months as Deputy Head of the IT Department of the State Pension Fund Supervision, a position he held in an internet service provider and then a network development company. In 2004, he started developing his own business, focusing on the design and development of IT systems.

He has maintained a close relationship with higher education, teaching continuously at the University of Eger, his main subjects being computer networks and operating systems. In 2013 he was appointed head of the IT department of the university, a position he held until August 2022. During this time, he reorganised the IT department of the university, centralised IT and created a specialised group for server and network operations. During this period, he passed several RedHat exams and completed the NKE Information Security Manager qualification. He then decided to further his education in the field of information security and applied to the Military Technical Doctoral School. During this training he obtained his Advanced Certificate in English, which he uses as a lecturer at both universities, teaching 2-6 hours of English lessons per week. During his doctoral studies, he has published several publications, an electronic textbook, several book chapters, and has presented papers at conferences relevant to academic and higher education IT systems operators, mainly on higher education systems operation.