ISSN 2676-9042

Vol 3, No 3, 2021.

2021, III. évf. 3. szám

Safety and Security Sciences Review

international, peer-reviewed, professional and scientific journal of safety and security sciences

Biztonságtudományi Szemle

a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

https://biztonsagtudomanyi.szemle.uni-obuda.hu

On the cover can be seen | A borítón
ÉZSIÁS István
sculptor/szobrászművész
An American in Paris statue | **Egy amerikai Párizsban** című szobra látható

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

COLUMNS	ROVATOK
Material Safety	Anyagbiztonság
Philosophy and History of the Safety and Security	Biztonságfilozófia és -történet
Security Policy	Biztonságpolitika
Security Systems	Biztonságtechnika
Security Awareness	Biztonságtudatosság
Domotics	Domotika
Health Security	Egészségbiztonság
Food Safety	Élelmiszerbiztonság
Economic Security	Gazdasági biztonság
War Security and Law Enforcement	Hadbiztonság és rendvédelem
Information Security	Információbiztonság
Industrial and Operational Safety	Ipar- és üzembiztonság
Legal and Social Security	Jog- és társadalombiztonság
Book Review	Könyvismertetés
Security of Environment	Környezetbiztonság
Traffic Safety	Közlekedésbiztonság
Private Security	Magánbiztonság
Artificial Intelligence	Mesterséges intelligencia
Safety and Security in General	Munkabiztonság
Technical Security	Műszaki biztonság

The aim of the journal is to publish studies, research reports, articles, book reviews of the broad discipline of security science for professionals working in or related fields of security science, thereby developing security awareness and security culture.	A **folyóirat célja** a biztonságtudomány területén, vagy ahhoz kapcsolódó területeken dolgozó szakemberek és a téma iránt érdeklődők számára a biztonságtudomány tágan értelmezett diszciplináris keretébe tartozó tanulmányok, kutatási jelentések, beszámolók, könyvismertetők megjelentetése, s ennek révén a biztonságtudatosság és a biztonsági kultúra fejlesztése.
Published quarterly, typically in Hungarian, occasionally in a foreign language. Special and/or thematic issues related to conferences and topics are occasionally published in Hungarian or in foreign languages.	**Megjelenés** negyedévente, jellemzően magyar, eseti jelleggel idegen nyelven. Konferenciákhoz és témákhoz kapcsolódóan különszámok, tematikus számok alkalmi jelleggel magyar, vagy idegen nyelven jelennek meg.
Only those papers will be published which reviewed by two independent reviewers and recommended suitable for publication in the Safety and Security Sciences Review. The submitted manuscripts must meet the requirements both of the form and the content which can be found in the journal's website. Please note: we will not return unapproved manuscripts.	A Biztonságtudományi Szemle folyóiratban csak két független lektor által lektorált és megjelentetésre alkalmasnak tartott tanulmányok jelenhetnek meg. A beküldött kéziratoknak formai és tartalmi szempontból egyaránt meg kell felelnie a Folyóirat weboldalán közölt elvárásoknak. El nem fogadott kéziratokat nem áll módunkban visszaküldeni.
Articles in the Safety and Security Sciences Review are archived in the Digital Archives of Óbuda University (ÓDA). The studies of the staff and students of Óbuda University, published in the Journal, are recorded by the staff of the University Library at the Hungarian Scientific Works Library (MTMT).	A Biztonságtudományi Szemle folyóiratban megjelenő cikkek az Óbudai Egyetem Digitális Archívumában (ÓDA) archiválásra kerülnek. Az Óbudai Egyetem munkatársainak és hallgatóinak a Folyóiratban megjelent tanulmányait az Egyetemi Könyvtár munkatársai rögzítik a Magyar Tudományos Művek Tárában (MTMT).

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

ISSN 2676-9042
https://biztonsagtudomanyi.szemle.uni-obuda.hu

Editorial office | Szerkesztőség
Óbudai Egyetem
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
Biztonságtudományi Doktori Iskola
1081 Budapest, Népszínház utca 8.

Publisher | Kiadó
Óbudai Egyetem, 1034 Budapest, Bécsi út 96/B.

Responsible for publishing | A kiadásért felel
Prof. Dr. KOVÁCS Levente
Rector of the Óbuda University | az Óbudai Egyetem rektora

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

Vol 3, No 3, 2021. | **2021. III. évf. 3. szám**

Authors of this issue | **E számunk szerzői**

FÁBIÁN Péter

fabianpeter@topcopgroup.com

The author is a police officer, lawyer, criminologist, national security analyst. For many years he worked as a criminal intelligence officer at various police departments. He has been working as a leader in the private security sector for more than 20 years. Private forensic security expert, security consultant for several large multinational corporations. Expert of the PTE Center for Defense Research. He is a doctoral candidate of the Doctoral School of Security Sciences of the University of Óbuda. His research topic is private security.

A szerző rendőrtiszt, jogász, kriminológus, nemzetbiztonsági elemző. Sok évig bűnügyi hírszerzőként dolgozott a Rendőrség különböző szerveinél. Több, mint 20 éve a magánbiztonsági szektorban dolgozik vezetőként. Igazságügyi magánbiztonsági szakértő, több multinacionális nagyvállalat biztonsági tanácsadója. A PTE Védelmi Kutatások Központ szakértője. Az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorjelöltje. Kutatási témája a magánbiztonság.

GULYÁS Attila

agulyas66@gmail.com

Attila GULYÁS ret. Lt.Colonel graduated from the Kossuth Lajos Military college as an infantry officer in 1988. After serving a four-year period of time as a troop officer he was transferred to the Military Security Office, where he served in different positions. He retired from the service as a head of department and in the rank of Lieutenant Colonel in 2010. He has been interested in IT for a quarter century. His hobby is computer programming (VB.net, Visual C++, and Python), as well as computer forensic on personal computers on MS Windows, and Linux operating systems. He is a doctoral student at the Óbuda University Doctoral School on Safety and Security Sciences, where he is researching the connection between the terrorism and the Dark Net.

GULYÁS Attila ny. alezredes 1988-ban végezte el a Kossuth Lajos Katonai Főiskolát gépesített lövész szakon, majd négyéves csapatszolgálat után a MK Katonai Biztonsági Hivatal állományába került, ahol különböző beosztások betöltését követően 2010-ben osztályvezetőként, alezredesi rendfokozattal került szolgálati nyugállományba. Az informatikával közel negyed százada került kapcsolatba. Érdeklődik a programozás (VB.net, Visual C++, valamint Python) és a digitális bizonyítékok megszerzésének és eltűntetésének kérdésével személyi számítógépeken MS Windows és Linux rendszereken, jelenleg az Óbudai Egyetem Biztonság tudományi Doktori Iskola doktorandusza, ahol a Dark Net és a terrorizmus összefüggéseit kutatja.

KERTI András

kerti.andras@uni-obuda.hu

I am dr habil András KERTI, an associate professor at the Faculty of Military Science and Officer Training of the University of Public Service. I have been participating in university education since 2006, before that I have performed various info-communication tasks at the units of the Hungarian Armed Forces. I have been involved in the work of the Óbuda University Doctoral School on Safety and Security Sciences since 2016. Research field: "Information security of public service organizations".

Dr. habil KERTI András vagyok, a Nemzeti közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, Híradó Tanszék docense. Az egyetemi oktatásban 2006 óta veszek részt, előtte a Magyar Honvédség alakulatainál láttam el különböző infokommunikációs feladatokat. Az Óbudai Egyetem Biztonságtudományi Doktori Iskola munkájában 2016-óta veszek részt. Kutatási területem: „A közfeladatot ellátószervezetek információbiztonsága".

KOVÁCS Tibor

kovacs.tibor@bgk.uni-obuda.hu

Prof. Dr. Tibor KOVÁCS (1961) M.Sc. telecommunication specialist, M.Sc. electrical engineer, head of department at the Institute of Mechanical and Security Sciences, Óbuda University, associate professor at the Department of Security Engineering. Research interests: Critical Infrastructure Protection, Technical Approach to Emergency Behavior, Laser Ultrasonic Detection of Chemicals, Development Possibilities of the Early Nuclear Alert System of the Re-public of Hungary. Currently, he is a lecturer at the Doctoral School on Safety and Security Sciences at Óbuda University, the Doctoral School of Military Engineering at the National University of Public Service, the Óbuda University and the National University of Public Service.

Prof. Dr. KOVÁCS Tibor (1961) okl. híradástechnikai szakmérnök, okl. villamosmérnök, az Óbudai Egyetem Gépészeti és Biztonságtudományi Intézet, Biztonságtechnikai Intézeti Tanszék tanszékvezetője, egyetemi docens. Kutatási területei: Kritikus infrastruktúra védelem, Veszélyhelyzeti viselkedés technikai megközelítése, Vegyi anyagok lézerultrahangos detektálása, A Magyar Köztársaság Korai Nukleáris Riasztási Rendszerének fejlesztési lehetőségei. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola, a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, az Óbudai Egyetem és a Nemzeti Közszolgálati Egyetem oktatója.

LAUFER Edit

laufer.edit@bgk.uni-obuda.hu

Edit TÓTH-LAUFER received the B.Sc. degree in information technology from the John von Neumann Faculty of Informatics of the Budapest Polytechnic, Budapest, in 2001, the M.Sc. degree in teacher of informatics from the Faculty of Natural Science and Informatics, Eötvös Loránd University, Budapest, in 2004, the Ph.D. degree from the Doctoral School of Applied Informatics and Applied Mathematics, Óbuda University, Budapest, in 2014, and Dr. habil title in 2020. She joined the Institute of Mechatronics and Vehicle Engineering, Budapest Polytechnic, in 2001 (from 2021 also Head of Institute), and its legal successor Óbuda University, where she has been involved in a number of scientific research projects. Her current research interests include soft computing, risk assessment and complex systems. Dr. Tóth-Laufer is member of several scientific society including IEEE, John von Neumann Computer Society, Hungary, and Hungarian Fuzzy Association. She is the president of the Hungarian Fuzzy Association.

TÓTH-LAUFER Edit a Budapesti Műszaki Főiskolán szerzett mérnök informatikus B.Sc. diplomát 2001-ben, informatika szakos tanár M.Sc. diplomát az Eötvös Loránd Tudományegyetem Természettudományi és Informatika Karán 2004-ben, Ph.D fokozatot az Óbudai Egyetem Alkalmazott Informatikai és Alkalmazott Matematikai Doktori Iskolájában 2014, majd habilitált doktori címet 2020-ban. 2001 óta oktat az Óbudai Egyetem (korábban Budapesti Műszaki Főiskola) Mechatronikai és Járműtechnikai Intézetében (2021-től intézetigazgató). Számos tudományos kutatásban vesz részt. Fő kutatási területei: lágy számítási módszerek, kockázat kezelés és complex rendszerek. Dr. Tóth-Laufer számos tudományos társaság, köztük az IEEE, a Neumann János Számítógép-tudományi Társaság, valamint a Magyar Fuzzy Társaság tagja. A Magyar Fuzzy Társaság elnöke.

MIKLÓS Gellért

gellert.miklos@gmail.com

The author is a lawyer, infocommunication specialist. He is currently a doctoral student at the Doctoral School of Security Sciences of the University of Óbuda. His studies and research focus on domestic and international regulation of cyber security, data security and data protection. He is also a regulatory manager for an international telecommunications company, specializing in the regulation of IoT de-

A szerző jogász, infokommunikációs szakjogász. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának doktorandusz hallgatója. Tanulmányai és kutatásai középpontjában a kiberbiztonság, adatbiztonság és adatvédelem hazai és nemzetközi szabályozása áll. Emellett egy nemzetközi távközlési vállalat jogszabályi megfeleléssel foglalkozó munkatársa, szakterülete az IoT eszközök és az ál-

vices and permanent roaming. On a daily basis, he deals with the evaluation of legislation and draft legislation relevant to the above topic, and with the examination of the legal compliance of various products and services.

landó barangolás (permanent roaming) szabályozása. Napi szinten foglalkozik a fenti témakörben releváns jogszabályok, jogszabály tervezetek értékelésével, a különböző termékek, szolgáltatások jogszabályi megfelelőségének vizsgálatával.

NYÁRI Norbert

nyari.norbert@uni-obuda.hu

So far, I have studied mainly in the field of informatics, I have degrees in engineering, teaching and computer science. I have been working as a software developer for more than 10 years at a budgetary institution of the Hungarian public administration. Due to my studies and professional experience, I have extensive knowledge in the fields of application development, information security, and psychology. The aim of my doctoral research is to find tools, methods and solutions for strengthening the information security of the Hungarian public administration.

Eddigi tanulmányaimat alapvetően informatikai területen végeztem, rendelkezem mérnöki, tanári, programtervezői diplomákkal. Több mint 10 éve dolgozom szoftverfejlesztőként a magyar közigazgatás egyik költségvetési szervénél. Tanulmányaimnál és szakmai tapasztalatomnál fogva széleskörű ismeretekkel rendelkezem az alkalmazásfejlesztés, az információbiztonság, valamint a pszichológia területén. Doktori kutatásom célja a magyar közigazgatás információbiztonságának erősítését szolgáló eszközök, módszerek, megoldások felkutatása.

PRISZNYÁK Szabolcs

prisznyak.szabolcs@outlook.com

Szabolcs PRISZNYÁK PhD is a computer engineer (BSc), a certified defence C3 system manager (MSc), PhD in military technical sciences, Executive MBA for IT. I have been working in the Hungarian public administration since 1993, I previously worked in the IT department of the Border Guard, the Police Office and the Hungarian Prison Service, and since 2019 I have been the Head of the IT Department of the Central Administration of the National Tax and Customs Administration. In 2020, I obtained a PhD degree in the research field Safety and Security Sciences at the Doctoral School of Security Sciences of the Óbuda University. In 2021 I obtained an Executive MBA for IT qualification at the Budapest Metropolitan University. My research area is informatics, law enforcement informatics.

Dr. PRISZNYÁK Szabolcs mérnök-informatikus (BSc), okleveles védelmi vezetéstechnikai rendszertervező (MSc), a katonai műszaki tudományok PhD fokozatosa, Executive MBA for IT. 1993-tól dolgozom a hazai közigazgatásban, korábban a Határőrség, a Rendőrség és a Büntetés-végrehajtási Szervezet informatikai szakterületén dolgoztam, 2019-től a Nemzeti Adó- és Vámhivatal Központi Irányítás informatikai főosztályvezetője vagyok. 2020-ban szereztem PhD fokozatot katonai műszaki tudományok tudományágban az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában. 2021-ben Executive MBA for IT képesítést a Budapesti Metropolitan Egyetemen. Kutatási területem az informatika, rendvédelmi informatika.

SZÁDECZKY Tamás

szadeczky.tamas@kvk.uni-obuda.hu

Tamás SZÁDECZKY is an associate professor of Budapest University of Technology and Economics. He graduated as an engineer and MBA. He has defended his PhD thesis about regulation of IT security. He has been working in the field of information security since 2003. He is holding multiple professional certificates, like CISSP, CISM, CISA, PCI QSA and IRCA ISO 27001 lead auditor. He is also a lecturer and researcher of the topic for more than a decade in multiple universities in Hungary and Germany.

Dr. SZÁDECZKY Tamás a Budapesti Műszaki és Gazdaságtudományi Egyetem egyetemi docense, mérnök, MBA, a katonai műszaki tudományokból habilitált, az információbiztonság területén dolgozik 2003 óta. Számos nemzetközi szakmai címmel, így például a CISSP, CISM, CISA, PCI QSA és az IRCA ISO 27001 lead auditor rendelkezik. Információbiztonsági témákat több, mint egy évtizede oktat magyar és német egyetemeken.

SZŰCS Endre

szucs.endre@bgk.uni-obuda.hu

Endre SZŰCS (1963) has a PhD degree in military science, graduate engineer on security technology, mechanical engineer and engineering teacher. He is currently a lecturer at the Óbuda University Doctoral School on Safety and Security Science in Budapest. His main subjects are history and the key events of security technology. He also gives lectures at the Donát Bánki Faculty of Mechanical and Security Engineering of the University of Óbuda, Institute of Mechanical and Security Sciences. His field of research: Possibilities of using renewable energy sources in security technology. Exploring the milestones in the development of security technology.

SZŰCS Endre (1963) a hadtudomány PhD fokozatosa, okleveles biztonságtechnikai mérnök, gépészmérnök, mérnök tanár. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában témavezető, A biztonságtechnika történetének, eseményeinek áttekintése, elemzése című tantárgyat oktatja, illetve az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Gépészeti és Biztonságtudományi Intézet óradója. Kutatási területe: A megújuló energiaforrások alkalmazásának lehetőségei a biztonságtechnikában. A biztonságtechnika történetének vizsgálata.

VÁCZI Dániel

vaczi.daniel@uni-obuda.hu

Dániel VÁCZI is a doctoral student at the Doctoral School on Safety and Security Sciences of Óbuda University, a graduate security engineer who specified the human risks of cybersecurity during his studies and civil work. He is the former president of the Military Science Section of the National Association of Doctoral Students and a member of the Electronics, Informatics and Robotics Department of the Hungarian Military Science Society. He has worked as a cybersecurity consultant with small and medium-sized enterprises, multinational organizations and various entities in the government sector. He is CEH certified. For years, he has been the main organizer of the National Cyber Challenge cybersecurity simulation competition, which will become an international event from this year. At the end of 2018, he co-founded a startup, cyex to increase cybersecurity awareness.

VÁCZI Dániel az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának doktor várományosa, végzett biztonságtechnikai mérnök, aki tanulmányai és civil munkássága során a kiberbiztonság humán kockázataira specifikálódott. A Doktoranduszok Országos Szövetségének Hadtudományi Osztályának korábbi elnöke és a Magyar Hadtudományi Társaság Elektronikai, Informatikai és Robotikai Szakosztályának tagja. Kiberbiztonsági tanácsadóként dolgozott kis- és középvállalatokkal, multinacionális szervezetekkel és a kormányzati szektor különböző entitásaival. Rendelkezik CEH minősítéssel. Évek óta főszervezője az idén nemzetközivé váló, egyetemi kiberbiztonsági szimulációs versenynek, a Nemzeti Kiberversenynek. 2018 végén társalapítóként létrehozott egy kiberbiztonsági tudatosság növelését célzó startupot, a cyexet.

ZÁHONYI Lajos

zahonyi.lajos@phd.uni-obuda.hu

Corporate management and controlling economist, operations manager, project manager, quality- and information security manager and auditor. He is currently a PhD student at the Doctoral School of Security Sciences of the University of Óbuda. Research interests: Developmental history of information security, systems of reference tools and information security aspects of corporate governance systems and the impact of the use of the tools and methods developed.

Vállalatirányítás és kontrolling szakközgazdász, operatív vezető, projektmenedzser, minőségirányítási- és információbiztonsági vezető és auditor. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának PhD hallgatója. Kutatási területe: Az információbiztonság fejlődéstörténeti vizsgálata, viszonyulási eszközrendszerei és a vállalatirányítási rendszerek információbiztonság szempontú aspektusai, illetve a kialakított eszközök és módszerek használatának hatása.

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

Vol 3, No 3, 2021. | **2021. III. évf. 3. szám**

CONTENT | TARTALOM

ISIS IS A JIHADIST MISTAKE, OR ISLAM AND THE TERRORISM

ISIS A DZSIHADISTA TÉVEDÉS, AVAGY AZ ISZLÁM ÉS A TERRORIZMUS

FÁBIÁN Péter[1]

Abstract

"Finis sanctificat media" - this creed provided the basis for many ideological, religious-based campaigns, wars that caused the senseless deaths of millions of people. One might think that the Peace of Westphalia solved and ended the era of religious wars, and at this stage in the development of our world it was accepted that religion had no pur-pose and no object of politics, and an interpretation and philosophy of religion with the opposite content could only be wrong. In contrast, one of the most significant global challenges is the fight against terrorism, in which Islamic fun-damentalism plays a leading role. In my view, the only reasons for this are to look for the same misinterpretation, but already collectivised, and a way of thinking that is almost 1,500 years old and unacceptable under any circum-stances. The same thing that guided II. William in his quest for a violent Catholic.

Keywords

Islam, Terrorism, Jihad

Absztrakt

"Finis sanctificat media"- ezen hitvallás alapot adott számos ideológiai, vallási alapú hadjáratra, háborúra, amelyek emberek millióinak az értelmetlen halálát okozták. Gondolhatnánk, hogy a Vestfaliai Béke megoldotta és lezárta a vallásháborúk korszakát, s világunk fejlődésének jelen stádiumában már elfogadott nézett, hogy a vallásnak nem célja és nem tárgya a politika, s az ezzel ellentétes tartalmú vallásértelmezés és vallásfilozófia csak és kizárólag téves lehet.A globális kihívások között egyik legmeghatározóbb a terrorizmus elleni küzdelem, amelyben vezető szerepet játszik az iszlám fundamentalizmus. Álláspontom szerint ennek okai között kizárólag ugyanolyan téves - de már kollektivizálódott - értelmezést és közel 1500 évvel meghaladott, semmilyen körülmények között el nem fogadható gondolkodásmódot kell keresni, mint ami II. Vilmost vezérelte az erőszakos katolicizáló törekvései során.

Kulcsszavak

Iszlám, Terrorizmus, Dzsihad

[1] fabianpeter@topcopgroup.com| ORCID: 0000-0003-0640-6557 | Founder / Alapító | Top Cop Group

INTRODUCTION

In the middle of the twentieth century, most of humanity reached the level of socialization evolution that, through our historical failures, saw that wars along economic and political or even religious, ideological conflicts of interest and values, and the peace treaties that ended them, they are unable to resolve the original conflict. Typically, it is rather suppressed for time and hours, further strengthened, or positioned over time and space. It was still a socially accepted scenario in the early 1900s to assert the legitimate interest of a nation in the form of war or armed struggle. The devastation of World War 2, the development of weapons of mass destruction, has illuminated the way in which the population of our Earth arrives if they do not understand the word of time. After 1945, there was a general need in Europe and much of the world to establish and maintain peace and to reject wars. Mankind has entered a new era, with the establishment of the organizations that form the basis of the United Nations, NATO and later the EU. Peace and a freedom-based prosperity have arrived in Europe.

The undisguised goal of the development of the Union and international cooperation is to extend peace to the whole of Europe and to other continents.

Of course, global and total peace on Earth has not yet been achieved. There are a number of seemingly unresolved, religious, ideological conflicts in Europe and beyond, which end up in a continuous armed struggle, even beyond the category of an isolated act of terrorism. Perhaps the most significant of these is Islam's opposition to the rest of the world. In many cases, we confuse Islam with terrorism itself, and we tend to interpret jihad specifically as a terrorist act of violence or a process of it. In the historical relation, a more thorough understanding of the issue can bring us closer to forming an adequate position. The topicality of my dissertation is highlighted by what happened in Afghanistan in the days that are possible, they will in themselves draw new interpretations and rules on the subject, in the great book of history. Hopefully not with blood, but with reason and acceptance.

THE JIHAD

The word "jihad", in Arabic, means aspiration. Muslim jurists refer to it as "fighting by the way of Allah". [1] The Qur'an puts it even more nuancedly: "Fight in the way of Allah against those who fight against you! But do not transgress the commandments of Allah! Kill them wherever they are found! Fight them until there is no more temptation, and until the creed is only that of Allah!" [2]

The question is whether it is possible to accurately describe the meaning of jihad in a single term, when it was born in the context of a completely different age and many explanations and interpretations of it have come to light over the centuries. Radical organizations in the 20th century, such as al-Qaeda or the Islamic State (IS), use the concept of jihad unilaterally, as an armed struggle, as a holy war.

"The debate over Islam and jihad that began after 9/11 was often influenced by a superficial interpretation of the concept." [3]

Islamic scholars make a distinction between internal and external jihad. Inner jihad is nothing more than an effort to create a life that pleases God. [4]

External jihad does not always mean armed struggle, but there are other forms, such as the jihad of the heart as an internal struggle against evil, the jihad of language as a conversion, a form of mission, a jihad of pen and knowledge, this pursuit through the sciences against evil, and theologians even distinguish the jihad of the hand, which is a good fight against evil by wealth, this interpretation includes quite a lot of everything from caring for an elderly relative to donating money to political struggle.

Jihad "by the sword" was used by al-Qaeda and the IS to justify acts of terrorism against civilians.

ESTABLISHMENT OF THE RELIGIOUS BACKGROUND

The history of Islam began in the Arabian Peninsula when, in a cave near Mecca, through the mediation of Archangel Gabriel, Allah revealed himself to Muhammad, who was chosen to lead the peoples of the world back to the true faith. Islam is a monotheistic faith, just like Judaism, but according to Islam there is one God and he is Allah. This is one of the cornerstones of Islam, that is, There is no God but Allah. [5] An extremely important date for the Muslim religion 622. 06.16. History books refer to this day as "Muhammad's Run," however, this is a flawed position.

Tamás M. Tarján, historian, thinks of this: "The Islamic community migrated in several waves from Mecca to the city of Jathrib, about 300 kilometers north, where the distorted clans received Mohamed as a justice of the peace. The settlement, which later took on the name "the city of the Prophet," that is, the Medina, provided the right setting for the founder of religion to put into practice the order he had dreamed of."

And "hijra" does not mean running, but leaving one's own tribe to join a new community, i.e. moving, wandering. [6]

The Qur'an also used the word jihad in the time of Mecca, but it was much more referring to the previously mentioned inner jihad, that is, after the peaceful journey and migration to Medina, the term jihad was already filled with a militant dimension. [7]

After the death of Muhammad, Islam was torn into three branches. It was up to the Muslims left behind to make a decision on which direction the community should go. One of the Prophet's companions, Abu Bakr, thought that Muslims needed a leader, others thought that Mohammed's closest male relative could be the new leader, Ali ibn Abi Taliban. The majority eventually chose Abu Bakr. We call them Sunnis. The other camp is Ali's camp, or rather Ali's party of the Shiites.[8]

Later, the Shiite direction further decomposes into a "hariji" direction. Currently, the state religion of Oman is the hariji alone. Events in the Middle East have since been determined by the opposition of Shiites (e.g., Iran, Syria) and Sunnis (e.g., Saudi Arabia, parts of Iraq)

BIRTH AND BEGINNINGS OF JIHAD

The very first - external - jihad took place when he turned against armed Mohamed Mecca, clearly pursuing jihad. Over the centuries, several interpretations of jihad have emerged. The second time came when Mohamed's successor (Sunni) Abu Bakr found himself facing reluctant tribes in the Arabian Peninsula and launched a war over "apostasy". The third meaning appeared to the pursuit of jihad against their own incompetent leaders in the middle of the thirteenth century, as they did not live in a Muslim-dignified manner and

did not submit to the Syrian, that is, Islamic legal system. This is the medieval meaning of jihad, which is today's primary ideological weapon for al-Qaeda and the Islamic State. [9]

In the 18th century, jihad served as resistance to British and French colonizers in North Africa, the Middle East, and India. Over the centuries, the meaning of jihad has shaped and evolved. Each age had a great philosopher of religion who provided sufficient background in "reshaping" the meaning of jihad to put true Muslims in battle to avert the danger of that age, or to serve as an justification for an expansionary pursuit, as was the case with the proclamation of the Crusades or the Inquisition. .

"The fifth interpretation of jihad […] comes from Abul A'la Maududi, who developed the theory for decades. From this, the decisive Egyptian Sayid Kutb, an intellectual grandfather of groups such as al-Qaeda and ISIS, eventually developed the modern concept of jihad." [10]

Kutb read the writings of Maududi, the writings of Maududi, who modeled Pakistan on his teachings. Kutb combined versions of previous jihads. For example, he used the ideas of the former "third" jihad — the removal of an unsuitable leader by jihad — in the spirit of today. His works were published by his brother in Saudi Arabia and he taught at Umm al-Qura University in Mecca. Among his students there were Osama bin Laden and Ajman al-Zavahiri.

1979 IS THE YEAR OF CHANGE

The Soviet Union asserts its dominance over Afghanistan. As a result, according to Gorka, the sixth jihad emerged, which is already clearly a global and combat call for all true Muslims against the occupying power. [11]

His creation was proclaimed by Jordanian religious leader Abdullah Azzam. It is now a personal obligation and it is not necessary to call the caliph. This is an extremely important and significant change.

Azzam died in 1989 and his legacy is not only a global and personal interpretation of jihad, but the recruitment of fifty-five thousand guerrilla warriors. The organization (Office of Arab Mujahedeen Services) will be taken over by its former deputy, Osama bin-Laden.

And with the end of the Cold War, the Saudis, who had previously refused the organization's help in the Iraq war, are letting American soldiers into the Arabian Peninsula as an ally of the United States. Saudi bin-Laden is changing the name of the organization - al-Qaeda is starting to operate - and is finding a new enemy in the person of the United States.[12] This process leads all the way to the 9/11 terrorist attack. This year also saw the outbreak of the Iranian revolution, which also revealed a global version of jihad to the world.

Iran settled with Pahlavi - American puppet power - and Khomeini took his place. Washington has lost an extremely important ally in the Middle East. Iran became a target with its Shiite state religion after Saddam came to power.

Iraq is predominantly Sunni, but feared an uprising by the Shiite minority. The war without a message of war was started by Iraq on September 22, 1988. The Kurds sided with the Iranians, giving Saddam a great excuse for genocide.

ON THE WAY TO THE ISLAMIC STATE

One of the most significant security policy challenges these days is clearly caused by the presence of a terrorist organization called the Islamic State. In fact, it is two separate but interconnected organizations that operate in Syria and Iraq, but its members are also present in other countries. Five distinct cycles are distinguished, which gives a great picture of the organization. [13]

HISTORY (1999-2013)

The IS was established in 2013 from an organization called Islam in Iraq and Syria. Its operation can be traced back to 1999. It operated in Iraq and then, following the fall of Saddam Hussein in 2003, several organizations took up the fight against Westerners undergoing reconstruction.

One was the Monotheism and Jihad Group led by Abu Musz'ab al-Zarkavi. The organization was not popular with jihadists because of its radical views. While al-Qaeda - and later IS - was a kind of "brand" to the population, Zarkavi was an extremely radical jihadist. He did not want to win over the population, but to intimidate him through a series of suicide bombings. They did not have a good relationship with bin Laden. He founded his Zarkavi group at home in Jordan and saw the opportunity in the 2003 Iraqi offensive and relocated its headquarters. Zarkavi persecuted the Shiite population and wanted to address the Sunni majority.

Its group in Zarkavi became increasingly popular due to his rapid success. Al-Qaeda wanted to set foot in Iraq as a promising jihad opportunity. In 2004, Zarkavi swore allegiance to Osama bin-Laden and his group continued to operate under the name Iraqi al-Qaeda. Zarkavi was too radical, even according to bin-Laden, and this clashed with differing interpretations of the struggle to win over the population. Zarkavi did not want to jihad against American soldiers, but wanted to rule the people with a weapon of terror. Al Qaeda successfully expanded into the Arabian Peninsula and North Africa, while against Zarkavi, the local tribes, united with brutality, banded together and clashed. By 2007, with the arrival of American reinforcements, local tribes were also cooperating against terror. An airstrike ended Zarkavi's life on June 7th. Osama bin-Laden was replaced by Abu Omar al-Baghdad, while the Iraqi branch was taken over by Abu Alyab al-Misri. The importance of supporting local tribes was recognized. What was a total failure, however, was the introduction of an individual interpretation of sharia in the occupied territories. Even the Sunnis rejected this. Thus, support for the Islamic State of Iraq has declined. When both Abu Omar al-Baghdad and Abu Ajub al-Misri were killed in an American airstrike in 2010, Abu Bakr al-Baghdad took control of the entire organization.

It carried out a reorganization consisting of three main elements:

- He abolished public executions so he did not provoke the locals.
- The organization has put locals in place of foreign Arab leaders.
- It has set up three councils in the organization: Surah Council, Military Council, Security and Intelligence Council.

He filled his intelligence with Saddam's former intelligence men, who brought with him deep local knowledge and logistics. What helped al-Baghdad operate is the "fallen

state" in Iraq, state dysfunction, and the fact that bin Laden was killed in 2011 and al-Qaeda disintegrated without him. However, the final push came from the outbreak of the Syrian civil war, which, as during the Iraqi offensive, was now a great opportunity for the expansion of the Islamic State. Al-Kadi began operations in Syria using the Baghdad line, but al-Baghdad announced the creation of the Islamic State of Iraq and the Levant (ISIS) and merged with one of the increasingly successful and strengthening organizations in Syria, the Nusra Front. Al-Qaeda has asked al-Baghdad to disband the new organization, but this has not happened and has also become increasingly popular in al-Qaeda's Iraqi branch.

BREAKING UP WITH AL QAEDA

In 2013 - then still as the Islamic State of Iraq - a campaign was launched in northern Syria against the Kurds. The Nusra Front was initially under the protection of the Free Syrian Army. The FSA was a very heterogeneous alliance, with the sole aim of overthrowing the existing Bassar el-Assad regime, but there was no consensus on the post-regime regime. After the occupation of the northern city of Rakka, the army consisted largely of Nusra fighters who joined the Islamic State of Iraq and the subsequent ISIS. ISIS appeared in Rakka, without going there.

In the city, ISIS tried to restore the administration and track down spies linked to Damascus. ISIS has a huge advantage over other organizations in the "hinterland" of Iraq.

One of his greatest military successes was the capture of the Iraqi city of Fallujah. Subsequently, attacks on Kurds were launched from the city of Rakka in Syria. Islamic organizations in Syria have formed an alliance, but ISIS has not been included. A German doctor arrived at the hospital in the city of Azaz (under the Doctors Without Borders program) and ISIS demanded that the doctor leave the hospital where the FSA and ISIS fighters were being cared for. This did not happen, for this ISIS attacked the soldiers of the FSA.

Overall, although ISIS has lost territories during its campaigns, it has managed to consolidate its power in central Rakka and Iraq. It was then that the break-up with al-Qaeda took place. [14]

THE PROCLAMATION OF THE CALIPHATE

The formation of the Islamic State was announced on June 29, 2014, as a result of which various Islamist groups began to join immediately, so that the number of IS forces grew. Three different campaigns were launched against symbolic Shiite targets.

It was a shock to the Iraqi government that the Islamists took over the two-million-strong city of Mosul, the citadel of the Iraqi oil industry. With five thousand attackers, they occupied the city with sixty thousand defenses. The soldiers feared the myth of the invincibility of the IS and deserted in a row, including three generals and the remaining forces, who had taken up the fight, were left without central control.

The Kurds were unable to take the issue of secession and statehood to a referendum because of the IS attack. The third target of the IA was Kobane, a symbol of Kurdish autonomy.[15]

THE DECLINE OF THE ISLAMIC STATE

The IS has suffered a military defeat from the "counter-terrorism coalition," which is not annihilation, as military means are insufficient. Moszult was recaptured from the terrorist organization in October last year after a long siege, while Rakka was seized in October last year. In June last year, al-Baghdad was killed in a Russian air raid on Rakka.

At the moment, the Islamic State is present in Afghanistan, where some Taliban commanders have switched. The United States has stationed fifteen thousand soldiers in Afghanistan who will only go "off the wire" if the locals cling to the people of the Islamic State. [16] However, the United States has recently withdrawn its troops from the region, and as a result, news of successful Taliban attacks, the occupation of Kabul and the escape of millions of Afghans has been rumored in recent days. Although the world press needed such an "almost war" as a mouthful of bread, I, for my part, have reservations about the news in various media outlets that the Taliban leadership aims for peace and will refrain from and will refrain from any violence. Although the Taliban have declared a complete amnesty and perhaps we can also say that they are also beginning to liberalize their spirituality, or rather to bend its interpretation.

While writing this study, watching CNN television, I see a Taliban commander giving an interview to a female journalist. Where further, the Taliban have also pledged to reform the situation and rights of women. Nevertheless, it is a matter of fact that analysts envision the strengthening of al-Qaeda / IS, it is a matter of fact that there are already indescribable conditions at Kabul airport, from which tens of thousands of people are fleeing. And the IS came up with further assassinations, followed by very quick retaliation from the US. The surrounding countries began to arm themselves. It is irresponsible for any business that wants to make a prediction about when and what kind of refugee influx and migration threat this will pose to Europe. However, it is hard to imagine that the Afghan-Taliban relationship would be able to stabilize the region on the basis of consensus and reconciliation.

CLOSING THOUGHTS

It is my belief that it leads to the trap of jihad, misguided and one-sided cognition interpreted as violence. External jihad has changed over the course of world history, like any other ideology or religious view, in the order and manner, reflecting the challenges of that era. The offensive and expansive jihad of our time, first pursued by al-Qaeda and later by the Islamic State, was determined by the events of 1979 as international. Although this scenario only made sense in retrospect, blaming the previous generation with any kind of irresponsibility would be as viable as attacking Newton for crashing planes. The turbulent years of the Middle East were exploited by radical Islamist organizations and in some places they used the slogan of jihad to justify their expansion plans shrouded in individual religious interpretations. Years of brutal violence and total chaos have shown that the terror used as a tool of jihad cannot be sustained in the long run and breeds malice in the eyes of the people. The Islamic State has never really been able to gain ground outside the Sunni lands. Islamic law, interpreted in its unique form, that is, the Sira, also aroused resentment among the Sunni population. And the anti-terror coalition inflicted military defeat on the Islamic State. However, as long as there are failed states in the world where administration and legislation are dysfunctional, these places - and especially their border zones - carry the

germ of the possibility of arms conflict. Afghanistan, Pakistan, Yemen. North Africa. Where armed conflict appears or where one of the interest groups is pushed out of the legislature and becomes radicalized, there are extremists, terrorist organizations. There is no guarantee that in the future we will not come to know a new kind of dimension-laden interpretation of jihad. It is possible that a philosopher of religion has already created it somewhere, but it only makes sense in retrospect.

BIBLIOGRAPHY

[1] Wikipedia 2021. https://hu.wikipedia.org/wiki/Dzsihád
[2] The Quran. Oxford: Oxford University Press. pp. 190-193, 2004.
[3] Gorka, S. Defeating Jihad. Washington: Regnery Publishing. pp. 22., 2019.
[4] iszlam.com/iszlam-az-elet-vallasa/iszlam-es-nyugat/item/1311-a-dzsihad-valodi-jelentese [Online] [ACCESSED: 12.08.2021]
[5] https://wahiduddin.net/words/tahlil.htm [Online] [ACCESSED: 12.08.2021]
[6] Simon R. Iszlám Kulturális Lexikon. Budapest: Corvina Kiadó, pp. 54., 2009.
[7] Gorka, S. Defeating Jihad. Washington: Regnery Publishing. pp. 41-44., 2019.
[8] Amstrong, K. Islam-short history. London: Orion Publishing. pp. 34-36., 2001.
[9] Gorka, S. Defeating Jihad. Washington: Regnery Publishing. pp. 53., 2019.
[10] Gorka, S. Defeating Jihad. Washington: Regnery Publishing. pp. 56., 2019.
[11] Gorka, S. Defeating Jihad. Washington: Regnery Publishing. pp. 57., 2019.
[12] Gorka, S. Defeating Jihad. Washington: Regnery Publishing. pp. 61., 2019.
[13] Arany A. – Rózsa E. – Szalai M. Az Iszlám Állam Kalifátusa. Budapest, Osiris Kiadó. pp.34., 2016.
[14] Arany A. – Rózsa E. – Szalai M. Az Iszlám Állam Kalifátusa. Budapest, Osiris Kiadó. pp.45., 2016.
[15] Arany A. – Rózsa E. – Szalai M. Az Iszlám Állam Kalifátusa. Budapest, Osiris Kiadó. pp. 51., 2016.
[16] Dobai G. Az Iszlám Állam felemelkedése és bukása. Budapest: magánkiadás. pp. 43-49., 2016.

DATA-PROTECTION ANALYSIS OF BIOMETRIC SYSTEMS

A BIOMETRIKUS RENDSZEREK ADATVÉDELMI SZEMPONTÚ ELEMZÉSE

KOVÁCS Tibor[1] – MIKLÓS Gellért[2]

Abstract

This article aims to provide a brief overview of the data protection considerations and requirements for the use of biometric data in different identification systems. The author illustrates the widespread use of biometric data in personal identification with international examples, as well as the regulatory requirements and potential dangers of this growing trend.

Keywords

biometrics, personal data, data protection, personal identification, GDPR, migration, border control

Absztrakt

Jelen cikk rövid áttekintést kíván nyújtani a biometrikus adatok különböző azonosító rendszerekben történő felhasználásának adatvédelmi megfontolásaival és követelményeivel kapcsolatban. A szerző nemzetközi példákkal illusztrálja a biometrikus adatok széleskörű felhasználási körét a személyazonosítás terén, ismertetve ennek az egyre növekvő trendnek a szabályozási követelményeit és lehetséges veszélyeit is.

Kulcsszavak

biometria, személyes adat, adatvédelem, személyazonosítás, GDPR, migráció, határellenőrzés

[1] kovacs.tibor@bgk.uni-obuda.hu | ORCID: 0000-0001-7609-9287 | associate professor, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering | egyetemi docens, tanszékvezető, Óbudai Egyetem Bánki Donát Gépész és Biztonság-technikai Mérnöki Kar

[2] gellert.miklos@gmail.com | ORCID: 0000-0002-3757-6834 | doctoral candidate, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Az illegális határátlépés és a bevándorlás, a terrorizmus, a kiberbűnözés csak néhány olyan társadalmi feszültséget okozó jelenség napjainkban, amely fokozódó kihívás elé állítja a világ országait. Ez a növekvő nyomás és a biztonság iránti vágy egyben megteremti az igényt a megbízható, pontos és nem utolsó sorban költséghatékony személyazonosítás iránt.

A biometria, azaz egy élőlény – jellemzően ember – mérhető biológiai és viselkedési jegyeinek mérése és rögzítése, valamint az ezen alapuló azonosítás már régóta rendelkezésre áll. Az arc és hang alapján történő személyazonosítás egyidős az emberi civilizációval, a XIX. századtól kezdődően, a bűnüldöző hatóságok által rendszeresített ujjnyomat alapú azonosítás pedig széles körben elterjesztette a mérhető élettani tulajdonságok alapján történő azonosítás gyakorlatát. [1] Az élettani jellemzők felhasználhatók egy személy azonosítására és ellenőrzés céljából is. Személyazonosítás során az azonosítandó személy összevetésre kerül az adatállományban tárolt adatokkal, párosítva az egyező mintával és a hozzá társított adatokkal és jogosultságokkal (1:n típusú minta összehasonlítás). Ellenőrzés során a személy mért biológiai jellemzője összevetésre kerül a korábban már mért és a rendszerben tárolt mintával (1:1 típusú minta összehasonlítás). [2] A mérhető biológiai jellemzők köre a tudomány fejlődésével bővül, jelenleg a DNS, az arc és annak hőképe, a bőr mintázata, az ujjnyomat, ujjlenyomat vagy tenyérnyomat, a tenyér erezete vagy hőképe, a kéz geometriája, az írisz, a retina, míg a mért viselkedési jellemzők közül a kézírás, egy gomb vagy billentyű leütésének módja és sebessége, a beszédhang, valamint a járás módja a legjellemzőbben mért tulajdonságok.

A biológiai jellemzők egyik előnye, hogy azok rendszerint az azonosítandó személy tulajdonában vannak – mondhatni mindig kéznél vannak – és azok egy része huzamosabb ideig változatlanul lehetővé teszi a személy azonosítását. Ennek köszönhetően a biometrikus adatok széles körben felhasználásra kerülnek, legyen szó bűnüldözésről, vagy a határrendészet által rendszeresített biometrikus adatokat tartalmazó útiokmányokról. Napjainkban azonban a robbanásszerű technológiai fejlődés és a biztonság iránti növekvő igény megteremti a lehetőséget a korábbinál pontosabb azonosító eszközök, szenzorok költséghatékony létrehozására, a széleskörű mintavételre és azok tárolására, valamint a különböző biometrikus adatbázisok összekapcsolására.

A biometrikus azonosítás során, az élettani jellemzőkről készített sablonok és minták a hatályos adatvédelmi jogszabályok szerint személyes adatnak tekintendők, így az azonosítási eljárás kialakítása, valamint a minták kezelése során is érvényre kell jutnia az alkalmazandó alkotmányos és adatvédelmi jogi alapelveknek.

Az alábbiakban néhány tervezett, vagy már megvalósított biometrikus adatok felhasználására épülő személyazonosítás rendszer kerül bemutatásra, amelyek elemzése értékes tanulsággal szolgálhat a jövőben tervezett biometrikus adatbázisok vonatkozásában is.

NEMZETKÖZI KITEKINTÉS

Biometrikus SIM kártya regisztráció

A thai kormány 2017-től kötelezi a telekommunikációs szolgáltatókat, hogy SIM kártyák értékesítése során kötelezően rögzítsék az előfizetők ujjnyomatát vagy arcképét. A

biometrikus adatok az előfizető telefonszámához kapcsolódnak, majd az adatok egy központi nyilvántartásban kerülnek tárolásra, amelyet a Nemzeti Műsorszóró és Telekommunikációs Bizottság (National Broadcasting and Tele-communications Commission) felügyel. A regisztrációs kötelezettség egyaránt kiterjed az előfizetéses és a feltöltőkártyás SIM kártyákra is. A szolgáltatók a regisztrációs kötelezettségük elmulasztása esetén bírságra számíthatnak, szélsőséges esetben azonban az engedélyük is felfüggesztésre kerülhet. A szabályozás szigorításának indokául az elmúlt években elszaporodó terrorista merényletek szolgáltak. 2015-ben és 2016-ban is több olyan terrorista indíttatású merénylet történt Thaiföld forgalmasabb turista központjait célozva, amelyek során a pokolgépeket mobiltelefonokkal hozták működésbe. Az új, szigorúbb regisztrációs kötelezettségektől a thai kormány azt várja, hogy az megkönnyíti a korábbiakhoz hasonló terrorista cselekmények és egyéb bűncselekmény megakadályozását és felderítését is az által, hogy a bűncselekmény során felhasznált telefon tulajdonosa egyértelműen beazonosítható lesz a rendszerben tárolt adatok alapján. [3] A thaiföldi kezdeményezés csak egy, a világon számos más államban működő hasonló, biometrikus adatokon alapuló regisztrációs rendszerhez képest. Pakisztán és Banglades már 2015-ben bevezette az ujjnyomaton alapuló SIM kártya regisztrációt, míg Nigériában 2011 óta működik hasonló rendszer.

A kritikusok szerint azonban a thaihoz hasonló kötelező, biometrikus adatok rögzítésére alapuló regisztrációs rendszerek súlyosan korlátozzák az érintettek magánélethez való jogát, valamint nem váltják be a hozzájuk fűzött reményeket a terrorizmus ellen folytatott harc során. Egyrészt a SIM kártya kötelező regisztrációja megszünteti az anonim, névtelen kommunikáció lehetőségét az érintettek számára, míg az állam számára lehetővé teszi az érintettek helyének és személyazonosságának pontos meghatározását. Egy biometrikus adatokat, telefonszámot és helymeghatározási adatokat is tartalmazó nyilvántartás könnyen visszaélésekhez vezethet, vagy lehetővé teheti az érintettekkel kapcsolatos profilalkotást is. A névtelenség ugyan valóban megnehezítheti a bűncselekmények felderítését, azonban az újságírok, emberi jogi aktivisták, vagy más sérülékeny közösségek tagjai számára egy eszköz is, amely lehetővé teszi, hogy gyakorolják a szólásszabadsághoz fűződő jogukat. Könnyen belátható, hogy egy ilyen rendszer nagymértékben kiszolgáltatottá teszi ezeket a csoportokat, különösképpen, ha a rendszerrel szemben kritikus hangon szólalnak meg. [4] A tapasztalatok alapján hátránya továbbá a kötelező regisztráción alapuló rendszereknek, hogy hatásukra megnő a kereslet a nem regisztrált, vagy fals személyiséggel regisztrált SIM kártyák iránt, amely igényt a feketepiac siet kielégíteni. Ezzel összefüggésben megnő a személyiség lopások, valamint a már regisztrált eszközök ellen elkövetett lopások száma is. Nincs azonban kimutatható össze-függés azon bűncselekmények számával, amelyekre hivatkozással a kormányok indokolták a regisztráció bevezetését. Erre a tanulságra jutott mind a Pakisztánban, mind a Mexikóban bevezetett hasonló rendszer elemzése kapcsán a telekommunikációs szolgáltatókat tömörítő GSMA szervezet is. [5]

A fentiek alapján javasolta 2015-ben az ENSZ szólásszabadságért felelős különleges előadója vizsgálata eredményeként, hogy az államok tartózkodjanak attól a gyakorlattól, hogy a digitális kommunikációhoz és az online szolgáltatásokhoz való hozzáférést a felhasználók azonosításához kössék és a mobil felhasználók számára a SIM-kártya kötelező regisztrációját követeljék meg. [6]

Az indiai Aadhaar rendszer

Napjainkban hatalmas problémát jelent a világ számos részén, hogy a lakosság egy jelentős része – főleg a vidéki, nehezen megközelíthető, gyéren lakott területeken – nem rendelkezik semmilyen személyazonosító dokumentummal. Különösen igaz ez a szubszaharai Afrikára és Ázsia egyes részeire. Ezek a személyazonosító okmányokkal nem rendelkező emberek sok szempontból láthatatlanok a kormányok számára és a megfelelő dokumentumok hiányában a társadalmi ellátórendszeren kívül rekednek. További nehézséget jelent a fejlődő világ országaiban a társadalmi juttatásokkal kapcsolatos korrupció, valamint azok nem hatékony elosztása. Az indai kormány becslése szerint a legszegényebb társadalmi csoportok számára biztosított rizs támogatás 15%-a, a búza támogatás 54%-a, míg a cukor támogatás 48%-a veszett el a korrupció és a nem hatékony elosztás következtében. [7] Indiában az ezredforduló környékén kezdődött meg a párbeszéd egy új nemzeti személyazonosítási rendszer szükségességéről és annak megvalósításáról. Az új rendszer a tervek szerint erősítette volna a nemzetbiztonságot (főleg a személyek egyértelmű azonosítása által a vitatott hovatartozású és kevert etnikumú területeken), valamint megszüntette volna a fennálló személyazonosítási rendszerhez kapcsolódó hamis személyazonosságokat.

Az Aadhaar névre keresztelt biometrikus adatokon alapuló személyazonosító rendszer 2010-es indulása óta hatalmas fejlődésen ment keresztül. Jelenleg 1,2 milliárd ember rendelkezik Aadhaar azonosítóval, amely a világ össznépességének 16%-a. A rendszer egy tizenkét számjegyből álló személyi azonosító számra épül, amelyet elektronikusan és plasztik kártyán is megküldenek a regisztrálók számára. A rendszer célja kettős, egyrészt megbízhatóan azonosítani a számsor birtokosát és csökkenteni az azonosítással összefüggő hibákat, másrészt pedig biztosítani, hogy a különböző kormányzati támogatásokat csak az arra jogosultak vehessék igénybe.

A regisztráció nincs nemzetiséghez kötve, bámely indiai lakos jogosult Aadhaar azonosítót létrehozni, ehhez elég bemennie a legközelebbi felvételi központba és megadni a szükséges adatait. Az azonosító létrehozásához szükséges a név, születési idő, a nem, valamint a lakcím megadása, valamint egy arcképet ábrázoló fénykép. A telefonszám és az email cím megadása opcionális, azonban számos szolgáltatás igénybevételének feltétele. A fentieken túlmenően a regisztráció során mind a tíz ujjról mintát készítenek. Ennek oka, hogy Indiában a lakosság jelentős része mezőgazdasági és ipari munkából tartja fent magát és családját, így gyakran előfordul, hogy az ujjak barázdái a kétkezi munkától kopnak, ezáltal meg-nehezítve vagy ellehetetlenítve a pontos azonosítást. Erre tekintettel az ujjnyomat mellett a személyek mindkét íriszéről is mintát vesznek. A minták és a felvett adatok titkosításra, majd továbbításra kerülnek a Központi Személyes Adat Nyilvántartásba (Central Identities Data Repository). Ott a beérkezett adatok összevetésre kerülnek a rendszerben tárolt többi adattal, hogy kiszűrjék a duplikációkat vagy egyéb hibákat. Ezt az ellenőrzést egy ügyintéző felügyeli, így egyetlen jelentkező regisztrációját sem utasíthatja el automatikusan a rendszer emberi felülvizsgálat nélkül. Ezt követően kerül generálásra a véletlenszerű tizenkét számjegyből álló Aadhaar számsor, amely önmagában nem hordoz információt a tulajdonosáról. Abból nem lehet következtetéseket levonni, ellentétben számos más személyazonosításra használt számmal, mint amilyen a magyar lakcímkártyákon szereplő személyi szám is. A rendszer használata 2016-tól kötelező feltétele a kormányzati támogatások és segélyek igénybevételének. Az indiai kormány állítása szerint a rendszer a regiszt-

rált tagok számának növekedésével párhuzamosan eredményez évről évre egyre több megtakarítást az állam számára. Ezzel párhuzamosan számos szolgáltató, köztük bankok és telekommunikációs cégek is Aadhaar azonosításhoz kötötték szolgáltatásuk nyújtását.

Az Aadhaar rendszer öt módon teszi lehetővé a személyek azonosítását. Egyrészt a szolgáltatók vagy a támogatást folyósító intézmények összevethetik a rendszerben tárolt adatokat a személy által megadott és igazolt személyi adatokkal, másrészt amennyiben a személy a regisztráció során megadott telefonszámot vagy email címet, úgy a rendszer arra egyszer használatos jelszót küldhet az azonosítás céljából. Az azonosítás további módja az ujjnyomat vagy az írisz vagy mindkét biometrikus jellemző rendszerben tárolt mintával való összevetése, valamint kétfaktoros hitelesítés, amely során a biometrikus azonosításon túl egy egyszer használatos jelszó is megküldésre kerül a megadott elérhetőségek valamelyikére. Az azonosítás során a rendszer az igényeknek megfelelően kétféle visszajelzésre képes. Az egyik egy igen/nem típusú azonosítás, amely során az ellenőrizendő személy adatai kerülnek összevetésre a rendszerben tárolt adatokkal. A másik egy „ismerd meg az ügyfeled" („know your customer" vagy „KYC") jellegű azonosítás, amely sikeres azonosítás esetén a szolgáltató rendelkezésre bocsátja a személy személyazonosító adatait is. [8]

Egy ilyen hatalmas, biometrikus adatokon alapuló rendszernek robosztus információbiztonsági követelményeknek kell megfelelnie az esetleges adatszivárgások, adatlopások és egyéb incidensek megakadályozása érdekében, máskülönben megrendülhet az emberek rendszerbe vetett bizalma. Az Aadhaar rendszer fejlődését is számos botrány, valamint bírósági ítélet kísérte és szorosan összefonódott az adatvédelemi jog és a személyes adatok védelmének indiai fejlődésével. A rendszer megalkotásának idején Indiában nem volt önálló adatvédelmi törvény, amely az Aadhaar rendszerhez kapcsolódó adatkezelés és adattovábbítást szabályozta volna. 2017-ben a Puttaswamy kontra India ügyben az indiai legfelsőbb bíróság az Aadhaar rendszer vizsgálatával kapcsolatban megállapította, hogy az indiai alkotmány 21 cikke alapján a magánélethez való jog egy alkotmányosan védett alapjog. A döntés mérföldkőnek számított a magánélethez való jog indiai értelmezésében, valamint egy egységes adatvédelmi jogszabály megalkotásának folyamatában, amely feltehetőleg továbbgyűrűző hatást fog gyakorolni az alapvető jogok és személyes szabadságok indiai rendszerére. [9] 2018-ban egy francia információbiztonsági szakértő arról számolt be, hogy több mint húszezer nyilvánosan hozzáférhető Aadhaar számhoz kapcsolódó adatot tárt fel a hozzájuk tartozó bankszámla adatokkal különböző kormányzati honlapokon. [10] Más esetekben újságírók arról számoltak be, hogy bizonyos összegekért hozzáférhettek volna több ezer, vagy esetenként több millió Aadhaar számhoz, valamint a hozzájuk kapcsolódó személyes adatokhoz is. [7] További probléma a regisztráció elhúzódása, amely közvetetten több ember halálát is okozhatta, ugyanis a sikeres regisztrációt megelőzően nem folyósítható az igénylők számára a kormányzati segély. Az elhúzódó regisztráció azonban szélsőséges esetben több hónapig is eltarthat, amely időtartam alatt az igénylők segély nélkül maradnak. Számos esetben számoltak be az Aadhaar azonosítóhoz kapcsolódó személyiséglopásról is, amelynek során a bűnözők más személyek Aadhaar azonosítójával vettek igénybe szolgáltatásokat vagy követtek el visszaéléseket, amelyekkel szemben az áldozatok és a hatóságok gyakorlatilag tehetetlenek. Az áldozatok számára a profiljuk törlését javasolja az Aadhaar rendszer üzemeltetője, azonban ezzel együtt elveszítenék hozzáférésüket számos szolgálatáshoz, segélyhez is. [11]

EU igazságügyi, bűnüldözési és határőrizeti rendszereinek összekapcsolásáról szóló interoperabilitási rendeletek

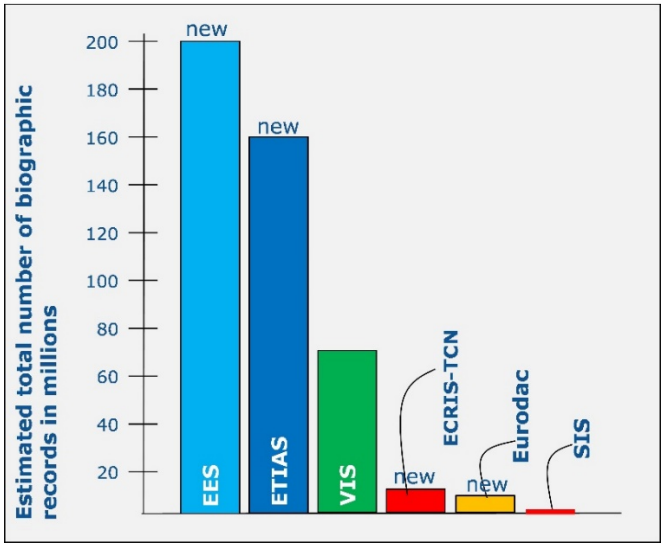
Az Európai Unió külső határaira nehezedő migrációs nyomásra válaszul, valamint a belső biztonság fokozása érdekében mind az Európai Parlament, mind az Európai Bizottság jogalkotási programjában szorgalmazta a már létező határőrizeti és bűnüldözési rendszerek fejlesztését, valamint új rendszerek megalkotását. A hatékonyságnövelés egyik módja a már meglévő rendszerek interoperabilitásának, azaz együttműködésre való képességének megteremtése. Ezáltal a korábban különálló adatbázisok összekapcsolásra kerülnek és a bennük tárolt adatok egyetlen kereséssel elérhetővé válnak az arra feljogosított szervek és személyek számára, ezzel időt és erőforrásokat megtakarítva. Több korábbi felmérés és hatásvizsgálat is megállapította, hogy a nem megfelelő mennyiségű, fajtájú és megbízhatóságú adat megnehezíti a személyiség elleni csalások elleni eredményes küzdelmet. Hosszas előkészítés után 2019. május 20-án fogadta el az interoperabilitás kereteinek megállapításáról szóló 2019/817, valamint 2019/818 számú rendeleteket az Európai Unió (a továbbiakban rendeletek). A két rendeletet együtt kell olvasni, azok felépítése, logikája, megegyezik. A fenti két rendelet mellett kidolgozásra és elfogadásra kerültek azok a további jogi aktusok, amelyek megteremtik az interoperabilitáshoz szükséges keretrendszert. Az interoperabilitás megteremtése érdekében 2019. június 11-én hatályba lépett az Európai Parlament és a Tanács 2019/816 rendelete, amely a harmadik országbeli állampolgárok és a hontalan személyekkel szemben hozott ítéletekre vonatkozó információval egészíti ki az Európai Bűnügyi Nyilvántartási Információs Rendszert (ECRIS-TCN), 2017 decemberében lépett hatályba a tagállamok külső határait átlépő harmadik országbeli állampolgárok belépésére és kilépésére, valamint beléptetésének megtagadására vonatkozó adatok rögzítésére szolgáló határregisztrációs rendszer (EES) létrehozásáról szóló 2017/2226 EU rendelet, biztosítva az összekapcsolhatóságát a vízuminformációs rendszerrel (VIS). Az ujjlenyomatok összehasonlítását szolgáló EURODAC rendszer (603/2013/EU rendelet) felülvizsgálatáról szóló döntés jelenleg az Európai Parlament első olvasatára vár. Az Európai Utasinformációs és Engedélyezési Rendszer (ETIAS) létrehozásra került 2018. októberében a 2018/1240 EU rendelet által. Az ETIAS olyan harmadik országbeli állampolgárokra vonatkozóan került megalkotásra, akik mentességet élveznek a vízumkötelezettség alól. Részükre bevezetésre kerül az utazási engedély, valamint meghatározásra kerülnek az annak kiadására, illetve megtagadására vonatkozó feltételek és eljárások. Megvalósult a Schengeni Információs Rendszer (SIS) alkalmazásának kiterjesztése a jogellenesen tartózkodó harmadik országbeli állampolgárok visszaküldése céljából a 2018 decembere óta hatályos 2018/1860 rendelet által és végezetül 2018 decembere óta hatályos a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző európai uniós ügynökségről szóló (eu-LISA) 2018/1726 EU rendelet.

Amint az az előzőekből is látszik, az interoperabilitás megteremtése egy összetett, több lépcsőből álló jogszabályalkotási folyamat eredménye. A folyamat eredményeként létrehozásra kerül:

- az európai keresőportál („european search portal" vagy „ESP"), amely lehetővé teszi az összes vonatkozó információs rendszer egyidejű keresését és az összes ellenőrzés eredményének egyetlen számítógépes képernyőn történő elérését. A portál nem tárol vagy dolgoz fel új adatokat, és nem változtatja meg a felhasználók hozzáférési jogait;

- a közös biometrikus megfeleltetési szolgáltatás („shared biometric matching service”, a továbbiakban: közös BMS), amely lehetővé teszi a biometrikus adatok (ujjlenyomatok és arcképek) lekérdezését és összehasonlítását a fentebb felsorolt központi rendszerekből (SIS, az Eurodac, VIS, az EES és az ECRIS-TCN);
- a közös személyazonosítóadattár („common identity repository”, a továbbiakban: CIR), amely tárolná az Eurodac-ban, a VIS-ben, az EES-ben, az ETIAS-ban és az ECRIS-TCN-ben rögzített harmadik országbeli állampolgárokkal kapcsolatos alapvető személyi adatokat (név, születési hely és idő) és biometrikus adatokat, lehetővé téve a hatékony személyazonosság ellenőrzést az EU tagállamai területén,
- a többszörös személyazonosságot felismerő rendszer („multiple-identity detector”, a továbbiakban: MID), amely lehetővé tenné a személyek helyes személyazonosságának felderítését, valamint a személyiségcsalások és többszörös személyazonosságok felderítését.

A rendeletek egy kétlépcsős adatbetekintési megközelítést alkalmaznak a CIR-ben történő keresés esetén. A kétlépcsős adatbetekintés során a naplóknak tartalmazniuk kell a nyomozás vagy az ügy nemzeti aktájára való hivatkozást, ami azt jelzi, hogy a lekérdezést terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából kezdeményezték, valamint a lekérdezések célját is. A kétlépcsős adatbetekintés során a keresett személlyel kapcsolatos lekérdezés során először csak egy egyezés megjelölés típusú válasz jelenik meg, amely arra utal, hogy az adat szerepel az EES-ben, a VIS-ben, az ETIAS-ban vagy az Eurodacban. A kétlépcsős adatbetekintés már önmagában adatkezelésnek minősül, ugyanis már a keresett személyre vonatkozó igen/nem találat és az abból levonható következtetések (tehát, hogy a keresett személy megtalálható valamelyik adatbázisban) személyes adatnak minősül. Az új rendszer a becslések szerint 2021-ig 218 millió harmadik országbeli személy személyazonosító és biometrikus adatait tartalmazná. [12]



1. Ábra: A rendszerek által kezelt biometrikus adatok becsült száma millióban. Forrás: Európai Bizottság, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017SC0473&from=EN

Az adatbázisban tárolandó adatok mennyiségének nagysága és jellege miatt egy esetleges adatvédelmi incidens súlyos károkat okozhatna sok személy számára. Amennyiben ezek a személyes adatok rossz kezekbe kerülnének, az adatbázis veszélyes eszközzé válhat az alapvető jogok ellen. Erre tekintettel fogalmazott úgy a rendeletekhez fűzött véleményében az Európai Adatvédelmi Biztos, hogy a rendeletek által létrehozott központosított adatbázis egy olyan pont, ahonnan nincs visszatérés. [13] A rendeletek egy olyan komplex rendszert hoznak létre, amelyre egyaránt vonatkozik az általános adatvédelmi rendelet (2016/679 EU rendelet), a bűnügyi adatvédelmi irányelv (2016/680 EU irányelv), az azt nemzeti jogba átültető jogszabályok, valamint a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról szóló 2018/1725 EU rendelet. A rendeletek szövegükben nevesítik is ezen jogszabályokat, azonban azt már nem határozzák meg, hogy pontosan mely adatkezelési műveletekre mely jogszabály rendelkezései az irányadók.

Az interoperabilitási rendeletek megalkotásának folyamatban szakértőként mind az Európai Adatvédelmi Biztos (EDPS), mind a 29. cikk alapján létrehozott Adatvédelmi Munkacsoport is részt vett és azt számos kritikával illette. Állásfoglalásában az Európai Adatvédelmi Biztos rámutatott, hogy amint arra a rendeletek 40. preambulumbekezdése is utal, az érintett személyek pontos azonosítása céljából végzett adatkezelési műveletek az Európai Alapjogi Charta 7. és 8. cikke által védett alapvető jogaikba való beavatkozásnak minősül, ezért ezeket az új adatkezelési műveleteket a Charta 52. cikk (2) bekezdés alapján alá kell vetni a szükségesség arányosság tesztnek. Ennek során kiemelt jelentősége van az adatkezelések szükségességét alátámasztó, kellően konkrétan megfogalmazott indokra és az azt alátámasztó bizonyítékokra. A rendeletek indokolása ugyan megnevezi a többes személyazonosságok, a személyazonosság csalások, valamint a terrorizmus elleni küzdelmet, azonban elmulasztja számszerűsíteni a hivatkozott jelenségek mértékét, amely megnehezíti a teszt elvégzését. Önmagában az „illegális migráció elleni küzdelem és a biztonság magas szintjének biztosítása" túl tág megfogalmazás és ezen nem változtat az sem, az uniós jogszabály a rendelkezés további megfogalmazását a tagállami jogalkotásra bízza, mint ahogyan a rendeletek 20. cikke teszi. Ez semmiképpen sem felel meg az Európai Unió Bírósága (CJEU) által a Digital Right Ireland ügyben lefektetett korlátozottság és pontosan körülhatároltság követelményeinek.

Az Európai Adatvédelmi Biztos felhívta továbbá a figyelmet a beépített és alapértelmezett adatvédelem elvének alkalmazására a rendszer tervezése és kialakítása során és annak alapján a megfelelő adatvédelmi biztosítékok beépítését. [13] Mind az Európai Adatvédelmi Biztos, mind a 29. cikk szerinti munkacsoport felhívta továbbá a figyelmet arra, hogy adatbiztonsági szempontból egy központosított adatbázis létrehozása növeli a visszaélés és az adatok jogellenes felhasználásának, valamint az eredeti funkción való túlterjeszkedés („function creep") kockázatát. [14] Tekintettel arra, hogy az adatbázisokhoz a tagállamok rendvédelmi és határvédelmi szervei is hozzáféréssel fognak rendelkezni, a hozzáférési pontok száma ezzel több ezerre lesz tehető, amely súlyos biztonsági kockázatot jelent. Ennek ellenére a rendeletek 42. cikke csak a rendszereket kifejlesztő és irányító eu-Lisa számára fogalmaz meg konkrét adatbiztonsági előírásokat, míg tagállamok, az Europol és az ETIAS központi egysége részére csak azokkal egyenértékű intézkedések meghozatalát

írja elő. Ez a megfogalmazás azonban könnyen eltérő szintű adatbiztonsági intézkedések gyakorlati megvalósításához vezethet.

ADATVÉDELMI MEGFONTOLÁSOK

A magyar adatvédelmi jog, valamint az Európai Unió általános adatvédelmi rendelete alapján személyes adatnak minősül az azonosított vagy azonosítható személyre vonatkozó bármely információ. Ebből kifolyólag, mind a biometrikus adat, mind az abból leképzett sablonok kezelésének meg kell felelnie az adatvédelmi jog által meghatározott elveknek és előírásoknak. A biometrikus adatok az általános adatvédelmi rendelet alapján a személyes adatok különleges kategóriájába tartoznak és kezelésükre további szabályok vonatkoznak. A biometrikus adatok kezelése csak abban az esetben jogszerű, amennyiben az adatkezelés rendelkezik egy 6. cikk szerinti jogalappal és attól függetlenül azonosításra és megjelölésre kerül legalább egy, a 9. cikk (2) bekezdésében felsorolt valamely speciális feltétel is. A 6. cikk szerinti választott jogalapnak és a 9. cikk szerinti speciális esetkörnek nem kell egymással összefüggésben állnia. [15]

A biometrikus adatok fokozott védelmének indoka az, hogy a biometrikus adatok közvetlenül kapcsolódnak az érintetthez, csak rájuk jellemzőek és állandók, ezért nem, vagy csak nehezen változtathatók meg, nem tagadhatók le, ezért visszavonhatatlanok. [16] Éppen ezért a biometrikus adatokkal kapcsolatos bármely jogsértés veszélyezteti a biometrikus adat további felhasználását és felhasználhatóságát, amelyekre vonatkozóan nincs lehetőség a jogsértés következményeinek enyhítésére.

Az Európai Unió Alapjogi Chartájának 8. (1) bekezdése kimondja, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. A személyes adatokat csak az érintett személy hozzájárulása vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Az 52. cikk (1) bekezdése azonban rögzíti, hogy a Chartában elismert jogok és szabadságok gyakorlása csak a törvény által, és a jogok lényeges tartalmának tiszteletben tartásával korlátozhatók. Az arányosság elvére figyelemmel, korlátozásukra csak akkor és annyiban kerülhet sor, ha és amennyiben az elengedhetetlen és ténylegesen az Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálja.

Magyarország Alaptörvénye szintén védelemben részesíti a személyes adatokat. Az alaptörvény VI. (3) bekezdése alapján, mindenkinek joga van személyes adatai védelméhez. A személyes adatok védelméhez fűződő jog tehát alkotmányos alapjog. Magyarország alkotmányos hagyományai, valamint az Alkotmánybíróság töretlen gyakorlata és az Alaptörvény jelenleg is hatályos rendelkezése alapján alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható. A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) számos állásfoglalásában következetesen képviselte azt az álláspontot, hogy a biometrikus adatok kezelése során érvényesülnie kell a szükségesség és arányosság elvének. Egy alkotmányjogi panasszal kapcsolatos ügy során elkészített szakértői véleményében a NAIH hivatkozással az Irányelv 29. cikke alapján létrehozott Adatvédelmi Munkacsoport biometrikus technológiák terén történt fejleményekről szóló 3/2012. számú véleményére (WP193), kifejti, hogy a biometrikus rendszerek alkalmazása felveti az arányosság kérdését a feldolgozott adatok

tekintetében. Mivel a biometrikus adatok csak akkor kezelhetők, ha megfelelőek, relevánsak és nem túlzott mértékűek, ezért minden esetben mérlegelni kell a kezelt adatok szükségességét, arányosságát, valamint azt, hogy az adatkezelés által elérni kívánt cél megvalósítható lenne-e a magánszférát kevésbé korlátozó módon. Ezért egy biomerikus rendszer arányosságának elemzése során „előzetesen mérlegelni kell, hogy a rendszer szükséges-e a meghatározott igény kielégítéséhez, azaz használata elengedhetetlen-e ehhez, vagy inkább annak legkényelmesebb vagy legköltséghatékonyabb módja. Egy második megfontolandó tényező az, hogy a rendszer valószínűleg elég hatékony lesz-e az adott igény kielégítésében, tekintettel a használni tervezett biometrikus technológia sajátos jellemzőire. A harmadik mérlegelendő szempont, hogy arányos-e az elvárt előnyökkel, ha a rendszer miatt sérül a magánélet védelme. Ha az előnyök viszonylag kisebbek, például kényelmesebb az eljárás vagy kismértékű költségmegtakarítás érhető el, akkor nem helyénvaló, ha sérül a magánélet védelme. Egy biometrikus rendszer megfelelőségének értékelése során a negyedik szempont annak megfontolása, hogy a magánéletbe kisebb mértékben beavatkozó módszerek elérhetnék-e a kívánt célt" [17] Abban az esetben, ha a kívánt cél más, a magánéletbe kisebb mértékben beavatkozó módszerrel is elérhető, úgy az adatkezelőnek annak megvalósítására kell törekednie.

A biometrikus adatok kezelésének a fentieken túlmenően természetesen meg kell felelnie a személyes adatok kezelésére vonatkozó elveknek és előírásoknak. Így az adatkezelésnek, jogszerűnek, tisztességesnek, valamint az érintettek számára átláthatónak kell lennie. A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet és azoknak az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk. A kezelt biometrikus adatoknak továbbá pontosnak és szükség esetén naprakésznek kell lenniük, a pontatlan személyes adatokat pedig törölni, vagy helyesbíteni kell.

KÖVETKEZTETÉSEK

A fenti példákon keresztül megállapítható, hogy a biometrikus adatok rendkívül sokoldalúan felhasználhatók személyazonosítás céljából. Kijelenthető, hogy a technológiai fejlődés eredményeképp már csak a politikai akarat és a jogszabályi környezet határozza meg a biometrikus azonosításra épülő rendszerek korlátait. Az indiai Aadhaar rendszer például pozitív példája annak, hogy hogyan lehet a világ legnépesebb működő demokráciájában viszonylag rövid idő alatt bevezetni egy ilyen személyazonosító rendszert, valamint, hogy egy ilyen rendszer és az azzal járó digitális megoldások milyen járulékos előnyökkel járnak az azt kiépítők számára. Indiában a felmérések szerint csökkent a kormányzati segélyekhez kapcsolódó csalások száma és ezáltal a költségvetésre nehezedő teher is, ami lehetővé tette a tényleges rászorulóknak járó összegek folyamatos emelését is. Azonban ugyan ilyen fontos a negatív tapasztalatok, példák elemzése is. A személyes adatok – köztük a biometrikus adatok – nem megfelelő védelme fizikai, vagyoni vagy nem vagyoni károkhoz vezethet a rendszerben tárolt személyek számára.

Amint az a biometrikus azonosításhoz kötött SIM kártya regisztráció kapcsán is ismertetésre került, a biometrikus azonosítás nem minden esetben éri el önmagában a kitűzött célt. A személyazonosítás megnövelt pontossága pedig nem minden esetben felel meg a szükségesség arányosság követelményének. Mivel a magánélethez és a személyes adatok védelméhez fűződő jog a legtöbb államban nemzetközi szerződések és az alkotmány által

védett alapvető jog, így a biomterikus adatok kezelése esetén szükségszerű ennek a tesztnek az elvégzése. Különösképp igaz ez az Európai Unió intézményeire és annak tagállamaira, köztük Magyarországra. A NAIH gyakorlatában következetesen érvényre juttatta a biometrikus adatok fokozottabb védelmét és számos esetben írta elő adatkezelők számára a biometrikus azonosítás helyett (NAIH-6300-2/2012/V.) más, a személyhez fűződő jogokat kevésbé korlátozó módszerek alkalmazását.

Már ma is számos olyan személyazonosító szolgáltatás vehető igénybe a fogyasztók számára, amely biometrikus adatok felhasználására épül. Ilyenek például az okostelefonokba vagy laptopokba épített kapacitív ujj-nyomat érzékelők. Ezen szolgáltatások a legtöbb esetben azonban nem kötelezőek a fogyasztók számára, akik az általános adatvédelmi rendelet alapján kifejezett hozzájárulásukkal felhatalmazhatják a szolgáltatókat ezen adatok kezelésére. Más a helyzet azonban olyan esetekben, amikor az adatkezelő és az érintettek között aszimmetrikus viszony van. Ilyen lehet egy munkáltató és a munkavállaló, vagy az állam és az állampolgárok viszonya. Ezekben az esetekben fokozottan érvényesül a szükségesség és arányosság, hiszen a kifejezett hozzájárulás, mint jogosító körülmény az aszimmetrikus viszonyra tekintettel nem lehet jogszerű. Ebből adódóan például munkahelyi körülmények között csak kifejezetten indokolt esetben ad teret az adatvédelmi hatóság a kötelező biometrikus azonosításnak, mint például egy gyógyszeripari kutató laborítórium, ahol vírusokat is tárolnak, vagy egy erőmű.

Az általános adatvédelmi rendelet alapján, a biometrikus adatok kezelhetők jelentős közérdekre történő hivatkozással is, amennyiben az azt előíró uniós jog vagy tagállami jog arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő. A világon megfigyelhető általános jelenség, hogy a közterületeket egyre több, egyre jobb minőségű képet készítő, arcfelismerésre is képes kamera figyeli meg, amelyek másként pótolhatatlan segítséget nyújtanak a bűnüldöző szerveztek részére a bűncselekmények felderítése során. Ezek a kamerák azonban alkalmasak arra is, hogy az állam megfigyelje állampolgárait. Fokozottan igaz ez a biometrikus azonosítók kezelése esetén. Amint arra véleményében mind a NAIH, mind az Európai Adatvédelmi Biztos és a 29. cikk szerinti Adatvédelmi Munkacsoport kitért, a biometrikus azonosítók elválaszthatatlanok az érintettektől, így azok elvesztése, kompromittálódása visszafordíthatatlan következményekkel járhat az érintettek számára. Erre tekintettel nevezte az Európai Adatvédelmi Biztos a különböző Európai Uniós határvédelmi, bűnüldözési és igazságszolgáltatási rendszereinek összekapcsolását egy olyan pontnak, ahonnan nincs visszatérés. Mind a jelenlegi, mind a jövőben megalkotandó biometrikus adatbázisok felé elvárás az, hogy létrehozásuk indoka, kellőképpen konkrétan és megfelelően alátámasztottan igazolásra kerüljön. Egy homályosan, vagy túl általánosan megfogalmazott indok, egy jövőbeli fenyegetésre való hivatkozás könnyen a célhoz kötött adatkezelés és a készletező adatgyűjtés tilalmába ütközhet. A bűnügyi nyilvántartás jelenleg is tartalmaz biometrikus adatokat Magyarországon. A nyilvántartást szabályozó törvény azonban részletesen szabályozza a nyilvántartott biometrikus adatok körét, valamint felhasználásuk célját, megőrzésük idejét és részletesen szabályozza az érintetteket megillető jogokat, valamint az őket védő garanciális szabályokat.

Az Európai Unió tagállamai közül Franciaország kívánja először bevezetni az arcfelismerésre és biometrikus adatokra épülő széleskörű személyazonosítási rendszert (Alicem), azonban a francia adatvédelmi hatóság (CNIL) már jelezte a jogalkotó számára fenntartásait a tervezettel kapcsolatban, ugyanis álláspontja szerint annak megvalósítása uniós jogba ütközik és nemzetközi kötelezettségekbe ütközik. Amennyiben más uniós tagállamok is hasonló rendszer bevezetését terveznék, úgy feltehetőleg a nemzeti adatvédelmi hatóságok ott is hasonló következtetésre jutnának. Ennek oka, hogy az Európai Unió tagállamaira vonatkozó nemzetközi szerződések, uniós jogszabályok és nemzeti jogszabályok olyan komplex rend-szert alkotnak, amelyek jelentősen behatárolják ezeknek a rendszereknek a megvalósíthatóságát, valamint meghatározzák az érvényesítendő elveket és garanciákat is. Máig ható elvi éllel jelentette ki például a magyar Alkotmánybíróság, hogy a korlátozás nélkül használható, általános és egységes személyazonosító jel alkalmazása alkotmányellenes, mert az az érintetett az adatkezelővel szemben kiszolgáltatottá teszi, egyenlőtlen helyzetet teremtve ezzel. Erre tekintettel egy olyan általános személyazonosító rendszer, amely a lakosság minden tagjára kiterjedően tartalmazza az érintettek biometrikus adatait egyelőre nem valószínű Magyarországon.

FELHASZNÁLT FORRÁSOK

[1] BALLA J. „Biometrikus adatok a személyazonosításban” megjelent „A változó rendészet aktuális kihívásai” című konferenciakötetben, Pécs, 2013. pp. 287-294

[2] KOVÁCS T., MILÁK I., OTTI CS. „A biztonságtudomány biometriai aspektusai” megjelent „A biztonság rendészettudományi dimenziói – változások és hatások” című konferenciakötetben, Pécs, 2012. pp. 485-496

[3] “Thailand to require biometric registration for SIM cards” [Online]. Elérhető: https://asia.nikkei.com/Politics/Thailand-to-require-biometric-registration-for-SIM-cards [Hozzáférés dátuma: 2021 március 12.].

[4] “101: SIM Card Registration” [Online]. Elérhető: https://privacyinternational.org/explainer/2654/101-sim-card-registration [Hozzáférés dátuma: 2021 március 12.].

[5] “Mandatory registration of prepaid SIM cards - Addressing challenges through best practice” [Online]. Elérhető: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf [Hozzáférés dátuma: 2021 március 12.].

[6] “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” [Online]. Elérhető: https://www.undocs.org/A/HRC/29/32 [Hozzáférés dátuma: 2021 március 12.].

[7] „Lessons from Aadhaar: Analog aspects of digital governance shouldn’t be overlooked” [Online]. Elérhető: https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-09/lessons_from_aadhaar.pdf [Hozzáférés dátuma: 2021 március 12.].

[8] https://uidai.gov.in/ecosystem/authentication-ecosystem/operation-model.html [Online] [Hozzáférés dátuma: 2021 március 12.].

[9] https://globalfreedomofexpression.columbia.edu/cases/puttaswamy-v-india/ [Online] [Hozzáférés dátuma: 2021 március 12.].

[10] https://timesofindia.indiatimes.com/business/india-business/vigilante-hacker-flags-security-concerns-in-aadhaar-govt-websites-again/articleshow/63298630.cms [Online] [Hozzáférés dátuma: 2021 március 12.].

[11] https://www.moneylife.in/article/aadhaar-nightmares-coming-true-how-ameya-dhapre-is-enduring-living-hell-with-his-aadhaar-report/59034.html [Online] [Hozzáférés dátuma: 2021 március 12.].

[12] „Document 52017SC0473 - Az interoperabilitási rendeleteket kísérő hatástanulmány" [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019R0818&from=EN [Hozzáférés dátuma: 2021 március 12.].

[13] „Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems" [Online]. Elérhető: https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf [Hozzáférés dátuma: 2021 március 12.].

[14] „Opinion on Commission proposals on establishing a framework for interoperability - wp266" [Online]. Elérhető: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624198 [Hozzáférés dátuma: 2021 március 12.].

[15] Miklós G., Kovács T. „A biometrikus adatok kezelésének jogi szabályozása," Hadmérnök, XIV. kötet 1. szám, 2019., Elérhető: http://www.hadmer-nok.hu/191_01_miklos.pdf

[16] http://public.mkab.hu/dev/dontesek.nsf/0/99aeb34aebaa6c68c1257dda005de077/$FILE/IV_6_7_2015_NAIH_allasfoglalas.pdf [Online] [Hozzáférés dátuma: 2021 március 12.].

[17] „3/2012. sz. vélemény a biometrikus technológiák terén történt fejleményekről" [Online]. Elérhető: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_hu.pdf [Hozzáférés dátuma: 2021 március 12.].

[18] Berek L., Berek T., Berek L., Személy- és vagyonbiztonság, Budapest: Óbudai Egyetem, 2016, p. 174.

CORPORATE SECURITY AND THE DARK WEB

VÁLLALATBIZTONSÁG ÉS A DARK WEB

GULYÁS Attila[1]

Abstract

The changes that have taken place in recent decades have posed significant challenges to companies. Responses to new challenges have not only yielded positive results, but there have also been new risks to which companies need to provide new types of responses. New tools and technologies that appeared in the field of information technology revolutionized production technologies, and the role of information as a corporate asset increased. This wealth is threatened by new, unprecedented risks, such as the growing use of Dark Web technology, which, with the anonymity it provides, challenges corporate security professionals who can only meet the challenges with special training and preparedness. The aim of the study is to highlight the possible meeting points between information security and the Dark Web.

Keywords

security,dark web,information asset, crypto currency, hacker

Absztrakt

Az elmúlt évtizedekben a környezetünkben lezajlott változások jelentős kihívások elé állították a vállalatokat. Az új kihívásokra adott válaszok nem csak pozitív eredménnyel jártak, hanem új kockázatok is jelentkeztek, amelyekre a vállalatoknak új típusú korábban nem alkalmazott válaszokat kell adniuk. Az informatikai területén megjelent új eszközök, technológiák forradalmasították a termelési technológiákat, az információ mint vállalati vagyon szerepe felértékelődött. Ezt a vagyont olyan új, eddig nem látott kockázatok fenyegetik, mint az egyre elterjedtebb Dark Webes technológia, amely az általa biztosított anonimitással kihívás elé állítja a vállalati biztonsági szakembereket, akik csak speciális képzettséggel és felkészültséggel tudnak megfelelni a kihívásoknak. A tanulmány célja, hogy rávilágítson az információbiztonság és a Dark Web lehetséges találkozási pontjaira.

Kulcsszavak

biztonság, dark web, adatvagyon, kriptovaluta, hacker, darknet piac

[1] agulyas66@gmail.com | ORCID: 0000-0001-5645-144X | Retired military officer, PhD student, Óbuda University Doctoral School on Safety and Security Sciences | nyugállományú hivatásos katona, doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Az elmúlt évtizedekben a környezetünkben lezajlott változások jelentős kihívások elé állították a vállalatokat. Az új kihívásokra adott válaszok nem csak pozitív eredménnyel jártak, hanem új kockázatok is jelentkeztek, amelyekre a vállalatoknak új típusú korábban nem alkalmazott válaszokat kell adniuk. Az informatikai területén megjelent új eszközök, technológiák forradalmasították a termelési technológiákat, az információ mint vállalati vagyon szerepe felértékelődött. Ezt a vagyont olyan új, eddig nem látott kockázatok fenyegetik mint az egyre elterjedtebb Dark Webes technológia, amely az általa biztosított anonimitással kihívás elé állítja a vállalati biztonsági szakembereket, akik csak speciális képzettséggel és felkészültséggel tudnak megfelelni a kihívásoknak. A tanulmány célja, hogy rávilágítson az információbiztonság és a Dark Web lehetséges találkozási pontjaira.

VÁLLALAT ÉS INFORMÁCIÓS VAGYON

Az elmúlt évtizedekben a környezetünkben lezajlott változások következtében jelentős változásokon mentek át hazánkban a vállalatok [1].

Említés szintjén néhány a kihívások közül:

- A határokon átívelő globalizáció új felfogást és szemléletet követel meg
- A tudásalapú társadalomban megnőtt a szerepe a szellemi tőkének
- A vállalati informatikai rendszereknek szervesen kell kapcsolódniuk nemzetközi hálózatokba, a világhálóba és annak felismerése, hogy a hagyományos papír alapú irodai munka egyre inkább elektronikussá válik annak előnyeivel és hátrányaival

Ezekre a kihívásokra adott válaszok azonban nem csak pozitív eredményeket hoztak, nem csak a hatékonyságot és az eredményességet növelték, hanem új kockázatokkal is járnak. A vállalatirányításnak ezekre az új fenyegetésekre is meg kell találniuk a választ.

A vállalatokat valamilyen feladatra hozzák létre. Ez a vállat tevékenységének alapja, létrehozásának értelme. Ebben a vonatkozásban nem fontos, hogy az adott vállalat kereskedelmi vagy más egyéb céllal került-e létrehozásra.

A vállalat küldetése tulajdonképpen annak a megjelenítése, hogy a vállalat ezt a célt milyen módon kívánja teljesíteni. A küldetésében tükröződnie kell a működési területének, belső működési elveknek, a külső gazdasági környezettel kiépítendő kapcsolatoknak.

A fentiekből következik, hogy az üzleti követelményeknek kell alárendelni minden vállalaton belül végbemenő tevékenységet, amelyek az üzleti cél elérése érdekében szükségesek.

A COBIT kocka alapján az alábbi üzleti követelményekről beszélhetünk:

- Minőség: magas színvonal, gazdaságosság, időbeni teljesítés
- Megbízhatóság: hatékonyság, kiszámíthatóság, jogszabályi megfelelőség
- Biztonság: bizalmasság, sértetlenség, rendelkezésre állás (MSZ ISO/IEC 27001)

A tanulmány szempontjából kiemelendő, hogy a biztonság üzleti követelmény, ebből adódóan az üzleti célok biztonság nélkül nem teljesíthetőek.

Az információbiztonság nem azonos az informatikai biztonsággal. Az előbbi egy tágabb szélesebb fogalom. Amíg az informatikai biztonság az informatikai rendszerek biztonságát jelenti az egyértelmű hozzáférés hitelesítéssel, tűzfalrendszerekkel, illetve vírusirtó szoftverek telepítésével, illetve futtatásával, addig az információs biztonság magába foglalja a vállalati adatvagyon védelmét beleértve a stratégiai partnerek, beszállítók, pénzügyi

partnerek részéről jelentkező esetleges nem szándékos fenyegetések elleni intézkedéseket is. A saját belső információk, a partnerek, ügyfelek adatai bizalmasságának, sértetlenségének és vagy rendelkezésre állásának sérülése anyagi, erkölcsi, reputációs és egyéb járulékos károkkal járhat, nem beszélve a törvényi kötelezettség megszegéséért járó büntetés, illetve szankció következményeiről. A vállalati információ vagyon védelme érdekében általánosságban az információ és információhordozók kezelése kerül szabályozásra. Ebből a szempontból érdektelen, hogy milyen az információ megjelenési formája. A helyes védelem érdekében meg kell határozni a védendő információkat, a lehetséges külső-belső fenyegetéseket, ezek bekövetkezésének valószínűségét és az ezek kivédéséhez szükséges szabályozást és eszközrendszert. (ISO/IEC 27002) [2].

Az információvédelem nem korlátozódhat az informatikai és ügyviteli rendszerek védelmére a védelmi intézkedéseknek ki kell terjedniük az adatok feldolgozására, kezelésére, átadására és tárolására, amely így már magában foglalja a fizikai biztonságot, a humán erőforrás biztonságát, a hozzáférés-jogosultságkezelést és az üzletmenet folytonos működésének biztosítását. Gyakori hiba, hogy a védelmi intézkedések szegmensenként kerülnek kidolgozásra és végrehajtásra ugyanakkor ez a megoldás nem hatékony, átfedések, hiányosságok alakulhatnak ki, amelyek ellen a rendszerszemléletű holisztikus megközelítésű komplex védelmi rendszer kialakítása jelenti a kiutat.

1. ábra: Információbiztonsági irányítási rendszer. Forrás: Oroszi (2014), Információbiztonsági stratégia és vezetés, Budapest: Nemzeti Közszolgálati Egyetem p.9.

Az 1. számú ábrán látható Információbiztonsági irányítási rendszer vázlatán jól látható, hogy a technológiai és az adminisztratív információbiztonsági intézkedések összehangolásával egymással összefüggő komplex rendszer alakítható ki. Egy ilyen rendszer kialakításával egy szervezet képes a védelmi intézkedések és kontrolok kialakítására és hatékony alkalmazására.

A rendszer alappillére az információbiztonsági politika, illetve egy megfelelő információbiztonsági stratégia kidolgozása és annak megvalósításáért felelős szervezet felállítása, továbbá a megfelelő irányítás, vezetés, valamint a hatékony működés figyelemmel kísérése és visszaellenőrzése.

A vállalti adatvagyon több területen is értéket teremthet, ezek a teljesség igénye nélkül az alábbiak lehetnek: [3]

- Hatékony üzleti döntéstámogatás: ügyfelek, termékeink, szolgáltatásaink és a versenytársak és piacaik jobb megismerésére, a saját pénzügyi folyamatok nyomon követésére, az emberi és egyéb erőforrások jobb és hatékonyabb kihasználására.

- Folyamat, termék és szolgáltatásoptimalizálás: a rendelkezésre álló adatvagyon birtokában lehetőség van a vállalati folyamatok, termékek és szolgáltatások optimalizálására. Ezáltal versenyképesebb termék vagy szolgáltatás előállítására, biztosítására

Néhány példa a konkrét felhasználásra:

- A gyártás: hibás termékek arányának csökkentése, minőségjavítás, intelligens leállás tervezés a gépek kopásának folyamatos figyelemmel kísérésével, anyag, eszköz, idő megtakarítás
- Üzleti folyamatok javítása, optimalizálása: adatalapú kockázatbecslés, csalás, visszaélés felfedése
- Raktározás, szállítás: szállítási útvonal optimalizáció, automatizált raktárkészlet, költség optimalizáció
- Értékesítés: ügyfélmegtartás, elvándorlás előrejelzés, személyre szabott termékajánlás, ügyfél elégedettség mérés stb..

A fenti felsorolás kellőképpen érzékelteti a vállalati adatvagyon jelentőségét, ebből adódóan ennek sérülése, elérhetetlenné tétele, vagy megváltoztatása a vállalati cél teljesítésének időleges, vagy akár szélsőséges esetben teljes meghiúsulását okozhatja, nem beszélve az esetleges erkölcsi kárról, amelynek mértéke esetenként felbecsülhetetlen és helyreállítása jóval több időt vesz igénybe, mint valamely fizikai káresemény.

A vállalati információvagyont a teljesség igénye nélkül az alábbi veszélyek fenyegethetik:

- hibás szoftveralkalmazások (sebezhetőségek, javító csomagok hiánya)
- szakszerűtlen információs technológiai tervezés, vagy üzemeltetés
- jogosulatlan hozzáférés, illetve használat
- meg nem engedett, ellenőrizetlen, vagy nem kompatibilis szoftverhasználat
- vírusok, kémprogramok, zsaroló programok
- a hálózat szándékos túlterhelése
- nem megfelelő archiválási politika
- felkészületlen személyi állomány
- szándékos belülről eredő, bennfentes személy támadása, károkozása
- szerződéses partner, együttműködő szándékos, vagy felelőtlen információkezelése

A tanulmány továbbiakban arra próbál választ adni, hogy a vállalati adatvagyont veszélyeztető fentebb felsorolt tevékenységek eredménye hogyan és milyen formában jelenhet meg a Dark Weben. Leginkább arra keresi a választ, hogy egy vállalatnak szükséges-e monitoroznia a Dark Webet, ha igen akkor azt saját erőből, vagy esetleg outsourcing útján más erre szakosodott vállalkozások szolgáltatásainak felhasználásával. Az erre vonatkozó döntésnek mik az előnyei és hátrányai, milyen tényezőket figyelembe venni a döntés meghozatalkor.

Mielőtt ez a kérdés részletes tárgyalásra kerülne elengedhetetlen, hogy az olvasó megismerkedjen a Dark Web lényegével és azon zajló – a tanulmány szempontjából releváns – folyamatokkal.

A DARK WEB

Mielőtt a Dark Web mibenlétének tisztázására sor kerülne néhány alapfogalom értelmezése elengedhetetlen. Még a szakirodalomban is előfordul, hogy az Internet és a World Wide Web fogalmát felcserélik, vagy egyiket a másikkal helyettesítik, holott az Internet tulajdonképpen hálózatok hálózatának bonyolult rendszere, míg a World Wide Web (a továbbiakban: WWW, vagy web) csak egyike a számos protokollnak, amelyeken keresztül a zajlik a kommunikáció az Interneten. Ez a nyelv a HTML nyelv, amelyet 1989-ben alkotott meg Tim Berners-Lee, majd 1990-ben megírta az első böngésző programot. Az internet böngésző 1991-ben indult el világhódító útjára [4, pp.32,33].

A Word Wide Web alapvetően három fő részre osztható fel. A könnyebb érthetőség érdekében a felosztást gyakran a jéghegy hasonlattal szoktak szemléltetni (2. ábra).

Az első rész a Nyílt Web, amelyre a „Clear Net", vagy „Surface Web", esetleg „Open Net" néven szokás hivatkozni. Ez a web arra a részére vonatkozik, amely bárki számára elérhető és hozzáférhető mindössze Internet hozzáférés, és valamilyen böngésző szükséges hozzá. Az ismert kereső motorok, mint „Google", vagy a „Bing" ezeket az oldalakat a robotjaik által bejárják, feldolgozzák, indexelik és a keresését indító felhasználó számára találatként visszaadják az oldal elérhetőségét. Ilyen típusú oldalból több milliárd érhető el és számuk napról napra növekszik.

A következő rész, amelyre valódi magyar kifejezést nem igazán alkalmaznak a „Deep Web", amely gyakorlatilag hasonló a Nyílt Web-hez, de az ebbe a kategóriába sorolható oldalak csak valamiféle belépési jogosultság ellenőrzést követően érhetők el. Ilyenek lehetnek vállalati adatbázisok, vagy hálózatok, egészségügyi adatok, vagy akár az olvasó email fiókja. Ezek az oldalak már alap esetben nincsenek nyilvántartva a kereső motorok adatbázisaiban, az oldalak tartalmára nem lehet rákeresni. Az ilyen típusú oldalból is ugyancsak több milliárd található szerte az világhálón.

Az előbbi két kategóriában közös vonás, hogy a felhasználók, a weboldalakat meglátogatók nyomon követhetők, viszonylag egyszerűen beazonosíthatók, tartózkodási helyük megállapítható.

Végül a harmadik rész a „Dark Web", Dark Net, vagy „Sötét Web". Ez az Internet olyan része, amely hagyományos eszközökkel már nem érhető el. Az itt tárolt tartalmak csak speciális böngészőkkel, kifejezetten erre a célra fejlesztett szoftverekkel érhetők el. Azonban ez a szegmens korántsem egységes, ugyanis több szoftver megoldás is létezik, amelyeknek a célja ugyan az nevezetesen: az anonimitás, a követhetetlenség és lenyomozhatatlanság biztosítása. Ezek alapján meg kell említenünk, a TOR [5] hálózatot, az I2p [6], a Freenet [7], vagy az egyébként magyar vonatkozással is rendelkező ZeroNet [8] rendszereket. Ezek a rendszerek egyenként mind egy részét fedik a Dark Webnek, és közöttük alapesetben nincs átjárhatóság.

Jelentős eltérés a nyílt Internettel szemben, hogy a Dark Weben nem működnek érdemi kereső motorok. Tekintettel arra, hogy ezek az oldalak a támadások kivédése érdekében általában valamilyen módszerrel blokkolják a közvetlen hozzáférést, amely lehet CAPTCHA, vagy regisztrációhoz kötött belépés a kereső robotok mint a már említett Google vagy Bing [9] nem tudják indexelni az oldal témáját illetve tartalmát.

A meglévő keresők leginkább a weboldalak készítőinek önkéntes regisztrációján, illetve a linkgyűjtemények alapján épített adatbázisokból építkeznek. Ez a körülmény jelentősen megnehezíti a Dark Web feltérképezését és a tájékozódást ebben a viszonylag új közegben.

Az alábbi ábra a World Wide Web felosztását szemlélteti, a már említett jéghegy hasonlat bemutatásával.

2. ábra: A World Wide Web felosztása. Forrás: https://www.webhostingsecretrevealed.net/wp-content/uploads/our-web.jpg

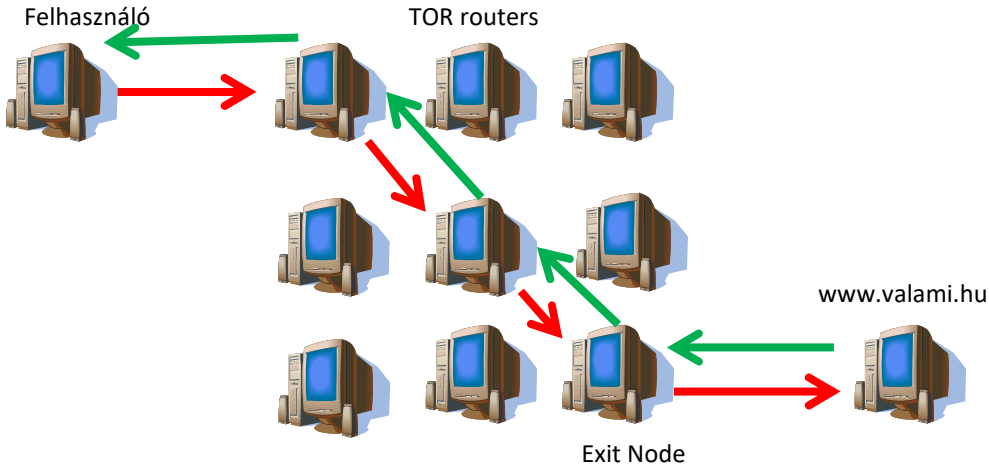
Eredetileg a Dark Web (a TOR rendszer elődje) egy rejtett réteg volt az 1970-es években az amerikai ARPANET hálózaton, és azzal a céllal hozták létre, hogy titkosított összeköttetést biztosítson az egyes munkaállomások között. A Dark Web tudott adatokat fogadni az ARPANET-től, de ugyanakkor láthatatlan maradt annak munkaállomásai számára. Időközben az ARPANET Internetté nőtte ki magát és a Dark Web bárki számára elérhetővé vált, mi több népszerűsége napról napra növekszik.

A Dark Web eléréshez a felhasználónak le kell töltenie és telepítenie valamelyik szoftvert a fentebb felsoroltak közül. Tekintettel arra, hogy az elérhető szoftverek közül a TOR rendszer rendelkezik a legnagyobb felhasználó táborral és a legtöbb úgynevezett rejtett szolgáltatással (a TOR rendszerben „hidden service”-nek nevezik a rendszer segítségével létrehozott weboldalakat), ezért ennek telepítése és használata javasolt. A továbbiakban a Dark Web megjelölés alatt ezt a rendszert takarja.

A TOR a The Onion Router kifejezés első betűiből összeállított mozaikszó. Az „onion router” kifejezés arra utal, hogy a TOR rendszeren belül az adatok a hálózat egyes elemi között titkosítva rétegesen egymásra építve kerülnek továbbításra és a köztes állomások egy titkosított réteget lefejtve jutnak hozzá a következő munkaállomás címéhez és oda továbbítják a megmaradt tikosított adatcsomagot. A következő állomás szintén lefejt egy réteget és ismét továbbítja a csomagot a következő routerhez, amíg csak el nem jut a célállomáshoz, ahol az utolsó réteget lefejtve megmarad az eredeti adat.[10] Ezzel a módszerrel megoldható, hogy a csomag eredete ismeretlen marad, és az egyes állomások nincsenek tudatában annak milyen adatot továbbítanak. A TOR rendszer kommunikációja természetesen jóval összetettebb, de jelen cikknek nem célja a működés részletekbe menő ismertetése. A rendszer egyik sajátságos vonása, hogy úgynevezett rejtett szolgáltatást (weboldalt)

bárki létrehozhat a rendszeren, anélkül, hogy bármilyen azonosító adatot hátrahagyna így a létrehozó kiléte, illetve földrajzi elhelyezkedése titokban marad [11]. A másik különlegesség, hogy a létrehozott weboldal alapesetben csak addig lesz elérhető a rendszeren, amíg a létrehozója a csatlakozik a rendszerhez, hiszen a weboldalt a számítógépén futó web szerverén hozta létre. Ennek köszönhető, hogy a Dark Webes oldalak fluktuációja óriási, ugyanis, ha a felhasználó kilép a rendszerből a weboldala elérhetetlenné válik. Természetesen léteznek a nyílt webhez hasonló tárhely szolgáltatók is a TOR rendszeren is, de az alapértelmezés az első eset.

A TOR rendszer másik sajátossága, hogy kialakításánál fogva lehetővé teszi a TOR rendszeren keresztül az Nyílt Internetes tartalmakhoz történő hozzáférést. A felhasználó a TOR rendszert elindítva a TOR böngészőn keresztül meglátogathat hagyományos weboldalakat, úgy hogy a kiléte a rendszer által biztosított anonimitás miatt gyakorlatilag azonosíthatatlan marad. A rendszer önkéntesek által működtetett úgynevezett „Exit Node" –okon keresztül csatlakozik a Nyílt Webhez. Egy ilyen „Exit Node" adott esetben több ezer TOR felhasználó kérését továbbítja az nyílt webes szolgáltatókhoz anélkül, hogy tudatában lenne annak a kérés honnan érdekezett és a válasz hová tart. A 2. ábra ezt a folyamatot ábrázolja. A képen látható nyilak a titkosított kommunikációt mutatják a felhasználó és a webszolgáltatás között.



3. ábra: A nyílt webes tartalom felkeresése a TOR rendszeren keresztül. Saját szerkesztés.

A Dark Web biztosította anonimitás kedvez a különböző bűnelkövetőknek, [12] akik a hatóságoktól való elrejtőzés és a biztonságos bűnelkövetés érdekében a bűncselekmények széles körét követik el a Dark Weben [12], [x3]. Ezek közül a legjellemzőbbek, a különböző fizetőeszközzel, vagy azt helyettesítő szolgáltatásokkal történő visszaélés, hamis dokumentumok, és személyazonosító okmányok forgalmazása, kábítószer és gyógyszer kereskedelem, beleértve a hamisított gyógyszerek forgalmazását is nem beszélve a fegyverkereskedelemről. Ezen felül különféle szolgáltatások is igénybe vehetők a hackerbérléstől kezdve a bérgyilkosságig, de akár migráns útvonalat is lehet vásárolni az érdeklődőknek.

A felsorolt bűncselekmények színtere általában valamelyik „Black Market", vagy más néven „Crypto Market" (a továbbiakban itt darknet piac), ahol a fizetőeszköz jellemzően valamely virtuális valuta, mint a Bitcoin, vagy a Monero [4, pp. 107-111]. A tanulmány szempontjából azonban két területet célszerű külön szemügyre venni. Egyik a már említett darknet piacok, a másik terület azok az oldalak és fórumok, chatszobák, Pastebin stílusú oldalak, ahol a kiberbűnözők árusítják termékeiket és szolgáltatásaikat, illetve kölcsönös információcserével fejlesztik eszközeiket, technikájukat, valamint módszereiket. A megvásárolható sérülékenységeknek, exploitoknak a már említett piacokon kívül dedikált oldalaik is vannak, ahol akár nulladik napi sérülékenységeket (0Day vulnerability), vagy különböző rendszerekhez exploitokat, lehet vásárolni részletes utasítással egyetemben.[4,pp.85-112] A fentieken túl beszélhetünk még az úgynevezett „Doxing" oldalakról. Ezek olyan tartalmakat takarnak, amelyek ismert személyek, „celebek", üzletemberek, politikusok magánéletével kapcsolatos bizalmas adatokat illegális úton megszerezve azokat nyilvánosságra hozva erkölcsi károkat okoznak, etikai szempontból rossz színben tűntetik fel az áldozatot. Az ilyen oldalak célja általában nem a közvetlen anyagi haszonszerzés, inkább valamiféle bosszú, vagy politikai indok állhat a háttérben.

A következőkben a könnyebb áttekinthetőség érdekében a hacker fórumok vagy dedikált hacker oldalak és a darknet piacok működésének néhány jellemző vonása kerül összehasonlításra.

Hacker fórumok	**Darknet piac**
Téma specifikus	Kialakítása hasonló az online áruházakhoz
Az árukínálat jellemzően csak informatikával, illetve informatikai bűncselekményekkel kapcsolatos	A kínálat változatos, a drogoktól kezdve a lopott telefonig gyakorlatilag bármi kapható. A vásárlók értékelhetik az eladókat és termékeiket
Fórumoktól függően ingyenes vagy fizetős tudás, eljárás, és technika megosztás	Biztosítékkezelő rendszer (csak a szolgáltatás teljesítését követően kapja meg az eladó az ellenértéket)
Ingyenes vagy fizetős illegálisan szerzett adatbázis letölthetőség	Változatos árukészlet általában drog, pénzügyi szolgáltatások, adatbázisok, sebezhetőségek, exploitok stb..
Az illegális módon szerzett adatokat az elkövető trófeaként kezeli és megosztja a közösséggel.	Egyszerű belépés, illetve regisztráció
A bejutás esetenként többszintű ellenőrzést követően lehetséges. Nem ritka, hogy a jelöltnek bizonyítania kell rátermettségét valamely bűncselekmény kategóriába tartozó feladat végrehajtásával.	Belső fórum a termékekkel és az eladókkal kapcsolatban

Hacker fórumok	Darknet piac
A sebezhetőségek, technikák módszerek a legfrissebbek lehetnek	A piacon árusított technikák és sebezhetőségek leginkább már a speciális fórumokon feldolgozott, esetleg már a IT biztonsági szervek által is ismertek
Zárt közösség	Nyitott közönség

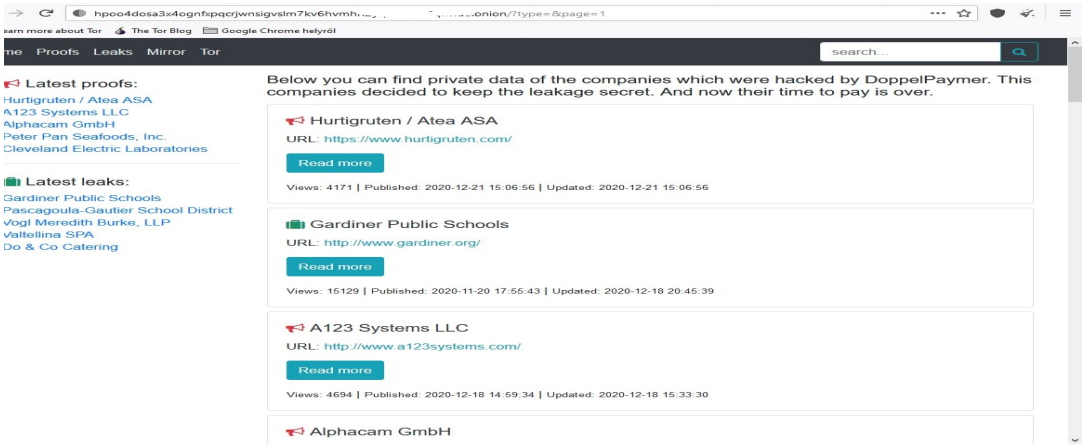
1. táblázat: A hacker fórumok és a darknet piacok összehasonlítása. Saját szerkesztés.

AZ ADATOK SORSA A DARK WEBEN

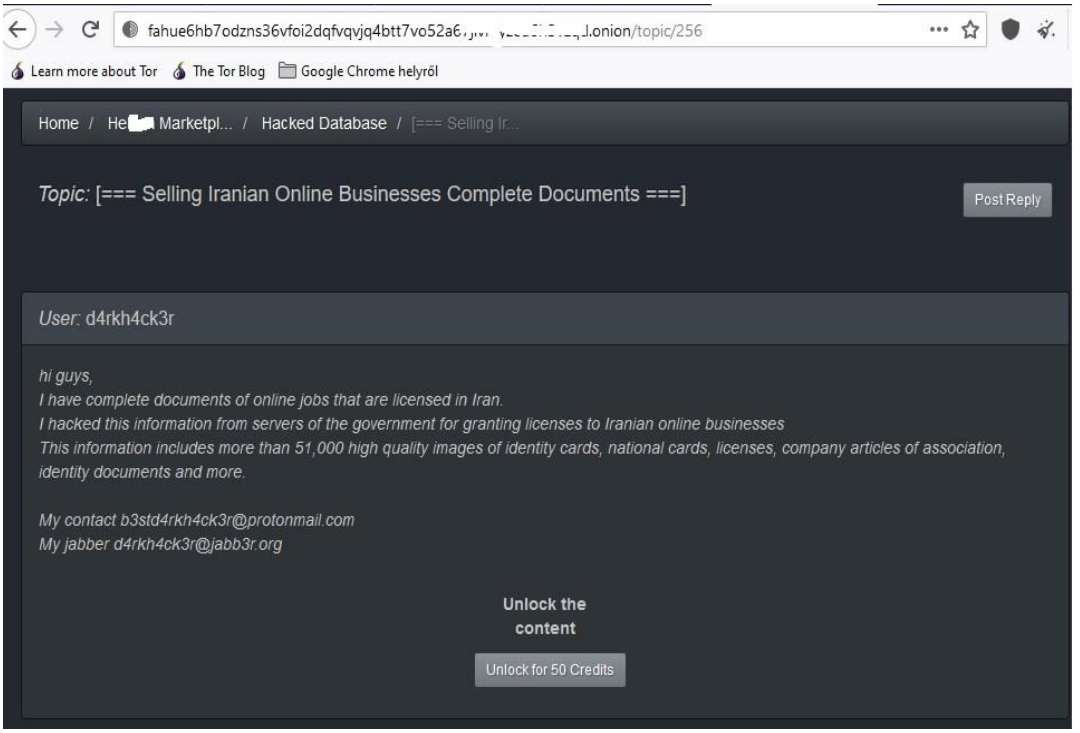
A feketepiacra kerülő adatot jellemzően célirányos hackertámadás útján szerzik meg, azonban ennek részletezése túlnyúlik a tanulmány határain. A kettős célú zsarolóprogramok (ellopja a felhasználó fájljait, majd titkosítással megakadályozza az azokhoz való hozzáférést.) használatát követően az áldozat fizetési hajlandóságától függetlenül, az ellopott adatot először felkínálják visszavásárlásra, és /vagy nyilvánosan áruba bocsájtják. Erre a darknet piacokon számtalan példa előfordul. A fentiek alapján nem célszerű a váltságdíj kifizetése, ugyanis így a keletkezett kár valamelyest csökkenthető.

A másik jellemző forrás a bennfentes elkövető útján szándékosan anyagi haszonszerzés, vagy bosszú céljából kijuttatott adat.

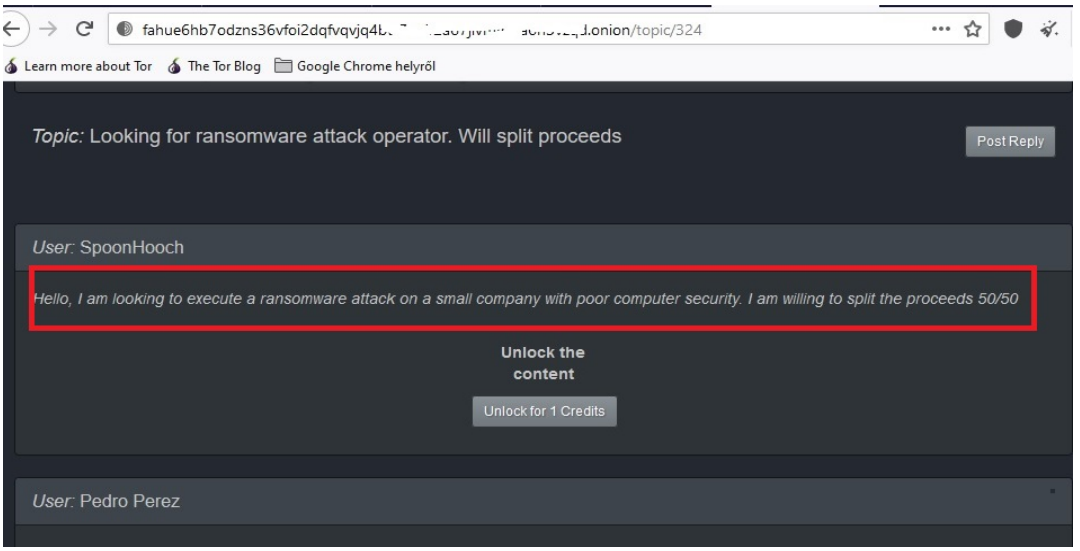
A vállalattól ellopott, vagy kiszivárgott adat több lépcsőn is keresztülmegy mire valamely hacker oldalon, vagy a darknet piacon megjelenik. A bennfentesek az adatot ellenőrzik, egymás között eladják, újracsomagolják, újra eladják, újracsomagolják, esetleg több részre osztják el, majd ez után kerül ki a nyilvános darknet piacokra [13] , [14]. A 4-es és 5-ös számú képeken az olvasó példákat láthat az ellopott adatok árusítására, míg a 6-os számú képernyőfotón egy kisvállalkozás elleni zsarolóvírus támadás irányítására keresnek jelentkezőt.



4. ábra: Ellopott információk a Dark Web egyik darknet piacán. A szerző felvétele.



5. ábra: Dark Web hacker fórumon iráni üzleti adatbázist kínálnak eladásra. A szerző felvétele



6. ábra: Ransomware operatort keres a megrendelő egy vállalkozás elleni támadáshoz. A szerző felvétele

A DARK WEB MONITOROZÁSÁNAK LEHETŐSÉGEI

Napjainkban a Dark Web térhódításával a vállalatok információ biztonsági helyzetének szilárdan tartása érdekében az ellenük tervezett támadások szándékának, illetve az onnan már megszerzett, vagy kiszivárgott adatok felderítésének érdekében elengedhetetlen a Dark Web monitorozása [15]. Ehhez azonban komoly helyismerettel, és pozícióval kell rendelkezni a vizsgálatot végzőnek. Mint az már korábban említésre került a Dark Webnek nincs érdemi kereső rendszere, annak ellenére, hogy van néhány próbálkozás ezek csak részleges és megbízhatatlan eredményeket tudnak produkálni. A Dark Webet kutató szakembernek a különböző linkgyűjteményekből, nyílt webes utalásokból, fórumbejegyzésekből kell elindulnia és építkeznie [15]. Azonban ez még nem elég, hiszen az informatikai bűncselekményeket elkövető hackerek minőségi fórumaikra, vagy chatszobáiba csak alapos ellenőrzési procedúrát követően engednek be új belépőket. Ezekbe a belső körökbe történő bejutás még egy felkészült biztonsági szakembernek is hosszú időt igényel, nem beszélve az esetleges próbafeladatok végrehajtásáról, hiszen a bűnös körnek érdeke, hogy kiszűrje a rendfenntartó erők tagjait és a biztonsági IT szakembereket. A rendfenntartó erők akcióira a fórumok, erősebb titkosítással még szigorúbb és agresszívabb ellenőrzéssel válaszolnak ezzel tovább nehezítve a bűnüldöző szervek munkáját [16].

A másik nehézség, hogy egyszerre több ilyen oldalt kell figyelemmel kísérni, ezek száma a több tucatot is elérheti, nem beszélve a számtalan darknet piacról. Egy bizonyos méret alatt vállalatok nem engedhetik meg maguknak, hogy külön Dark Web ellenőrző részleget tartsanak fenn és most nem említve a tanulmány határain kívül eső Nyílt Web ellenőrzését, amely legalább ennyire fontos.

Az ellenőrzéssel kapcsolatban van még egy olyan tényező, amelyet semmiképpen sem szabad figyelmen kívül hagyni. A Dark Web oldalak keresése és elemzése rendkívüli körültekintést kíván az ellenőrzők részéről, ugyanis nagyon könnyen törvényszegést követhet el, az ellenőrző, aki nem kellő odafigyeléssel meggondolatlanul navigál bizonyos oldalakra. A Dark Webnek külön nyelvezete és zsargonja van, aki ezt nem ismeri, könnyen gyermek pornó, vagy más tiltott oldalra navigálhat, ahol a tartalmak akár véletlen letöltésével is bűncselekményt követhet el, vonatkozik ez a helytelenül beállított automata keresőkre is. [17] Tehát a tapasztalat és jártasság olyan tényezők, amelyek a profi elemző vállalkozás megbízása felé lendítik a mérleg nyelvét. [18]

A felsorolt kihívásokra válaszokat az úgynevezett „Threat Intelligence" vállalkozások nyújthatják, amelyek magukra vállalják a Nyílt Web és a Dark Web megrendelő igényeinek megfelelő szempontok alapján történő monitorozását.[6]. Ezek a vállalatok profiljukból adódóan feltérképezték a Nyílt és Dark Web releváns részét, folyamatosan aktualizálják adatbázisaikat, figyelemmel kísérik a változásokat, munkatársaik útján, illetve a mesterséges intelligenciát felhasználva szoftveres úton ellenőrzik és elemzik az internetes tartalmakat és jelzést adnak a megrendelőnek, ha érdeklődésére számot tartó információ vagy adatot derítenek fel. A nemzetközi színtéren már számos külföldi vállalat nyújt ilyen szolgáltatást, de már hazánkban is akad példa ilyen szolgáltatókra. [19].

ÖSSZEGZÉS

A vállalati információvagyon esetleges kiszivárgásának felderítése, illetve az vállalatot érintő esetleges támadási szándékok időbeni felfedési jelentős előnyt jelent a vállalati vezetés számára az időbeni megelőző, vagy kárenyhítő intézkedések bevezetésére, a vétkesek felderítésére, illetve felelősségre vonására. A Dark Web vonatkozásában mindehhez speciális szakértelem, jártasság és eszközrendszer szükséges, amelynek megteremtése saját erőforrásokból nem tűnik járható útnak. Ezzel szemben egy erre a célra szakosodott vállalat megbízása reális választásnak tűnik [19]. A tanulmánynak nem célja, hogy gazdaságossági hatástanulmányt végezzen, mindössze a Dark Webnek és az vállalati adatvagyon megőrzésének összefüggéseire kívánt rávilágítani.

FELHASZNÁLT FORRÁSOK

[1] Vasvári, G., Lengyel, C. and Valádi, Z., 2006. *Vállati Biztonság Keretrendszere*. Budapest: Budapesti Műszaki és Gazdaságtudományi Egyetem, Biztonságmenedzsment kutató csoport, pp.5, 12,21-26.

[2] Dr. Michelberger, P., 2020. *Információ-, Folyamat- és Vállalatbiztonság*. 2nd ed. Budapest: Óbudai Egyetem, pp.9,10,25,26,29-45.

[3] https://www.pwc.com/hu/hu/szolgaltatasok/technologiai_tanacsadas/data_analytics/adatstrategia.html

[4] Akhgar, B., Gercke, M., Vrochidis, S. and Gibson, H., 2020. *Dark Web investigation*. 1st ed. Cham,Switzerland: Springer Nature Switzerland AG,

[5] https://www.torproject.org/download/

[6] https://geti2p.net/en/

[7] https://freenetproject.org/

[8] https://zeronet.io/

[9] https://www.imf.org/external/pubs/ft/fandd/2019/09/the-truth-about-the-dark-web-kumar.htm

[10] https://tb-manual.torproject.org/about/

[11] https://tb-manual.torproject.org/onion-services/

[12] Márton Tibor, D., 2020. *Dr. Serbakov Márton Tibor: Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem | Büntető Törvénykönyv (új Btk.) a gyakorlatban*. [online] Ujbtk.hu. <https://ujbtk.hu/dr-serbakov-marton-tibor-kriminalitas-a-dark-weben-illegalis-piacok-pedofil-oldalak-terroristak-es-az-ellenuk-valo-kuzdelem/> [Letöltve: 2021.04.16.].

[13] https://www.vaadata.com/blog/are-your-corporate-data-and-sensitive-documents-on-the-dark-web/

[14] Hhs.gov. 2020. *HHS Cyber Security Program*. [online]. <https://www.hhs.gov/sites/default/files/dark-web-and-cybercrime.pdf> [Letöltve: 2021.05.02.].

[15] Pascucci, M., 2016. *Threat monitoring: Why watching the dark web is crucial*. [online] SearchSecurity.<https://searchsecurity.techtarget.com/tip/Threat-monitoring-Why-watching-the-dark-web-is-crucial> [Letöltve: 2021.04.22.].

[16] Ablon, L., Libicki, M. and Golay, A., 2014. *Markets for Cybercrime Tools and Stolen Data*. [online] Rand.org. https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf> [Letöltve: 2021.04.28.].

[17] https://iaca-darkweb-tools.com/dictionary/
[18] https://www.comparitech.com/net-admin/best-dark-web-monitoring-tools/
[19] Lewis, N., 2019. *Should large enterprises add dark web monitoring to their security policies?*. [online] SearchSecurity. https://searchsecurity.techtarget.com/answer/Should-large-enterprises-add-dark-web-monitoring-to-their-security-policies> [Letöltve: 2021.04.14.].

SOFTWARE DEVELOPMENT TEAMWORK FROM AN INFORMATION SECURITY PERSPECTIVE

SZOFTVERFEJLESZTÉSI CSOPORTMUNKA AZ INFORMÁCIÓBIZTONSÁG SZEMSZÖGÉBŐL

KERTI András[1] – NYÁRI Norbert[2]

Abstract

The present study demonstrates how to combine the international standard ISO/IEC 27005 and the US standard NIST SP 800-30 to perform risk analyzes, through the example of a fictional software development company. Starting with a brief introduction to the company, the reader can get acquainted with the basic concepts of the DevOps approach in order to have a more accurate view of the processes taking place within the development company. Subsequently, starting from the Hungarian regulatory environment, an overview is presented of the current state of information security standards, taking into account the NATO and ENISA information security product catalogues. After that an ISO-NIST combined risk analysis technique is briefly described, the foundations of which were laid in 2017 by Putra, Fandi A., and others. A simple example of the application of the technique is also shown.

Keywords

risk assessment, IT security, information security, standards theory, software development

Absztrakt

Jelen tanulmány egy kitalált szoftverfejlesztőcég példáján keresztül mutatja be, hogy hogyan kombinálható kockázatelemzések végrehajtása céljából az ISO/IEC 27005 nemzetközi és a NIST SP 800-30 amerikai szabvány. A cég rövid bemutatásától indulva az olvasó megismerkedhet a DevOps megközelítés alapfogalmaival, annak érdekében, hogy pontosabb rálátása legyen a fejlesztő cégen belül zajló folyamatokra. Ezt követően a magyar szabályozási környezetből kiindulva áttekintő képet kaphat az információbiztonsági szabványok aktuális helyzetéről figyelembe véve a NATO és az ENISA információbiztonsági termékkatalógusait. Ezt követően röviden ismertetésre kerül egy ISO-NIST kombinált kockázatelemzési technika, melynek alapjait 2017-ben fektették le Putra, Fandi A. és mások. A technika alkalmazására is láthatunk egy egyszerű példát.

Kulcsszavak

kockázatelemzés, IT biztonság, információbiztonság, szabványelmélet, szoftverfejlesztés

[1] kerti.andras@uni-obuda.hu | ORCID: 0000-0003-2149-5500 | associate professor, Faculty of Military Science and Officer Training of the University of Public Service | egyetemi docens, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar

[2] nyari.norbert@uni-obuda.hu | ORCID: 0000-0003-0229-7584 | doctoral candidate, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

INTRODUCTION

Information security is a key factor in today's life, regarding that many aspects of our life depends on data stored and managed in various IT systems operated by either governmental bodies or business organizations.

This study aims to address the IT security aspects of the modern software development process including agile development, devops, cloud technology etc. In order to facilitate full understanding, the aforementioned methodologies and techniques shall also be briefly described.

After that a risk analysis shall be presented based on a fictional software development company called SoDevCo Ltd. (it stands for Software Development Company Ltd.). The complete risk analysis however would be way too lengthy to fit into an article like this, so I shall focus on the software development related risks.

The following section introduces the organization under inspection, the SoDevCo Ltd starting with a short historic overview.

SODEVCO LTD. COMPANY OVERVIEW

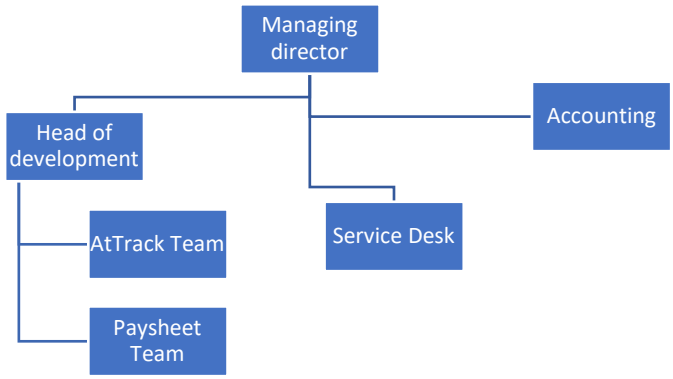
SoDevCo Ltd. is a fictional software development company based in Budapest, Hungary. The main activity of the company is the development of a cloud-based attendance tracking and payroll software. The owners of the firm are a Hungarian married couple. The husband is the managing director with a 90% share.

Founded in 2009, the company started to develop a payroll software called Paysheet with five developers. At first Paysheet was an on-prem intranet web application. A few years later, in 2014, thanks to the success of Paysheet, the company was able to embark on the development of a cloud-based attendance tracking software called AtTrack. In 2016 Paysheet was also moved to the cloud, however there are a few clients who still uses the on-prem version of Paysheet.

Since 2011 the company has an ISO 9001 certified quality management system. In 2012, the company introduced the self-developed payroll application for its own employees, and starting from 2018 AtTrack is also in use within the company.

The current organigram can be seen on the diagram below. Due to size constraints, I shall only describe IT-related organizational units in detail. The number of employees in the past years is ranging from 25 to 35. The company currently has two devops teams, one for each product. The teams are led by the Head of Development.

There is also a Service desk in the company with five employees. Led by a Service Desk Manager the four Service Desk Analysts provide the 1st line support of the company for the clients. It is a relatively newly established organizational unit, due to the growing clientele, operating since 2020 in an ITIL-like manner. The client-reported issues are stored in a third-party issue tracker application in the cloud, called JetBrains YouTrack with a monthly subscription.



1. Table: The organigram of SoDevCo Ltd. Self-editing.

The composition of the two DevOps teams is shown in the table below. Each of the teams has a product manager. They are in charge of the long-term product strategies and the roadmaps of each product; they also work on requirements coming from the clients. Sales activities are also performed by product managers, complemented by the managing director.

Role name	Paysheet Team	AtTrack Team
Product manager	1	1
Developer	6	5
Team lead	1	1
Tester	2	3
Cloud architect	1	2
System administrator	2	2

2. Table: Teams of SoDevCo Ltd. Self-editing.

Both teams have a Team lead, who works on the requirements in conjunction with the product manager, makes architectural decisions and delegates task to the team members. The cloud architects are specialized in cloud technologies, they are in charge of cloud architecture related tasks. Tasks of System administrators include operations related tasks, like cloud monitoring and 2nd line support, they are also in charge of the operation of the OpenVPN solution to support Home Office, and the on-prem third-party build server, called JetBrains TeamCity.

Among the developers there are experts of various fields related to both frontend and backend, they also provide 3rd line support if needed.

The codebase (the collection of all related source codes) of the two applications are also stored in the cloud, on GitHub.com. The scrum process of the developers is also supported by the aforementioned third-party issue tracker application, YouTrack. The team practices Continuous Integration, and Continuous Deployment.

The firm has an OpenVPN based infrastructure to support the telecommuting of mainly the System administrators. Telecommuting is the primary form of work from the spring of 2020, due to the COVID-19 situation. The main communication channel for teleworkers is a third-party cloud-based solution called Slack, with a monthly subscription.

One last thing before moving to the next topic is the pricing of the products of the company. Each product (Paysheet and AtTrack) has a monthly subscription-based licensing, having 3 plans (Free, Standard and Enterprise). The Free plan is quite limited though in both services and number of users. The Standard plan makes all services available to up to 100 users. The Enterpise plan is individually priced, supporting unlimited number of users

The company plans to implement an ISO/IEC 27001 certified information security management system, during the process a risk assessment must be done. [1] But before moving on to risk assessment, I shall introduce some basic concepts of DevOps.

The term DevOps however does not seem to have a concrete shared definition. [2] It is somewhat striking though that it comes from the combination of the words: developer and operations, being a practice based on close collaboration between software developers and software operators it aims to deliver services and applications quicker and more effectively than other conventional software development processes. [3] [4]

In the 2015 book DevOps: A Software Architect's Perspective the authors suggested a definition as follows "a set of practices intended to reduce the time between committing a change to a system and the change being placed into normal production, while ensuring high quality". [5]

DevOps however on its own is only a theoretical framework providing a seamless and cohesive functioning of the operations and development teams within the company when properly adapted utilizing tools and techniques like automation (infrastructure and tests), configuration management, monitoring and log management. One possible adaptation is the CAMS framework. [3] [4]

CAMS is an acronym for the words Community (or Culture), Automation, Measurement, and Sharing, which are the high-level concepts of the framework detailed as follows. [3]

Firstly Culture, DevOps mainly intended to eliminate conflicts of interest between developers and operators, so it deals with problems related to people and organizational culture. While developers tend to try out cutting-edge technologies and solutions, operators strive to maintain a stable environment and infrastructure. Traditionally developers and operators were often separated into different teams speaking "two different languages" making the situation even worse. Sharing responsibility is a major goal of DevOps. Culture can also bring in good practices like applying Scrum. [6] [7]

Secondly Automation, with proper automation significant amount of effort and money can be saved. Not only it speeds up the processes and the information flow but also minimizes human error. Two main concepts come along with automation: Infrastructure as Code and Continuous Deployment Pipelines. [6] [7]

Continuous integration is a primary DevOps practice of automating the integration of code changes from multiple contributors into a single software project, through the use of a central version control system. [8]

Continuous deployment (CD) is the process of rapidly deploying software or services automatically to end-users without any human interaction. If no automated test case or quality check fails the changes made to software and services are automatically deployed to production servers. Infrastructure as Code is a key element in implementing CD. [9]

Simply put, Infrastructure as Code (IaC) means managing an IT infrastructure using configuration files. In other words, IaC is the practice of automatically defining and managing system configurations through source code. [9]

Thirdly Measurement, measuring the correct metrics will help determine if progress is being made in the intended direction, they can also help in making the right decisions. [6] [7]

Sharing is the last word in CAMS, DevOps places a great emphasis on information exchange, transparency and openness. The team's comprehensive, collective knowledge greatly enhances its effectiveness. [6] [7]

In the 2019 article authors state that on one hand there is not enough evidence on DevOps facilitating software quality, on the other hand CAMS has a positive effect on it. [3]

In the following I shall present a quick review on various risk assessment frameworks.

RISK MANAGEMENT METHODOLOGIES

So many risk management methodologies exist that introducing all of them would surely not fit into this article, in the 2012 study "A comparative study of risk assessment methods, MEHARI & CRAMM with a new formal model of risk assessment (FoMRA) in Information Systems" the author stated that the number of the different available methods was about 200, so I shall describe only some of them based on the Hungarian regulatory environment. [10]

In 2008 the Hungarian Administrative IT Committee (Közigazgatási Informatikai Bizottság, KIB) published recommendations regarding IT security called Hungarian IT Security Recommendations (Magyar Informatikai Biztonsági Ajánlások, MIBA). The Hungarian IT Security Framework (Magyar Informatikai Biztonsági Keretrendszer, MIBIK) is one of these recomendations. [11]

MIBIK is a Hungarian framework for the management, requirements and examination of IT security, which is based on relevant international ISO standards, technical reports, NATO Council Memorandums and regulations of the European Union. [11]

Speaking of NATO and EU regulations, NATO has a website called NATO Information Assurance Product Catalogue (NIAPC), which provides a catalogue of Information Assurance products, Protection Profiles and Packages that are in use or available for procurement to meet operational requirements for NATO nations and affiliated civil or military bodies. [12]

The official website of European Union Agency for Cybersecurity (ENISA) states that "ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow." [13]

Should someone be interested in this topic the aforementioned product catalogues could serve as a good place to start for gathering information. During my research I have checked both of them for the products and technologies in this topic, I shall share my findings at the description of each product.

The Examination of IT Security Management (Informatikai Biztonság Irányításának Vizsgálata, IBIV) is a methodology providing unified approach for examining IT

systems of an organization in order to be able to prove that the IT system meets its own security requirements and that security threats affecting interested external parties are duly taken into account. IBIV helps in conforming ISO/IEC 27001:2005 as well. [11]

IBIV recommends the performing of a risk analysis describing two different approaches. The first procedure is based on the NIST SP 800-30 and the FIPS 199 documents. This methodology allows for relatively simple risk assessment with little effort. The second approach is based on CRAMM (CCTA Risk Analysis and Management Method), which is costly, since it explores the risks of each and every threat. [11]

NIST (National Institute of Standards and Technology) is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce, promoting industrial competitiveness and innovation since its foundation. [14]

NIST has six research laboratories, one of them is ITL (Information Technology Laboratory). ITL is focusing on IT measurements, testing and standards. ITL publishes papers in numerous series, the two relevant to this article are FIPS PUBS (Federal Information Processing Standards Publications) and Special Publication (SP) 800 series. [14] The following table contains the relevant NIST publications.

NIST number	Title
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
SP 800-30 revision 1	Guide for Conducting Risk Assessments
SP 800-37 revision 2	Risk Management Framework for Information Systems and Organizations: A system Life Cycle Approach for Security and Privacy
SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
SP 800-61 revision 2	Computer Security Incident Handling Guide

3. Table: Relevant NIST publications. Self-editing.

SP 800-30 provide guidelines conducting risk assessments in accordance with other NIST recommendations standards aiming to promote the organization's risk management abilities. [15]

SP 800-37 defines the Risk Management Framework which is a United States federal government policy and standards providing structured and yet flexible process for managing security and privacy risks relying on the concepts defined in FIPS 199, FIPS 200 and SP 800-53. [16]

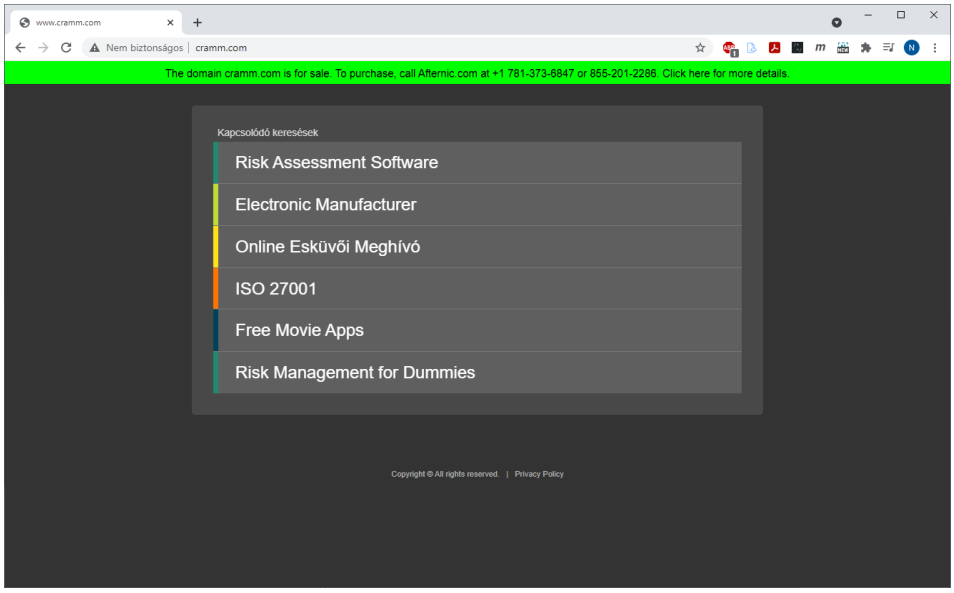
The 2002 version of SP 800-30 has an ENISA product page, but unfortunately the "Official website" link is outdated being broken. [17] NIAPC has no information on SP 800-30 whatsoever. [12]

The other method of IBIV is based on CRAMM. I was really trying to gather information on the CRAMM methodology. The ENISA product page for CRAMM states that CRAMM was created in 1987 by the Central Computer and Telecommunications Agency (CCTA), now renamed into Cabinet Office, of the United Kingdom government. It is currently on its fifth version, CRAMM Version 5.0. [18] CRAMM is stated to be a comprehensive risk assessment tool that's fully compliant with the British BS7799 and the international ISO/IEC 17799. [19]

Based on the Manufacturer's Brochure which can be downloaded from the NIAPC product page of CRAMM, the latest version of CRAMM supports ISO/IEC 27005. The NIAPC product page of CRAMM was updated in 2013 though, which was quite long ago. [19]

The two standards, ISO/IEC 17799 and ISO/IEC 27001, based on the BS7799 British standard, the former is derived from the BS7799:1 and the latter on BS799:2. [20] ISO/IEC 17799 was however superseded by the ISO/IEC 27002 in 2005. [21] With this in mind, CRAMM theoretically seems compatible with the ISO/IEC 27000 series.

CRAMM looks also somewhat neglected or abandoned, given that the official website domain name, www.cramm.com, is for sale at the moment as it can be seen on the figure below. [22] In addition, I have not been able to find any information on the Internet that proves CRAMM being either in effect or withdrawn.



4. Table: www.cramm.com

However, the Hungarian IBIV is based on the ISO/IEC 27000 series of standards it never mentions ISO/IEC 27005 as an option for risk assessment, no wonder, because its first version was published in 2008, in the same year as MIBIK. [21] Given all the above information on MIBIK and CRAMM, performing a risk assessment based on ISO/IEC 27005 is not against the principles of MIBIK. On one hand MIBIK is a recommendation, this means no prohibition to deviate from its principles at all. On the other hand, the latest version of CRAMM supports ISO/IEC 27005 as stated before. [19] MIBIK however references the predecessor of ISO/IEC 27005, the ISO/IEC TR 13335-3 and ISO/IEC TR 13335-4. [11]

As for the Hungarian standards situation, according to the official site of the Hungarian Standards Board (Magyar Szabványügyi Testület, MSZT) the ISO/IEC 27001 was published in Hungary in 2014, but the naturalization of the other standards of the series has not started yet. ISO/IEC 27002 is published though in Hungary, but only in English. [23]

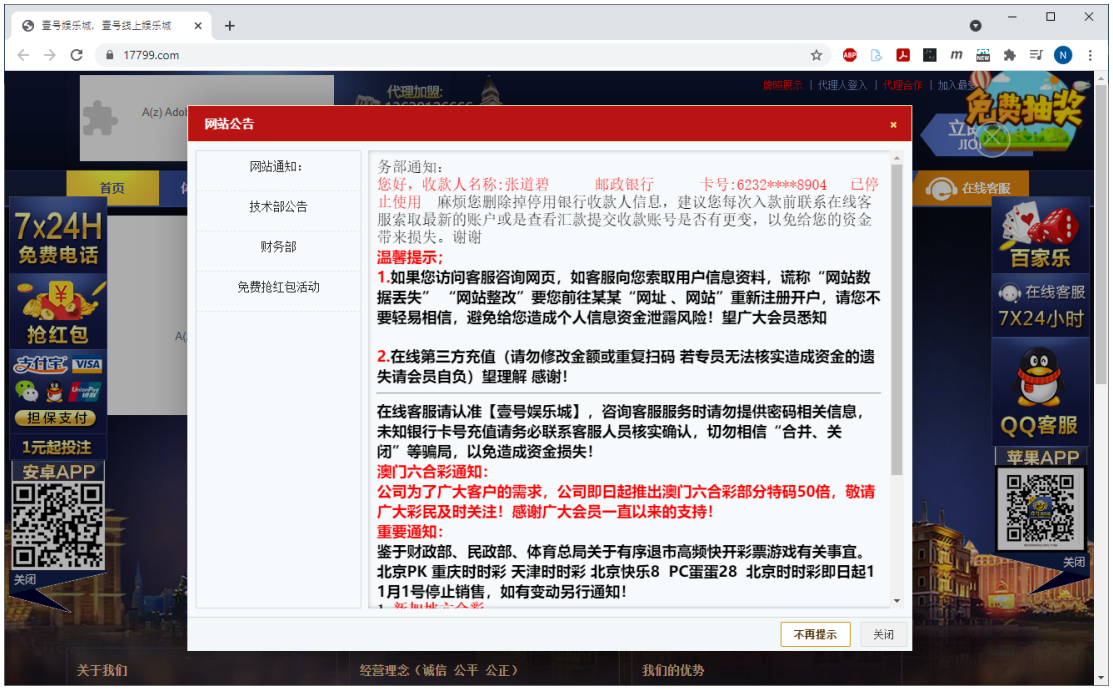
MSZT is an observing member of the ISO/IEC JTC 1/SC 27 technical committee which develops ISO/IEC 27005. [21] It would be highly desirable to be a participating member.

According to the official site of National Accreditation Authority (Nemzeti Akkreditáló Hatóság, NAH), nah.gov.hu five organizations are entitled to certificate ISMS's based on the MSZ ISO / IEC 27001: 2014 standard and two organizations are accredited to perform services based on MIBÉTS:2009. [24]

NIAPC does not seem to have anything on ISO/IEC 27000 series. [12] ENISA has a product page for ISO/IEC 27001 but it is way too much out of date. It has a link to www.17799.com, which is a working page, but its content has presumably changed significantly over the years for currently it seems to be a Chinese phishing site, as it can be seen on the figure below. [25]

Based on my experience with either NIAPC or the ENISA Catalogue they are unfortunately both seem to be somewhat outdated, neglected. A comprehensive content analysis and an analysis-dependent update should be considered.

Back to IBIV, the combined methodology proves to be a valid approach over the years though, since there are other studies that support its effectiveness. In the 2017 article "Design of Information Security Risk Management using ISO/IEC 27005 and NIST SP 800-30 Revision 1: A Case Study at Communication Data Applications of XYZ Institute" the issue of combining ISO/IEC 27005 and NIST SP 800-30 had been discussed, resulting in a new technique for information security risk assessment. [26]



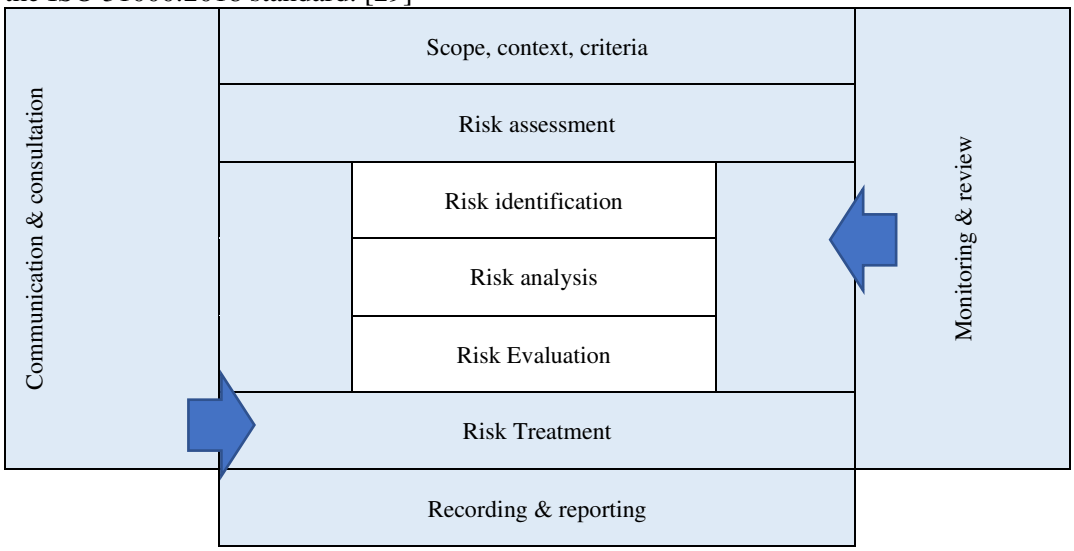
5. Table: www.17799.com

Two years later, in 2019, in the article "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency" the authors also stated that

"NIST SP 800-30 revision 1 can be used as a complement to the risk assessment process and can be applied to the ISO 27005 risk management framework". [27]

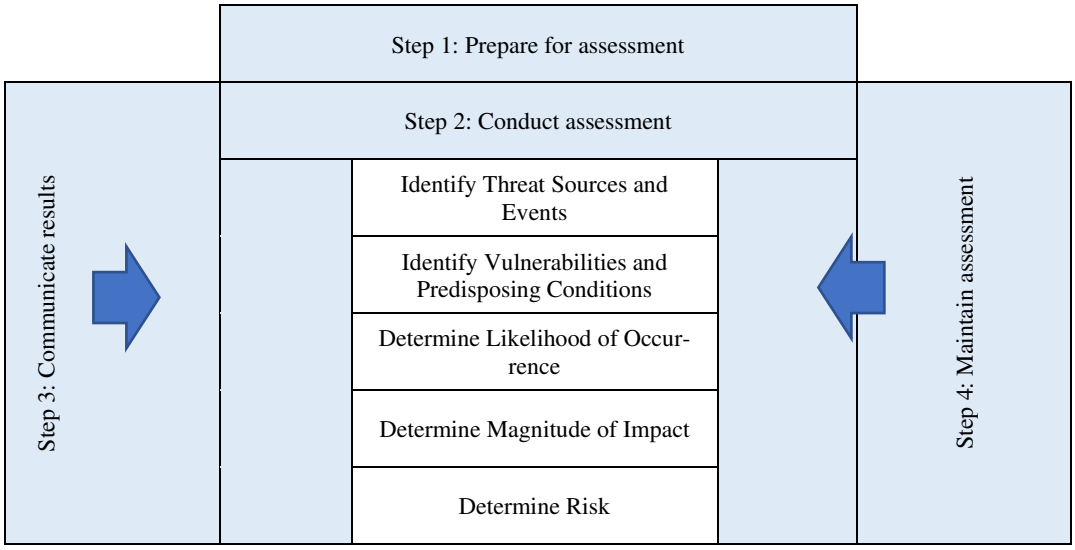
ISO/IEC 27005 references ISO 31000 Risk management — Guidelines when describing the high-level risk management process. [28] ISO 31000 describes an industry and sector independent risk management approach. [29]

The high-level risk management process is shown in the following figure, based on the ISO 31000:2018 standard. [29]



6. Table: Risk management process. Self-editing.

The NIST way of assessing risks are quite similar as it can be seen on the figure below.



7. Table: NIST SP 800-30 rev 1 Risk Assessment Process. Self-editing.

The combination of the ISO and NIST approach can be seen in the table below, based the standards and on the 2019 article. [27] [28] [15]

No.	ISO 27005/ISO 31000	NIST SP 800-30 rev1	Updated Combination technique
Context Establishment			
1.	Scope, context, criteria	Prepare for assessment	Determination of Risk Assessment Criteria and Scale
Risk Assessment			
2.	Risk Identification	1. Threat Source Identification 2. Threat Event Identification 3. Vulnerability Identification	1. Risk Identification, a) Threat Source Identification; b) Threat Event Identification; c) Vulnerability Identification
3.	Risk Analysis	4. Determining the Likelihood 5. Determining Impact	2. Risk Analysis, a) Determining the likelihood in the risk scenario; b) Determining the impact on the risk scenario
4.	Risk Evaluation	6. Determine Information Security Risk Level	3. Risk Evaluation, a) Determining the level of information security risk; b) Determining Risk Priority

8. Table: ISO-NIST combination risk assessment technique [27]

The combined approach basically follows the steps of ISO/IEC 27005, while using some features of the NIST SP 800-30 revision 1, when applicable. For example, in the Threat Event Identification step, the Threat Event categories come from the ISO standard, but the Relevance scale is used from the NIST publication.

In the following a possible application is described of the above-mentioned NIST-ISO combination technique assessing the risks of SoDevCo Ltd.

RISK ASSESSMENT OF SODEVCO LTD.

First things first, the *establishment of the risk management context* including a risk management approach, risk evaluation criteria, impact criteria, and risk acceptance criteria. ISO/IEC 27005 only recommends that these criteria should be developed somehow. [28] According to ISO 31000, the organization should specify the amount and type of risk that it may or may not take, relative to objectives. This is often called Risk Appetite. [29]

Applying the NIST SP 800-30 rev 1 scales, Impact of Threat events, Likelihood of Occurrence, Likelihood of Adverse Events as suggested in the 2019 article can simplify the task of setting up these criteria. I shall not list these scales due to size constraints; they can easily be looked up in the NIST recommendation. [15] [27]

A company like SoDevCo Ltd. has to face many types of risks, including human risk, financial risks, information security risks etc. A comprehensive risk management framework would cover all of them, but describing the assessment all these types of risks would be way too lengthy, so the scope of risk analysis has to be narrowed down to information security risks related to the software development process.

The next step is the *risk identification*, which starts with the *identification of the assets*. According to ISO 27005 assets can be categorized into two main categories: primary

(denoted as P) and supporting (S) assets. Primary assets can be of two types: the core processes and activities of the company and information. Any other types of assets like hardware, software and personnel are considered as supporting assets. [28]

In the following table I shall list a few examples of the assets of the company, the type of asset is identified based on the asset category of the ISO standard. Besides these examples many other assets would be incorporated in the risk assessment, including network equipment, hardware etc. Each asset has a unique identifier so that they can be referenced later.

ID	Type	Name	Kind of asset	Owner	Location
A1	Information	Source code repository of AtTrack	P	AtTrack DevOps team	Data center
A2	Information	Source code working copies of AtTrack	P	AtTrack DevOps team	Employee's workstations
A3	Information	Documentation of AtTrack	P	AtTrack DevOps team	Data center
A4	Process	CD pipelines	P	AtTrack DevOps team	Data center
A5	Information	User-reported issues and responses	P	Service Desk	Data center
A6	Information	Scrum process documentation (epics, user stories etc.)	P	AtTrack DevOps team	Data center
A7	Information	Collective knowledge base of the company	P	The company	Data center
A8	Technology	Production AtTrack Application	S	The company	Data center
A9	Information	Production AtTrack Database	P	The users	Data center
A10	Personnel	DevOps team members	S	The company	Site
A11	Hardware	Workstations for team members	S	AtTrack DevOps team	Employee
…	…	…	…	…	…

9. Table: Example assest of SoDevCo Ltd. Self-editing.

Next, the *threat sources should be identified*, ISO 27005 has an annex (Annex C) of typical threats which can be complemented by the NIST SP 800-30 exemplary taxonomy of threat sources (Table D-2 in the recommendation). [28] [15] Threats can be broadly categorized as adversarial and non-adversarial (accidental, structural and environmental). [15] The threat sources identified are shown in the following listing with a unique identifier.

ID	Name
Adversarial Threat Sources	
S1	Hacker, cracker
S2	Computer criminal
S3	Industrial espionage
S4	Insider
S5	Trusted insider
S6	Privileged insider
S7	Outsider
S8	Competitor Organization
S9	Supplier Organization

ID	Name
S10	Customer Organization
Accidental Threat Sources	
S11	Human error – user
S12	Human error – administrator
Structural Threat Sources	
S13	Communications Equipment
S14	Networking
S15	General-Purpose Application
S16	Mission-Specific Application
Environmental Threat Sources	
S17	Fire
S18	Flood
S19	Telecommunications Outage

10. Table: Threat sources of SoDevCo Ltd.

Threat events are connected to assets; threat sources capable of exploit vulnerabilities of assets cause threat events. The following matrix shows a few examples of the *possible threat events*. The values of the threat event column come from the ISO/IEC 27005 Annex D. [28] The relevance of a threatening event is intended to express the probability that the event in question may occur in the course of the company's operations, SP 800-30 revision 1 describes an exemplary scale for reference. [15]

No.	Asset ID	Threat event	Threat Sources	Relevance
1	A1	Abuse of rights (T1)	S1, S2, S3, S4, S5, S6, S7, S8, S12	Anticipated
2	A1	Forging of rights (T2)	S1, S2, S3, S4, S5, S6, S7, S8	Predicted
3	A1	Theft of media or document (T3)	S1, S2, S3, S4, S5, S6, S7, S8	Possible
4	A1	Failure of telecommunication equipment (T4)	S11, S12, S13, S14, S19	Confirmed
5	A8	Illegal processing of data (T5)	S1, S2, S3, S4, S5, S6, S7, S8, S10	Possible
6	A8	Tampering with software (T6)	S1, S2, S3, S7, S11, S12	Anticipated
7	A9	Abuse of rights (T1)	S1, S2, S3, S4, S5, S6, S7, S8, S12	Predicted
…				

11. Table: Example threat events

The next step is the *identification of existing controls*, surely every company has controls already in place before conducting a risk assessment. According to ISO/IEC 27005 this step is important for multiple reasons: on one hand unnecessary work and expenses can be avoided, on the other hand ensuring the proper operation of existing controls is also achievable. [28]

The following controls were identified regarding the DevOps process of the company, password policy on team members' workstations (C1), two-factor authentication with smart cards on workstations (C2), full-disk encryption on workstations (C3), security awareness training of employees (C4), group policy on team members' workstations (C5),

GitHub.com two-factor authentication (C6), GitHub.com password policy (C7). There are a few controls incorporated in connection with the production AtTrack application (A8), which are the following: storing user passwords hashes (C8), user password policy (C9), automated tests incorporated in the CD pipelines (C10), database encryption (C11) of the Production AtTrack database (A9).

Next, the *Identification of vulnerabilities*, in this step vulnerabilities that can be exploited by threats to cause harm to assets or to the organization should be identified. [28] In the 2019 article, the suggested NIST-ISO approach focuses on the implemented, existing controls to protect assets from threats, utilizing the NIST-based vulnerability measurement, which is known as the Vulnerability Severity. [27] [15]

Asset	Existing Control	Vulnerability	Vulnerability Severity
A1	C3, C6, C7, C8	Lack of identification and authentication mechanisms like user authentication	High
A3		Wrong allocation of access rights	Moderate
A11	C4, C5	Uncontrolled downloading and use of software	Moderate
A2	C4, C5	No 'logout' when leaving the workstation	Moderate
A8	C10	No or insufficient software testing	High
A8	C8	Unprotected password tables	High
A10	C4	Lack of security awareness	High
…	…	…	…

12. Table: Example Vulnerabilities. Self-editing.

The table above shows, among other things, that the organization does not have any existing controls regarding the access right management of product documentations.

Risk analysis is the core step in conducting a risk assessment. The combined approach utilizes the NIST SP 800-30 revision 1 semi-quantitative scales of overall likelihood and level of impact to create a matrix which can describe the risk appetite of the company. [27]

Risk appetite needs to be defined with the company's goals, capabilities, and the interests of all stakeholders in mind. [28]

Overall Likelihood	Level of Impact				
	Very low (0)	Low (2)	Moderate (5)	High (8)	Very High (10)
Very Low (0)	Accept	Accept	Accept	Mitigation	Mitigation
Low (2)	Accept	Accept	Mitigation	Mitigation	Mitigation
Moderate (5)	Accept	Mitigation	Mitigation	Share	Share
High (8)	Accept	Mitigation	Mitigation	Share	Share
Very High (10)	Accept	Mitigation	Mitigation	Share	Share

13. Table: Risk Appetite of SoDevCo Ltd.

The above table shows that the company is willing to accept risk with Very Low Level of Impact and even risks with Moderate impact if the Overall Likelihood is low enough, and plans to share the responsibility of risk management in cases where the impact of the risk is High or Very High and the Overall likelihood of the risk is above Low. In any other cases the risk treatment is Mitigation.

The following table is the risk analysis table, showing the connections between assets, threat sources, threat events with the corresponding likelihoods and levels of impact. [27] Based on the Likelihood of Attack Initiation and Likelihood of Attack Success the Overall Likelihood can be read from the Table G-5: Assessment Scale – Overall Likelihood table of the NIST SP 800-30 revision 1. The Level of Risk comes from the above Risk Appetite table based on the Overall Likelihood and Level of Impact values of the rows. [15]

No.	Asset	Threat Event	Threat Sources	Likelihood of Attack Initiation	Likelihood of Attack Success	Overall Likelihood	Level of Impact	Level of Risk/Treatment
1	A1	T1	S1, S2, S3, S4, S5, S6, S7, S8, S12	Moderate	Moderate	Moderate	High	Moderate (Share)
2	A1	T2	S1, S2, S3, S4, S5, S6, S7, S8	Low	Moderate	Low	High	Low (Mitigate)
3	A1	T3	S1, S2, S3, S4, S5, S6, S7, S8	Low	High	Moderate	Very High	High (Share)
4	A1	T4	S11, S12, S13, S14, S19	Moderate	Low	Low	Low	Low (Accept)
5	A8	T5	S1, S2, S3, S4, S5, S6, S7, S8, S10	Moderate	Moderate	Moderate	High	Moderate (Share)
6	A8	T6	S1, S2, S3, S7, S11, S12	Moderate	Moderate	Moderate	High	Moderate (Share)
7	A9	T1	S1, S2, S3, S4, S5, S6, S7, S8, S12	Low	Moderate	Low	High	Low (Mitigate)
…								

14. Table: Risk analysis table. Self-editing.

To highlight just a few examples, firstly the asset of the greatest value of a software development company is the codebase of its product (denoted as A1). Row #1 in the table above means that the responsibility should be shared in case of the risk of right abuse on the main source code repository, which is fulfilled since the codebase is stored in a GitHub repository which has its own measures, controls and solutions regarding security.

Another example of sharing responsibility is row #6 the tampering with the production AtTrack Software (A8), it is shared with customer organizations, since they are the end-users of the application, so it is their responsibility as well that the users of the application are well-trained, trustworthy and disciplined.

The last step of a Risk Assessment process is the *Risk evaluation*, the goal is to create a prioritized list of risks according to the risk criteria. The following table show the risk priority matrix, classified based on the NIST SP 800-30 revision 1, describing the relationship between assets and threats. [27]

		Threats						
		T1	T2	T3	T4	T5	T6	…
Assets	A1							
	…							
	A8							
	A9							
	…							

Priority color codes
Very High
High
Moderate
Low
Very Low

15. Table: Risk priority matrix. Self-editing.

SUMMARY

The combination technique focuses on information security risk assessment resulting in a comprehensive risk assessment by following the ISO 27005 standard, utilizing the simplicity of the NIST SP 800-30 semi-quantitative scales. Using these supports the ISO standard when it requires the development of metrics. Although the example in this study is based on a business organization, the methodology is surely suitable for government bodies as well.

Based on my experience, unfortunately the product catalogues of ENISA and NATO (NIAPC) are both seem out of date. In my humble opinion it seems timely to conduct a comprehensive content review and update on both catalogues.

ISO/IEC 27001 certification is a hot topic these days even in Hungary, but unfortunately not all standards of the ISO/IEC 27000 series are published in our country. It would be highly desirable to publish all standards of the series in Hungarian and also MSZT being a participating member of the technical committee in charge of developing the series.

A family of Hungarian national recommendations such as the KIB-published MIBA is of great importance on information security trends, being a great initiative, it should be kept updated through regular revisions.

RESOURCES USED

[1] ISO, ISO/IEC 27001:2013, ISO, 2013.
[2] F. Erich, C. Amrit and M. Daneva, Report: DevOps Literature Review. University of Twente, Enschede, Netherlands, 2014.
[3] R. T. Yarlagadda, How DevOps Enhances the Software Dévelopment Quality, International Journal of Creative Research Thoughts (IJCRT), vol. 7, no. 3, pp. 358-364, 2019.
[4] R. T. Yarlagadda, DevOps and Its Practices, International Journal of Creative Research Thoughts (IJCRT), vol. 9, no. 3, pp. 111-119, 2021.
[5] L. Bass, I. Weber and L. Zhu, DevOps: A Software Architect's Perspective, Pearson Education, Inc., 2015.
[6] B. Delb, The CAMS model to better understand the DevOps movement, 22 07 2018. [Online]. Available: https://brunodelb.medium.com/the-cams-model-to-better-understand-the-devops-movement-ffe6713c3fd7. [Accessed 07 05 2021].

[7] S. Guthrie, DevOps Principles- The CAMS Model, 05 05 2019. [Online]. Available: https://medium.com/@seanguthrie/devops-principles-the-cams-model-9687591ca37a. [Accessed 07 05 2021].
[8] Atlassian, What is Continuous Integration?, [Online]. Available: https://www.atlassian.com/continuous-delivery/continuous-integration. [Accessed 15 05 2021].
[9] Mohammed Mehedi Hasan; Farzana Ahamed Bhuiyan; Akond Rahman, Testing Practices for Infrastructure as Code, ESEC/FSE '20: 28th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, 2020.
[10] I. El Fray, A comparative study of risk assessment methods, MEHARI & CRAMM with a new formal model of risk assessment (FoMRA) in Information Systems, In: Cortesi A., Chaki N., Saeed K., Wierzchoń S. (eds) Computer Information Systems and Industrial Management. CISIM 2012. Lecture Notes in Computer Science, vol. 7564, 2012.
[11] Magyar Informatikai Biztonsági Keretrendszer (MIBIK), KIB, 2008.
[12] NIAPC (NATO Information Assurance Product Catalogue), NATO Information Assurance Product Catalogue, [Online]. Available: https://www.ia.nato.int/NIAPC. [Accessed 02 05 2021].
[13] ENISA, European Union Agency for Cybersecurity, ENISA, [Online]. Available: https://www.enisa.europa.eu/. [Accessed 07 05 2021].
[14] NIST, NIST, [Online]. Available: http://nist.gov. [Accessed 02 05 2021].
[15] NIST, SP 800-30 revision 1, NIST, 2012.
[16] NIST, NIST SP 800-37 revision 2, NIST, 2018.
[17] ENISA, SP800-30 (NIST), [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_sp800_30.html. [Accessed 02 05 2021].
[18] ENISA, Cramm, [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html. [Accessed 30 04 2021].
[19] NIAPC (NATO Information Assurance Product Catalogue), CRAMM, [Online]. Available: https://www.ia.nato.int/niapc/Product/CRAMM_257. [Accessed 30 04 2021].
[20] IT Governance , Information Security and ISO27001 – an Introduction, [Online]. Available: https://www.itgovernance.co.uk/files/Infosec%20101v1.1.pdf. [Accessed 30 04 2021].
[21] ISO, iso.org, ISO, [Online]. Available: www.iso.org. [Accessed 05 04 2021].
[22] CRAMM, CRAMM, [Online]. Available: http://www.cramm.com/. [Accessed 30 04 2021].
[23] MSZT, Magyar Szabványügyi Testület - Az információbiztonság-irányítás szabványai, [Online]. Available: http://prod.mszt.hu/hu-hu/szabvanyositas/hirek/2015/03/az-informaciobiztonsag-iranyitas-szabvanyai. [Accessed 29 04 2021].
[24] NAH, NAH, NAH, [Online]. Available: https://www.nah.gov.hu/. [Accessed 10 04 2021].

[25] ENISA, ISO/IEC 27001, [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_iso27001.html. [Accessed 02 05 2021].
[26] Putra, Fandi A., S. Hermawan, and R.P. Anggi., Design of Information Security Risk Management using ISO/IEC 27005 and NIST SP 800-30 Revision 1: A Case Study at Communication Data Applications of XYZ Institute, International Conference on Information Technology Systems and Innovation, vol. 8, no. 4, pp. 251-256, 2017.
[27] Muhamad Al Fikri et al., Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency, Procedia Computer Science - The Fifth Information Systems International Conference, vol. 161, pp. 1206-1215, 2019.
[28] ISO, ISO/IEC 27005:2011, ISO, 2011.
[29] ISO, ISO 31000:2018, ISO, 2018.

HUMAN RISK FACTORS TO MEASURE THE POTENTIAL OF DIGITAL INFORMATION LEAKAGE

EMBERI KOCKÁZATI TÉNYEZŐK DIGITÁLIS INFORMÁCIÓ SZIVÁRGÁS POTENCIÁLJÁNAK MÉRÉSÉRE

LAUFER Edit[1] – SZÁDECZKY Tamás[2] – VÁCZI Dániel[3]

Abstract

One of the most challenging risk factors of cybersecurity to measure is the human factor. Each individual working for a given organization has a different personality, environmental conditions, and everyone within the organization holds a different position. The various factors are often difficult to quantify, and furthermore, each is highly interdependent from the other. It is necessary to know this risk factor and then build stronger security based on it, as attacks in cyberspace often take advantage of the lack of user knowledge or the mistakes made by developers and operators. To establish a risk factor approaching reality, the authors aim to create a fuzzy system, as this mathematical method is best suited for modeling human logic in addition to handling uncertainties. In this study, the authors present the results of the survey they have conducted, exploring risk factors relevant to digital information leakage.

Keywords

Cybersecurity, Human factor, Risk factor

Absztrakt

A kiberbiztonság egyik legnehezebben számszerűsíthető kockázati faktora az emberi tényező. Ennek oka, hogy egy adott szervezetnél dolgozó egyén más személyiséggel, környezeti körülményekkel rendelkezik és a szervezeten belül is mindenki más pozíciót tölt be. A különböző tényezők sokszor nehezen számszerűsíthetők és ráadásul nagymértékben függenek egymástól. Ennek a kockázati tényezőnek a megismerése, majd ez alapján az erősebb védelem kialakítása szükséges, hiszen a kibertérben lévő támadások sokszor használják ki a felhasználók ismereteinek hiányát, vagy a fejlesztők, üzemeltetők hibáit. A valóságot megközelítő kockázati tényező megállapításához a szerzők célja egy fuzzy rendszer megalkotása, mivel ez a matematikai módszer alkalmas a leginkább a bizonytalanságok kezelése mellett az emberi logika modellezésére. Jelen tanulmányban a szerzők ismertetik annak a kérdőíves kutatásnak az eredményét, amely a digitális információ szivárgás szempontjából releváns kockázati tényezők feltárására irányult.

Kulcsszavak

Kiberbiztonság, Emberi faktor, Kockázati tényezők

[1] laufer.edit@bgk.uni-obuda.hu | ORCID: 0000-0001-8362-4334 | institute director, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering Institute of Mechatronics and Vehicle Engineering | intézetigazgató, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Mechatronikai és Autótechnikai Intézet

[2] szadeczky.tamas@kvk.uni-obuda.hu | ORCID: 0000-0001-7191-4924 | associate professor, Óbuda University Kandó Kálmán Faculty of Electrical Engineering Institute of Instrumentation and Automation | egyetemi docens, Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar Műszertechnikai és Automatizálási Intézet

[3] vaczi.daniel@uni-obuda.hu | ORCID: 0000-0001-6770-6954 | doctoral student, Óbuda University Doctoral School on Safety and Security Sciences | doktoravrományos, Óbudai Egyetem Biztonságtudományi Doktori Iskola

DIGITAL INFORMATION LEAKAGE AS A CYEBERSECURITY THREAT

Nowadays, people have easy access to various sorts of information. Previously in history, the flow of information has been a much slower process. Today, thanks to IT and network systems, we have many tools to acquire new knowledge. By the 2020s, we have come to the conclusion that digital transformation is not an option but an essential direction of development for companies. Because of the information-based operation processes, not only the companies can maximize their profits, but governmental and academic stakeholders can be more effective as well.

Besides our professional life, our private life becomes more and more information-centric. Our smartphones and wearable devices allow the development of cutting-edge technologies [1]. People intentionally or unconsciously share a lot of information about themselves, including their workplaces without thinking about what consequences their actions might cause. A reckless act can, unfortunately, easily lead to the economic disadvantage of an organization.

Even if professionals build state-of-the-art security solutions, they will never be completely effective against the human factor. That is why the cybersecurity sector needs to pay bigger attention to the people besides technology.

Targeted attacks are usually driven by a specific motive. It can be cybercrime, hacktivism, cyberterrorism, cyber espionage, or cyber warfare [2]. The goal can be gaining information, harming, blackmailing, holding back, making money, and many other reasons. The malicious party usually has enough time to gather the right amount and quality of information about security solutions, various IT solutions, and the workforce as well as at the target. Based on them the action is deliberately directed against an object or person.

If companies are surrounding themselves with dissatisfied, offended, underpaid employees, they can be a perfect next step of a targeted attack. In such cases, the attacker may offer an appropriate amount in exchange for inserting a flash drive into one of the company's computers. After that, the malicious program code executes. This is just an example. Attacks like this can make the attacker's job easier, because they do not need to crack complex systems, they just ask the user to do something. Of course, these have to be well prepared. They have to find the weakest link among the company and make any so-called social engineering (manipulation) attack [3].

Many people think they are too insignificant to be victims of a cyber attack, but in the case of a multinational company or a governmental organization, anyone can. Furthermore, the SME sector is not protected either. For example, if a ransomware virus purchased by a malicious competitor hits a small enterprise, all of its data can be lost without a proper data backup process. At the end of the day, it can easily lead to bankruptcy.

The social engineering attacks can be divided into two main types [4]. The first one, the human-based attacks do not require any technological tools. In these cases, the attackers usually steal someone's identity or use a fictional one to have access to different IT systems or gather classified (or at least sensitive) information.

The other group includes attacks where there is no real cracking of a system, but the attackers use some technology to pull the wool over the victim's eye. These are called IT-based social engineering attacks. For example, sending phishing emails, using keyloggers, or searching with Google Hacking Database or at different social media platforms are belong here [5].

CYBERSECURITY RISK MANAGEMENT WITH THE HELP OF FUZZY LOGIC

There are many risks in an organization's life, such as strategic, environmental, market, financial, operational, cybersecurity, or even compliance risks. In order to run a business properly nowadays, it is necessary to find the right optimum in the functionality, usability, and security of its information system. To optimize it, organizations use different risk assessment methods.

From the perspective of cybersecurity, the goal is to find the balance where preventive and reactive security controls are cost-effective. Firstly, it is necessary to identify potential security events with their mechanism and their effects. Then the impact on the organization should be estimated and quantified based on the recommendations and past experience [6]. This is typically done by the following calculation:

$$Risk = Probability * Loss$$

Based on the management's decision the company either takes the risks or onboard professionals to minimalize them. This decision depends on the risk exposure of the organization. One of the professionally accepted information security risk management methodologies is described in ISO/IEC 27005:2018 [7]. Cybersecurity risk management should be implemented along with a continuously developed business strategy [8]. This strategy should include the human risk as well, despite the fact that this is a risk that is very difficult to measure.

The reason behind the difficulty is the fact that each employee has various cybersecurity risks depending on their personality, personal background, and position in the organization. In addition, these factors are usually subjective and/or cannot be described by exact numbers. In addition, most cybersecurity professionals have a technological background, and human behavioral studies fall out of their focus.

Soft computing methods, and within that, fuzzy logic, is the most suitable to deal with these problems. A fuzzy model with a modular structure is suitable for handling the human factor in the field of cybersecurity [9], because this approach is able to deal with the uncertainty and subjectivity in the system and not just work with sharp boundaries.

HUMAN RISK FACTORS OF DIGITAL INFORMATION LEAKAGE

In order to develop an appropriate risk assessment model, it is necessary to identify risk factors. In order to identify cybersecurity risks, an extensive investigation is needed. It is necessary to know the individual's personality, private and professional environmental conditions.

In many cases, the factors explored in this chapter are only partially visible to the employer. Nevertheless, the authors have strived for a complete exploration, as the flexibility provided by fuzzy logic allows an organization to create its own model based on the information available.

In this article, the authors explicitly investigate the intentional or negligent leakage of digital information. Accordingly, when examining other cyber security threats, it may be necessary to review the composition and interaction of the factors described here.

Identification of risk factors

Digital information leakage can be interpreted as a planned behavior unless it is carelessly committed due to an individual's lack of competence or personality. It means that in order to find the risk factors we should examine how planned behavior works and what are the modifiers which can most likely eventuate by negligence rather than intent.

Ajzen's Theory of Planned Behavior (TPB) [10] guides us to understand how a person acts in a planned situation. It shows how *attitude*, *subjective norms*, *perceived behavioral controls* affect each other and the *intention*. Based on this theory Hunyady and Münnich conducted further research. Their goal was to find additional factors besides the primal ones which also have an impact on a much more specific course of action: corruption. Their model (Solid Moral Index) [11] insert *organizational norm*, *personality traits*, *self-assessment*, *social norm*, *moral perception*, *profit*, *loss valuation*, and *experience* as important factors.

Previous studies [12] [13] show that if we would like to examine a specific behavior prediction (in our case the digital information leakage) the merged enquires are not usable. Therefore, in order to explore as many factors as possible, it is necessary to synthesize the results of existing and relevant researches [14] [15] [16] and conduct further ones.

It is important to emphasize, the authors do not intend to create an extended version of the TPB model or any more specific version of it. The focus is on examining various factors that may be suitable as inputs for a risk assessment fuzzy model.

In addition to examining the models in the previous subsection, it was necessary to explore additional factors to find as many possible inputs of the fuzzy model as possible. For this reason, the authors examined the national security questionnaire [17] and also made in-depth interviews with professionals familiar with various aspects of information leakage.

Demographical data of the questionnaire

Incorporating the processing of the listed sources a questionnaire was created to examine whether the cybersecurity profession can validate the hypothetical risk factors. A total of 174 surveys were completed, which, although not a representative sample, but can be used due to the specific selection of the focus group. The completion consisted of the following stages:

- First version created in Alchemer[4].
- Seventeen professionals working in different cybersecurity areas has been selected to fill the questioner and give feedbacks of it.
- Based on their completion, minimal stylistic and content changes were made. As no substantive changes have been made, their completion can also be considered during the evaluation.
- The questionnaire was published on the mailing lists of various professional organizations (ISACA Budapest Chapter and Hétpecsét Információbiztonsági Egyesület[5]) and in specific social media groups.

Although a total of 341 people started to complete the questionnaire, more than half of the respondents did not finish it. Due to the unrealistically short time of a number of

[4] In the beggining of the research it was named as SurveyGizmo.
[5] In mirror translation: „Seven Seal Information Security Association"

respondents have spent with filling the questionnaire, several ones can be considered invalid during the evaluation. The professional composition of the valid responders (several options could be selected) is described in the following table:

Role	**Number of fillers**
Security auditor	47
Security analyst	14
Security engineer	7
Security system administrator	4
Security strategist	7
Security consultant	36
Security tester/ethical hacker	2
CSO/CISO/CIAO/ISO	21
Deputy CSO/CISO/CIAO/ISO	3
Network administrator	3
Forensics specialist	3
Incident manager (organizational)	4
Information security manager	17
Project manager	17
SOC (monitoring, incident analyst)	2
Technical consultant	10
Operation manager	6
Other security	12
Other	44

1. Table: Rolls of the responders (own comparative analysis, edited based on own research)

The respondents were evaluated in two ways for issues related to the determination of risk factors. First, everyone's response was taken into account, and secondly, only the emphasized security professionals. In this second group the *Project managers*, *Technical consultants*, *Operation managers*, and those who clearly not security profession from *Other* roll was not included. People who answered *None* at the question *How many years of experience do you have in IT/cyber/information security?* were also not included in the second category, despite the fact that their position was relevant.

Timeframe	Number of fillers
None	28
I am an intern	18
3 years or less	20
4 -6 years	31
7-10 years	28
11-15 years	32
16-25 years	15
More than 25 years	2

2. Table: Rolls of the responders (own comparative analysis, edited based on own research)

The responders have experiences in many cybersecurity areas as the following table shows (several options could be selected):

Security area	Number of fillers
Safety awareness of end-users	103
Data protection	105
Application security	54
Auditing	93
Security administration	58
Security architecture and models	37
Planning cybersecurity exercises	37
Security management	74
Security regulations (not data protection)	49
Security planning	42
BYOD	26
Security of cloud-based services	32
Threat modeling	31
Incident response	63
Access management	89
Risk management	83
Forensics	16

Security area	Number of fillers
Mobile device protection	32
Education	72
Personal security risks management	34
Telecommunications and network security	42
Operational safety	57
Business continuity and disaster recovery planning	70
None of them	34

3. Table: Cybersecurity areas of the responders (own comparative analysis, edited based on own research)

Most of the responders work at relevant sectors, such as telecommunication, financial, governmental and IT. Hence the main focus was the human factor, the questionnaire contained also the question *How much do you consider yourself a good judge of character?* From the 5 possibilities a total of eighty percent responded *Average*, *Better than average*, or *Very good* and the rest fifteen percent selected only from the *Not at all* or the *Little* answers. It means that the result is evaluable.

Exploring additional factors using a questionnaire

The first not sociodemographic part of the questioner focused on the risk of the different roles in a company. The assumption is that individuals working in different jobs represent different levels of risk with respect to digital leakage. The goal was not to define all kinds of jobs at a multinational company but to find the most typical ones. Additional uncertainty is further specifications could be used within a role. A member of the cleaning staff who also has access to the server room may pose a higher risk than an accountant with few privileges. Although a more specific result would be closer to reality, the answers show that the assumption is correct, as there is a clear difference between the risks of each job based on the answers' median (*Table 4*). In this sense, it is an important risk factor in the fuzzy model.

Job	Median in a 1-10 scale
Assistant (non-managerial)	4
Security guard at the reception	4
Controller	4
Trainee	4
Hostess	3
HR officer	4
Education	6

Job	Median in a 1-10 scale
Computer scientist	5
IT security officer	4
Lawyer	4
Branch manager	4
Accountant (finance and accounting)	4
Marketing	3
Cleaning / maintenance staff	4
Customer Service Representative	3
Management Assistant	5

4. Table: Median of the job risk (own comparative analysis, edited based on own research)

One of the most important parts of the questionnaire was character analysis. Sixteen character descriptions were given to the responders. In each, specifics were placed indirectly that emerged as a risk factor during literature research, in-depth interviews, and real social engineering audits. In addition to the characteristics of the workplace, there were also elements related to lifestyle, marital status, or even personality traits. Each description looked like the following one (without underscores and numbers):

An agile college student (7;5), who has a partner (6;0), but often flirts with others within the company (45;35). She has a weak financial background (64;42), coming from a poor family (6;4). Due to her age, she is more receptive to technology (11;8). She is an average active user (9;7) who also uses social media a lot (53;41). She does a monotonous job with precision (13;10), which is underestimated (77;53). She could do a lot more work (7;5). She failed to fully integrate with full-time employees (26;14), who treat her as "just a trainee" (24;16). Her moral values have not yet fully been developed (87;69). She smokes (6;5) and goes to parties a lot (11;8).

The responders had to select a minimum of one, maximum of three words or short phrases in each characteristic, which they consider to be risky for leaking sensitive information upon external request, voluntarily or negligently. All the given answers were analyzed. The separate underlined sections in the previous paragraph are considered as an element. The first number in parentheses shows how many of the one hundred and seventy-four respondents marked out of them in total as risky. The second value shows how many of these have relevant cyber security experience. If more than twenty percent of all respondents or professionals indicated the element as risky, it was highlighted as a relevant risk factor (input) in the fuzzy model.

To explore other factors, items in the list below also needed to be evaluated. The consideration was to what extent it increased the risk of a person becoming blackmailed so they could leak sensitive information. The list, sorted by results (starting with less risky) is as follows:

- The relationship status of a given person, in which case s/he is also responsible for her/his partner.
- Having extensive work experience in the given location and position.
- The fact that the given person is an external staff member.
- Inadequate health condition.
- Insufficient life experience.
- Lack of a proper, attentive leader.
- The ability to bear psychological load (stress and frustration tolerance).
- Marginalization from the workplace community.
- Lack of self-knowledge.
- Low level of EQ.
- Social environment voicing negative opinion towards the given person.
- Inattentiveness.
- Low level of IQ.
- The person must support several children.
- The person has already committed minor offenses.
- Large-scale access to sensitive data.
- Hidden deviation from social norms (religious, sexual, political, etc.).
- Poor financial background (perceived or real existential problems).
- Lack of loyalty to the organization.
- Infringement (salary increase, lack of promotion).
- Poor value judgment / value system.
- Addiction.
- Weak morals.

SUMMARY

Reducing cybersecurity risks is essential for an organization in order to preserve proper functioning from a business perspective. The treatment of human factors is crucial, however, it is a challenging process, hence human beings are very complex, and the threats they pose are often subjective and difficult to quantify.

Understanding human risk factors as a specific threat, digital information leakage has been selected and examined with the help of literature research, in-depth interview, and questionnaire research. During the exploration, many risk factors have been found.

Knowing the right factors, a complex model can help to identify the riskiest employees from the perspective of digital data leakage. Each explored element can be an input of a complex fuzzy model that help the managing board and the cybersecurity professionals of an organization to identify employees who pose a potential risk. The model can also help to examine other weaknesses after performing appropriate changes.

LITERATURE

[1] Gottdank T., *Szolgáltatásalapú világ*. Bicske: SZAK Kiadó, 2013.

[2] C. Krasznay, „A polgárok védelme egy kiberkonfliktusban”, *HADMÉRNÖK*, köt. VII, o. 142–151, 2012. [Online] Available: http://hadmernok.hu/2012_4_krasznay.pdf [Accessed 19 08 2021]

[3] D. Váczi, „Célzott támadások módszertana”, in *Célzott kibertámadások*, 2018, o. 52–75. [Online] Available: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/7237/C%E9lzott%20ki-bert%E1mad%E1sok%203_jav.pdf;jsessio-nid=073EEE9139D87BF87C010387DBB0E054?sequence=1 [Accessed 19 08 2021]

[4] K. D. Mitnick és W. L. Simon, *A legendás hacker - A megtévesztés művészete*. Budapest: Perfact-Pro Kft., 2003.

[5] H. Cristopher, *Social Engineering - The scinece of Human Hacking*. Indianapolis: John Wiley & Sons, Inc., 2018.

[6] J. Beinschróth, *A kockázatok kezelése, védelmi intézkedések*. 2018.

[7] „ISO/IEC 27005:2018”, *ISO*. [Online] Available: https://www.iso.org/cms/ren-der/live/en/sites/isoorg/contents/data/standard/07/52/75281.html [Accessed 19 08 2021]

[8] L. Kovács, *Kiberbiztonság és -stratégia*. Dialóg Campus Kiadó - Nordex Kft, 2018.

[9] D. Vaczi, E. Toth-Laufer, és T. Szadeczky, „Fuzzy-based Cybersecurity Risk Analysis of the Human Factor from the Perspective of Classified Information Leakage”, in *2020 IEEE 18th International Symposium on Intelligent Systems and Informatics (SISY)*, szept. 2020, [Online] Available: https://ieeexplore.ieee.org/document/9217053 [Accessed 19 08 2021]

[10] I. Ajzen, „The theory of planned behavior”, *Organizational Behavior and Human Decision Processes*, köt. 50, sz. 2, o. 179–211, 0 1991, doi: 10.1016/0749-5978(91)90020-T. [Online] Available: https://www.sciencedirect.com/science/article/abs/pii/074959789190020T [Accessed 19 08 2021]

[11] Hunyady G. és Münnich Á., „A szilárd erkölcsiség elvárása a rendvédelemben: egy lehetséges pszichológiai modell”, *Belügyi Szemle*, köt. 64, sz. 6, Art. sz. 6, jún. 2016, doi: 10.38146/BSZ.2016.6.2. [Online] Available: https://belugyi-szemle.hu/hu/node/1415 [Accessed 19 08 2021]

[12] A. W. Wicker, „Attitudes versus Actions: The Relationship of Verbal and Overt Behavioral Responses to Attitude Objects”, *Journal of Social Issues*, köt. 25, sz. 4, o. 41–78, 1969, [Online] Available: https://spssi.onlinelib-rary.wiley.com/doi/10.1111/j.1540-4560.1969.tb00619.x [Accessed 19 08 2021]

[13] M. Walter, *Personality and Assessment*. Wiley, 1968.

[14] C.-H. S. Lin és C.-F. Chen, „Application of Theory of Planned Behavior on the Study of Workplace Dishonesty”, előadás 2010 International Conference on Economics, Business and Management, Manila, Philippines, 2010. [Online]. Available: http://www.ipedr.com/vol2/14-P00029.pdf [Accessed 19 08 2021]

[15] Hunyadi G., Malét-Szabó E., és Münnich Á., „A rendvédelmi szervek szervezeti normáinak és kultúrájának, mint a szilárd erkölcsiség egyik alapvető háttértényezőjének

empirikus próbavizsgálata", 2016, [Online]. Available: http://www.bm-tt.hu/assets/letolt/kutat/2016/SZEM.kulktura.tanulmany.pdf [Accessed 19 08 2021]

[16] P. Csató, G. Hunyadi, E. Malét-Szabó, és Á. Münnich, *Az erkölcsi értékrend és a személyiség közötti kapcsolat vizsgálati szempontjai*. Budapest: Crew Kft, 2015. Elérés: márc. 07, 2021. [Online]. Available: https://bmprojektek.kormany.hu/download/5/0a/51000/Az%20erk%C3%B6lcsi%20%C3%A9rt%C3%A9krend%20%C3%A9s%20a%20szem%C3%A9lyis%C3%A9g%20k%C3%B6z%C3%B6tti%20kapcsolat.pdf?fbclid=IwAR1HlU1A5XVJ3ufU1toGW1tM3sJPM-tD4z8KN__c5T8BoceAgVP7E4wnlPQ [Accessed 19 08 2021]

[17] „Nemzetbiztonsági ellenőrzés - NBF" [Online] Available: https://www.nbf.hu/hasznos-informaciok/nemzetbiztonsagi-ellenorzes/. [Accessed 19 08 2021]

THE CHALLENGE OF THE SOFTWARE ASSET MANAGEMENT IN PUBLIC SECTOR OF HUNGARY

A SZOFTVERLICENC-GAZDÁLKODÁS KIHÍVÁSAI A HAZAI KÖZIGAZGATÁSBAN

PRISZNYÁK Szabolcs [1]

Abstract

My thesis focuses on the current position and development paths of software asset management in Hungarian public administration. This subject matter's particular significance and topicality are enhanced by the fact that effective software asset management of public administration organisation was also highlighted by governmental policy through the 2021 amendment of the relevant legal act. With my research, I seek to answer the questions of what maturity level software asset management currently has, how its organisation, policy systems, and processes should be constructed, and what special requirements and considerations should be reinforced with regards to the supporting IT system.

Keywords

software asset management, maturity level, process, register, public sector

Absztrakt

Publikációm témája a szoftverlicenc-gazdálkodás jelenlegi helyzete, fejlesztési lehetőségei a hazai közigazgatásban. A téma különös jelentőségét, aktualitását kiemeli, hogy 2021-ben jogszabálymódosítás következtében a kormányzati szakpolitika is előtérbe helyezi a közigazgatási szervezetek hatékony szoftverlicenc-gazdálkodását. Kutatásomban arra kerestem a választ, hogy a közigazgatásban a szoftverlicenc-gazdálkodás milyen érettségi szinten van, hogy célszerű kialakítani a szervezeti, szabályozási rendszerét, folyamatait, továbbá, hogy milyen speciális követelményeket kell érvényesíteni a tevékenységet támogató informatikai rendszerre vonatkozóan.

Kulcsszavak

szoftverlicenc-gazdálkodás, érettségi szint, folyamat, nyilvántartás, közigazgatás

[1] prisznyak.szabolcs@outlook.com | ORCID: 0000-0002-3234-7485 | head of IT department, National Tax and Customs Administration of Hungary | informatikai főosztályvezető, Nemzeti Adó- és Vámhivatal

BEVEZETÉS

Mindannyian tapasztaljuk, hogy modern technológia, informatika nélkül ma már szinte egyetlen mikróvállalkozás sem tud működni. A nagyobb szervezeteknél pedig az informatika – korábbi támogató, kiszolgáló szerepéből kilépve, - ma már a szervezeti stratégia megvalósításának alapvető pillére [1, p. 78]. A versenyszféra mellett nincs ez másként a közigazgatásban sem, fontos kormányzati cél a szolgáltató állam kialakítása, a digitális közszolgáltatások szerepének növelése. „A közigazgatás egyik lényeges újítása az Elektronikus támogatások fejlesztése (Digitális Állam felépítése) program megvalósítása." [2, p. 274] Fentiekből következően a közigazgatási szervezeteknél is egyre inkább kiemelt szerepe van az informatika fejlődésének.

Az ezredforduló éveiben „A szoftver éhség a vezetés részéről is egyre határozottabban jelenik meg, tényleges vezetői irányító megoldások igényében, döntéselőkészítést támogató automatikus adatszolgáltatásban." [3, p. 30]. Napjainkra nagyon széles az alkalmazott szoftverek köre, megjelennek az operációs rendszerek, az adatbáziskezelők, az irodai munkát, a csoportmunkát támogató rendszerek, térinformatikai, vállalatirányítási megoldások, valamint sok más további termék mellett – napjainkban kiemelt jelentőséggel – a videókommunikációs alkalmazások. Ezen – úgynevezett dobozos termékek mellett – a speciális szaktevékenységek informatikai támogatását egyedileg fejlesztett megoldásokkal valósítják meg. A közigazgatási szervezetek napjainkra széleskörű szoftver porfólióval rendelkeznek, amelyek értéke – a szervezet feladatkörétől, méretétől függően – akár a több tízmilliárd forintot is elérheti. A szoftverlicencek nyilvántartására azonos jogszabályok vonatkoznak, mint más javakra. Ezek a nyilvántartások azonban nem tartalmaznak valamennyi adatot az egyes termékek használatának lehetőségeivel, szabályaival kapcsolatosan. Ezt fokozza, hogy az egyes gyártók szabályrendszere egymástól jelentősen eltérő. Ebből következően a szoftverlicencek nyilvántartása, életciklusa során történő kezelése speciális folyamatokat, eljárásrendet, szabályozást és szakértelmet igényel.

A közigazgatási informatika fejlődését támasztja alá a Központi Statisztikai hivatal mérése is, hiszen 2010-2020 között közel duplájára emelkedett az elektronikus közszolgáltatásokat igénybe vevő felhasználók aránya [4]. Magyarország saját költségvetésből és az Európai Unió által biztosított alapok felhasználásával jelentős forrásokat (az Európai Szociális Alapból 2021. április 30-ig több, mint 892 millió Euro) fordított a közigazgatás fejlesztésére, ennek meghatározó része a digitalizációt, az állampolgárok által elérhető szolgáltatások számának növelését, minőségének bővítését szolgálja [5, pp. 77-78.]. Az elektronikus közszolgáltatások folyamatos fejlesztéséhez, funkcionalitásának bővítéséhez elengedhetetlen a közigazgatási szervezetek által – a háttérben - működtetett informatikai rendszerek – eszközök, rendelkezésre állást biztosító infrastruktúra és szoftverek – ciklikus megújítása, bővítése. Ebből következően az alkalmazott szoftverek, valamint a működtetésükhöz szükséges gyártói támogatások (support) mennyisége, ezzel együtt értéke is folyamatosan növekedik. A dinamikusan növekvő szoftvervagyon megköveteli ezen érték professzionális megoldással történő kezelését.

A szoftverlicenc-gazdálkodás az utóbbi években azon informatikához köthető egyik újszerű feladat, ami – a digitalizáció, a mesterséges intelligencia, a robotizáció, az adatvagyon gazdálkodás mellett - egyre fontosabb szerepet tölt be a vállalatok működésben. Az új feladatok a korábbi – elsősorban technológiai szemléletű kompetenciát kiszélesítve – a szervezetek több szakterületét átfogó komplexebb látásmódot igényelnek. Ezen új kihívások

egyike a szoftverlicenc-gazdálkodás, amely a közigazgatási szervezeteknél – azok működésének szabályrendszere, ebből következő sajátosságai, valamint a versenypiaci szereplőktől eltérő gazdálkodása okán – a piaci szféra résztvevőihez hasonlítva bár közel azonos alapelveken, de végeredményben – elsősorban a szervezeti, szabályozási, technológiai oldalt tekintve - részben eltérő módon valósul meg.

A szoftverlicence-gazdálkodás rendszerének, folyamatainak, szervezeti kereteinek kialakítása évtizedes adósság a közigazgatásban, ez hatványozottan igaz a nagy mennyiségű és ebből következően nagy értékű szoftverekkel rendelkező szervezeteknél. E hiátus kezelésének szükségességét kormányzati szinten is a megoldandó problémák közé sorolta a szakpolitika. Ennek eredményeként 2021. január 1-től módosult a Nemzeti Hírközlési és Informatikai Tanácsról, valamint a Digitális Kormányzati Ügynökség Zártkörűen Működő Részvénytársaság és a kormányzati informatikai beszerzések központosított közbeszerzési rendszeréről szóló 301/2018. (XII. 27.) Korm. rendelet. A korábban az informatikai közbeszerzések egységes kezelését szabályozó Korm. rendelet kiegészült a szoftverlicenc-gazdálkodásra vonatkozó rendelkezésekkel. A szoftverlicenc-gazdálkodást a jogszabály „a szoftverlicencek, a kapcsolódó licenckövetési és támogatási szolgáltatások nyilvántartásához, menedzsmentjéhez, optimalizálásához, valamint céltudatos, hatékony felhasználásához, beszerzéséhez kapcsolódó tevékenységek összessége”-ként határozza meg. A jogszabály 14/A. § -a részletesen szabályozza a szoftverlicenc-gazdálkodással kapcsolatosan a Digitális Kormányzati Ügynökség Zrt. (továbbiakban DKÜ Zrt.) feladat- és hatáskörét. A DKÜ Zrt. a kormányzati szoftverlicenc-gazdálkodási feladatait – jogszabályban foglalt felhatalmazása alapján - a Kormányzati Szoftverlicenc-gazdálkodási Kft. (továbbiakban KSZG Kft.) bevonásával látja el. Fontos kiemelni, hogy a DKÜ Zrt. és a KSZG Kft. jogosult az érintett szervezetektől – tehát valamennyi közigazgatási szervezettől - a szoftverlicenc szerződései adatairól, gazdálkodása körülményeiről vagy egyéb szükséges adatokról adatszolgáltatást kérni. Ezt a közigazgatási szervezetek tíz munkanapon belül kötelesek teljesíteni.

Fenti jogszabálymódosítás okán tehát valamennyi közigazgatási szervezetnél rövidvagy középtávon ki kell alakítani a szoftverlicenc-gazdálkodás rendszerét – személyi, szervezeti, szabályozási és eszköz feltételeit - hiszen a szervezetek csak ezzel válhatnak képessé a jogszabályban meghatározott adatszolgáltatás teljesítésére. A fajsúlyos informatikai rendszerekkel rendelkező szervezeteknél szükséges lehet, hogy a szoftverlicenc-gazdálkodás folyamatait informatikai rendszer támogassa, ezzel biztosítva az automatizálást, beleértve a DKÜ Zrt. és a KSZG Kft. részére történő adatszolgáltatást is.

A SZOFTVERESZKÖZ-GAZDÁLKODÁS HIÁNYÁNAK KOCKÁZATAI

A kifejezetten szoftvereszköz-gazdálkodással foglalkozó terület, tevékenység hiánya miatt a közigazgatási szervezeteknek kockázatok sorával kell szembenéznie. Egyrészt jelentős gazdasági, anyagi kockázatot rejt magában, ha a szervezetek nincsenek tisztában a rendelkezésükre álló eszközökkel, mivel így nehezebbé vagy esetleg teljesen lehetetlenné válik a hatékony tervezés, melynek következtében jelentős többlet forrást igényelhet az informatikai infrastruktúra fenntartása.

Fennáll az illegális szoftverfelhasználás veszélye is, amely polgári jogi és büntetőjogi felelősségre vonást is eredményezhet, és további anyagi hátrányokat jelenthet, valamint a szervezet reputációját is veszélyezteti. Az illegális szoftverfelhasználás biztonsági, adatvédelmi kockázatokat is jelent. Mindezeken túl az alábbi kockázatok merülhetnek fel:

A szoftver felhasználás pontos nyilvántartása és a változáskezelés hiánya miatt elfordulhat szükségtelen szoftver beszerzés.

A nem használt szoftver licencek esetében elfordulhat – szükségtelen - támogatás (support) beszerzés.

Ha nem ismert a pontos felhasználás, akkor az érintett szakterület nem értesül arról, hogy új beszerzést kell indítani. A későn elindított közbeszerzési (vagy beszerzési) eljárás kockázatos lehet a szervezetek jogszabályban meghatározott tevékenységére.

A nem konszolidált igények okán rosszul előkészített beszerzés miatt a szervezet eleshet a nagyobb arányú szállítói kedvezménytől.

A szoftvereszköz-gazdálkodás hiánya miatt a szervezet az adatszolgáltatási kötelezettségének sem tud jó minőségben eleget tenni, ezzel a jogszabályban meghatározott határidő mulasztását is kockáztatja. Ugyanakkor kontraproduktív, hogy az adatszolgáltatáshoz szükséges információk összegyűjtése időigényes, erőforráspazarló tevékenység.

JOGI HÁTTÉR, NYILVÁNTARTÁSI KÖTELEZETTSÉG

A szoftverek nagy értékű immateriális javak, melyek nyilvántartására a számvitelről szóló 2000. évi C. törvény kötelezettséget ír elő. A könyvelésben is meg kell különböztetni, hogy az adott szervezet használati jogot szerez a szoftverre, vagy véglegesen tulajdonába kerül. Előbbi esetben a szoftvert vagyoni értékű jogként, míg utóbbiban szellemi termékként kell könyvelni [6].

Jogi szempontból a szoftverekre, a szellemi alkotások felhasználására vonatkozó szerzői jogi szabályok, mellett más jogterületek normái is érvényesek. Elsősorban ilyen a szerzői jog anyajogát képező polgári jog, azonban jogsértő magatartás estén a Büntető Törvénykönyv rendelkezései szerint kell eljárni. Ugyanakkor egyes szakértők véleménye szerint „a szoftverjog a szerzői jogból kinövő jogterületként egyre inkább önálló és differenciáltabb szabályozást igényel, hiszen … a jogkimerülés intézménye sem értelmezhető és alkalmazható más szerzői művekkel teljesen analóg módon” [7, p. 1.].

A szoftvereszköz-gazdálkodás a szervezet számára egyrészt az informatikai működés biztonsága, másrészt a jogi és pénzügyi kockázatok csökkentése végett is elengedhetetlen.

Amennyiben egy szervezet nem alkalmaz dedikált, kifejezetten erre a célra készült szoftverlicenc nyilvántartást, törvényi kötelezettségének akkor is eleget tesz, mivel a főkönyvi nyilvántartásban, valamint különböző további nyilvántartásokban (beszerzést támogató rendszer, szerződés-nyilvántartás, elektronikus iktató rendszer, stb.) megtalálhatók a szoftverlicencekre vonatkozó adatok. Tekintettel arra, hogy ezek a nyilvántartások nem kifejezetten szoftverlicenc nyilvántartásra készültek, az adatszolgáltatási kötelezettséget hosszútávon csak támogató informatikai rendszerrel, szakértő humán erőforrás bevonásával és részletesen meghatározott folyamatokkal lehet pontosan és szakszerűen teljesíteni.

SZOFTVERESZKÖZ-KEZELÉS (SAM) MEGKÖZELÍTÉSE

A szoftvereszköz-kezelés (SAM – Software Asset Management angol nyelvű rövidítése) bevezetésével egy olyan rendszert - jó gyakorlatot – kell kialakítani, amely magába

foglalja a szoftverek beszerzésének, telepítésének, karbantartásának, hasznosításának, selejtezésének (megsemmisítésének) kezelését, valamint a standardizálást és az optimalizálást is.

A SAM szabványosított megoldási módokat biztosít a szervezeteknek. Ezek közül a legjobb iparági gyakorlatokat összegző szabvány - az informatikai szolgáltatás irányítási rendszerének MSZ ISO/IEC 20000-1 számú szabványa, amely alapját az ITIL adta - az, amit célszerű a SAM koncepció kialakításakor alapul venni. Az ITIL a következőképpen határozza meg a SAM hatókörét: „A szoftvereszköz kezelés (SAM) azon szükséges infrastruktúrák és folyamatok összessége, amelyek a szoftvervagyon hatékony kezeléséhez, ellenőrzéséhez és védelméhez szükségesek egy szervezetben, a szoftver életciklus minden szakaszában." [8, p. 4.]

A szoftvereszköz kezelés alapvető célja, hogy a licenc nyilvántartás – a szervezet informatikai stratégiájának részeként – csökkentse az informatikára fordított költségeket, valamint korlátozza a szoftverek tulajdonjogával és alkalmazásával kapcsolatos üzleti és jogi kockázatokat [9, p. 13]. Mindemellett hatókörének fontos eleme, hogy növelje az informatikai szervezet reagáló készségét ezzel erősítve a szervezet rugalmasságát, sőt ezen túllépve pillére legyen egy reziliens működésű szervezetnek (azaz képes legyen ellenállni a szervezetet ért hatásoknak). A szoftverlicenc-gazdálkodást támogató technológiák nyomon követik a licenc életciklusát, ezáltal biztosítva a közigazgatási szervezetek számára, hogy a szoftver-megfelelőségi előírások betartásával működjön, ez fontos mind a licencszerződések megsértéséhez, mind a szoftverhasználati joghoz kapcsolódó kockázatok kezelése szempontjából is.

A szoftverlicenc-gazdálkodás folyamatainak, szervezeti kereteinek, szabályozásának kialakítása során egyedileg fel kell mérni az érintett közigazgatási szervezetnél, hogy az alaptevékenységéhez milyen szinten kapcsolódik az informatika. Elengedhetetlen annak meghatározása, hogy az informatika klasszikus kiszolgáló szerepkörben működik, vagy ezen túllépve – folyamatszervező képességét is kihasználva - a szervezeti stratégia végrehajtásának meghatározó elemévé vált [1, p. 55]. Fel kell mérni, hogy az informatika a vizsgált szervezetnél milyen belső és külső szolgáltatásokat nyújt, ezt milyen infrastruktúra és milyen szoftver portfólió használatával valósítja meg. Az így kialakításra kerülő SAM program stratégiai jelentőségűvé válik abban az esetben, ha maga az informatika is a szervezeti stratégia megvalósításának alapja, illetve erős támogató funkciója lesz abban az esetben, ha az informatika működése kiszolgáló jellegű. A szoftverlicenc-gazdálkodásnak valamennyi szervezetnél kifejezetten a megvásárolt és a felhasznált szoftverlicencek optimalizálása a feladata, így biztosítania kell a megvásárolt és a felhasznált szoftver mennyiség kiegyensúlyozását, úgy, hogy a telepített szoftverek használata megfeleljen a licencszerződésben meghatározott követelményeknek.

A SAM ÉRETTSÉGI SZINT MEGHATÁROZÁSA

A részletes szoftverleltár kialakítását – majd annak folyamatos karbantartását - meg kell, hogy előzze az érintett szervezet – szoftverlicenc-gazdálkodásra vonatkozó – érettségi szintjének megállapítása. A közigazgatási szervezeteknél első lépésként ehhez el kell végezni egy felmérést, amelynek adatai alapján meghatározásra kerül az érettségi szint. Ennek ismeretében lehet tervezni, majd meghatározni a szoftverlicenc-gazdálkodás kialakításának

– vagy továbbfejlesztésének – részletekre lebontott lépéseit, folyamatát, az egyes szakaszok mérföldköveit.

Az érettségi modellen belül minden szint tovább léphet a következő szintre, fontos azonban, hogy mindig csak az adott szint – valamennyi kritériumának teljes körű - teljesítését követően lehetséges a továbblépés, és mindig csak a következő érettségi szint következhet. A szakirodalom négy - egyes esetekben öt - érettségi szintet határoz meg, amelyek az alábbiak:

Alap: Jellemzője az alacsony kontrolláltsági szint, az eszközök használatára vonatkozóan, továbbá hiányoznak a folyamatok, a szabályozás, az erőforrások és az eszközök. A szervezet ezen a szinten is megfelelhet az alkalmankénti vizsgálatoknak, de az adatszolgáltatás nagy erőforrást igénylő manuális tevékenységen alapul, ahol több különböző – egymással nem összekapcsolt – rendszerből – amelyek sok esetben keresési lehetőséget sem biztosítanak – történik az adatgyűjtés. Az így szerzett információkat – céleszköz hiányában – táblázatkezelő rendszerbe töltik be, és kezelik.

Standardizált: A szoftverlicenc-gazdálkodás eszközei elérhetők, kialakított a folyamat. Rendelkezésre állnak az adatok, ezek azonban nem teljeskörűek és nem minden esetben pontosak. Az is jellemzője ennek a szintnek, hogy – mivel a nyilvántartás nem teljeskörű és pontos – az információkat nem használják fel döntésekre. A standardizált szint feladata a beszerzési folyamatok egységesítése, a licencraktár aktualizálása és a szoftverek kategorizálása. Ezen a szinten a szervezet már megfelel a gyártói auditoknak, illetve képes saját magára vonatkozó auditot végezni önellenőrzés céljából. Ez a szint már biztosíthatja a jogtiszta szoftverhasználatot, az adatgyűjtő rendszerek mellett megvalósul a licenckezelés, a raktár és a leltár.

Racionalizált (Aktív): Stratégiát, szabályzatokat, eljárásokat és eszközöket használnak a szoftverek teljes életciklusa alatt. Az információk megbízhatók, így alkalmasak a vezetői döntések támogatására. Ezen a szinten a szoftverhasználat a szükséges mértékű. A szoftverkatalógus teljes körű. A racionalizált szinten megvalósul a különböző informatikai rendszerek feltérképezése és a szoftverhasználat mérésének kialakítása.

Dinamikus (Optimalizált): Közel valós időben követik az igényeket, a szoftverlicenc-gazdálkodás rendszere stratégiai eszköz a szervezeti – stratégiában meghatározott – céljainak elérésében. Ezt a szintet a naprakész adatok és a hatékony folyamatok jellemzik. Folyamatos a licenc- és szoftverleltárak frissítése, a licencek optimalizálása. Megvalósulhat az integráció más rendszerekkel (pl. üzleti elemző rendszerek, BI), valamint elérhető a szoftver önkiszolgálás [10].

Egyes szakértők által készített érettségi modellben egy ötödik érettségi szint is beiktatásra került. Az öt szintű érettségi modellben az egyes szinteket elnevezése: Ad-hoc, Kezdetleges, Követő, Gazdálkodó, Hatékony [11]

A szakértők döntő többsége a négy szintű érettségi modellt használja a szervezetek érettségi szintjének meghatározása során, de a közigazgatási szervezetek esetében hasznos lehet az öt szintű modell is, hiszen sok szervezet rendelkezik olyan informatikai üzemeltetést támogató menedzsment rendszerrel, amelynek segítségével a szoftverlicenceinek egy részét képes felmérni (Kezdetleges szint).

A LEGFONTOSABB SAM FOLYAMATOK, SZABVÁNYOK

A szervezet érettségi szintjétől függően kell elkészíteni azt a stratégiát, majd ennek alapján a részfeladatokat is tartalmazó akciótervet, amelynek segítségével elérhető a dinamikus érettségi szint. Fontos, hogy a technológiai támogatás bevezetése előtt fel kell mérni a folyamatokat, ki kell alakítani a nyilvántartást, létre kell hozni, vagy ki kell jelölni a szervezetet, és szabályozni kell a tevékenység teljes folyamatát.

Azt azonban már a stratégia kialakításánál meg kell határoznunk, hogy a technológiának mely legfontosabb feladatokat kell támogatnia, ezek az alábbiak [8, pp. 47-66].

- Szoftverleltár (software inventory) készítés,
- Licenckezelő megoldás (license manager),
- Szoftverlicenc felhasználást mérő eszközök (software metering)
- Alkalmazásellenőrző eszközök (application control)
- Szoftvertelepítő (software deployment) eszközök
- Javítócsomagokat kezelő eszközök (patch management)
- Igénykezelő eszközök (request management)
- Termékkatalógus eszközök (product catalog)

A technológiával támogatott szoftverlicenc-gazdálkodás kialakítása során törekedni kell a szabványos megoldásra. A fent említett ITIL alapú szabvány (MSZ ISO/IEC 20000-1) mellett kifejezetten a szoftverlicenc-gazdálkodás magvalósítására vonatkozó nemzetközi szabványok is léteznek az alábbiak szerint.

- ISO 19770-1 keretrendszert biztosít a szoftverlicenc-gazdálkodás folyamatainak kialakításához, végrehajtásához [12, pp. 25-27].
- ISO 19770-2 a szoftver azonosító (SWID) címkék kialakítására és alkalmazására ad egységes előírást és eljárásrendet.
- ISO 19770-3 a szoftverjogosultsági címkézésre ad útmutatást.

Az ISO 19770-1 [13, p. 7] az informatikai vagyonelemek egyik nagy csoportjaként határozza meg a digitális vagyont (Digital Asset), amelyet további két csoportra oszt. Egyik csoport a „Digitális információ tartalmú vagyon", ebbe tartoznak a különböző dokumentumok, hang, kép és videóformátumok, valamint adatbázisok. A másik csoport a „Szoftver vagyon", ezen belül a szabvány megkülönbözteti a futtatható programokat - amennyiben rendelkezésre áll, úgy forráskóddal -, illetve a nem futtatható szoftvereket. Emellett megkülönbözteti a virtuális gépek működéséhez szükséges szoftvereket. A szabvány alapján a csoportosítás tehát technológiai alapon, és nem licencelés szerint történik. Az ITIL alapú szoftverlicenc-gazdálkodásról szóló könyvének függelékében Rudd részletesen csoportosítja a szoftverlicencek típusait és ebben a csoportosításban licenc alapú megközelítést alkalmaz [8, pp. 111-119].

Egyes szakmai fórumok a licencek csoportosítását - részben technológiai szempontok alapján, de - a szabványnál bővebben, több csoportot elkülönítve végzik [14]. Mások – mind hazai mind nemzetközi viszonylatban - azonban – a szabvánnyal ellentétesen – nem műszaki-technológiai, hanem jogi megközelítésből csoportosítják a szoftvereket. A licencelés vizsgálata szempontjából „a licencelés metódusa, valamint a jogtulajdonosi érdekérvényesítés szempontja szerint" [15, p. 1] történő csoportosítás a jobb megközelítés. A jogi

szakterület sok esetben nem is magát a szoftvert vizsgálja, hanem a szoftverlicenc-szerződések típusait [16].

SZOFTVERLICENC-GAZDÁLKODÁS ÉRETTSÉGE A KÖZIGAZGATÁSBAN

A szoftverlicenc-gazdálkodás kialakítása előtt elengedhetetlen, hogy az érintett szervezet alapos és részletes szakmai átvilágításon essen át annak érdekében, hogy a területről átfogó információval rendelkezzen. Egy ilyen felmérést célszerű külső szakértőkkel végeztetni, hiszen egyrészt olyan szaktudást igényel a tevékenység, amely csak specialisták által elvégezhető, másrészt a független külső szakértő bevonásával valamennyi területről objektív képet kaphatunk.

Nyilvánvalóan egy rendszer kialakításánál a szervezeteket egyesével kell felmérni, de a dolgozatomban egy átfogó helyzetképet szeretnék exponálni a közigazgatásban jelenleg tapasztalható szoftverlicenc-gazdálkodással kapcsolatos információkra vonatkozóan. A felmérés eszközéül a mélyinterjút választottam, de megoldást jelenthet egy kifejezetten erre a célra kidolgozott kérdőív is. Az érettségi szint felméréséhez alkalmazható módszertan bemutatása, valamint a mélyinterjú kérdéseinek, az azokra kapott válaszoknak részletes ismertetése meghaladja jelen mű kereteit, ezeket önálló cikkben tervezem feldolgozni. Jelen műben a felmérés eredményét ismertetem.

Interjúm alanyainak országos hatáskörű, több szintű hierarchiával rendelkező szervezetek szakembereit választottam. Összesen tíz szervezetet vizsgáltam, ezek közül nyolc klasszikus közigazgatási szervezet, kettő pedig 100%-ban állami tulajdonú gazdasági társaság. Valamennyi szervezet több ezer számítógépből álló informatikai rendszerrel és nagy értékű szoftver vagyonnal rendelkezik. A kutatásban résztvevő szervezeteket nem kívánom konkrétan megnevezni, célom, hogy a teljes közigazgatásra vonatkozó megállapításokat tegyek. A kérdéscsoportokba sorolt kérdések a szervezetek és az informatikai rendszerek méretére, az alkalmazott legfontosabb szoftverrendszerekre, ezek nyilvántartására, a kifejezetten szoftverlicenc-gazdálkodást támogató informatikai rendszerre, szervezetre, szabályozásra vonatkoztak.

A kérdéscsoportra adott válaszok értékelésével megállapítottam, hogy a szervezetek melyik érettségi szinten állnak a szoftverlicenc-gazdálkodás érettségi modellje szerint. Azt is megállapítottam hogy, ahol szoftverlicenc-gazdálkodást támogató informatikai rendszer bevezetése mellett döntenek, ott szervezeti és szabályozási oldalon ezzel párhuzamosan megtörténik a szükséges előrelépés. A négy szintű modellt vizsgálva megállapítottam, hogy hat közigazgatási szervezet alap szinten van, három racionalizált, egy pedig dinamikus szinten. Célszerűnek tartottam azonban az érettségi szintet megvizsgálni a ritkábban alkalmazott – de bizonyos szempontokból pontosabb eredményt adó - öt szintű modellt tekintve is. Nyilvánvalóan ebben az esetben csak a négy szintű modellben az alap szinten lévő hat szervezet helyzete változhat. Ebből a hat szervezetből négy esetében volt megállapítható, hogy rendelkeznek olyan megoldással, amely részinformációkat ad a szoftverlicencekkel kapcsolatosan, jellemzően egyes gyártók egyes termékek, vagy az informatikai rendszer egy meghatározott szegmensére vonatkozóan. Az öt szintű modellben tehát az általam vizsgált szervezetek közül kettő ad-hoc, négy kezdetleges, három gazdálkodó, egy pedig hatékony szinten van. Összességében megállapítottam, hogy a közigazgatási szervezetek többsége a szoftverlicenc-gazdálkodást tekintve alacsony érettségi szinten áll. Jelentős fejlesztések szükségesek mind a támogató informatikai rendszer vonatkozásában, mind a szervezeti és

szabályozási területen, hogy képesek legyenek megfelelni a jogszabályokban foglalt adatszolgáltatási kötelezettségnek.

Fontos eredménynek tartom annak megállapítását is, hogy a négy magasabb érettségi szinten álló szervezet közül kettő 100% állami tulajdon gazdasági társaság. Az állami tulajdonú gazdasági társaságok működése részben eltér a versenyszféra szereplőinek működésétől, hiszen jellemzően jogszabályban történik működésük rendjének és feladataiknak a meghatározása. Ugyanakkor abban viszont eltérnek a közigazgatás szereplőitől, hogy üzleti tervet készítenek, és működésüket jelentősen meghatározza gazdálkodásuk alakulása, a bevételeik és kiadásaik összefüggése tevékenységük értékének egyik lényeges mérőszáma. Fentiek alapján megállapítható, hogy egy felelősen gazdálkodó szervezetnek alapvető üzleti érdeke azt diktálja, hogy működtessen szoftverlicenc-gazdálkodást. Az interjúkból nyilvánvalóvá vált, hogy ezek a szervezetek valóban kiemelten fontosnak tartják a szoftverlicenc-gazdálkodási tevékenységre történő ráfordítást, ez abból következik, hogy ismert számukra az optimális felhasználásból következő megtakarítás lehetősége.

FEJLESZTENDŐ TERÜLETEK

Folyamatok meghatározása

A korábban jelzett előzetes felmérés egyik eleme, a szervezeten belüli folyamatok meghatározása, ezeket testre kell szabni az adott szervezet igényei, lehetőségei szerint, majd ennek megfelelően kell kialakítani a szervezetet és elkészíteni a belső szabályozást.

A folyamatok tervezésénél minden egyes folyamat valamennyi folyamatlépését meg kell határozni, továbbá azt is, hogy az egyes folyamatlépésekben milyen szervezetek, szerepkörök érintettek. A folyamatokat az egyértelmű rendszer kialakítása, az egyszerűbb megérthetőség érdekében javasolt vizuális formában, folyamatábrákon is megjeleníteni. Így szemléltethetők a szerepkörök, felelősségek, döntési pontok.

Az érettségi modell alap (ad-hoc) szintjén lévő szervezeteknél az alábbi folyamatokat javaslom részletesen kidolgozni és dokumentálni: szoftverlicenc szükségletek tervezése, igénylés folyamata, szoftverlicenc konstrukció kiválasztás folyamata, módszere és a beszerzés folyamata, számlakezelés a nyilvántartó rendszerekben, szoftverlicenc nyilvántartásba vétel, nyilvántartásokhoz való hozzáférések kezelése, szoftverlicenc aktiválás, eltávolítás (raktárba visszavétel), selejtezés, szoftverlicenc felülvizsgálatok (konszolidáció, optimalizáció, frissítés, licenc konstrukció váltás), telepítések felmérése, leltározás, eltérések kezelése (hiány, többlet), szoftverlicencek kivezetése (törlése), engedély nélküli szoftverlicencek kezelése, szoftverlicenc-gazdálkodással kapcsolatos információk szolgáltatása (lekérdezések, jelentések, riportok) , (KPMG Tanácsadó Kft., 2013. p. 6) (Rudd, 2014. pp. 47-66).

Szervezet kialakítása, szabályozás

A közigazgatási szervezetek informatikai működéséhez szükséges szoftverlicencek nyilvántartásához, a jogszabályi feltételek és a beszállítói szerződések betartásához, az optimális gazdálkodás, továbbá a DKÜ Zrt. és a KSZG Kft. részére történő adatszolgáltatási kötelezettség biztosítása érdekében szoftverlicenc-gazdálkodási területet kell kialakítani.

Az, hogy ez a terület a szervezet melyik szervezeti egységének irányításával jön, milyen mérettel, létszámmal, munkamegosztással működik, vagy esetleg ezt a tevékenységet egyes szervezetek kiszervezik, vagyis külső szállítóval kötött szolgáltatási szerződés

keretében valósítják meg a szoftverlicenc-gazdálkodási tevékenységet vezetői (felsővezetői) döntés kérdése. Ezt a döntést befolyásolhatja a szervezet mérete, az informatikai rendszer felépítése, kiterjedtsége, az érintett szoftvervagyon értéke, esetleg állhat a háttérben szakmai vagy gazdasági megfontolás. Véleményem szerint a hierarchikus – lineáris-funkcionális - felépítésű, több ezer alkalmazottal rendelkező és nagy kiterjedésű informatikai rendszert üzemeltető közigazgatási szervezeteknél, ahol több száz vagy egyes esetekben akár több ezer szervert és kulcsfontosságú adatbáziskezelő rendszereket üzemeltetnek, a szoftvervagyon értéke eléri vagy meghaladja a milliárdos – egyes nagyobb informatikai rendszerrel rendelkező szervezeteknél a tízmilliárdos – értéket, ott szükségszerű és indokolt, hogy a szervezeten belül is megvalósuljon a szoftverlicenc-gazdálkodás területén szakértő alkalmazott foglalkoztatása.

A szoftverlicenc-gazdálkodás a teljes vállalton átívelő tevékenység, több szakterület (jogi, pénzügyi, informatikai, beszerzési) együttműködését igényli. A szervezeti egység irányítását a szervezet informatikai vezetőjének hatáskörébe célszerű delegálni. A szervezeti egységet a szoftverlicenc-gazdálkodási terület vezetője vezeti, irányításával dolgozik az informatikai (licenc) szakértő és a folyamatszervező, valamint a pénzügyi, a nyilvántartási és a jogi szakértő. A vezetőnek, az informatikai szakértő és a folyamatszervező munkatársaknak célszerű együtt, egy szervezeti egységnél, egy vezető irányításával – praktikusan az informatikai szakterületen - dolgozni. A létszám a szervezet és a feladat függvényében változhat, igény szerint eseti külső szakértelem bevonásával.

A közigazgatási szerveken belüli feladatok szervezeti egységekhez rendelését a szervezeti és működési szabályzatok, az egyes szervezeti egységek belső működését pedig az ügyrendek határozzák meg. Az egyes szaktevékenységek folyamatait – különösen abban az esetben., ha a szervezeten belül több szervezeti egységet is érintenek – úgynevezett közjogi szervezetszabályozó eszközök határozzák meg. Ezeknek az egyes szervezeteknél egymástól eltérő az elnevezésük, de összefoglaló néven belső utasításnak nevezhetjük őket.

A szoftverlicenc-gazdálkodási tevékenységet – mivel több szervezeti egység is érintett - indokolt belső utasításban szabályozni. Szintén a szabályozást determinálja, az a speciális helyzet, hogy a szoftvereket is számviteli nyilvántartásban kell nyilvántartani, megjelenik a gazdálkodási és a selejtezési folyamat is, de ezek eltérnek más tárgyi eszközökkel végzett hasonló tevékenységektől.

A belső szabályzatnak a szervezet egészére érvényesnek kell lennie, ez garantálja az egységes tevékenységet. A szabályzat hatóköre mellett meg kell határozni a szoftverlicenc-gazdálkodási tevékenység célját, valamint a szervezeten belüli felügyeletet gyakorló vezetőt.

A szabályzatban célszerű meghatározni, hogy a szoftverlicenc-gazdálkodási terület tevékenységéhez milyen eszközöket – elsősorban szoftvereket – használ és feladatai végrehajtása során milyen nyilvántartásokat vezet.

A szabályzat mellett előnyös lehet kiadni a szervezet szoftverlicenc-gazdálkodási politikáját is. Ebben a – 4-8 pontból álló - dokumentumban a szervezet a szoftverlicenc-gazdálkodási tevékenysége alapelveit határozza meg. A szoftverlicenc-gazdálkodási politika egyrészt a feladat szervezeten belüli súlyát hangsúlyozza, másrészt a szervezet elkötelezettségére hívja fel a figyelmet. Ilyen elkötelezettség lehet a jogtiszta, legális, licenc-szerződésben megfogalmazott követelmények szerinti szoftver használata, valamint a szerződi jogok védelme, érvényesítése melletti kiállás.

Informatikai támogató eszköz kiválasztásának szempontjai

Az informatikai támogató eszköz kiválasztásának első lépése a lehetséges szoftverek körének meghatározása, felmérése. Ezt végezheti maga az érintett szervezet, vagy egy – szerződés alapján - megbízott speciális szakértelemmel rendelkező külső szolgáltató. Szoftverlicenc-gazdálkodást támogató rendszerekkel kapcsolatosan nyilvánosan is elérhetők információk mértékadó tanácsadó cégek kutatásai, felmérései, rangsorolása alapján, az egyik legismertebb a Gartner szakmai listája [17].

A tevékenységet támogató informatikai rendszer kiválasztása előtti előkészítő munka során meg kell vizsgálni, hogy a szervezetnél van-e használatban olyan rendszer, menedzsment szoftver, igénykezelő rendszer, esetleg más olyan megoldás, amelynek képességeit, a benne tárolt információkat a szoftverlicenc-gazdálkodást támogató rendszer hasznosítani tudja. Amennyiben van ilyen rendszer, akkor azt is meg kell vizsgálni, hogy lehetséges-e erre felépíteni a szoftverlicenc-gazdálkodást támogató rendszert. Ha ez lehetséges és a rendszer a további követelményeknek is megfelel, vagy vállalható – aránytalan kockázatot nem jelentő - kompromisszummal kezelhető a megfeleltetés, akkor több szempontból is célszerű annak bevezetése. Egyrészt az informatikai rendszer a homogén, együttműködő rendszer irányába lép tovább, másrészt a meglévő megoldások, licencek az új rendszer (modul) bevezetésének költségeit mérsékelik, továbbá kevesebb műszaki kockázattal kell számolnunk, illetve rövidebb lehet a bevezetés időtartama is.

A jogszabályokban foglaltak, illetve a Nemzeti Kibervédelmi Intézet iránymutatása alapján a közigazgatási szervezeteknek célszerű olyan szoftverlicenc-gazdálkodást támogató informatikai rendszer beszerezni, amely képes kizárólag a megrendelő szervezet saját hálózatába telepítve működni (úgynevezett on-premise), úgy, hogy működése során nem folytat adatcserét felhőben működő informatikai rendszerrel.

ÖSSZEFOGLALÁS, KUTATÁSI EREDMÉNYEK

Munkám során a hazai közigazgatási szervezetek szoftverlicenc-gazdálkodási helyzetével foglalkoztam. Témaválasztásom aktualitását a 2021-ben történt jogszabályi változások indokolják, hiszen kormányzati szinten is szükségesnek tartják a terület fejlesztését.

Dolgozatomban elemeztem a szoftverlicenc-gazdálkodás jogi környezetét, illetve a nyilvántartás elmaradásának kockázatait. Egyidejűleg ismertettem a tevékenység felépítését, rávilágítottam lényeges elemeire a nemzetközi szabványok és a legjobb gyakorlatok alapján. Ezt követően – mélyinterjúk alapján - megállapítottam, hogy a közigazgatási szervezetek a szoftverlicenc-gazdálkodás milyen érettségi szintjén vannak. Ezután javaslatot dolgoztam ki a szoftverlicenc-gazdálkodáshoz szükséges folyamatok és szervezeti keretek kialakítására, a belső szabályozás legfontosabb elemeire. illetve javaslatot tettem arra, hogy egy szoftverlicenc-gazdálkodást támogató informatikai rendszer beszerzése során milyen körülményeket kell hangsúlyosan kezelni.

Összefoglalva – véleményem szerint – publikációm jól hasznosítható a szoftverlicenc-gazdálkodás területén fejlesztést, előrelépést tervező közigazgatási szervezeteknél a közép- és hosszútávon fejlődést eredményező legfontosabb teendők tervezéséhez.

IRODALOMJEGYZÉK

[1] PRISZNYÁK, Szabolcs: A rendvédelmi informatika egyes szervezési és oktatási kérdései [PhD értekezés] Óbudai Egyetem 2020. p. 55; p. 78
[2] CZUPRÁK, Ottó, & KOVÁCS, Gábor: A szervezetvezetés elmélete. Budapest: Dialóg Campus Kiadó. 2017. ISBN 978-615-5764-43-1. p. 274
[3] SEBESTYÉN, Attila: Stációk és determinánsok a rendvédelmi szervek informatikai működésének fejlődésében [PhD értekezés]. Zrínyi Miklós Nemzetvédelmi Egyetem 2010. p. 30
[4] Központi Statisztikai Hivatal https://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_oni018.html (letöltve: 2021. április 27.)
[5] Nemzeti Digitalizációs Stratégia 2021-2030, pp. 77-78.
[6] LEHOCZKY, Mónika: Szoftvert hova könyveljük? http://merlegkepestanoncok.hu/szamvitel/szoftvert-hova-konyveljuk 2014 (letöltve: 2021. április 20.)
[7] JACZÓ, Dániel: A használt szoftverekkel való kereskedés szerzői jogi értékelése és bírósági gyakorlata az Európai Unió irányelveinek és esetjogának tükrében. Infokommunikáció és Jog, 2014. p. 1.
[8] RUDD, Colin: ITIL V3 Guide to Software Asset Management. Norwich, United Kingdom, 2014., ISBN 978 0 11 331106 4. p. 4, pp. 47-66, pp. 111-119.
[9] KPMG International: Software Asset Management: Mitigating Risk and Realizing Opportunities. 2009., p. 13
[10] AUERHAMMER, Nóra: Így építhető ki a hatékony szoftvergazdálkodási rendszer. bitport.hu., https://bitport.hu/igy-epitheto-ki-a-hatekony-szoftvergazdalkodasi-rendszer (2019. május 30.) (letöltve: 2021. március 28.)
[11] B. SZABÓ, Edina: Intelligens szoftvermenedzsment, Innotéka. https://www.innoteka.hu/cikk/intelligens_szoftvermenedzsment.1234.html (2015. október 2.) (letöltve: 2021. április 20.)
[12] KAY, Peter: Shaping the software agenda. ISO Focus, 2007. 4. évfolyam, 5. szám, ISSN 1729-8709. pp. 25-27
[13] International Standard ISO/IEC 19770-1. (2017. december). Vernier, Svájc: iso.org
[14] Freshservice.com https://freshservice.com/software-license-management (évszám nélkül) (letöltve: 2021. április 27.)
[15] JACZÓ, Dániel: A szoftverlicencek tipológiája. https://jdlaw.hu/wp-content/uploads/2015/03/A_szoftverlicencek_tipologiaja.pdf (2015. március 12.) (letöltve: 2021. január 30.)
[16] GROSS, Balázs: A szoftver-licenc szerződések típusai. Jogi Fórum. Pécs: Jogászoknak Kft., https://www.jogiforum.hu/publikaciok/19 (2001. május 5) (letöltve: 2021. április 28.)
[17] GARTNER: Software Asset Management (SAM) Tools Reviews and Ratings https://www.gartner.com/reviews/market/software-asset-management-tools (letöltve: 2021. április 27.)

JOGSZABÁLYOK

301/2018. (XII. 27.) Korm. rendelet a Nemzeti Hírközlési és Informatikai Tanácsról, valamint a Digitális Kormányzati Ügynökség Zártkörűen Működő Részvénytársaság és a kormányzati informatikai beszerzések központosított közbeszerzési rendszeréről
2000. évi C. törvény a számvitelről
2016. évi XCIII. törvény a szerzői jogok és a szerzői joghoz kapcsolódó jogok közös kezeléséről
2013. évi V. törvény a Polgári Törvénykönyvről
2012. évi C. törvény a Büntető Törvénykönyvről

SZABVÁNYOK

MSZ ISO/IEC 20000-1:2013 Informatika. Szolgáltatásirányítás. 1. rész: A szolgáltatásirányítási rendszer követelményei http://www.mszt.hu/web/guest/webaruhaz?p_p_id=msztwebshop_WAR_MsztWAportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_pos=1&p_p_col_count=2&_msztwebshop_WAR_MsztWAportlet_ref=154719&_msztwebshop_WAR_MsztWAportlet_javax.portlet.action=search (letöltve: 2021. április 30.)

MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények http://www.mszt.hu/web/guest/ingyenes-szabvanylista?p_p_id=msztwebshop_WAR_MsztWAportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_msztwebshop_WAR_MsztWAportlet_ref=157993&_msztwebshop_WAR_MsztWAportlet_javax.portlet.action=search (letöltve: 2021. április 30.)

ISO/IEC 19770-1:2017(en) Information technology — IT asset management — Part 1: IT asset management systems https://www.iso.org/obp/ui/#iso:std:iso-iec:19770:-1:ed-3:v1:en (letöltve: 2021. március 28.)

ISO/IEC 19770-2:2015(en) Information technology — Software asset management — Part 2: Software identification tag https://www.iso.org/obp/ui/#iso:std:iso-iec:19770:-2:ed-2:v2:en (letöltve: 2021. március 28.)

ISO/IEC 19770-3:2016(en) Information technology — IT asset management — Part 3: Entitlement schema https://www.iso.org/obp/ui/#iso:std:iso-iec:19770:-3:ed-1:v1:en (letöltve: 2021. március 28.)

ISO/IEC 27005:2018(en) Information technology — Security techniques — Information security risk management https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en (letöltve:2021. április 30.)

EXAMINATION OF THE HISTORY OF INFORMATION SECURITY MILESTONES, EVENTS AND ANSWERS

INFORMÁCIÓBIZTONSÁG FEJLŐDÉSTÖRTÉNETI VIZSGÁLATA MÉRFÖLDKÖVEK, ESEMÉNYEK ÉS VÁLASZOK

SZŰCS Endre[1], ZÁHONYI Lajos[2]

Abstract

No discipline can exist without antecedents. All science is on the move, every science is looking for answers and thus evolving. These answers are built on each other and this raises new questions. Development is unstoppable. To better understand the problems of the present age, we must look back and learn from these answers. The focus of the present study is also on the milestones, tools, and toolkits that have significantly influenced the development of information security. In this study, we examined the history of the development of information security, in the framework of which we reviewed a significant event of the 20th and 21st centuries that can be highlighted from the point of view of information security, and the answers given to it.

Keywords

information security, history of information security, principles of information security, milestones of information security

Absztrakt

Egy tudományterület sem létezhet előzmények nélkül. Minden tudomány mozgásban van, minden tudomány keresi a válaszokat és ezáltal fejlődik. Ezek a válaszok egymásra épülnek és ebből újabb kérdések keletkeznek. A fejlődés megállíthatatlan. Ahhoz hogy jobban megértsük a jelen kor problémáit bátran vissza kell tekinteni a múltban és tanulni ezen válaszokból. Jelen tanulmány fókuszában azon mérföldkőnek is tekinthető események, eszközök és eszközrendszerek állnak, amelyek jelentősen befolyásolták az információbiztonság fejlődését. A tanulmányban információbiztonság fejlődésének történetiségét vizsgáltuk, melynek keretében a 20. és a 21. század egy-egy jelentős információbiztonság szempontból kiemelhető eseményét és az arra adott válaszokat tekintettük át.

Kulcsszavak

információbiztonság, információbiztonság fejlődéstörténete, információbiztonsági elvek, információbiztonsági mérföldkövek

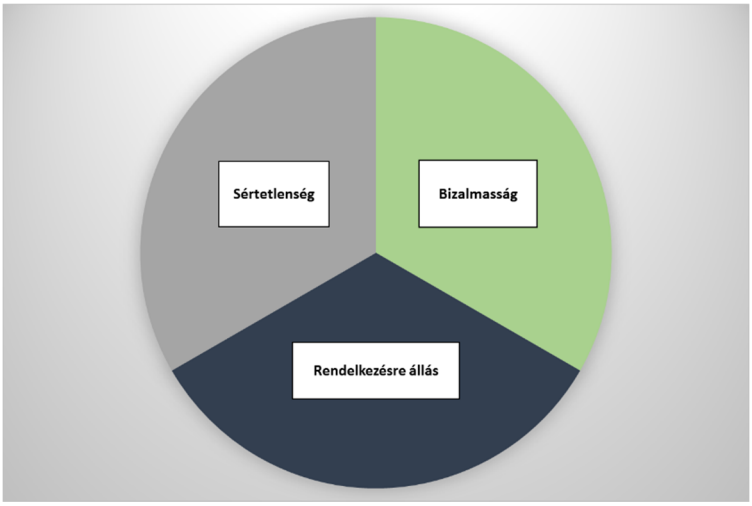
[1] szucs.endre@bgk.uni-obuda.hu | ORCID: 0000-0003-2818-262X | assistant professor, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering Institute of Mechanical Engineering and Security Sciences | adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Gépészeti és Biztonságtudományi Intézet
[2] zahonyi.lajos@phd.uni-obuda.hu | ORCID: 0000-0001-9999-9624 | PhD Student, Óbuda University Doctoral School on Safety and Security Sciences | PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Jelen tanulmány fókuszában azon mérföldkőnek is tekinthető események, eszközök és eszközrendszerek állnak, amelyek jelentősen befolyásolták az információbiztonság fejlődését.

„Az információbiztonság helyzete sajátos, egyszerre van jelen egy szervezet minden területén, sőt, a feltételeinek megfelelő kialakítása és működtetése jóval túlmutat az információ biztonságos kezelésén. A szervezet minden erőforrásának, az embereknek, az eszközöknek, az információs rendszereknek, és más vagyontárgyaknak a szabályozását, viselkedését, használatát, ellenőrzését jelenti." [1]

Az információbiztonság három alappillérre épül. Az első, hogy az adott információ sértetlen legyen, pontos maradjon és ne torzuljon a második, hogy az arra felhatalmazott felhasználó mindig hozzáférjen az adott információhoz és kapcsolódó értékekhez végül pedig a harmadik a jogosultság, avagy bizalmasság kérdése azaz csak az arra jogosult vagy felhatalmazott személy számára legyen elérhető az adott információ.



1. Ábra: Információbiztonság alapelvei. Lehet tanulni a múltból. [2]

Ezen alappillérek mentén vizsgáljuk meg milyen eszközökkel és eszközrendszerekkel találkoztunk az elmúlt 100 évben milyen válaszok születtek a kor kihívásainak és technikai lehetőségeinek figyelembevételével egy-egy információbiztonsági „incidens" kezelésére, illetve kivédésére. Jelen írás keretei arra adnak lehetőséget, hogy a kor egy-egy jellegzetes incidensének és eszközrendszerének helyzetét vizsgáljuk meg. Ezen incidensek vizsgálata lehetőséget ad, hogy a jelen kor kihívásaira nagyobb hatásfokú választ legyünk képesek adni. A tanulmányban információbiztonsági incidensnek tekintjük „azokat a nem kívánt, illetve nem várt egyedi vagy sorozatos információbiztonsági eseményeket, amelyek nagy valószínűséggel veszélyeztetik a működési tevékenységet és fenyegetik az információk biztonságát" [3].

A számítógépek megjelenésével és gyors fejlődésével a kezelt információs adatok száma, mennyisége és tárolási nagyságrendje sokszorosára növekedett az azt megelőző időszakokhoz képest. A nagy koncentrációban történő adattárolás pedig új dimenziókat nyitott

az adatok mennyiségi feldolgozása területén. Aki ezekhez az adatokhoz hozzáfér, óriási információs erőforrásokhoz tud hozzájutni.

„Az információtechnológiai rendszerek és összetevők új sebezhetőségeket hordoznak, új - elsősorban információs jellegű - veszélyeztető hatások számára teremtenek lehetőségeket." [4] Az információk kezelőinek és használóinak óriásira nőtt a felelőssége abban, hogy ezen információk ne sérüljenek és ne torzuljanak, hogy a felhatalmazott felhasználók számára ezek az információk és kapcsolódó értékek mindig elérhetőek legyenek illetve hogy csak az arra jogosult vagy felhatalmazott személy számára legyenek elérhetőek. Ez egy védelmi rendszer kiépítését igényli, amely rendszer védelmi módszereket kíván.

INCIDENSEK, AMELYEK HATÁSSAL VOLTAK A FEJLŐDÉSRE

Jelen tanulmányunkat néhány jellegzetes példával indítjuk, amelyek a múltban az információbiztonság fejlődéstörténetében meghatározóak voltak. [5]

- A 1971-ben jelent meg az első vírus a „Creeper" [6]. Ez egy önreplikáló program volt, amelyet az internet elődjeként tekintett ARPANET-et használta a DEC PDP-10 számítógépek megfertőzéséhez és az alábbi üzenet megjelenítéséhez: „I'm the creeper, catch me if you can!" azaz „Én vagyok a Creeper, kapj el ha tudsz!".
- 1976 és 2006 között, azaz mintegy 30 éven át, Greg Chung Boeing alkalmazott 2 milliárd dollár értékű űrrepülési dokumentumokat adott át Kínának. A vizsgálat során 225.000 oldalnyi érzékeny információkat tartalmazó dokumentumokat fedeztek fel az otthonában. Ez volt a történelem legnagyobb léptékű rendszeren belülről jövő rosszindulatú támadása, amelynek az volt a célja, hogy egy idegen országnak juttassanak el katonai és űrkutatási szabadalmakat, dokumentumokat. Ez az incidens nem „csak" a Boeing vállaltot érintette, hanem az Amerikai Egyesült Államok nemzetbiztonságát is.
- 2013-ban „robbant" a Snowden ügy. Edward Snowden a CIA alkalmazottja volt és az Egyesül Államok kormányával volt munkaszerződése. A minősített információkat a National Security Agency-től másolta és szivárogtatta ki. Noha nem ez volt a legnagyobb belülről jövő támadás mégis ez az incidens volt az, amelyik a legnagyobb társadalmi vitát váltotta ki az Egyesült Államokban. A cselekedete megosztotta a társadalmat, sokan elvesztették a bizalmukat az állami szervekben ugyanakkor sokan a mai napig is hősnek tekintik Snowdent.
- Szintén még ez évben történt, hogy a hackerek egy csoportja feltörte mintegy 3 milliárd (!) Yahoo felhasználó fiókját. Nevek, jelszavak, valamint biztonsági kérdésekre adott válaszok kerültek veszélybe. A Yahoo próbálta eltusolni az ügyet és egészen 2016-ig nem jelentette be a jogsértést. Végül is az Egyesült Államok bírósága 35 millió dolláros kártérítést szabott ki a vállalatra amiért elmulasztotta az időben történő jelentést. Az ügy a Yahoo eladási árát 350 millió dollárral csökkentette.
- 2015-ben Az Egyesült Államok Személyzeti Ügyekért Felelős Hivatala (The U.S. Office of Personnel Management) támadás áldozatává vált. Az incidens során 4,2 millió volt és jelenlegi kormányzati személy, állományi adatait lopták el. Ez 21,5 millió átvilágítási vizsgálati fájlt és 5,6 millió ujjlenyomatot tartalmazott. Ez az esemény cselekvése ösztönözte a civil szervezeteket az adatbiztonság ügyének felkarolására.

- Az első „váltságdíjas" kriptoféreg a „Wannacry" 2017-ben jelent meg a Microsoft Windows operációs rendszer hiátusait kihasználva. A rendszer kódolta a gépen lévő adatokat és a helyreállító kulcsért cserébe Bitcoin kriptovalutát kért. A globális világunkban ez volt az első „féreg vírus", amely sokkolta a felhasználókat. Csak az első napon már megközelítőleg 230.000 számítógépet fertőzött meg 150 országban.
- Szintén 2017-ben jelent meg a NotPetya féregvírus, ami a Microsoft Operációs rendszer sebezhetőségét kihasználva több mint 12.500 – köztük energiaipari cégek, bankok, repülőterek és magasrangú állami tisztviselők - informatikai rendszeréből törölt adatokat és kért „váltságdíjat" a visszaállító kulcs megküldéséért cserébe.
- Az eddigi legnagyobb Hitelkártya adatlopási ügy is 2017-ben történt, amikor is a becslések szerint 143 millió adat került veszélybe amikor az Equifax Hitelintézet (Credit bureau, Equifax) 209.000 partnerének hitelkártyájához fértek hozzá a hackerek. Ez az incidens a vezérigazgató lemondásához vezetett.
- 2020 februárban az Amazon Web Services (AWS) a nyilvántartott eseteket tekintve az eddig legsúlyosabb túlterheléses (DDoS) támadást szenvedte el. A támadás során a legnagyobb adatforgalom 2,3 Tbps volt.
- 2021 május: a Colonial Pipeline amely az Egyesült Államok keleti partvidékét látja el üzemanyaggal, zsarolóvírusos kibertámadás áldozata lett. Ez a fajta vírus az, amely zárolja és titkosítja az áldozat számítógépes rendszerét és a feloldásért pedig váltságdíjat kér. Tekintve a támadás volumenét és célját, ez már az amerikai nemzetbiztonság helyzetét is befolyásolja.

Tudománytörténeti alapok

Egy tudományterület sem létezhet előzmények nélkül. Minden tudomány mozgásban van, minden tudomány keresi a válaszokat és ezáltal fejlődik. Ezek a válaszok egymásra épülnek és ebből újabb kérdések keletkeznek. A fejlődés megállíthatatlan. Ahhoz hogy jobban megértsük a jelen kor problémáit bátran vissza kell tekinteni a múltban és tanulni ezen válaszokból. Nincs ez másképpen a biztonságtudomány területén sem.

„A biztonságtudomány célja, hogy: a rendszerek biztonsági funkciói a kezdeti állapotuktól fogva elemzésre kerüljenek, a rendszerek biztonságának tervezése a lehetséges legnagyobb részletességgel kerüljön végrehajtásra." [7]

Az időben előre haladva a technika fejlődésével, újabb és újabb információvédelmi kihívások jelenek meg. Kicsit több mint, egy évtizede jelent meg az ISO27001-es információbiztonsági rendszer szabványcsalád, amely akkor egy megfelelő szabályozási válasz volt a kor kihívásaira. Magyarországon a jogalkotási rendszer szintén próbálja felvenni a tempót, amelyet ez a fejlődés okoz. A világ minden területén köztük az Európai Unióban és Magyarországon is folyamatosan születnek vonatkozó szabályozási formák, előírások és jogszabályok. [8] Ha az ok-okozati összefüggéseket vizsgáljuk, látjuk, hogy a biztonsági eszközrendszerek is folyamatosan változnak, alkalmazkodnak. Az adott kor kihívásaira az adott kor eszközrendszereinek és technikai színvonalának megfelelő válaszok érkeznek.

A biztonság megismerésének folyamatát történetileg négy szakaszra tudjuk felosztani. Ezek:

Az első szakasz az „ártatlanság kora" [9] amely az ipari forradalom előtti – a XVII.-XVIII. századig tartó – időt jelöli. E korszak jellemzője, hogy az ember még nem foglakozott tudatosan a biztonság mai értelemben vett problémáival, nem mérte és nem is elemezte

azokat. A természeti csapások, katasztrófák, járványok, de maga a háború jelenléte is egy elfogadott helyzetnek az élet velejáró részének tekintették. Bár az adott kor konfliktusai szintén válaszokat kényszerítettek ki, mégis a válaszok az eszközök és eszközrendszerek még inkább ösztönösnek tekinthetőek voltak, mint tudatosnak.

Második szakasz a „felfedezés kora" [10] amely az ipari forradalom bekövetkezését követő és a XIX.- XX. század fordulójáig tartó időszakot jelöli. Ebben az időszakban már felismerték a biztonság fontosságát és már kidolgoztak elméleti alapokat. A műszaki tudományok vagy az orvostudomány már rendelkezett bizonyos eszközökkel, amely alapján feljegyezték és használták az elméleti alapokat. Ebben az időszakban a társadalmi fejlődés magával hozta az igényt a biztonság szükségességére. „Az új eszközök és technológiák alkalmazása során az ember felfedezte a biztonsági problémákat maga körül és így tehetett néhány kezdeti lépést a veszélyes szituációk feloldása felé." [11]

Harmadik szakasz a „rendszerbiztonság" [12] kora, amely XX. század elejétől induló fejlődési robbanásra adott válaszok mentén jegyezhető. Magas fokú ipari fejlődés, a hadipar fejlődése, az új technikai vívmányok, mint a repülő, az automobil kifejlődése és elterjedése vagy később az űripar kialakulása jellemzi.

A negyedik a „biztonságtudomány" [13] szakasza, amely már a tudomány és technológia fejlődésére egzakt és érdemleges válaszokat nyújt. Az ember már felismeri a biztonsággal kapcsolatos alapelveket és összefüggéseket, kialakítja a maga eszközrendszereit és ezen eszközrendszereinek segítségével kidolgozza az erre vonatkozó válaszokat. Legyenek azok akár különböző technikák vagy rendszerek.

Tudománytörténetiséget tekintve a jelen tanulmány az Első Világháború információbiztonsági kihívásaiból indulva tekinti végig a XX. és XXI század jellegzetes információbiztonsági incidenseit.

„Cher Ami" – egy élő „eszköz" az Első Világháborúból

Az információ eljuttatásának módja és az információ védelme nagyban az adott kor jellemző eszközeinek hatékonyságán alapul. Ha manapság megírunk egy e-mailt és annak egyértelmű és valós címzettet adunk, akkor az az üzenet továbbításra kerül. 100 évvel ezelőtt a kézbesítés szerepét sok esetben a kor eszközrendszer részének is tekinthető postagalambok látták el. [14]

Az Amerikai Egyesült Államok 1917-ben belépett az Első Világháborúba az Antant oldalán. 1918. októberében az argonne-i erdőben az amerikai hadsereg tüzérsége a saját alakulatainak állásait lövi, ugyanis nem áll rendelkezésre az a pontos információ, amelyben a pontos koordinátákat vagy helyet jelölnék. Ekkor indítják útnak az utolsó hírvivő galambjukat az alábbi üzenettel: "We are along the road parallel to 276.4. Our own artillery is dropping a barrage directly on us. For heaven's sake, stop it." Major Charles W. Whittlesey 4 October1918. Magyar fordításban: „A 276,4-el párhuzamos úton haladunk. Saját tüzérségünk közvetlenül ránk lő. Az ég szerelmére állítsátok le. – Charles W. Whittlesey őrnagy" [15]

2. Ábra: Az információk rendelkezésre állása nem tekinthető evidenciának – A korabeli eszközrendszerek része a galamb, amely lehetővé tette, hogy az információk elérhetővé váljanak. [16]

Ez a hírvivő galamb akit úgy hívtak „Cher Ami" (Kedves Barát), 25 mérföldet repül, 25 perc alatt és eljuttatja az üzenetet az amerikai főhadiszállásra, miután azonnal beszüntetik az ágyúzást, ezzel megmentve mintegy 200 amerikai katona életét. „Cher Ami"-t útja során többször eltalálták, elvesztette az egyik szemét és az egyik lábát. Az üzenet azonban elérhetővé vált. Az Első Világháborúban a postagalambokat mind az Antant mind a Központi Hatalmak széles körben alkalmazták. Az egyik legbiztosabb információs eszközök voltak az adott korban. Korabeli megfigyelések szerint, a postagalambokkal indított üzenetek 95%-a célba ért. Ez mai szemmel nézve is egy komoly eredmény.

Enigma - kódolás

Mint ahogy a kiberbűnözés világában úgy 80 évvel ezelőtt a II. Világháborúban sem volt más a cél: adatok megszerzése és a megszerzett adatok valamely előnyös felhasználása.

Az információbiztonság történet vizsgálatának az egyik mérföldköve, a kódoló gépek megjelenése amelyek már bizonyosfajta számítógépnek is tekinthetőek. A kódoló gépek szerepe az, hogy az információkat csak és kizárólag az arra jogosult felhasználó tudja értelmezni. A háborúban minden információ szerepe felértékelődik és a gépekkel küldött üzenetek védettsége nagyban a kódolás összetettségén múlik. Ezért a kódoló gépek feltörése és ezáltal a szó szerint életbevágó információk megszerzése elemi érdeke mindegyik harcoló félnek. A kódoló gépek biztonságának szükségessége – beleértve maga szerkezetet és a benne lévő adatokat is – a második világháború idején merült fel először, amikor is az első nagygépeket, - amelyeket a kommunikációs kódok törésének számításainak elősegítésére fejlesztettek ki - használatba vették. Védeni kellett a gép fizikai helyét, a benne lévő szerkezetet (hardver) és kódolási elveket (szoftver) a fenyegetések ellen. Több szintű biztonság eszköze volt melyek között a védett katonai helyszínek a jelvények, a kulcsok és arckezelés használata volt a legjellemzőbb és amelyeket dedikált biztonsági személyzet segítségével ellenőriztek.

3. Ábra: Az Enigma – német gyártmányú, forgótárcsás, elektromechanikus berendezés, amelyet a II. Világháború alatt használtak a németek. [17]

Az Enigma név termékcsaládot takar, amely számos modellből állt 1923-1945 között. A gépeket többször is feltörték és ezzel a háború idején a Szövetségesek jelentős információs lépéselőnyben voltak [18].

Hidegháború korszaka és a 60-as évek

A hidegháború idején jelentősen megnőtt az igény bonyolultabb és kifinomultabb feladatok elvégzésére és az adatok tárolására. Szükségessé vált a gyakran teremnyi méretű nagygépek közötti kommunikáció javítása és az akkor használatos mágnesszalagos adattovábbítás, illetve adatkommunikáció hatékonyabbá tétele. Az Egyesült Államok Honvédelmi Minisztériumának Fejlett Kutatási Projekt Ügynöksége (Department of Defense's Advanced Research Project Agency, a továbbiakban ARPA) megkezdte egy redundáns és közös hálózatba kapcsolt kommunikációs rendszer megvalósíthatóságának vizsgálatát annak érdekében, hogy támogassák a katonai információcserét. A programot 1969-ben az internet alapítójaként is emlegetett Larry Roberts koordinálta. Ezt a rendszert nevezték ARPANET-nek amely gyakorlatilag a ma ismert internet történeti előzménye volt.

A 70-es 80-as évek

A következő évtizedek során az ARPANET népszerűvé és széles körben elterjedté vált. Az ARPANET-ben lévő potenciál egyre erősebb kihasználása miatt a visszaélések száma is gyakoribbá vált. 1973 decemberében Robert M. "Bob" Metcalfe, - akinek nevéhez később az egyik legnépszerűbb hálózati protokoll az Ethernet fejlesztése fűződik - felismerte az ARPANET biztonságával kapcsolatos alapvető problémákat. Az rendszerben lévő egyes távoli helyszínek nem rendelkeztek elegendő kontrollal és védelemmel az adatok illetéktelen felhasználóktól történő távoli megvédésére. Egyéb problémákkal is bővelkedett a rendszer, úgymint: a jelszó szerkezetének és formátumainak sebezhetősége, a telefonos kapcsolatokhoz igazodó biztonsági eljárások és felhasználói azonosítás hiánya.

A gazdagépek és felhasználók számának robbanásszerű ugrása következményeként a rendszerben lévő telefonszámokat széles körben terjesztették és nyíltan nyilvánosságra hozták a például a telefonfülkék falain. Ezek után nem csoda, hogy a korabeli „hackereknek" könnyű hozzáférésük lehetet az ARPANET-hez. Ezt a súlyos információbiztonsági rést egy 1978-ban megjelent tanulmány a „Protection Analysis: Final Report" leplezte le

egyértelműen. Ebben a tanulmányban írták le és fejtették ki az ARPANET operációs rendszerek biztonságának sebezhetőségét. Ezt követően az amerikai védelmi minisztérium reagált és kiadott egy mérföldkőnek tekinthető dokumentumot: Rand Report R-609. Ez az első dokumentum, amely definiálta a többszintű számítógépes rendszer tartalmát és ez az a papír amelytől számíthatjuk a számítógépes biztonság kezdetét.

A Rand Report R-609 volt az első széles körben elismert publikált dokumentum, amely azonosította a menedzsment szerepét és a szervezeti / vállalati policy jelentőségét a számítógépes biztonságban.

A riport megállapította, hogy a széles körű használat a katonai információs rendszerek hálózati komponenseinek bevezetése jelentős biztonsági kockázatokat hozott magával, amit nem tudtak enyhíteni az akkori elhárítási rutin gyakorlatok, amelyeket e rendszerek biztonsága érdekében használtak. A riport három lényeges területet azonosított:

- Az adatok biztonsága.
- Az adatok véletlenszerű és illetéktelen hozzáférésének korlátozása.
- A személyzet bevonása a szervezet több szintjéről az információbiztonság megteremtése érdekében.

A kor jellegzetes információbiztonsági eseményei:

Év	Információbiztonsági esemény
1967	Jelszóbiztonság megjelenése a számítógépes rendszerekben
1973	A katonai rendszerek többszörös biztonsági mechanizmusának megjelenése
1975	Digital Encryption Standard (DES) megjelenése
1978	Operációs rendszer biztonság és automatizált sebezhetőség észlelésének megjelenése
1979	Biztonságos felhasználó azonosítás
1984	Számítógépes biztonsági kontrolok azonosítása: fizikai ellenőrzés, menedzsment elkötelezettsége, alkalmazottak oktatása és adminisztratív eljárások kidolgozása
1984	Crypt parancs megjelenése az UNIX-ban és általános fájlbiztonság megjelenése
1990	A hitelesség, a rendelkezésre állás és a hasznosság kérdése kapcsán megjelenik az első információbiztonsági triád: titoktartás, elérhetőség és integritás.

1. Táblázat: Főbb információbiztonsági események a 70-es-80-as évekből. [19]

Az internet megjelenése a 90-es években

A 20. század végén a személyi számítógépek használata egyre inkább elterjedt és vele együtt az az igény is, hogy ezek a számítógépek hálózatban csatlakozzanak egymáshoz. Ez az igény hozta létre hálózatok globális hálózatát az internetet. Az internet gyakorlatilag minden számítógéphez csatlakozási lehetőséget adott, amelynek volt telefonvonali vagy csatlakoztatott helyi hálózat (LAN) elérése. Az internet kereskedelmi forgalomba hozatala után a technológia elterjedté vált, a világ szinte minden sarkába eljutott. Az internetes kapcsolatok eleinte, de facto szabályokon alapultak, amelyek alig tették lehetővé az információk biztonságát. Később, mivel ezeket az előd technológiákat széles körben elfogadták és ipari szabványokká váltak, és ez bizonyos fokú biztonságot eredményezett. A korai internetes telepítések azonban alacsony prioritásként kezelték a biztonságot, hiszen abban az időben, amikor szinte az összes internet és e-mail felhasználó informatikus volt, a mail szerver hitelesítés és az e-mail titkosítás nem tűnt szükségesnek. Valójában sok olyan probléma merül fel, amely manapság is levelező rendszerinket sújtja az interneten. Ahogy a számítógépek hálózatos összeköttetésbe kerültek, elveszett a hálózatba kötött számítógép fizikai biztonságának képessége, és a tárolt információk jobban ki voltak téve fenyegetéseknek.

2000-es évek válaszai

Az Internet a számítógépes hálózatok millióit hozza folyamatos kommunikációba egymással. Az egyes számítógépek tárolt adatainak biztonsága függ minden további számítógép biztonsági szintjétől, amellyel kapcsolódik. A 2000-es évek elejétől kezdve egyre nagyobb tudatosságot tapasztalunk az információbiztonság javításának szükségessége kapcsán. Megjelennek az ajánlások és a szabványok.

A szabványosítási törekvések az információtechnológia fejlődéssel parallel módon erősödtek. Az 1980-as évektől kezdve számítógépek üzleti célú felhasználása egyre elterjedtebbé vált. Az üzleti folyamatok és benne az adatok használata kezdett az egységes gyakorlat irányába haladni. Egyre nagyobb igény merült fel valamilyen egységesített keretrendszer létrehozására, amely mintegy „sorvezetőként" segíti a rendszerben lévő információk védelmét.

Erre az igényre először a COBIT (Control Objectives for Information and Related Technology) adott választ, amely nem szabvány és nincs szabványként bejegyezve, a gyakorlatban azonban sokszor szabványszerűen alkalmazzák. Ez egy informatikai ajánlási gyűjtemény egy keretrendszer, amely elsősorban az információtechnológiai auditálás céljait szolgálja.

A másik irány a szabványosítás. Erre példa az ISO27001 nemzetközi szabvány, amely abból a célból készült, hogy követelményeket adjon egy információbiztonság-irányítási rendszer kialakítására, bevezetésére, fenntartására és folyamatos fejlesztésére. [20] A szabvány folyamatközpontú, alkalmazza a Plan-Do-Check-Act (PDCA) modellt és a megvalósított IBIR integrálható a meglévő minőségirányítási (ISO 9001) és a környezetirányítási (ISO 14001) rendszerekkel. Egy adott szervezet számára stratégiai döntés, hogy bevezeti-e az információbiztonság-irányítási rendszert vagy sem. A rendszer kialakítását befolyásolja a szervezet céljai, folyamatai, a szervezet mérete és felépítése, illetve a biztonsági elvárásai.

Az információbiztonság-irányítási rendszer egy kockázatkezelési-folyamat segítségével őrzi meg az információk bizalmasságát, sértetlenségét és rendelkezésre állását, és az

érdekelt felekben bizalmat kelt a tekintetben, hogy a kockázatokkal kielégítő módon foglalkoznak. [21]

Záró gondolatok

Mint minden tudomány a biztonságtudomány területe is folyamatos fejlődésben van. Kiváltképp igaz ez biztonságtudományon belül az információbiztonság területére.

A cikk néhány sajátos példát megjelenítve rámutat arra, hogy az információbiztonság történelmének eseményei komoly hatással voltak és vannak az információbiztonság fejlődésére. Ezeket a hatásokat – az információbiztonság helyzete és viszonyulási eszközrendszereinek tekintetében - egyfajta mérföldköveknek is tekinthetjük.

„Az informatikai rendszerre vonatkozó információk tartalmazzák az adott rendszer felépítésére, működésére vonatkozó adatokat és a rendszerhez csatlakozó eszközök jellemzőit. Nem létezett és nem létezik tökéletes biztonság. A fejlődéssel párhuzamosan folyamatosan jelennek meg újabb és újabb támadási módszerek, biztonsági rések, ennek következtében minden kockázatra kiterjedő védelemről sem beszélhetünk.” [22]

FELHASZNÁLT FORRÁSOK

[1] Horváth G. K., Közérthetően az IT biztonságról. Budapest: KIFÜ, 2013 p.13
[2] Előadáson ismertetett saját ábra
[3] https://sealog.hu/tudastar/fogalomtar/informaciobiztonsagi-incidens [letöltés ideje: 2021.05.22.]
[4] Munk S., Információbiztonság vs. Informatikai biztonság. Hadmérnök Különszám Robothadviselés 7. Tudományos Szakmai Konferencia ROBOTHADVISELÉS 7. TUDOMÁNYOS SZAKMAI KONFERENCIA [2007. november 27.] p1
[5] S. Hospelhorn, Events That Changed Cybersecurity Forever 3/29/2020 [letöltés: 2020.05.25.] pp 1-5
[6] A „Creeper” angol kifejezést a https://gyerekaneten.hu/szocikk/creeper forrás alapján használjuk. Jelentése: olyan személy, akitől az embernek borsódzik a háta, vagy akiből simán kinézi, hogy zaklat másokat.
[7] Kiss S., Biztonságtechnika alapjai, Budapest: Óbudai Egyetem, 2019 p13
[8] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
[9] [10] [11] [12] [13] KISS S., A biztonságtechnika kialakulásának történetéről. Hadmérnök X. Évfolyam 4. szám 2015. december, pp. 26-28.
[14] Magyar Nemzeti Levéltár Katonagalambok az I. világháborúban http://mnl.gov.hu/mnl/nml/csak_a_legritkabb_esetben_tagadja_meg_a_szolgalatot [Letöltés ideje: 2021.05.20]
[15] Fordítás: Záhonyi Lajos
[16] https://www.worldwar1centennial.org/index.php/communicate/press-media/wwi-centennial-news/1210-cher-ami-the-pigeon-that-saved-the-lost-battalion.html [Letöltés ideje: 2021.05.20]
[17] https://www.smithsonianmag.com/smart-news/wwii-enigma-machine-found-flea-market-sells-51000-180964053/ [letöltés ideje: 2021.05.21.]

[18] Whitman, M. E., Introduction to Information Security cengage learning Principles of Information Security, 4th Edition, Institute for Cybersecurity Workforce Development, Kennesaw State University Herbert J. Mattord Michael J. Coles College of Business, Kennesaw State University pp4
[19] Moinak, A. M., Information Security – Evolution, Impact and Design Factors. International Journal of Computer Applications (0975 – 8887) Volume 100– No.2, August 2014 pp.3.
[20] [21] MSZ ISO/IEC 27001:2014 P6
[22] Az információbiztonság lélektana (Psychology of Information Security) https://nki.gov.hu/wp-content/uploads/2019/07/01-Az-inform%C3%A1ci%C3%B3biztons%C3%A1g-l%C3%A9lektana.pdf [letöltés ideje: 2021.05.21.] p10

Follow, like, post, publish! | Kövess, lájkolj, posztolj, publikálj!

https://biztonsagtudomanyi.szemle.uni-obuda.hu

https://www.linkedin.com/company/safety-and-security-sciences-review

https://www.facebook.com/biztonsagtudomanyi.szemle