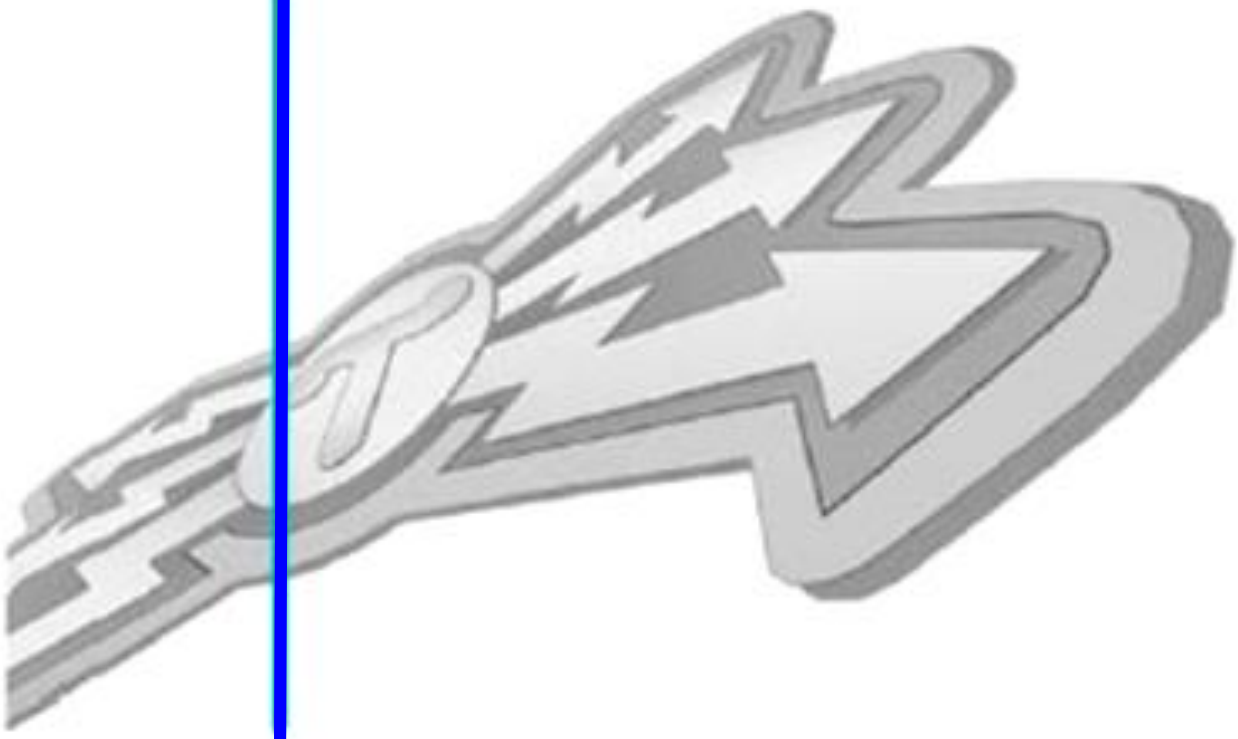
HÍRVILLÁM

A NEMZETI KÖZSZOLGÁLATI EGYETEM
Híradó Tanszék szakmai tudományos kiadványa

SIGNAL Badge

Professional journal of Signal Departement
at the National University of Public Service

9. évfolyam 1. szám
2018



2018. augusztus 1.

HÍRVILLÁM
a Nemzeti Közszolgálati Egyetem Híradó Tanszék
tudományos időszaki kiadványa

SIGNAL BADGE
Professional Journal of the Signal Departement
at the National University of Public Service

Megjelenik évente két alkalommal
Published twice a year

9. évfolyam 1. szám

Budapest, 2018

Felelős kiadó/Editor in Chief
Dr. Fekete Károly alezredes

Szerkesztőbizottság/Editorial Board

Elnök/Chairman of the Board
Prof. Dr. Rajnai Zoltán

Főszerkesztő/Co-ordinating Editor
Dr. habil. Kerti András alezredes

Tagok/Members
Dr. habil. Farkas Tibor százados
Dr. Horváth Zoltán alezredes
Dr. Jobbágy Szabolcs százados
Dr. Kassai Károly ezredes
Megyeri Lajos alezredes
Dr. Németh József Lajos
Paráda István hadnagy
Prof. Dr. Rajnai Zoltán
Dr. Szöllősi Sándor ny. őrnagy
Dr. Tóth András százados

Szerkesztette/Co-ordinating Editor
Dr. Tóth András százados

HU ISSN 2061-9499

NKE Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf.: 15
+36 1 432 9000 (29-407 mellék)

Tartalomjegyzék

Tartalom

Köszöntő 11

Czető Bálint: Pszichológiai befolyásolás, avagy Social engineering 13

István Paráda: Requirements for developing the Cisco Net Academy to Pearson Vue Exam Center 20

Kondás Katalin: A büntetés-végrehajtás informatikai fenyegetettsége 37

Oláh Dániel: Információbiztonsági irányítási rendszerek a köz- és magánszférában 53

Dr. Estók Sándor: A Hálózatok új tudománya reprezentatív iránya a Hálózatközpontú Rendszerlogisztika, Az új tudományos elvek behálózzák a társadalmi, szociális, gazdasági, kapcsolatokat 67

Darázs Tamás: Hálózati eszközök sérülékenysége 82

Oláh Dániel: A felhasználói viselkedés, mint belső veszélyforrás 92

Farkas Tibor, Tóth András: Csapatgyakorlat végrehajtása a Magyar Honvédség Összhaderőnemi Parancsnokság alakulatainál 103

Farkas Tibor, Tóth András: Csapatgyakorlat végrehajtása a Magyar Honvédség 43. Nagysándor József Híradó és Vezetéstámogató Ezrednél 110

Tóth András: Az Amerikai Egyesült Államok Védelmi Minisztériumának felhő koncepciója 115

Tóth András: A mesterséges intelligencia és az IoT összekapcsolásának lehetőségei 122

Szerzőink figyelmébe 132

Köszöntő

Tisztelettel köszöntjük Önt, Kedves Kolléga, Tisztelt Olvasó!

Tavaszi félévünk sikeres volt. Kimondottan. Hallgatóinkkal az estek nagy többségében elégedettek voltunk, csak néhjány kirívó eset volt, amikor egy-egy személy nem az elvártaknak megfelelően teljesített. Terveink sikerültek mind oktatási, mind tudományos szempontból.

Tehát a 2017/18. tanév tavaszi szemesztere kedvezően alakult oktatási egységünk számára. Szokásainkhoz híven ismételten megszerveztük Balatnakarattyán a Nemzetközi Katonai Információbiztonsági Konferenciát, amelyet eredményesnek értékelték mind a résztvevők, mind a szervezők.

Természetesen a társ tanszékek együttműködésével sikeres kiképzési gyakorlatokat folytattunk Püspökszilágyon, Csobánkán, illetve Ócsán.

Hasonlóan az elmúlt évhez, szintén az ERASMUS programnak köszönhetően a külföldi hallgatói részképzés mellett fiatal oktató kollégáink rendszeresen tartottak előadásokat társintézményeinkben a környező országokban, valamint különböző nemzetközi konferenciákon.

Végzős hallgatóink sikeres záróvizsgát tettek, így augusztus 20-át követően elfoglalhatják új, felelősségteljes beosztásukat.

Remélem, hogy egy kellemes nyári kikapcsolódást követően, ősszel, közösségünk ismét folytatja oktatási, kutatási és tudományos munkáját szakmai kultúránk elmélyítése és hírnevünk bővítése érdekében.

Ezen gondolatok jegyében kívánunk kellemes időtöltést az idei év első számának áttekintéséhez!

Budapest, 2018. június 30.

Kerti András
a Szerkesztőbizottság
elnöke

Czető Bálint: Pszichológiai befolyásolás, avagy Social engineering

Absztrakt

A támadók igyekeznek kihasználni a lehető legtöbb biztonsági rést egy hálózatban, rendszerben, azonban minden rendszer leggyengébb alkotóeleme maga az ember. A legegyszerűbb támadásokhoz nem kell több éves informatikai tapasztalat, de még komoly szakmai hozzáértés sem, elegendő az emberi naivitásra vagy jóhiszeműségre építeni a támadást. Ezt a social engineerek remekül ki is használják, a cikk ezen módszerekbe ad betekintést.

Kulcsszavak *social engineering, phising, pharming*

Bevezetés

„A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.”

Kevin D. Mitnick

Manapság naponta lehet olvasni különböző hackertámadásokról, rosszindulatú behatolásokról. A támadók különböző módszerekkel hatolnak be egy cég, vállalat, szervezet vagy akárcsak egy magánszemély hálózatába, értékes adatok után kutatva. A social engineering az egyik-, ha nem a legegyszerűbb módja az adatok eltulajdonításának. A „hackerek” az emberi jóindulatot, naivitást kihasználva jutnak hozzá szenzitív információkhoz, mellyel később komoly károkat tudnak okozni. A social engineerek módszerei és támadásaik kivitelezési módjai nagyon változatosak, sokszor még a támadás után is rejtve marad a tevékenységük. Mint már említettem,

a social engineerek által használt módszerek nem igényelnek komoly informatikai tudást, csupán az emberek manipulálhatóságát kell kihasználni. [1]

A social engineering támadásokat két nagy csoportra lehet osztani:

- Humán alapú social engineering technikák
- Számítógép alapú social engineering technikák

Humán alapú social engineering technikák

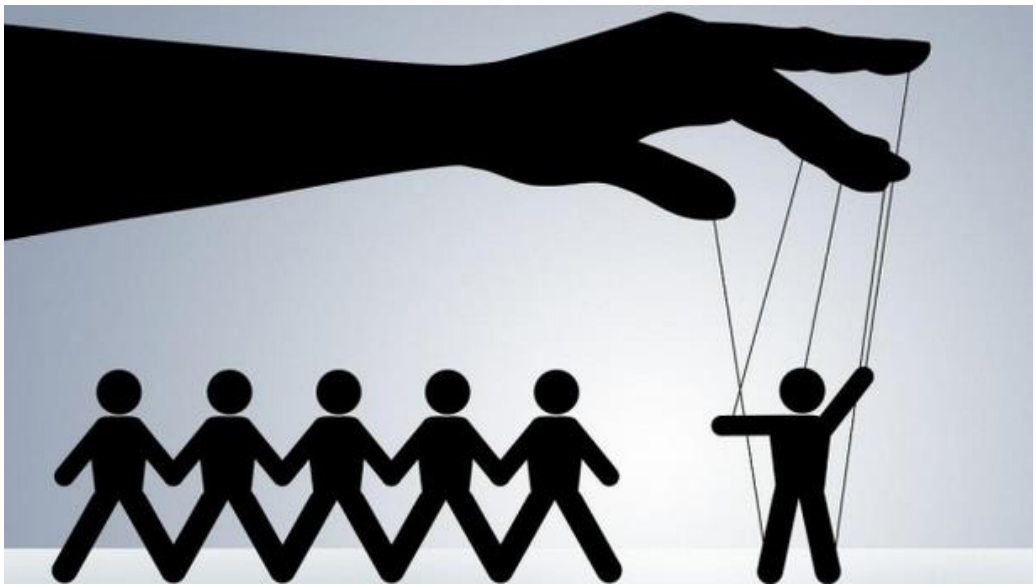
A social engineering ezen típusai nem igényelnek számítógép használatot, mindössze az emberek kihasználhatósága révén férnek hozzá információhoz. A nagyvállalatok számára ez információbiztonsági szempontból hatalmas kockázati tényezőket rejt magában. Ezeket a két csoportra lehet osztani:

- Személyzeti: Korlátozza, vagy teljesen ellehetetleníti a működéshez szükséges megfelelő képesítésű munkaerő hiánya a hatékony működést.
- Egészség és biztonsági: Ha az alkalmazottak jó közérzetének igénye, valamint a biztonságos munkaterület iránti igény elkerüli a vezetők figyelmet, akkor a munkaerő kevésbé hatékonyan tudja teljesíteni feladataikat. [2]

Védekezni nagyon nehéz ellenük, ugyanis általában más személynek adják ki magukat a támadók (pl. egy megbízható munkatársnak, bajbajutott személynek, egy vezető pozícióban lévő embernek, vagy akár rendőrnek is), így könnyen rávehetik a célpontot a saját személyes adatai átadására. A social engineerek először „felderítik a terepet” (interneten nyílt forrásokon utánanéznek egy vállalatnak, megtekintik az ott dolgozók facebook adatlapját, esetlegesen telefonon keresztül érdeklődnek információk iránt), majd csak kellő információ birtokában mennek a támadni kívánt helyre. [3]

Nézzünk egy egyszerű példát. Egy gyanútlan dolgozóhoz odamegy egy szerencsétlen ember, aki azt állítja, hogy otthon felejtette a kapun való bejutáshoz

szükséges mágneskártyáját. Megbetegedett a gyereke és orvoshoz kellett vinnie, a nagy kapkodásban otthon felejtette. Elmondja, hogy Kovács Béla osztályvezető beosztottja, és nagyon megüti a bokáját, ha ma is elkésik, az állása is veszélyben lehet. A gyanútlan dolgozó készségesen beengedi a szerencsétlen embert, aki innentől kezdve szabadon járhat az épületben.



1. ábra Social Engineering

Forrás: https://phoenixts.com/blog/is-your-company-vulnerable-social-engineering-attacks/

Ebben a példában egyszerűen az együttérzésre alapozott a támadó (beteg kisgyermek, elbocsátják a munkahelyéről). Mivel sokunkkal előfordult már, hogy otthonfelejtettük a kulcsunkat, nem gyanakszunk egyből rossz szándékra, ráadásul nem sokan kockáztatnák meg, hogy egy másik ember állásának az elvesztése az ő lelkén száradjon.

A példát tovább fűzve tételezzük fel, hogy az épületbe bejutott social engineer az egyik irodába odafárad egy gyanútlan dolgozóhoz, miszerint ő az informatikai

részlegről jött, mert gyorsan meg kell javítania valamit a számítógépen, utána jobb lesz a számítógép és még gyorsabb is. Megkéri, hogy jelentkezzen be a fiókjába, hogy segíthessen.

Itt is láthatjuk, hogy az emberi naivitást kihasználva jutott információhoz a támadó. A nagy vállalatoknál dolgozók gyakran nem ismerik a más részlegeken dolgozókat, ráadásul a legtöbb irodai munkás nem ért az informatikához, csak az ő munkájához szükséges programokhoz. Mivel a gyanútlan dolgozó nem ért hozzá, és ráadásul segítséget nyújtanak neki készségesen „átadja a székét" a támadónak.

Ebben a fiktív történetben természetesen rengeteg ponton szükséges volt a szerencse, komoly szerepe volt a social engineer színészi képességeinek, de a lényeg, hogy jól érzékelhetőek benne a humán alapú social engineering által használt támadásmódok. [4]

Számítógép alapú social engineering technikák

Az előző részben említésre került „ember alapú" social engineering technikáktól eltérően a számítógép alapú technikák nem igényelnek fizikai kontaktust a célszemélyekkel, egyszerűen az interneten keresztül manipulálják az embereket.

Ezekhez a módszerekhez már szükséges a komolyabb informatikai hozzáértés, azonban a világhálón rendelkezésre áll minden információ az ilyen támadások végrehajtásáról.

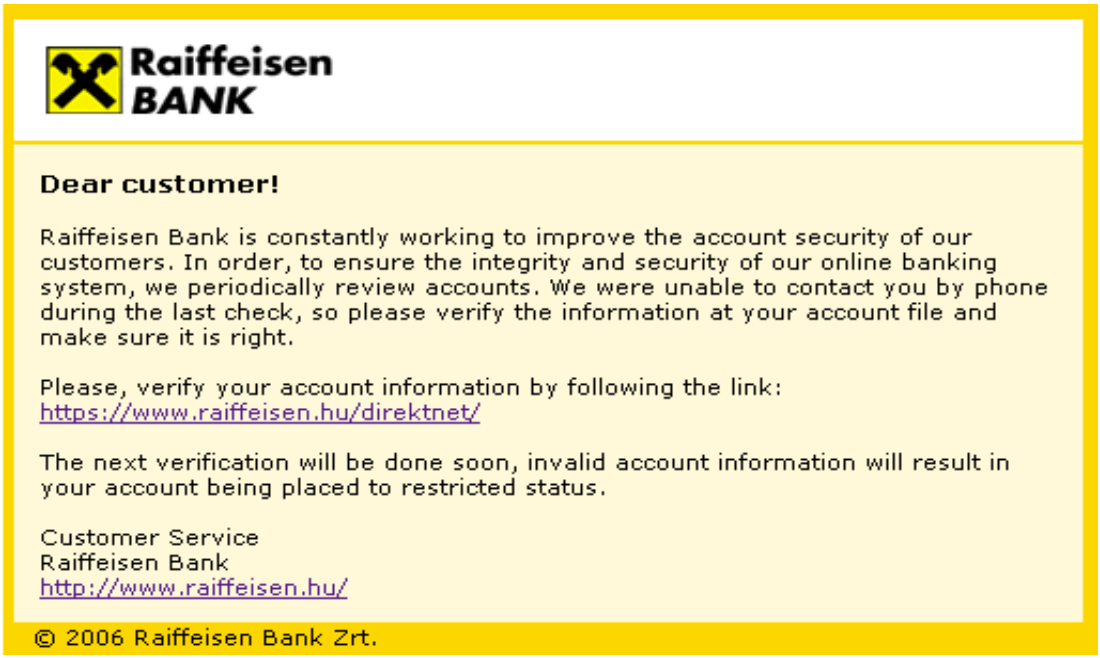
Phising

A phising (password harvesting fishing) vagyis adathalászat az egyik legismertebb social engineering technika, melyet sokszínűsége és változatossága tesz annyira veszélyessé.

Ezeknél a támadásoknál a hackerek általában egy e-mailt küldenek a felhasználónak, melyben megpróbálják átirányítani a felhasználót egy a hackerek

által készített weboldalra. Egyszerű példa, amikor az e-mailben egy bank nevében szólítják fel a felhasználót, hogy le fog járni a jelszava és kérik, hogy azt változtassa meg. Az e-mailben megtalálható egy hivatkozás is, ami a bankéhoz majdnem 100%-ban hasonlító oldalra irányítja a gyanútlan felhasználót. Itt megadja a felhasználónevét és jelszavát is, amit ettől kezdve felhasználhatnak a hackerek.

Az ilyen típusú támadások többnyire sikeresek, mivel kevesen veszik észre az eredeti és a hackerek által készített oldal közötti különbségeket, valamint ismét fontos megemlíteni a hiszékenységet, mint emberi tényezőt. [5]


Raiffeisen BANK

Dear customer!

Raiffeisen Bank is constantly working to improve the account security of our customers. In order, to ensure the integrity and security of our online banking system, we periodically review accounts. We were unable to contact you by phone during the last check, so please verify the information at your account file and make sure it is right.

Please, verify your account information by following the link:
https://www.raiffeisen.hu/direktnet/

The next verification will be done soon, invalid account information will result in your account being placed to restricted status.

Customer Service
Raiffeisen Bank
http://www.raiffeisen.hu/

© 2006 Raiffeisen Bank Zrt.

2. ábra Példa egy 2006-ban elkövetett phising típusú támadásra

Forrás: http://slideplayer.hu/slide/11777450/

Pharming

A social engineerek által használt támadásmódok közül talán ez az egyik leghatékonyabb, ugyanakkor ez áll a legtávolabb az eddig ismertetett social engineering technikáktól. Az eddig említett technikák mindegyikének az emberek manipulálhatósága adta az alapot, azonban a pharming (eltérítéses adathasználat) a

web böngészőprogramok és DNS szerverek biztonsági réseit használja ki egy hamis weboldalra való tereléshez.

A gyakran látogatott weboldalak IP címének gyorsabb fordítása érdekében a címek a számítógépen a DNS[1] gyorsítótárba mentődnek. Egy gyakran használt URL[2] beírásánál a számítógép először a gyorsítótárban keresi meg a címet, így sokkal gyorsabb elérést biztosít a weboldalhoz.

A pharming alapját hackerek által készített trójai programok képezik, melyek a DNS gyorsítótárba ágyazódnak be. Ezek a vírusok megváltoztatják a gyorsítótárban lévő címeket, így amikor egy általunk gyakran látogatott oldal címét írjuk be és a számítógép automatikusan a gyorsítótárból keresi ki a címet, nem az általunk kívánt oldalra jutunk, hanem a támadó által létrehozott, a céloldallal teljesen megegyező weboldalra. Legnagyobb veszélye, hogy látszólagosan semmi nem jelzi a felhasználó számára, hogy egy ál oldalon tartózkodik. [6][7][8]

Összegzés

Végezetül beláthatjuk, hogy a social engineering révén rengeteg módon sebezhető egy vállalat vagy akár egy magánszemély is. A fent összegyűjtött technikák betekintést nyújtottak a social engineerek világába és felhívják a figyelmet az emberek manipulálhatósága miatt kihasználható biztonsági résekre.

Ezeknek a támadásoknak a sikerességét nagymértékben vissza lehetne szorítani kellő odafigyeléssel és körültekintéssel, valamit az emberek tudásának bővítésével.

[1] Domain Name System (DNS), azaz a tartománynév rendszer egy hierarchikus, nagymértékben elosztott elnevezési rendszer számítógépek, szolgáltatások, illetve az internetre vagy egy magánhálózatra kötött bármilyen erőforrás számára

[2] Uniform Resource Locator (URL), azaz egységes erőforrás-hely, vagy más néven webcím, az interneten megtalálható bizonyos erőforrások (például szövegek, képek) szabványosított címe

Hivatkozások

[1] Paráda István – Bodnár István: Jelszó ellopás social engineering, e-mail spoofing és fake url segítségével; HÍRVILLÁM – SIGNAL BADGE 2016/1. szám

[2] Megyeri Lajos – Farkas Tibor: KOCKÁZATKEZELÉS, TUDOMÁNY VAGY KURUZSLÁS?; Hadmérnök - XII. Évfolyam 3. szám – 2017. szeptember

[3] Tóth András: Future Information Security Threats to the Defense Sector, HADTUDOMÁNYI SZEMLE X. évfolyam 4. szám: pp. 246-257. (2017)

[4] Oroszi Eszter Diána: Social Engineering Az emberi erőforrás, mint az információbiztonság kritikus tényezője; BCE – GTK szakdolgozat, 2008

[5] Kovács László: AZ INFORMÁCIÓS TERRORIZMUS ESZKÖZTÁRA; Robothadviselés 6. Tudományos Konferencia 2006. november 22.

[6] http://searchsecurity.techtarget.com/definition/pharming

[7] Paráda István: SOCIAL ENGINEERING IN INFORMATION INFRASTRUCTURE – CYBERSPACE In: Ivan MAJCHÚT, Vladimír ANDRASSY, Štefan GANOCZY, Michal HRNČIAR, Ondrej KREDATUS, Gabriela KREDATUSOVÁ, Jakub SASARÁK, Juraj ŠIMKO, Jaroslav VARECHA, Lubomír BELAN, Stanislav MORONG (szerk.) 8. medzinárodná vedecká konferencia: "NATIONAL AND INTERNATIONAL SECURITY 2017". 614 p. Konferencia helye, ideje: Liptovsky Mikulas, Szlovákia, 2017.10.26-2017.10.27. Liptovsky Mikulas: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2017. pp. 344-351. (ISBN:978-80-8040-551-9)

[8] Tóth András: INTERNATIONAL INFORMATION SECURITY IN HUNGARY, 8. medzinárodná vedecká konferencia: "NATIONAL AND INTERNATIONAL SECURITY 2017" pp. 548-557.

István Paráda: Requirements for developing the Cisco Net Academy to Pearson Vue Exam Center

Abstract

One of the most successful network courses is the Cisco Networking Academic at the National University of Public Service. This provides high quality knowledge for students attending BSc training and for officers, and military personnel participating in military network training.

However, completing the course is not enough, it is also necessary to go to an examination center where they can get the industrial qualification. In proposing this solution, I suggest that the existing networking academy should be developed into a Pearson Vue Exam Center. This article discusses the requirements of this question.

Keywords: *CISCO, Net Academy, training, education, exam center*

Introduction

An advanced, modern, infocommunication system, network important elements are not only the technological but also the network operator itself. Thus, it is imperative to have a modern, internationally acknowledged, accepted and value-oriented, internship-oriented, knowledge-based, skill-level, professional knowledge, qualification and qualification in the IT sector of the civil sphere. Education, training is the means of developing knowledge transfer, practice-oriented, skill-based professional skills. The outstanding achievement of this is the CISCO Network Academic Training – Networking Academy Program, an educational, training system, online, e-learning education and learning interface, labor market, knowledge base and virtual community, a wide-ranging technical science program. With the use of network academic training, it is conceivable and feasible, among other things, to equip the professional operator with modern, networking skills. As a result, they will

be able to meet expectations and requirements. This is done by designing them as a useful and excellent expert, and being able to show them as a competitive player in the civilian labor market, with the ability to translate them into easily transposable and up-to-date knowledge, the value-added, value-added in the civil sphere qualifications equivalent to those obtained there and qualifications. [1]

Next stage of the Network Academy Training successfully executed at National University of Public Service Faculty of Military Science and Officer Training, the Accademy continues to become a Perason Vue (Virtual University Enterprises) Examination Center, which will become a skill extension to the NetAcad program so far described as a possibility for transferring knowledge and knowledge opens up and exhibits official reviews. This kind of skill development contributes to the validation of the value-based professional knowledge and certification qualifications described above. Pearson VUE in the world of 165 countries is an international computer examiner company that conducts exams to acquire world-class licensing companies, including leading IT companies such as Novell[3], Oracle[4], SAP[5], Cisco Systems[6].

[3] Novell, Inc. is an IT company. Novell Nterprise, Directory-Based Identity Management and Integrated Security Solution (Novell Nsure), Business Application Integration, and Directory-Based Web Services (Novell exteNd), and Business and IT Consulting and Operational Support) are provided to its clients.

[4] Oracle Corporation is the world's largest provider of business software solutions, founded in 1977 in California. Larry Ellison has been the head of the company since then.

[5] SAP is the world's leading integrated enterprise management system. Under an integrated corporate governance system, we mean a program package covering all enterprise processes in a given company. SAP industry-specific solutions are used in more than 120 countries, approximately 32,000 companies, small and medium-sized businesses, and large companies alike.

[6] Cisco Systems, Inc. is an American multinational technology conglomerate headquartered in San Jose, California, in the center of Silicon Valley, that develops, manufactures and sells networking hardware, telecommunications equipment and other high-technology services and products.

Benefits for students and the exam center

- Access: The culmination of IT training is certification. By delivering Microsoft, CompTIA[7], Cisco, Oracle, VMware[8] and other exams, your students will validate what they've learned. That proof leads to advancing a current career or landing a new job.
- Reliable technology
- Smart scheduling: The advanced registration and scheduling system allows you to efficiently manage your testing center hours and staff resources while providing testing candidates with scheduling flexibility.
- Test administration: The Pearson VUE system utilises the speed and cost-effectiveness of the internet to reliably download exams and transmit results with a press of a button. There is no charge for Pearson VUE testing software or upgrades.
- Security: There is a one-time fee of $450 (USD) to purchase the Enhanced Security Protocol kit that includes digital cameras, signature pad and other security-related information. You may purchase this kit on mindhub.com/ESP or through another vendor using the exact specifications provided. For sites located outside of the United States, please contact your Channel Manager for options on how to order your ESP kit. [2]

[7] The Computing Technology Industry Association (CompTIA), a non-profit trade association, issuing professional certifications for the information technology (IT) industry. It is considered one of the IT industry's top trade associations

[8] VMware, Inc. is a subsidiary of Dell Technologies that provides cloud computing and platform virtualization software and services.[2] It was the first commercially successful company to virtualize the x86 architecture.

- Learning products: Being a Pearson VUE® Authorised Test Centre gives you access to volume discounts, special promotions and support tools to grow your business — information that shares the value of certification with your students, content for your website, signage and other marketing materials.
- Test centre support: The friendly and knowledgeable Pearson VUE Support Services (VSS) team is available 24/7 to help guide you through any issues that may arise. In addition, you will also have the ability to report and check the status of site cases, schedules and history via our VSS website. [3]

About the Installation Scenarios

This document describes the minimum hardware requirements to install the Pearson VUE Testing System (VTS) software in a Pearson VUE Authorized Test Center. The VTS software may be installed in one of two configurations: Workgroup scenario or Server scenario.

In a Workgroup scenario installation, exam delivery workstations are connected through a local area network (LAN) or workgroup to the Administration workstation which provides shared file storage. In a Server scenario installation, all exam delivery workstations are connected through a LAN, and a file server provides shared file storage. (Server scenario refers to a setup type and is not related to an Operating System.)

System Requirements

Effective May 1, 2018, the following pages list the minimum system requirements for installing and running the Pearson VUE Testing System, and for operating as a test center. Pearson recommends purchasing equipment that meets or exceeds the Recommended Specifications. The minimum requirements will change periodically based on the needs of our exam sponsors.

Hardware configuration: All-in-one PC's are permitted as long as they meet the minimum Technical Specification and do not have a Touch screen. Pearson VUE highly recommends that All-in-one PC's meet the Recommended Technical Specifications.

Software licenses: All test centers are required to have Windows operating systems that have completed online activation. Application software installed on all exam delivery workstations must also have current licensing. Windows Operating Systems must pass Genuine Windows Validation.

Network configuration: It is strongly recommended that all machines with VTS Software installed remain in the same domain or workgroup, VLAN, and subnet. Network configurations that do not follow this guideline may experience decreased exam delivery performance. You may be asked to make changes to your network configuration to comply with this guideline as part of problem resolution.

Internet bandwidth: Some exam deliveries will require an internet connection. For Internet Based Tests (IBT) a minimum base connection speed of 1 Mbps down/up is required. Additional bandwidth may be required for more than 10 simultaneous IBT exam deliveries.

Monitors – Exam Delivery

Requirement

- Monitor
  - 17” or larger
  - Must allow for the following display resolution settings:
  - 1280 x 1024
  - 1024 x 768
  - Monitor must be connected to the computer using DVI[9], DisplayPort, or HDMI[10]
- Desktop Graphics Adapter
  - Exam delivery workstations must have a graphics adapter that supports GPU[11] Scaling (ability to Maintain Aspect Ratio)

[9] DVI is a video capture standard. Its purpose is to create a compromise digital picture transfer between the computer and the monitor.

[10] HDMI (High-Definition Multimedia Interface) is a proprietary audio/video interface for transmitting uncompressed video data and compressed or uncompressed digital audio data from an HDMI-compliant source device, such as a display controller, to a compatible computer monitor, video projector, digital television, or digital audio device.

[11] A graphics processing unit (GPU) is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device.

- Exam delivery workstations must have the GPU Scaling feature enabled in the graphics adapter software
- The latest version of graphics drivers must be installed

Pearson VUE specific hardware

Some exams may require the use of test center admissions equipment. If required, these components may be purchased from Pearson VUE or a third-party source.

Requirement

- Web Camera
  - Logitech HD Webcam C615 or
  - Logitech Pro 9000
- Signature Device
  - ePadLink: ePad Signature Pad – Model VP9801

Administration and Proctor workstations

- Operating System
  - Windows 10 Professional or Enterprise (64-bit)
  - Windows 7 SP1 Professional or Enterprise (64-bit)

- Processor
  - Intel: i3 or higher
  - AMD: Phenom II series, FX-4000 series or newer
  - Intel: i5-series

Note: CPU[12] must have a minimum of two cores (dual-core)

- RAM[13]
    - 2GB of RAM
    - 4GB of RAM or more
- Hard Drive
    - 20GB free disk space in NTFS[14] format
    - 50GB free disk space in NTFS format
- Graphics Adapter
    - Video Adapter must support DirectX 10 or higher. Latest drivers installed. 128MB of dedicated Video RAM.
    - Video Adapter must support DirectX 11 or higher. Latest drivers installed. 512MB dedicated Video RAM or more.
- Display
    - All computers and monitors must be connected via DVI, DisplayPort, or HDMI. 17” monitor or larger
- Mouse & Keyboard
    - English QWERTY Keyboard, 2 Button Wheel Mouse
- USB Ports
    - 4 available USB 2.0 ports for:
        - English QWERTY Keyboard

[12] The CPU (Central Processing Unit) is also known as a processor or processor. microprocessor, the "brain" of the computer, the unit that controls the interpretation and execution of instructions, is a semiconductor complex electronic circuit.

[13] Random-access memory (RAM /ræm/) is a form of computer data storage that stores data and machine code currently being used.

[14] NTFS (New Technology File System) is a proprietary file system developed by Microsoft.Starting with Windows NT 3.1, it is the default file system of the Windows NT family.

        - 2 Button Wheel Mouse
        - Signature Pad admissions equipment
        - Camera admissions equipment
    - 6 available USB 2.0 ports for:
        - English QWERTY Keyboard
        - 2 Button Wheel Mouse
        - Signature Pad admissions equipment
        - Camera admissions equipment
        - 2 spare ports

- Network Connection
    - 100Mbps Full Duplex WIRED connection to the network switch.
    - 1Gbps Full Duplex WIRED connection to the network switch.
    - Strongly Recommended: All machines with VTS Software installed should remain in the same domain or workgroup, VLAN, and subnet.
- Internet Browser
    - Internet Explorer 11 and Microsoft Edge
- Printer
    - 600 DPI Laser Printer
- Additional Software
    - .NET 4.0 is installed with the VTS software.
    - If installing on Windows 10, .NET 3.5 must be enabled on the Administration/Proctor workstation to complete the VTS installation.
    - All workstations must have Anti-Virus software installed with a current update.

Exam Delivery workstation

- Operating System
  - Windows 10 Professional or Enterprise (64-bit)
  - Windows 7 SP1 Professional or Enterprise (64-bit)
- Processor
  - Intel: i3 or higher
  - AMD: Phenom II series, FX-4000 series or newer
  - Intel: i5-series

Note: CPU must have a minimum of two cores (dual-core)

- RAM
  - 2GB of RAM
  - 4GB of RAM or more
- Hard Drive
  - 10GB free disk space in NTFS format
  - 50GB free disk space in NTFS format
- Graphics Adapter
  - Video Adapter must support DirectX 10 or higher. Latest drivers installed. 128MB of dedicated Video RAM.
  - Video Adapter must support DirectX 11 or higher. Latest drivers installed. 512MB dedicated Video RAM or more.
  - All exam delivery workstations must have a Graphics Adapter that supports GPU Scaling (sometimes called Maintaining Aspect Ratio).
  - All exam delivery workstations must have the GPU Scaling feature enabled.
  - All computers and monitors must be connected via DVI, DisplayPort, or HDMI.

- Audio
    - Windows compatible audio playback capability.
- Mouse & Keyboard
    - English QWERTY Keyboard
    - 2 Button Wheel Mouse
- USB Ports
    - 2 available USB 2.0 ports for:
        - English QWERTY Keyboard
        - 2 Button Wheel Mouse
    - 4 available USB 2.0 ports for:
        - English QWERTY Keyboard
        - 2 Button Wheel Mouse
        - 2 spare ports
- Network Connection
    - 100Mbps Full Duplex WIRED connection to the network switch.
    - 1Gbps Full Duplex WIRED connection to the network switch.
    - Strongly Recommended: All machines with VTS Software installed should be in the same domain or workgroup, VLAN, and subnet.

Server: file storage

The file storage server must be accessible to the Administration workstation, Proctor workstation, and all exam delivery workstations. These requirements apply to Administration workstations with 1 – 15 exam delivery workstations, and to Servers with 15 – 30 exam delivery workstations.

- Operating System
    - Windows 10 Professional or Enterprise (64-bit)

  - Windows 7 Professional SP1 (64-bit)
  - Windows Server 2012 R2 with update (64-bit)
  - Windows Server 2008 SP2/2008 R2 (64-bit)
  - (Windows Server Core is not currently supported)
  - Windows Server 2012 R2 with update (64-bit)
  - Windows Server 2008 R2 (64-bit)
- Processor
  - Intel: i3 or higher
  - AMD: Phenom II series, FX-4000 series or newer
  - Intel: i5-series

Note: CPU must have a minimum of two cores (dual-core) [4]

Facility requirements

The following minimum requirements must be met when setting up a test center:

Test Center building & surrounding area

- Provide adequate parking and/or access to public transportation.
- Provide access to people with disabilities, in compliance with the Americans with Disabilities Act of 1990 (in the United States) or your country-specific requirements.

Candidate check-in and waiting area

  - Provide an area separate from the exam delivery room for checking in candidates. There should be a workspace for the test administrator where the computer (must be a desktop workstation) that will serve as your administration workstation is located.

- The ESP Security kit will be connected to this administration workstation that will be used for check in. (If purchasing the ESP security kit through Pearson VUE, you must be an approved site with a Site ID number before making this purchase.)
- There should also be seating for candidates who are waiting.

Lockable storage

- Provide lockers or other suitable storage for personal belongings, such as a lockable file cabinet, closet or backpacks with locks.
- The candidate cannot take items such as pagers, paper, books and briefcases into the exam delivery room. See "Storing Personal Belongings" in the policy & procedures guide for details.
- Lockable storage must be outside the exam delivery room.

Exam delivery room area

- Provide an enclosed, professional environment that is clean, comfortable, smoke-free and conducive to testing.
- Place the exam delivery workstations in a permanently enclosed area that is separate from the rest of the office space. It should be in a low-traffic area away from any training rooms in use to avoid the sounds of students talking and moving to and from the classroom. Also, avoid placing the exam delivery room near an area where people gather, such as a student cafeteria or busy corridor.

Tips:

- Insulate the exam delivery room to minimize noise. In addition to insulated walls, an insulated ceiling will help minimize noise.
- Commercially available acoustic privacy systems (or "white noise" generators) use sound-masking technology to effectively mute external noise. These may be helpful in areas where traffic or street noise is sometimes a problem.

- Provide adequate lighting and ventilation, along with comfortable seating and work surfaces. Room lighting should provide sufficient light for keyboard and noteboard while avoiding screen glare.
- In the exam delivery room, remove equipment such as printers, fax machines, copiers or telephones while testing is in progress.
- Minimize noise and distractions during testing.

Tips:

- While testing is in progress, place a sign alerting people in your office to be especially quiet near the exam delivery room. For example, you might post a sign that says: "Quiet! Testing in Progress."
- Headphones that cover the entire ear are successful in blocking most sounds. They should not be connected to any device. Some candidates prefer to use earplugs.

Workstation setup

- Place each exam delivery workstation on a clean surface that has no obstructions overhead and underneath. The desk space established for each workstation should measure approximately four feet (1.2 meters) wide. Only one workstation should be placed on each four feet (1.2 meter) of space.

- Separate candidates within the exam delivery room. Separate exam delivery workstations with at least four feet (1.2 meters) of empty space on all sides, or use privacy partitions.

If you are using partitions, please follow these guidelines:

- Though optional at Pearson VUE Authorized Test Centers (PVTCs), if you are using privacy partitions, which will create privacy and also absorb sound between workstations, you are required to have permanent partitions or walls that are at least 1.5m (5') in height from the ground up and extend outward from the wall at a 90-degree angle. Desktop partitions are acceptable as long as the height measured from the floor is at least 1.5m (5').

Candidate proctoring/monitoring options are available

Please note you must only meet one of the 3 options below.

- Clear glass viewing window or wall
    - Proctor sits outside the exam delivery room and looks through the window to monitor candidate testing.
- Live feed video surveillance system
    - You must configure camera(s) inside the exam delivery room with a video monitor outside the exam delivery room. The proctor sits outside the exam delivery room and uses the video surveillance equipment to view candidates during testing.
- Proctor inside exam delivery room
    - The test administrator is seated within the exam delivery room. The Proctor cannot have a computer inside the exam delivery room. They may be provided a desk and a chair. [5]

Conclusion

One of the ways in which to acquire knowledge of the state of the art, digital knowledge and infocommunication networks is not the only way to capture education and training. I came to the conclusions of the CISCO Network Academy - NetAcad, the CISCO Network Academic Training - NetAcad Program, its trainings and qualifications, that they are far enough to acquire this professional knowledge, practice-oriented, skill-based learning. [6]

Integrating the affected staff into this network academic training system can also provide them with a positive result that while meeting the requirements of the organization for the operation of modern, digital converged systems and network infrastructures that meet the expectations, requirements, user service requirements in the same time, it can be presented as an easily translatable, comparable, competitive knowledgeable workforce with an internationally acknowledged reputation in the civilian labor market, in the civil IT segment, in the event of a potential for an objective.

The development of the Cisco Net Academy Pearson Vue Examination Campaign signifies a significant increase in skills. After completing a course, we will have the opportunity to test our students and give them an accredited certificate.

Bibliography

[1] Jobbágy Szabolcs: A honvéd altiszt és zászlós híradó és informatikai üzemeltető állomány digitális szakmai ismereteinek fejlesztése, Doktori (PhD) értekezés, Budapest 2017, https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/jobbagy-szabolcs-szazados-a-digitalizacio-hatasa-___.original.pdf (Download:2018.05.28)

[2] Tóth András: INTERNATIONAL INFORMATION SECURITY IN HUNGARY, 8. medzinárodná vedecká konferencia: "NATIONAL AND INTERNATIONAL SECURITY 2017" pp. 548-557.

[3] Pearson Education, Inc.: Deliver the worlds leading exams as a Pearson VUE ® Authorised Test Centre, PV/H2B/Gen-UK/9-17, 2018. https://home.pearsonvue.com/Documents/Test-center/Overview-UK.aspx (Download:2018.04.15)

[4] Pearson Education, Inc.: PVTC Technical Requirements 2018. https://home.pearsonvue.com/Documents/Test-center/Overview-UK.aspx (Download:2018.04.16)

[5] Pearson Education, Inc.: PVTC Facility Requirements 2018. https://home.pearsonvue.com/Documents/Test-center/pearsonvue_facility_reqs.aspx (Download:2018.04.17)

[6] Jobbágy Szabolcs: CISCO Hálózati Akadémiai Képzés - NetAcad Program HADMÉRNÖK XII Évfolyam 1. szám – 2017. március pp. 290-300. (2017) http://www.hadmernok.hu/171_23_jobbagy.pdf (Download:2018.05.17)

Kondás Katalin: A büntetés-végrehajtás informatikai fenyegetettsége

Absztrakt
Az informatikai rendszerekben a számítógépterem kiemelt fontosságú helyiség. A rendszer fenyegetéseknek van kitéve. A büntetés-végrehajtás számítógépterem helyiségének lehetséges kockázatait felkutatom, javaslatot teszek további intézkedésekre annak védelme érdekében. Az informatikai rendszer egyéb fenyegetettségeit megvizsgálom. Összefoglalom, hogy az adatok módosítása, lopása, törlése milyen következményekkel járhat.
Kulcsszavak: *bűntetés-végrehajtás, informatikai rendszer, információbiztonság, informatikai biztonság, informatikai fenyegetés*

Bevezetés

Az elmúlt 10 évben a büntetés-végrehajtási szervezet (a továbbiakban: bv.) informatikai fejlesztése jelentős változásokon ment keresztül, a rendszerben azóta is folyamatos fejlesztések, újítások történnek. Mint azt már korábban ismertettem a Hadmérnök tudományos folyóirat XII. Évfolyam 2. számban megjelent „Informatikai korszakváltás egy büntetés-végrehajtási intézetben” publikációmban: a bv. támogatást kapott az EKOP-1.1.6 kiemelt pályázati projekt végül a teljes informatikai rendszer korszerűsítését tette lehetővé.

Az egész szervezet informatikai rendszere egységessé vált a szerverpark, a munkaállomás, a mentőegység, a hálózat, a jogosultságkezelés, aktív hálózati eszközök, távfelügyeleti- és táv-beavatkozási képességek kialakítása tekintetében egyaránt. A belső normatív környezet kialakítása, az informatikai szakállomány, illetve a végfelhasználók képzése megtörtént. [1]

A Büntetés-végrehajtás Országos Parancsnoksága (a továbbiakban: BVOP) informatikai rendszere a teljes szervezet informatikai központja. A rendelkezésre

állása kiemelt fontosságú. Azonban figyelemmel kell lenni az intézeti informatikai rendszerre is, hiszen helyi szinten jelentős szereppel bír. Éppen ezért a rendelkezésre állás biztosításához szükséges felmérni az intézetben meglévő kockázatokat. A felmérés során elsősorban az egyes helyiségeket kockázati csoportokba kell sorolni az informatikai rendszer működése szempontjából megvalósított funkcióik szerint. Ezt követően történhet meg a helyiségek kockázatelemzése.

A számítógépterem helyiségének lehetséges kockázatait felkutatva, annak megelőzésére, illetve elhárítására keresek megoldást. Átfogó képet adok a szerverterem rendelkezésre állásáról, működéséről, megnézem a szükséges fejlesztéseket. Munkám során személyes tapasztalataimat, tudományos publikációkat, a projekttel kapcsolatos dokumentációt vettem segítségül.

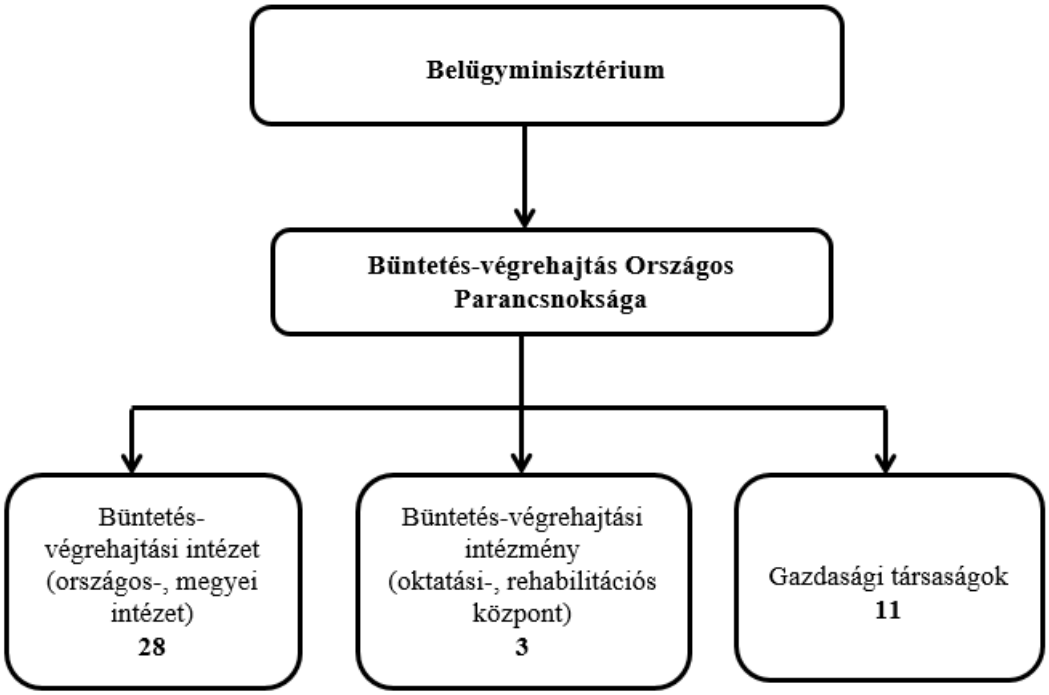
A büntetés-végrehajtási szervezet szerepe, felépítése

A magyarországi bv. munkájáról, szerepéről, illetve az elítéltekkel való foglalkozás jelentőségéről, s adataiknak nyilvántartásáról a büntetés-végrehajtási szervezetről szóló 1995. évi CVII. törvény és a büntetések, és a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról szóló 2013. évi CCXL. törvény (a továbbiakban: Bv. Kódex) ad áttekintést. A bv. felépítését az 1. számú ábra szemlélteti.

Magyarországon a fogvatartottak (jogerősen elítélt, illetve jogerős ítéletet még nem kapott bűnelkövető) elhelyezését, mint alaptevékenységet, ma összesen 28 büntetés-végrehajtási szerv hajtja végre. Ezeket különböző szempontok szerint kategorizálhatjuk, ezek között vannak:

- az előzetes letartóztatás foganatosítására hivatott megyei intézetek, az ún. előzetes házak (14 intézet), illetve

- a jogerős szabadságvesztés végrehajtását végző országos intézetek, az ún. letöltő házak (14 intézet), melyek az 1. ábrán is láthatók.



1. ábra: A magyar büntetés-végrehajtás szervezete (saját szerkesztés)

Egyéb fogvatartotti csoportok befogadására létrejött intézetek a fiatalkorúak regionális büntetés-végrehajtási intézetei, melyek Kecskeméten, Pécsett, illetve Szirmabesenyőn találhatók. A nők fogva tartását végrehajtó önálló intézet és intézeteken belüli alegységek Kalocsán, Pálhalmán, Egerben vannak. Ilyen szempontból jelentős elhelyezést biztosít Kecskeméten az anya-gyermek körlet, amely funkcióját a neve is jelzi. Léteznek további speciális faladatokat ellátó intézmények, ilyenek az egészségügyi feladatokat ellátó intézetek (Igazságügyi Megfigyelő és Elmegyógyító Intézet, Büntetés-végrehajtás Központi Kórház, Nagyfa). A fogva tartás során nagy jelentőséggel bírnak ezek az intézetek.

A szabadságvesztés végrehajtásának rendje a büntetés-végrehajtási rendszer legfontosabb tartalmi eleme, amely biztosítja az egyes kiszabott szankciók céljának megvalósítását. A szabadságvesztés kiszabása esetén a végrehajtási fokozat meghatározása az ítélkező bíróság feladata. A Büntető Törvénykönyv [2] értelmében, ha a bíróság szabadságvesztést szab ki valakire, akkor az a bűncselekmény és az elkövető társadalom veszélyességére, bűnösség fokára, egyéb súlyosbító és enyhítő körülményekre tekintettel különböző fokozatba sorolható be: fegyház, börtön, illetve fogház végrehajtási fokozatot állapíthat meg.

A bűntetés-végrehajtás informatikai struktúrája

A büntetés-végrehajtási szervezet rendszerszintű átalakítása 2010-ben kezdődött meg európai uniós (Elektronikus Közigazgatás Operatív Program) pályázati forrás felhasználásával, amely érintette az egész büntetés-végrehajtás hálózatának korszerűsítését és a végpontok számának növelését, a számítástechnikai eszközök (szerverek, munkaállomások) egészét, illetve az elavult szoftvertechnológiára épülő nyilvántartások cseréjét egyaránt. Az átalakítás célja egy homogén, szabványos, egyenszilárd, országos zárt célú informatikai rendszer kialakítása volt, amely a szervezet minden telephelyén, azonos infrastrukturális hátteret biztosít az újonnan kifejlesztett nyilvántartások működtetéséhez. [3]

A projekt keretében megvalósult a bv. valamennyi intézetében az egységes géptermek kialakítása, szerverparkok létesítése, szünetmentesítés és klímatizálás, NAS mentőrendszer-, távfelügyeleti- és táv-beavatkozási képességek kialakítása, egységes hozzáférés és jogosultságkezelés, teljes körű munkaállomás csere, új nyilvántartó programok fejlesztése. Összesen 3400 db vékonykliens és 700 db PC került beüzemelésre. Ennek következményeként az informatikai szakállomány,

illetve a végfelhasználók képzése is szükségessé vált, és az új Informatikai Biztonsági Szabályzat is kiadásra került.

A BVOP által üzemeltetett szerverszoba kiemelt fontosságú, hiszen az egész büntetés-végrehajtás informatikai rendszerében központi szereppel bír.

A bv. az információbiztonságot alapvető feltételnek tekinti, amely elengedhetetlen a szervezet eredményes működéshez, kialakítása során alkalmazandó alapelvek:

- a törvényesség biztosítása,
- megfelelés a nemzeti és nemzetközi szabványok, ajánlások, módszerek előírásainak,
- a védelmi intézkedéseknek a kockázatokkal arányosan történő meghatározása,
- a védelmi intézkedések költséghatékony kialakítása,
- a megelőzés szemléletű biztonság kialakítása,
- a biztonságtudatosság fokozása.

Az intézet informatikai alap infrastrukturális helyzetét tekintve egy telephelyes, egy összefüggő helyi hálózatból (LAN) álló, 1db táv-adatátviteli csatlakozási pontú (NTG-WAN) intézet. Az intézet egy szerverparkot és informatikai munkaállomás oldali infrastruktúrát, valamint egy telefonközpontos architektúrát működtet, megfelelő helyi szervezeti és szervezési adottságokkal.

A hír- és biztonságtechnikai szakterület, a biztonsági technológiák: telefonok, kamerák, érzékelők, rögzítők, EDR rádiók üzemeltetése az informatika (TCP/IP) irányába tart. A gazdasági szakterülethez tartozó nagy teljesítményű – multifunkciós – fénymásolók, faxok üzemben tartása, valamint a rádiótelefonos szolgáltatás sajátosságai, folyamatos feladatbeli, kompetenciái, szervezési, számonkérési, ellenőrzési, és nem utolsósorban szakirányítói anomáliákat okozhat. Ezek az eszközök funkcionálisan az informatikai hálózat működésének részévé válik.

Az informatikai működés tárgyi feltételei

A vizsgált intézet informatikai alap infrastrukturális helyzetét tekintve egy telephelyes, egy összefüggő helyi hálózatból (LAN) álló, 1db táv-adatátviteli csatlakozási pontú (NTG-WAN) intézet. Az intézet egy szerverparkot és informatikai munkaállomás oldali infrastruktúrát, valamint egy telefonközpontos architektúrát működtet, megfelelő helyi szervezeti és szervezési adottságokkal.

Az intézetben a BVOP által meghatározottak szerinti informatikai infrastruktúra került kiépítésre. Az intézetben összesen 81 munkaállomás üzemel a tartományi környezetben. Végponti eszközökből a szakterület rendelkezik kézi raktárkészlettel, mind a nyomtatók, mind a számítógépek tekintetében, amely fedezi az esetleges meghibásodásokból adódó igényeket. A szakterület tartalék szervert üzemeltet a nagyobb rendelkezésre állás és a stabil informatikai szolgáltatások biztosítására.

A szerverteremben az előírásoknak megfelelően telepítve van egy szünetmentes tápegység, mely áramkimaradás esetén a DC, File, TS, SQL szolgáltatásokat nyújtó szervereknek biztosítanak tápellátást. Az aktív hálózati eszközök folyamatos tápellátásának és feszültségproblémák okozta meghibásodások elleni biztosítására. Az intézet két aggregátorral rendelkezik, melyeknek indítása automatikus. A nagyobb teljesítményű aggregátor a teljes intézetet, a kisebb teljesítményű - a nagy meghibásodása esetén - a kulcsfontosságú eszközöket képes kiszolgálni. Célszerű lenne központi szünetmentes tápegység beüzemelése az aggregátorok indítási idejének áthidalására, ezáltal a kisebb helyi UPS-ek kiválthatóak lennének.

Az intézet táv-adatátviteli hálózati kapcsolódási pontját (WAN kijárat) az informatikai szakterület felügyeli, illetve fejlesztésében együttműködik a Nemzeti Infokommunikációs Zrt.-vel.

Szabványok

Az európai országokban megalakultak a nemzeti szabványügyi szervezetek, melyek megfogalmazott szabványainak alkalmazása nem kötelező, önkéntes. Az ITIL (Information Technology Infrastructure Library), azaz informatikaszolgáltatás módszertana az informatikára, mint szolgáltatás egészére kiterjedő, nemzetközileg széles körben elfogadott, az informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló módszertan, illetve ajánlás gyűjtemény neve. Az ISO 20000 az ezekből levezetett kötelező minimumkövetelmények, amelyek minimálisan elvárhatóak az információtechnológia szolgáltatások biztosítása terén.

Az ISO/IEC 27001 szabvány alapvető célja az Információbiztonsági Irányítási Rendszer létrehozása és működtetése. A szabvány felhasználóinak a biztonsági követelményeket, intézkedéseket a szervezet üzleti céljaiból és stratégiájából kell levezetniük. A szabvány a megfelelőségi és ellenőrzési követelményei alapján elvégezhető az informatikai (információs) rendszer tanúsítása.

Az ISO/IEC 27002 szabvány teljes szervezetre vonatkozó, az összes rendszerelemet magába foglaló informatikai biztonsági követelményeket és védelmi intézkedéseket tartalmaz a teljes körű informatikai biztonság megteremtéséhez. [4]

Az ISO/IEC 27003 az informatika, illetve a biztonságtechnikával kapcsolatos, az információbiztonság-irányítási rendszerek megvalósítási útmutatója.

Az ISO/IEC 27004 az informatikai biztonsági méréseivel, ellenőrzésével foglalkozik, abból a célból, hogy az irányítási rendszer hatékonyságát mérni lehessen.

Az ISO/IEC 27005 tartalmazza az információtechnológia, biztonságtechnika információbiztonsági kockázatmenedzsmentjét. Ennek C melléklete tartalmazza a tipikus fenyegetéseket, melyek alapján egy intézet informatikai rendszerelemeit elemzem. A kockázatelemzés megkezdése előtt az intézet helyiségeit az informatika

szempontjából betöltött funkciójuk szerinti csoportokba kell sorolni, a kockázatok ez alapján értelmezhetők. [5]

A szabványcsaládnak sok tagja már kiadásra került és továbbiak is fejlesztés alatt vannak.

Intézeti számítógép terem fenyegetettsége

Az intézet számítógépterme az informatikai rendszer működésének szempontjából betöltött funkció szerint kiemelt fontosságú helyiség.

A gépterem rendszer szintű kockázatelemzését az ISO/IEC 27005 szabvány C függelékében megfogalmazott leggyakoribb fenyegetések felsorolása alapján végzem [7]. Az elemzés rendszer szintű, ahol az esemény bekövetkezésének megelőzésére tett védelmi intézkedéseket, illetve a további elkerülés érdekében végrehajtható feladatokat foglalom össze.

Fizikai károk

A számítógépközpontot, a telefonközpontot, a gépteremet úgy kell kialakítani, hogy tűz-, baleset-, és munkavédelmi okokból nem lehet azzal közös elhelyezésben raktár, irodai munkahely, illetve ezekben a helyiségekben nem valósulhat meg készlet- és egyéb az informatikai működéshez szükséges papír alapú anyag tárolása. Kialakítása során figyelni kell, hogy felette, alatta, illetve mellette ne legyenek közművek, és a közművek ne veszélyeztessék semmilyen formában az ott működtetett végponti berendezéseket. A telepítés során ennek figyelembevétele megtörtént, azonban az épület adta lehetőségek a megfelelő elhelyezést nem tették lehetővé. A kialakított szerver központi fűtés mellett került elhelyezésre, mely kárt okozhat a rendszer működésében. [8]

Az informatikai berendezések használata során tönkremehetnek, ennek hatásai védelme érdekében redundanciával kerültek kialakításra, továbbá tartalék eszközök állnak rendelkezésre. A szoba zárt, tiszta, szennyeződés, por, rozsda nem éri, csak az engedélyezett személyek léphetnek be. Fagyás előfordulásának esélye szinte lehetetlen, de erre az esetre a klímaberendezéssel lehetőség van fűteni is.

Természeti esemény

Összességében elmondható, hogy Magyarországon a természeti események okozta károk nem relevánsak a géptermek tekintetében:

- szélsőséges éghajlati jelenségek,
- szeizmikus jelenség,
- vulkán kitörés,
- természeti csapás előfordulása nem jellemző.

Lehetséges fenyegetést jelent a villámcsapás, amely esetünkben már előfordult, az épület régi villámvédelemmel ellátott, ennek korszerűsítésére van szükség, mely a rendelkezésre álló anyagi fedezettől függ. Az épület elhelyezkedése, illetve a szerverterem kialakítása következményeként az árvíz nagyon alacsony kockázati tényezőt jelent.

Kulcsfontosságú szolgáltatás kiesése

A vízvezetékrendszer meghibásodása nem releváns kockázati tényező az informatikai rendszer működése szempontjából, hiszen annak kialakítása nem befolyásolja a rendszer működését. A terem rendelkezik megfelelő légkondicionáló berendezéssel, amely rendszeres karbantartás keretében ellenőrzött.

Az intézet régen épült, azonban az elektromos vezetékhálózata korszerűbb, hiszen a felújítások, javítások folyamatosak.

A szerverteremben az előírásoknak megfelelően telepítve van az EKOP projekt keretében beszerzett szünetmentes tápegység. Emellett az optikai végpontok és a telefonközpontban elhelyezett NTG berendezések mellé szintén szünetmentes tápegységek kerültek beszerzésre, az aktív hálózati eszközök folyamatos tápellátásának és feszültségproblémák okozta meghibásodások elleni biztosítására. Az intézet két aggregátorral rendelkezik, melyeknek indítása automatikus. A nagyobb teljesítményű aggregátor a teljes intézetet, a kisebb teljesítményű - a nagy meghibásodása esetén - a kulcsfontosságú eszközöket képes kiszolgálni. Így a rendszer rendelkezésre állása folyamatos, az áramkimaradás időtartamára a szolgáltatás biztosított.

A telekommunikációs berendezések meghibásodása a BVOP telefonközpontjának rendellenes működéséből következhetnek. A telefonközpont azonban redundáns. ami azt jelenti, hogy meghibásodás esetén egy másik intézetben elhelyezett ún. tartalékegység veszi át a vezérlést.

Információkompromittálódás

A bv. nem használ vezeték nélküli hálózatot, eszközöket. Az intézet területére történő belépésére csak fokozott ellenőrzés után van mód. Az egész bv. a kormányzati hálózat része, a távoli behatolás ellen több szintű logikai és fizikai védelemmel ellátott, ennek következtében a lehallgatás is sem releváns kockázati tényező.

Adatok, dokumentumok lopásának kockázatát elsősorban az informatikai rendszerbe belépő felhasználók jelentik. Ennek elkerülése érdekében a személyi állomány tájékoztatása, oktatása megtörtént. Az intézetbe belépés során az

adathordozók jelentéskötelesek. Az informatikai osztály által megvizsgált adathordozókat lehet csak az intézet területén használni, külön engedéllyel. Az eszközök, berendezések lopása nem releváns, hiszen az intézet elhagyása is ellenőrzés után lehetséges.

Minden használatból kivont adathordozón tárolt adat helyreállítását lehetetlenné teszi az informatikai osztály, visszaállítása nem megvalósítható.

A szervereken futó szoftverek logikailag és fizikailag is védettek. A szoftverekhez csak a kijelölt állomány férhet hozzá. A BVOP-n telepített központi rendszer megfelelő vírusvédelemmel rendelkezik, a vírusinformációs állomány frissítése rendszeres és automatikus. Minden szoftverelem csak előzetes tesztelés után kerül telepítésre.

A gépterem helye külső ember számára elérhetetlennek tűnik fizikailag, hiszen a szigorú ki-, beléptetés szabályozottsága ezt nem teszi lehetővé.

További intézkedések a számítógépterem védelmére

Az informatikai berendezések meghibásodása esetére szükséges van valamennyi rendszer esetében redundancia kialakítása. A terem elhelyezkedése nem a legmegfelelőbb. A víz okozta károk kiküszöbölése érdekében célszerű az egész központi egység áttelepítését elvégezni, egy közműmentes, fűtés nélküli helyiségben.

Villámcsapás okozta károk előfordulnak, az épület megfelelő műszaki színvonalon megoldott villámvédelmi rendszerének kialakításával azonban ez kiküszöbölhető.

A jelenlegi klímaberendezés meghibásodása esetén szükséges egy másik légkondicionáló kiépítése, a megfelelő hőmérséklet biztosítása céljából.

Célszerű központi szünetmentes tápegység beüzemelése az aggregátorok indítási idejének áthidalására, ezáltal a kisebb helyi UPS-ek kiválthatóak lennének, - nem lenne karbantartás, illetve akkumulátorcsere elmaradási probléma - és a teljes szükségáramforrásról működő infrastruktúra stabil energiaellátású lehetne ezáltal.

A telefonközpont teljes és alapos felülvizsgálata szükséges az üzemeltető által a hibás működés időtartamának csökkentése érdekében. A redundancia nem a legkorszerűbb megoldás, hiszen sok esetben a rendellenes működést követő helyreállítás manuális beavatkozást is igényel. Ennek megoldásához anyagi erőforrásra van szükség. [9]

Az adtok védelme érdekében a bv. szervezet személyi állományát - szakmai felkészültsége érdekében, - folyamatosan képezni kell. A jogszabályok, belső szabályozók rendszeresen változnak, bővülnek, újak kiadására kerül sor. Ezeket célszerű oktatás keretében évente legalább két alkalommal megismertetni, átismételni a kollégákkal. Az adatok védelmének fontosságát folyamatosan tudatosítani kell az adatokkal dolgozó munkatársakban.

Informatikai szakterületet érintő fenyegetettség

A bv. informatikai rendszerének védelme jelentős feladat a szakterület mindennapi életében. Elsődleges feladat, hogy a személyi állomány és a fogvatartotti állománnyal kapcsolatos adatokat illetéktelen hozzáférésektől megóvjuk.

A bv informatikai rendszerét elsősorban a személyektől kell védeni, akik lehetnek rendszert napi szinten használók, az állomány egy tagja, illetve külső – a bv-n kívüli ember. A belső személy bosszúállás céljából, szakképzetlenségéből, vagy a rendszer nem megfelelő szabályozottságából adódóan lehet fenyegető tényező. A munkatársak visszaélhetnek a mások jelszavának, ezáltal jogosultságuk megszerzésével. Bekövetkezésével adatmódosításokat végezhetnek, törölhetnek,

ellophatnak, amelyek következményeként a felhasználó büntetést kaphat. A megszerzett adatokkal visszaélhetnek pl.: fogvatartotti szabadulás dátumának módosítása esetén a fogvatartottat hamarabb szabadíthatják, vagy a bűnszervezetben elkövetett adatok kiszivárgása további bűnelkövetést eredményezhet.

Tudatosítani kell az informatikai biztonság fontosságát, a fenyegetések következményeit. Ennek érdekében ismertetni szükséges a szervezet szabályzatainak és intézkedéseinek betartását. Az informatikai eszközök megfelelő használatát meg kell tanítani a lehetséges biztonsági kockázatok minimalizálása érdekében. Ismertetni kell az állománnyal, hogy az adat a szervezet számára érték. Ami nekünk érték, az másnak is az lehet, így a bűnelkövetők számára célponttá válhat a szervezet informatikai rendszere.

A Büntető Törvénykönyvben foglaltak szerint, aki az információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

Aki az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy megváltoztat, töröl, vagy hozzáférhetetlenné tesz, az bűntett miatt három évig terjedő szabadságvesztéssel büntetendő. Egy évtől öt évig terjedő szabadságvesztés jár, ha a bűncselekmény jelentős számú információs rendszert érint. A büntetés két évtől nyolc évig terjedő szabadságvesztést von maga után, ha a bűncselekményt közérdekű üzem ellen követik el. [10]

A vírusfertőzés megelőzése érdekében vírusvédelmi rendszer kialakítása megtörtént, folyamatos frissítése megoldott. A bv.-ben rendszeresített programok listáján kívül más, illetéktelen program használatára, telepítésére nincs mód. A vírus fertőzés okozta adatveszteség esetén a bv. szervezet munkafolyamata ellehetetlenülne.

Az intézet területére adathordozó csak parancsnoki engedéllyel lehetséges. Célja, hogy ezen az úton semmilyen adat ne kerülhessen a bv.-be, illetve onnan ki. Az informatikai eszközökön az összes USB port letiltásra került. Ha valaki mégis egy ilyen csatlakozójú eszközt szeretne használni és engedéllyel is rendelkezik, akkor az informatikai szakterület az adott porthoz, adott eszközt hozzárendeli a használás idejére. Az adatok kikerülése a szervezeten kívül esetén magával vonja, hogy a személyes adatokkal visszaélhetnek, illetve a fogvatartottal kapcsolatos nem nyilvános adatok, nem megfelelő helyre kerüljenek. Zsarolás céljából is lophatnak adatot.

Az elektronikus, illetve a papír alapú dokumentumok bizalmasságának vagy hitelességének megsértése esetén folyamatos perek következhetnek, illetve pénzbüntetést róhatnak ki a szervezetre.

A bv. internetes oldalon nem megfelelő adatok közlése esetén a bv. könnyen a sajtónyilvánosság elé kerül, ami nem vet jó fényt a szervezetre. A tartalom illegális megváltoztatása hasonló következményekkel járna.

Összegezés

A bv.-nél az informatikai szakterületet érintő kockázati tényezők alapvetően két csoportba sorolhatók, vannak a központi, illetve az intézeti szinten előfordulók. Az informatikai rendszer homogén, egyenszilárd, nagyrészt központi biztosítású rendszerek hierarchikusan felépített rendszere, ennek következtében alapvetően itt nem intézet specifikus kockázati tényezők vannak, hanem olyanok, amelyek minden intézetet egyaránt érintenek.

Az informatikai biztonság megvalósítása szempontjából a személyi állomány folyamatos képzése elengedhetetlen, fel kell készíteni a szervezet alkalmazottait,

hogy feladatukat biztonságosan, a szabályokban rögzítetteknek megfelelően hajtsák végre.

Felhasznált irodalom

[1] KONDÁS K.: Informatikai korszakváltás egy büntetés végrehajtási intézetben, Hadmérnök 2017. 12. évf. 2. szám, ISSN 1788 – 1919, pp 272-279.

[2] 2012. évi C. törvény a Büntető Törvénykönyvről, III. Fejezet, A büntetőjogi felelősség

[3] Magyar Közlöny, 90. szám, 1236/2012. (VII. 12.) Korm. határozat Az Elektronikus Közigazgatás Operatív Program 2011–2013. évi akciótervének elfogadásáról, valamint kiemelt projektek nevesítéséről az Elektronikus Közigazgatás Operatív Program 2011– 2013.évi akciótervében és az Államreform Operatív Program 2011–2013.évi akciótervében

[4] MUHA L. – KRASZNAY Cs. Az elektronikus információs rendszerek biztonságáról vezetőknek, Nemzeti Közszolgálati Egyetem Vezető-és Továbbképzési Intézet, Budapest, 2014

[5] Tóth András: A hálózat nyújtotta képesség megvalósításának lehetőségei a Magyar Honvédség kommunikációs rendszerében, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, 2015, 240 p

[6] Dr. KERTI A. - SZENTE A.: Információbiztonsági szabványok, HÍRVILLÁM –SIGNAL BADGE 2013/1. szám, HU ISSN 2061-9499, pp. 80-94.

[7] 346/2010. (XII.28.) Kormányrendelet a kormányzati célú hálózatokról

[8] International Standard ISO/IEC 27005 Information technology – Security techniques – Information security risk management

[9] A büntetés-végrehajtás országos parancsnokának 9/2016. (II.16.) OP szakutasítása a büntetés-végrehajtási szervezet Informatikai Biztonsági Szabályzatáról

[10] PRISZNYÁK Sz.: A BVOP informatikai központjának kockázatelemzése, Hadmérnök 2014. 9. évf. 1. szám, ISSN 1788 – 1919, pp. 231-239.

[11] 2012. évi C. törvény a Büntető Törvénykönyvről, XLIII. Fejezet, Tiltott adatszerzés és az információs rendszer elleni bűncselekmények

[12] RAJNAI Z.: Információbiztonság tudatosság, A XXII. Fiatal Műszakiak Tudományos Ülésszak előadásai: Proceedings of the XXII-th International Scientific Conference of Young Engineers, Óbudai Egyetem, 2017. pp. 37-43., (Műszaki Tudományos Közlemények - Papers on Technical Science; 7.), ISBN:978-963-449-018-0

Oláh Dániel: Információbiztonsági irányítási rendszerek a köz- és magánszférában

Absztrakt

Az információbiztonsági irányítási rendszerek [1] megjelennek minden olyan szervezetnél, ahol érzékeny adatok kezelése történik. A rendszerek kialakítása és fenntartása során figyelembe kell venni bizonyos követelményeket, hogy az információk védelme megfelelő szinten legyen biztosítva. A követelményeknek való megfelelés megfelelő mérésekkel vizsgálható és tanúsítványokkal igazolható. A tanúsítványok megszerzése biztosítja a partnereket arról, hogy a szervezet megfelel a kívánalmaknak.

A köz- és magánszféra szervezetei eltérően működnek, így az információbiztonsági irányítási rendszerek tekintetében is számos különbség van. Eltérőek a követelmények, és eltérőek a vizsgáló és tanúsító szervezetek, azonban közös célként jelenik meg a követelményeknek megfelelő rendszerek kialakítása és fenntartása, ezáltal a megfelelő szintű biztonság elérése.

***Kulcsszavak**: információbiztonsági irányítási rendszer, audit, állami szféra, magánszféra*

Bevezetés

Napjainkban a mindennapi élet szerves részét képezik az infokommunikációs rendszerek, amelyek megtalálhatók az élet minden területén, így a közszférában és a magánszférában is. Míg a közszférában többek között a mindennapi életünket könnyítik meg az elektronikus ügyintézést lehetővé téve, vagy az államigazgatás

[1] Angolul: information security management system ISMS).

megfelelő működéséhez biztosítanak hátteret, addig a magánszféra résztvevői főként a piaci versenyben való előnyszerzés elősegítésére használják fel őket.

Az információs társadalom kialakulásával és a technológia fejlődésével párhuzamosan megnőtt a kezelni és tárolni kívánt adatok mennyisége az infokommunikációs rendszereken, valamint a fejlett hálózatoknak köszönhetően ezek a nagy mennyiségű adathalmazok egyre távolabbról és egyre gyorsabban érhetők el. A rendszerek és a társadalom fejlődésével együtt az információs fölény megszerzésének igénye is megerősödött, így a kockázatok fokozottan jelennek meg a kibertérben[2].

A köz- és magánszféra szervezeteinél egyaránt fontos a megfelelő biztonsági szint kialakítása és fenntartása, és ez által az információk bizalmasságának, sértetlenségének és rendelkezésre állásának[3] biztosítása. A különböző forrásokból érkező fenyegetések és a különböző típusú biztonsági események bekövetkezése mindkét szektor szervezeteire hatással vannak valamilyen módon, a károk a rövid idejű szolgáltatás-kimaradástól a nagy összegű anyagi kárig számos formában és mértékben realizálódhatnak.

A különböző szektorokra vonatkozó fenyegetések között nehéz éles határt húzni, de általánosságban elmondható, hogy az állami szektor a kiberterrorizmus fő célpontja, míg a civil szférára inkább az ipari kémkedés jellemző. Továbbá mindkettőben jelen vannak a személyes adatok, így azok védelmére kiemelt figyelmet kell fordítani minden területen.

Az információbiztonsági irányítási rendszerek kialakítása és fenntartása nagyban elősegíti a kívánt biztonsági szint elérését, tekintet nélkül arra, hogy azok önállóan vagy integrált rendszerként jelennek meg.

---

[2] Angolul: cyberspace.

[3] Angolul: confidentiality, integrity, availability. Gyakran találkozhatunk a „CIA triad” rövidítéssel is.

Az információbiztonsági irányítási rendszer

Fogalommagyarázat és alapelvek

Az *irányítási rendszer* magában foglalja mindazon eszközöket, erőforrásokat és folyamatokat, amely segítségével a rendszert működtető szervezet a célkitűzéseinek megfelelően, tervezetten, szabályozottan képes ellátni feladatát. Tartalmazza az alkalmazási területek, a folyamatok és azok felelőseinek meghatározását, és a folyamatos ellenőrzés és fejlesztés támogatásához minden folyamatot dokumentál. A rendszer – teljes életciklusában – alkalmazza a PDCA [4] elvet a minőség fenntartására és a dinamikusan változó körülményekhez való alkalmazkodásra. Röviden: „rendszer politika és célok megfogalmazásához, valamint a célok eléréséhez.”[1][2]

Az *információbiztonsági irányítási rendszer* kockázatkezelési eljárás alkalmazásával tartja fenn az információk bizalmasságát, sértetlenségét és rendelkezésre állását, valamint biztosítja az érdekelt feleket arról, hogy az azonosított kockázatok megfelelően vannak kezelve.[3] Az információbiztonsági irányítási rendszer lehet egy önálló rendszer, vagy az integrált irányítási rendszer egy része. Utóbbi esetben a rendszer működtetése és mérése a többi irányítási rendszerrel együtt történik.

A menedzsmentrendszerek ismétlődő életciklusa a tervezési folyamattal kezdődik, amelynek során a külső és belső elvárásokat egyaránt figyelembe kell venni. Külső elvárások lehetnek a vállalat vevőinek meghatározott igényei, de a

[4] Plan – Do – Check – Act cycle. Magyarul: Tervezés – Végrehajtás – Ellenőrzés – Reagálás ciklus. A tervezési fázisban a cél ismeretében a megfelelő folyamatok (és azok részletei) kerülnek meghatározásra. A végrehajtási fázisban a folyamatok részben vagy egészben realizálódnak. Az ellenőrzés során a végeredmény (vagy részeredmény) kerül a kitűzött céllal összehasonlításra. A reagálás a nemmegfelelőségek okainak meghatározása és azok kezelése.

jogszabályok által előírt követelmények is ide sorolhatók; a belső elvárások az adott szervezet politikájától és céljaitól függenek. Mindkét esetben pontosan meghatározott, dokumentált és mérhető elvárásokról beszélhetünk. A folyamat ezen szakaszában kell meghatározni, hogy mely információkat[5] milyen veszélyektől kell megvédeni[6], ezek a kockázatok mennyire súlyosak és gyakoriak[7], és hogy ezekből melyek a számunkra elfogadhatatlanok[8], és az elfogadhatatlan kockázatokra hogyan reagálunk[9]. Természetesen a kockázatmenedzsmentnek is ciklikus formában kell realizálódnia a megfelelő szintű biztonság fenntartása érdekében. A végrehajtási időszakban a tervezési folyamat során meghatározott folyamatok végrehajtása történik folyamatos dokumentáció mellett. Az ellenőrzés során a kitűzött cél és az elért eredmény kerül összehasonlításra, ahol a folyamatos dokumentáció segít megtalálni a nemmegfelelőségek okait, majd ezen okok elemzésével – a reagálási szakaszban – a korrekciós intézkedések meghatározása történik.

Az információbiztonsági irányítási rendszer – csakúgy, mint minden menedzsmentrendszer – akkor működhet megfelelően és lehet hatékony, ha a szervezet felső vezetésének szándékában áll a rendszert kialakítani, működtetni és folyamatosan fejleszteni. Emellett fontos a tudatossági szint emelése az egész szervezet tekintetében. Folyamatos képzéssel naprakészen kell tartani az érzékeny

[5] A vagyonleltár elkészítése során lista készül az összes védeni kívánt információról. A vagyonleltár az információk részletes vizsgálatát is tartalmazza, például kategóriába sorolja a vagyonelemeket azok érzékenysége szerint, adatgazdákat határoz meg, stb.

[6] Kockázatazonosítás: annak megállapítása, hogy az adott kockázatot mi okozza, és annak bekövetkezése milyen hatással van a vagyontárgyra.

[7] Kockázatelemzés: kockázatok összemérhetővé tétele.

[8] Kockázatértékelés: prioritások felállítása a kockázatok között.

[9] Kockázatkezelés: az elfogadhatatlan kockázatok csökkentésére tett intézkedések.

információk kezelésében érintett személyek tudását. Ennek célja elérni, hogy a szervezet egy egységként törekedjen az információbiztonsági szint fenntartására.

A fenti gondolatok ismeretében belátható, hogy az információbiztonsági irányítási rendszerek részben vagy egészben minden olyan szervezetnél megtalálhatók, ahol valamilyen információbiztonsági szabályzat[10] megfogalmazásra került. Ennek tükrében elmondható, hogy bár az egyes szervezetek céljai különböznek, a jogszabályoknak és szabványoknak való megfelelés — és ezen ténynek bizonyítása – valamilyen módon pozitív hatást gyakorol a szervezet működésére.

Ezek a pozitív hatások lehetnek többek között:

- a jogszabályok betartásával történő törvényes működés, és ezáltal a felelősségre vonás elkerülése;
- előnyszerzés a piaci versenyben a megbízhatóság tanúsításával a partnerek felé; és
- a szervezet folyamatainak optimalizálása, működési hatékonyságának növelése.

Szabványosítás

A megfelelőség és a megbízhatóság igazolásához mérni kell az irányítási rendszerek minőségét, azaz a folyamatokat és azok eredményeit az előre – külső vagy belső forrás által – meghatározott céllal össze kell hasonlítani. Ezen mérések segítenek fényt deríteni a nemmegfelelőségek okaira – ezzel elősegítve a folyamatok működésének optimalizálását. Azonban a különböző vállalatok és szervezetek eltérő jellegükből adódóan – és eltérő célok birtokában – eltérő folyamatokat alkalmaznak,

[10] Security Policy – Biztonsági Házirend mint biztonságot szabályozó előírás, szervezeti biztonságpolitika (EIBSZ, IBSZ).

amiket a valóságban nagyon nehéz összehasonlítani, így lehetetlen a megfelelőséget elősegítő szabályokat és módszereket általánosan alkalmazni. Ennek a problémának az áthidalására született meg a szabványosítás az információbiztonság területén is, ami az egységes működésre és általános szabályok betartására való törekvés. A szabványok alkalmazásának számos előnye van, például: segíti az együttműködést és hatékonyabb kommunikációt biztosít a szakterminológia meghatározásával, vagy a követelmények meghatározásával egy általánosan elfogadott minőségi szintet tart fenn.

„A szabvány elismert szervezet által alkotott vagy jóváhagyott, közmegegyezéssel elfogadott olyan műszaki (technikai) dokumentum, amely tevékenységre vagy azok eredményére vonatkozik, és olyan általános és ismételten alkalmazható szabályokat, útmutatókat vagy jellemzőket tartalmaz, amelyek alkalmazásával a rendező hatás az adott feltételek között a legkedvezőbb.” [4]

A szabványosításra való törekvés több szinten valósulhat meg. A legmagasabb szint a nemzetközi szabványosítás, amelyben a világ különböző országainak szabványosító szervezetei közösen végzik munkájukat. Ilyen szervezetek a Nemzetközi Szabványügyi Szervezet[11], a Nemzetközi Elektrotechnikai Bizottság[12] és a Nemzetközi Távközlési Egyesület [13]. A következő szint a regionális szabványosítás, amelyben egy földrajzi vagy érdekeltségi terület országai vesznek

[11] Angolul: International Organization for Standardization (ISO). A szabványok jelölése ISO jelzettel történik, amit a szabvány száma, majd kettőspont után a kiadás éve követ.

[12] Angolul: International Electrotechnical Commission (IEC). A szabványok jelölése IEC jelzettel történik, amit öt számjegy követ.

[13] Angolul: International Telecommunication Union (ITU). Az ITU az ENSZ infokommunikációra szakosodott része, melynek szabványosítási részlege az ITU-T. Az ITU-T által kiadott szabványok jelölése egy betűvel, ponttal, majd számmal történik.

részt. Ilyen szervezetek az Európai Szabványügyi Bizottság [14], Európai Elektrotechnikai Szabványügyi Bizottság[15] és az Európai Távközlési Szabványügyi Intézet[16]. A szabványosítás nemzeti szintjét hazánkban a Magyar Szabványügyi Testület[17] képviseli, létrehozásának célját a törvény így fogalmazza meg: „A nemzetközi és az európai szabványokat szabványként közzétenni Magyarországon csak nemzeti szabványként lehet.” [5] Az MSZT által kiadott szabványok nem minden esetben kerülnek lefordításra. A szabványosítás következő szintje a vállalati szabványosítás, amelyben az egyes vállalatok saját működésükre meghozott szabályrendszer alkalmazása történik. Ezen szabályok betartását a vállalatok sokszor a partnereiktől is elvárják. [6]

Megfelelőségi mérések, auditok

Egy rendszer megfelelőségének bizonyításához a folyamatok eredményét kell összevetni az eredetileg kitűzött céllal. Amennyiben a két állapot egyezik, úgy egy ideig nincs más teendő, mint folyamatosan felügyelni, naprakészen tartani a rendszert. Ha azonban a mérés folyamán különbözőségek kerülnek elő, akkor a folyamatokat vizsgálva és módosítva addig kell alakítani a rendszert, amíg meg nem felel a követelményeknek. A szabványkövető rendszerek mérése az audit.

[14] Angolul: European Committee for Standardization (CEN). A szabványok jelölése EN jelzettel történik, amit számok követnek.

[15] Angolul: European Committee for Electrotechnical Standardization (CENELEC). A szabványok jelölése EN IEC jelzettel történnek 2016 októberétől.

[16] Angolul: European Telecommunications Standards Institute (ETSI). A szabványok jelölése ETSI ES jelzettel történik, amit számok követnek.

[17] Rövidítve: MSZT. A szabványok hivatkozási száma az MSZ nemzeti kibocsátói jelből, az európai kibocsátói jelből, a nemzetközi kibocsátói jelből, az azonosítószámból és a közzététel évszámból képződik.

Az *audit* „módszeres, független és dokumentált folyamat auditbizonyíték megszerzésére és objektív értékelésére annak meghatározása céljából, hogy az auditkritériumok milyen mértékben teljesülnek.” [7] Ennek értelmében a hatósági vizsgálatok is auditnak tekinthetők, hiszen követelményként meghatározott jogszabályoknak való megfelelést vizsgál egy – a vállalattól – független szerv, és megfelelőség esetén tanúsítványt/engedélyt ad ki.

Rendszerauditról beszélünk, ha valamilyen irányítási rendszer megfelelőségét vizsgáljuk a vele szemben támasztott követelményeknek – például egy nemzetközi szabványnak. Az auditokat három fő csoportra oszthatjuk a végrehajtó szerint: első fél által végzett (belső) audit, második fél által végzett (vevői vagy beszállítói) audit és harmadik fél által végzett (tanúsító) audit. Az auditálás hazai szabványa az MSZ EN ISO 19011:2012, ami külső és belső auditokhoz egyaránt használható az irányítási rendszerek tekintetében; valamint az MSZ EN ISO/IEC 17021-1:2016 szabvány, ami az auditot és tanúsítást végző testületekre vonatkozó követelményeket taglalja. A tanúsítás során – a független, akkreditált tanúsító szervezet – az irányítási rendszer adott szabványnak való megfelelését vizsgálja. Ezen tanúsítványok meghatározott érvényességi idővel rendelkeznek. [8]

Hasonlóságok és különbségek a köz- és magánszférában az információbiztonság aspektusából

Az állami és önkormányzati szervezeteknél, valamint a versenyszféra vállalatainál egyaránt fontos az érzékeny információk biztonságának kialakítása és fenntartása, valamint ezen törekvések megkönnyítéséhez mérhető rendszerek létrehozása. Bár a különböző szektorok résztvevőire eltérő folyamatok jellemzők, mégis minden szegmens tekintetében egyértelműen meghatározható:

- az információbiztonság aspektusából kitűzött cél,

- a célhoz kapcsolódó követelményrendszer, valamint
- a követelményeknek való megfelelést vizsgáló szerv.

Információbiztonsági irányítási rendszer az állami és önkormányzati szervezeteknél

„A nemzet érdekében kiemelten fontos […] a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek […] biztonsága.
Társadalmi elvárás az […] adatok és információk […] védelmének biztosítása, ezáltal a kibertér védelme.” [9]

A törvény definiálja – többek között – a *globális kibertér*, a *kiberbiztonság* és a *kibervédelem* fogalmát. A törvény hatálya kiterjed – többek között – a központi államigazgatási szervekre, a fővárosi és megyei kormányhivatalokra, a helyi önkormányzatok képviselő-testületének hivatalaira, a Magyar Honvédségre, és minden olyan szervezetre, amely ezen szervek számára adatkezelést végez. A törvény értelmében az elektronikus információs rendszerek teljes életciklusában jelen kell lennie a CIA triádnak a rendszerben kezelt adatokat illetően; valamint zárt, teljes körű, folytonos és arányos védelmet kell kialakítani. Az elektronikus információs rendszereket a kockázatok alapján biztonsági osztályokba kell sorolni, amely besorolás tükrözi a kívánt védelmi szintet. A besorolást rögzíteni kell a biztonsági házirendben és legalább háromévenként meg kell ismételni.

A törvény hatálya alá tartozó rendszerek felügyeletét a *Nemzetbiztonsági Szakszolgálat* látja el mint *Nemzeti Elektronikus Információbiztonsági Hatóság*. A

honvédelmi szervek zárt célú elektronikus információs rendszereinek hatósági feladataiért a *Katonai Nemzetbiztonsági Szolgálat* főigazgatója felelős.[18][10]

Mivel az állam működése során keletkezett egyes adatok illetéktelenek által való megismerése sérti a közérdeket, ezért Magyarország érdekeinek védelme érdekében bizonyos nemzeti adatok megismerését korlátozni kell. Ez a törekvés a minősített adat védelméről szóló *2009. évi CLV. törvényként* realizálódott. A törvény definiálja – többek között – a *nemzeti minősített adat* fogalmát, meghatározza a minősítésre jogosultakat és a minősítési eljárás szabályait. A minősítési szintet az adatok sérülése esetén bekövetkező és a közérdeket érintő kármérték alapján kell megállapítani.

A minősített adat védelmének felügyeletével a törvény a *Nemzeti Biztonsági Felügyelet*et bízza meg. A hatóság működését, valamint a minősített adat kezelésének rendjét a *90/2010. (III. 26.) Korm. rendelet* részletezi. A Nemzeti Biztonsági Felügyelet a minősített adatot kezelő szerveket (és telephelyeket) auditálja, megfelelőség esetén hatósági engedélyt (és tanúsítványt) ad ki; a minősítők minősítési gyakorlatának ellenőrzésének eredményeként ajánlásokat bocsáthat ki.[11] A minősített adatok elektronikus biztonságával a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló *161/2010. (V. 6.) Korm. rendelet* foglalkozik.

Információbiztonsági irányítási rendszer a magánszférában

A magánszféra résztvevőinek alapvető célja a piaci versenyben való előnyszerzés. A vállaltok információs rendszereiben jelen vannak olyan érzékeny adatok, amelyek

[18] A 301/2013. (VII. 29.) Korm. rendeletet 2015. július 16-tól hatálytalanította a 187/2015. (VII. 13.) Korm. rendelet.

illetéktelenek által való megismerése, vagy elvesztése komoly anyagi károkat okozhatnak a szervezetnek. Az adatszivárgás kapcsán felmerülő anyagi kárt lehetetlen meghatározni, hiszen a vállalat hírnevének romlását, illetve a vállalat piaci és/vagy technológiai előnyének elvesztését nehéz számokban kifejezni. Az ilyen típusú biztonsági események bekövetkezése minden esetben visszaveti a vállalatot, így az üzleti titkok[19] megvédése célként jelenik meg az információbiztonsági irányítási rendszerek tekintetében.

Másik fontos motivációként jelenik meg a partnerek biztosítása – és ezzel bővebb piac kialakítása – arról, hogy a szervezet megfelel azoknak az elvárásoknak, amelyek az információbiztonság megfelelő szintjét hivatottak elérni. Ezek az elvárások szabványként realizálódnak, amelyek lehetnek nemzetközi, regionális, nemzeti vagy vállalati szabványok.

Az auditok három csoportját különböztetjük meg aszerint, hogy mi az audit célja. Itt a harmadik fél által végzett tanúsító auditokkal foglalkozunk, hiszen ennek eredménye a tanúsítási folyamat végén kiállított tanúsítvány, amely egy igazolás a követelményeknek való megfelelőségről. Ezeket a vizsgálatokat rendszeresen meg kell ismételni a tanúsítvány megújításához. Fontos szempont a megfelelő szabvány kiválasztása, hiszen egy elterjedt, általánosan és széles körűen használt szabvány több partner által elfogadott, mint kevésbé elterjed társaik – függetlenül azok minőségétől. Az információbiztonsági irányítási rendszerek alapvető szabványa az ISO/IEC 27000 jelzettel ellátott szabványcsalád, különösen az *ISO/IEC 27001:2013*, amelynek magyar megfelelője az *MSZ ISO/IEC 27001:2014*.

Tanúsító szervezetként számos vállalat megjelenik a piacon, így ebben a fejezetben nem lehet egyértelműen auditort meghatározni. Az auditorokra és tanúsítókra vonatkozó szabványok az *ISO/IEC 27006:2011* nemzetközi és az *MSZ*

[19] 2013. évi V. törvény (Ptk.) a személyiségi jogok között meghatározza a magántitokhoz és az üzleti titokhoz való jogot.

ISO/IEC 27006:2013 magyar szabvány. További fontos szempont a tanúsító kiválasztásánál annak figyelembevétele, hogy az általa kiadott tanúsítványnak mekkora értéke van az adott szektorban. [12]

A személyes adatok védelme

A köz- és magánszférában működő szervezetek elektronikus rendszereiben egyre nagyobb mennyiségű személyes adat található, amely adatok védelméhez való jog alkotmányi szinten biztosított: „Mindenkinek joga van személyes adatai védelméhez […]”[13], valamint a törvény egyértelműen kimondja, hogy a „személyiségi jogok sérelmét jelenti […] a magántitokhoz és a személyes adatok védelméhez való jog megsértése”.[14]

Ezekből a jogszabályokból kifolyólag jött létre *2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról* [20], amely a személyes adatok védelmének alapvető szabályait, valamint az azokat ellenőrző hatóságot határozza meg. A törvény definiálja – többek között – a személyes adat, a különleges adat és az adatkezelés fogalmát.

A törvény értelmében a *Nemzeti Adatvédelmi és Információszabadság Hatóság* a törvényben meghatározottak betartásának ellenőrzésére hivatott szerv, amely egy olyan független államigazgatási szerv, amely csak a törvénynek van alárendelve. [15] A Hatóság adatvédelmi vizsgálatokat folytat, így az információbiztonsági irányítási rendszerek aspektusából tekinthető külső, független auditornak; valamint általános jelleggel ajánlásokat bocsát ki, így járulva hozzá a szabványosításra való törekvéshez.

[20] Adatvédelmi törvény (Infotv.)

Összegzés

Minden információbiztonsági irányítási rendszert üzemeltető szervezetnél fontos a meghatározott követelményeknek való megfelelés, legyen szó akár a köz-, akár a magánszféráról. Bár az eltérő szektorokban tevékenykedő szervezetek céljai és a célok eléréséhez használt folyamatok eltérőek, mégis minden esetben egyértelműen meghatározhatók azok a követelmények, amelyeknek megfelelve – és erről tanúsítványt szerezve – a vizsgált fél megbizonyosodhat arról, hogy az általa kezelt érzékeny adatok biztonsága megfelelő szinten van biztosítva.

A követelmények számos formában realizálódhatnak. Míg a versenyszféra résztvevői a szabványoknak való megfelelésre törekednek leginkább, addig az állami és önkormányzati szervek információbiztonsági követelményeit legfőképp jogszabályok határozzák meg. A személyes adatok védelmét mindkét szektorban prioritásként kell kezelni. Mindenféle szabályozás (szabvány, ajánlás, törvény, rendelet) tekinthető auditkritériumnak.

A vizsgáló szerveket tekintve is találhatók különbségek a két területen. Míg a közérdeket szolgáló szervezeteknél jogszabály állapítja meg az ellenőrzést végző hatóságokat, addig a magánvállalatok szabadon választhatnak a tanúsítást végző szervek között. A megszerzett tanúsítványokat és engedélyeket rendszeresen felül kell vizsgálni, ezzel fenntartva az információbiztonságot.

Irodalomjegyzék

[1] MSZ EN ISO 9000:2005

[2] Horváth Zsolt László: Az információbiztonsági irányítási rendszer alapjai. Jegyzet.
Bp, 2016. p. 42-53.

[3] ISO/IEC 27001:2013(E) Information technology — Security techniques — Information security management systems — Requirements, p. v.

[4] 1995. évi XXVIII. törvény a nemzeti szabványosításról

[5] 1995. évi XXVIII. törvény a nemzeti szabványosításról, 5. § (2)

[6] Szádeczky Tamás: Információbiztonsági szabványok. Egyetemi jegyzet. Bp, 2014. p. 7-8.

[7] Horváth Zsolt László: Az információbiztonsági irányítási rendszer alapjai. Jegyzet. Bp, 2016. p. 77.

[8] Horváth Zsolt László: Információbiztonsági belső auditor. Jegyzet. Bp, 2016. pp. 6-8.

[9] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[10] 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról.

[11] 2009. évi CLV. törvény a minősített adat védelméről

[12] Tóth András: INFORMATION SECURITY FOR ELECTRIC CARS IN ACCORDANCE WITH NIST CRITICAL INFRASTRUCTURE CYBERSECURITY FRAMEWORK, HADMÉRNÖK XII. évf. 4. szám: pp. 195-206. (2017)

[13] Magyarország Alaptörvénye, VI. cikk (2)

[14] 2013. évi V. törvény a Polgári Törvénykönyvről, 2:43. §

[15] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, 38. §

Dr. Estók Sándor: A Hálózatok új tudománya reprezentatív iránya a Hálózatközpontú Rendszerlogisztika, Az új tudományos elvek behálózzák a társadalmi, szociális, gazdasági, kapcsolatokat

Absztrakt

A Hálózatközpontú rendszerlogisztika hálózatai különbözőek, nem központosítottak, központi csomóponttal nem rendelkeznek. Minden kapcsolat önmagától szerveződik, kiterjedésük grandiózus, de működésük látványos, szinte elképzelhetetlen. A hálók ismérve alapján hasonlítanak egymáshoz, viszont különféle rendszerekhez tartoznak. Ugyanakkor a Hálózatközpontú Rendszerlogisztika mögött bonyolult együttműködési háló húzódik meg. A hálózatok összetett rendszerre engednek következtetni, amelyek a felsoroltak alapján a komplexitás alapjait is magukban hordozzák. A csomópontok, kapcsolatok sokasága behálózzák a hálózatközpontú rendszerlogisztikát.

Kulcsszavak: *Rendszerlogisztika, globális háló, központi csomópont, komplexitás, komplex hálózatok*

A bizánci császár megalkotta a logisztikatudományt

VI. Leó császár (i.sz. 886 – 912) a Bizánci birodalom hatalomvédő erőinek megszervezését és alkalmazását tervezte az általa kidolgozott **Harcászat gyűjteménye** alapján. Ebben határozta meg a katonai alkalmazást, amelyet **harcászatra és hadászatra** osztott föl. Mindezeken túl **új hadtudományi fogalmat alkotott és ezt logisztikának nevezte és tudomány szintjére emelte.** Gondolkodása jóval megelőzte korát. Ő volt az első, aki a rend, szervezettség és a rendszer szintjén gondolkodott. elismerte fontosságát a logisztikának, más részről, elvárásait is megfogalmazta a gyakorlatban, amikor az élet a szükségét hozta az

alkalmazásban is megmérettetett. Kiemelkedően fontos szerepet töltött be a Bizánci Civilizáció katonai, védelmi és biztonsági feladatai végrehajtásában.

1100 évvel később Európában megtapasztaltuk, hogy a logisztikatudomány aranykorát éli a huszadik század utolsó évtizedében. Ekkor nevezik a történelemben **Logisztikatudománynak** az erősödő nagyreményű logisztikát. Újra erő feszül benne, a gazdaság, a társadalom és az Európai Unió lendítő erejévé vált. A 21. század egyik leghatékonyabb értékteremtő és szolgáltató erővé lett. Állandó változásban fejlődésben van. A tudásbázisa az informatikára, az infókommunikációra, a hálózatok fejlődésére, az új tudományok által feltárt eredményekre alapozott. Saját rendszerét alakította ki, megszervezte azokat és új virtuális, interaktív interdiszciplináris korszakot nyitott, ha szükséges akkor valós-virtuális vagy virtuális-valós, ha a fizikai térben levő logisztikai informatikai műveletek felgyorsításra van szükség akkor vertikálissá és virtuális valósággá formálható. Ezt a rendszert és a hálók kapcsolatait komplex, globális interdiszciplináris **Rendszerlogisztikaként** határoztam meg.

Barabási A László a Behálózva című könyvében azt vizsgálja hogyan kapcsolódik minden egymáshoz, és ez mit jelent a tudományban, és az üzleti mindennapi életben. Világunkban a meglevő hálózatok valódi természetének megértését keresi olyan kérdésekben, amelyek az emberiséget foglalkoztatja.

„A 21. század elejének talán legfontosabb tudományos felfedezése, annak megtalálása, hogy minden hálózat, rendszer azonos szervező elv alapján jön létre, és egyszerű, de hatékony szabályok révén működik (…), a vírusok leküzdése, gazdasági válságok kezelése, terrorizmus visszaszorítása, akár az emberi társadalom szociális gondjainak megoldása” Barabási Albert-László [1]

[1] Barabási Albert-László USA, Northeastern Egyetem; Komplex Hálózati Kutatóközpont vezetője, Egy új tudományterület a komplex hálózatok kutatásának területeit, főbb kérdéseit tárja elénk. Jelesül a **Hálózatok új tudománya,** hogyan kapcsolódik minden egymáshoz és ez mit jelent a tudományban, az üzleti és a mindennapi életben

Ebben a nagy rendszerben a hálózatok gazdaságában kutatom a logisztika 21. századi hálózatait és kapcsolatait. E rendszer napról napra változó, új hálózatok jönnek létre, mások átalakulnak, fúziós kapcsolatokat alkotnak, újakat építenek határon innen és túl egyaránt. Elmondható az is hogy az átszervezés szinte állandó folyamatként van jelen a gazdaságban. Valószínűsítem azt a jövő nem a versenyről szól majd, hanem az együttműködés plusz erőként lesz jelen a logisztikai terekben, amely értékteremtő erővé, erőtérré válhat.

A világomban a gazdaságot hatalmas logisztikai hálóként fogom fel, ami egy rendszer. Tudom azt, hogy az ezredforduló után eltelt közel két évtizedben a logisztika meghatározó ereje volt a gazdaságnak és az is marad. A logisztika globális része lesz a jövő gazdaságának és a társadalomnak., de nem választható el a szervezet műveleteitől, az időtől, tértől sem. Tudom minden logisztikai értékteremtés, szolgáltatás, megoldás, művelet gondosan felépített a vevő igényeinek megfelelően kell, hogy alakuljon.

Napjainkban már egyértelműen kimondható, a logisztikai hálózatok a legkisebbtől a globális hálózatokig néhány középpont tartja össze sok kapcsolattal.. A Hálózatközpontú rendszer egy bonyolult hálózat sok összetett hálózattal és rendszerrel.

A hálózatok új tudománya - napjaink hálózati kapcsolatai

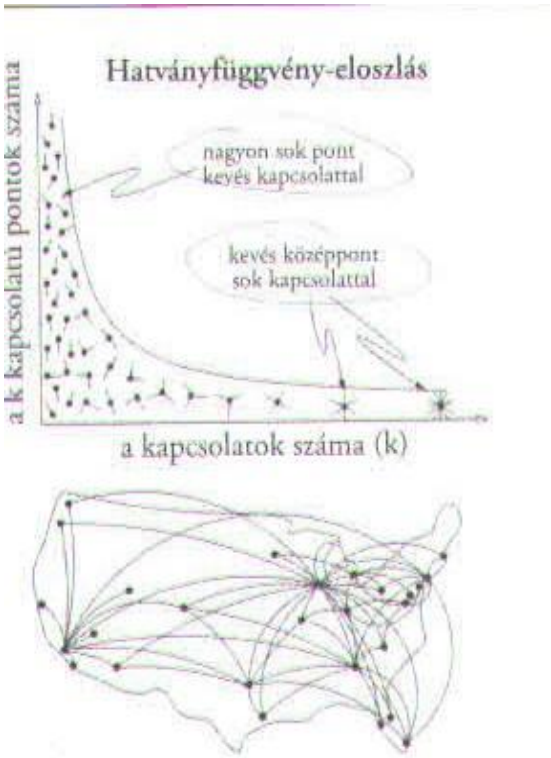
A 21. század elején az Internet hatékony eszköze az emberi kapcsolatok fenntartásának és újak létesítésének, de a mikroszkopikus univerzumtól a határtalan világokig minden elfér és képezhető a világhálón. A kutatók megtanulták feltérképezni és bemutatni a hálóhoz hasonló világunkat. Napjainkban felismertük semmi nem történik elszigetelten. A jelenségek egy univerzális kölcsönhatásban vannak egymással és mindennel össze vagyunk kapcsolva. A tudósok megtalálják,

felfedezik a szigorú szerkezetét a komplexitásnak. A gyorsan fejlődő hálózatok tudománya szédületes tempót kényszerít ránk. A jövő felgyorsul és a körülöttünk lévő világ megmutatja elővetíti új arcát. Ezzel jelezve fontosságát és meghatározó jelenlétét. Átalakítják szemléletünket, gondolkodásunkat, formálják nézeteinket és képzeletünket. A hozzánk kapcsolódó világ színesen sokféleképpen bemutatja a természetet, társadalmat, gazdasági és üzleti életet. Közelebb visz bennünket az új ismeretek megértéséhez és egy új jövőképet tár elénk és lehetővé teszi hálózatként szemlélni a minket körülvevő világot. [2]

A hálózatok mindenütt jelen vannak, szükséges megtanulni a társadalmat komplex ismeretségi hálózatként szemlélni és megismerni a kicsiny méretét annak a világnak, amelyben élünk. Az Internet létrejöttét teljesen az embereknek tulajdonítják. Az atomháború veszélye hozta létre a központi irányítású rendszerek helyett a decentralizált hálózati irányítást. Mindez meggyőzően mutatja az összes hálózatot szabályozó alaptörvények erejét. A különböző rendszerek közötti meglepő hasonlóságok, mint a gazdaság, a sejt, az internet, és felhasználja az egyiket a másik megértéséhez és a téma iránt érdeklődőket rábírja, hogy elhagyja az egyszerűsítés szemellenzőségét és láncszemről láncszemre haladva megismerje a következő tudományos forradalmat: **a hálózatok új tudományát.**

Egy skálafüggetlen hálózat hatványfüggvény szerinti fokszámelosztása azt jelzi előre, hogy a legtöbb pontnak csak kevés kapcsolata van, amelyet néhány, nagy összekötöttséggel rendelkező középpont tart össze. A hatványfüggvény megkülönböztető vonása az, hogy számos apró esemény együtt létezik néhány nagyon naggyal.

[2] Barabási Albert-László: Parafrázis a Behálózva című könyve, Bevezetés fejezetéből 7.o, Helikon Kiadó 2003, ISBN 978 963 227 2580.



1 ábra Skálafüggetlen hálózatok[3]

Vizuálisan ez nagyon hasonló a légiforgalmi rendszerhez, amelyben sok kicsi repülőteret néhány fő középponton át lehet összekötni. (alul levő ábra)

A hálózatok esetén a hatványfüggvény a csúcsok kapcsolatainak számát – csúcsok fokszámát – leíró elosztásra érvényes, a kitevőt gyakran fokszámkitevőnek nevezik.

A komplex hálózatok olyanok, amelyeket komplexitással foglalkozó kutatók képesek megérteni a rendről és a komplex hálózatok viselkedéséről szóló értelmezést.. A hálózatok komplex rendszerek átalános megértése ráirányított arra, hogy **sok más komplex rendszer mindegyike hatványfüggvényként viselkedik. A komplex hálózatok mögött valószínűleg léteznek törvények. A középpontok**

[3] Barabási A. László: Behálózva, Helikon Kiadó.2008.79. o

mögött egy igen precíz matematikai képlet, kifejezés, a hatványfüggvény jelenik meg.

A középpontok, hatványfüggvények **következményei az önszerveződés és a rend.** Így a hálózatok kiemelkednek a véletlen birodalmából. **A valódi hálózatok a rendezetlenből a rendezetté alakulás folytonos állapotában vannak.** A skálafüggetlen hálózatok elnevezés gyorsan elterjedt, olyan területen, ahol komplex hálózatok fordulnak elő,

A Hálózatközpontú rendszerlogisztika kialakulása az ezredforduló évtizedében

Magyarországon a logisztika a múlt század nyolcvanas évek közepén jelent meg. Ekkor alakult meg az Európai Logisztikai Szövetség, - 1984, Bern - és egy évvel később a Magyar Logisztikai Egyesület Budapesten. Ez volt a magyar logisztikai kezdet, amely nagy hatással volt a gazdaságra új dolgok iránt érdeklődő szereplőire, így rám is. 10 év kutatás után jutottam el a Hálózatközpontú Rendszerlogisztikához, amely saját kutatásom eredménye, ezt fejlesztem és írok a legújabb eredményeimről.

A hálózatközpontú rendszerlogisztika a legegyszerűbb logisztikai megoldásokból indult, ez volt a múlt század nyolcvanas évek közepén. Akkoriban sokan tették föl azt a kérdést **mi is az a logisztika**. A legtöbb esetben nem tudtak rá választ adni. Sok mindent értettek a logisztika alatt. Valójában a józan ész a vállalkozás fenntartása és a nyereség elérése motiválta a logisztikai tevékenységet. Az adott helyzetből és a rendezetlen lehetőségből mozdult el a rendezettség és a rendszer irányába, ahol már szervezetten és együttműködésben fejlődött a logisztikai és informatikai-információs rendszer az adott kor tudásbázisán és színvonalán. A fejlődést az hozta, amikor a gazdaság és a logisztika, valamint az informatika szereplői előtérbe helyezték a kommunikációt, a kooperációt és a koordinációt. Ennek következtében létrejöttek az értékláncok, ellátási láncok és a hálózatok. Ezek

a logisztikai formációk már rendezettek, szervezettek és a technikai fejlődésben is új eszközöket alkalmaztak. A rend volt a meghatározó, ez viszont csak átgondolt logisztikai műveletek által vált egyértelművé.

Az ellátási lánc/hálózat ebben az időben hatalmas fejlődésen ment keresztül. Erősítette az ellátási láncot a rendszeres átszervezés és szinte állandó folyamattá vált. A fejlődés minden területen az ellátási láncban uralkodó tendencia lett. Régiókon, határokon kontinensen átnyúló erőt képviseltek és meghatározó szerepük van a nemzeti és nemzetközi logisztikai környezetben is. Ez volt a XX. század vége, amikor Prof. Porter és Knoll, a logisztikát értékteremtő filozófiának nevezték. Ebben az évtizedben a logisztika minőséget váltott, a század végén Európa logisztika tudósai Logisztikatudományként fogalmazták meg.

A Hálózatközpontú Rendszerlogisztika felépítmény rendszere és jellegzetességei

A hálózatközpontú logisztika résztvevői és az infokommunikációs társadalom rendszerének képviselői a 21. század első évtizedeiben létrehozták a legmagasabb színtű szervezett együttműködést. Új logisztikai korszak kezdete nyílt meg új távlatokkal és lehetőségekkel. Ez a formáció teljesen átalakította a logisztika rendszereit, műveleteit, környezetét, üzleti, gazdasági és társadalmi, nemzetközi kapcsolatait. Alkalmazása és közös tevékenységük minden környezetben jelentős változásokat generált. A már meglevő horizontális logisztikai ipart és a kereskedelmet felgyorsította. A versenyt és az együttműködést átformálta, a kapcsolatok a fizikai és a virtuális térben lett meghatározó ebben a nagy globális rendszerben.

A logisztika különféle formákban minden értékteremtő és más jellegű szerveződésekben jelen van és nem lehet felülmúlni időben térben, gyorsaságban és

nem utolsó sorban eredményességben sem. Mindig konkrét feladatra szerveződik, időben térben determinált, vezetett, de ugyanakkor a műveleti szabadság jelen van a logisztikában.

Működési rendszerét a logisztikatudomány bázisán működő logisztikai rendszerek és felépítmények képezik. A két nagy rendszerelem között infokommunikációs együttműködés van, ahol az információ kulcstényező, új értékteremtő filozófiát alkot, keretet az információáramlás és az **Információ Just in Time** adja szervezett rendszerben. Felgyorsítja minden hálózat működését, reagálóképességét. Növeli hatékonyságát, átláthatóságát, a hatásfokát. A kis vállalkozástól a globális logisztikáig, ellátási láncig/hálózatig tud partnerként együttműködni. A civil, nonprofit, üzleti, gazdasági környezetben üzleti alapon szerveződik, képes együttműködni és közreműködni különféle logisztikai és interdiszciplináris rendszerekkel. Az előzőkre figyelemmel az információ Just in Time megszervezett mozgása konkrét értékteremtő és együttműködő forrássá vált. Egyre nagyobb hálóformáció kialakítására képes, elérhetővé vált az elérhetetlennek hitt távoli földrész, vagy üzleti kapcsolat, amely az infokommunikációs hálózatnak köszönhetően a láthatatlan virtuális információs térből indul el a folyamatok felgyorsítása. Ez változtatta meg a hálózatok működésének rendszerét. Ez az újfajta probléma felvetés és megoldás értelmezésem alapján az Információ JIT a vezérlő képességét teszi nyilvánvalóvá. Így minden hálózat együttműködő hálózata az információra koncentrál, amely a logisztikai és más döntésekhez szükséges megbízható hiteles forrás. Az együttműködő partnerek részére bárhol a műveleti környezetben elérhető, amikor arra szüksége van. Jelentése egyértelmű, az információ hozzáférhetősége, megbízhatósága, átláthatósága biztosítja a teljes körű működéshez az alapfeltételeket a döntések meghozatalához, a hálózatok minden szintjén és minden elemében. Az Információ JIT rendszer gondoskodik erről, napjainkban már szervezett megjelenésében egyre több formában lehet hasznosítani

az info- kommunikációt egyszerre mindenki igényeinek megfelelően valós egyidejű értelmezésben képes áramlani. Ennek érdekében szükséges a logisztikai szervezetek, cégek, háló tevékenységét és információit összehangolni, megszervezni.

Megállapításom az, hogy a logisztika és az infokommunikáció együttműködésében akkor születnek nagy dolgok, amikor az információ mozgása szabad, nem korlátozott, de szervezett. Napjainkban az információ mozgása az általam fentiekben kifejtett rendszerbben önálló, szabad, szervezett, állandó és folyamatosan mozgásban van, mindenkihez eljut a JIT rendszerben.

A logisztikai műveletek működését az infokommunikációs hálózatok, rendszerek, infrastruktúrák biztosítják. A felsoroltak teljesítményének le kell fedni azt a teret, ahol a logisztika hálózatai, hálózatközpontú rendszerben működnek.

Viszont a katonai logisztikai támogatásban, alkalmazásban, nemzeti, regionális, nemzetközi és integrációs logisztikai műveletekben is képes részt venni.

Az Információs társadalom, információ és a hálózatközpontú logisztika

Az információs társadalom [4] jelen időszakban átmeneti szakaszának utolsó negyedében van, annak is a végéhez közelít. A társadalom szerkezeti rendszere, globális piac alapú, demokráciára épülő, ultrafejlett kapitalizmus. Ebben a formában a tudomány intenzív alkalmazására alapozott, információ technikán alapuló számítógép hálózatig integrált társadalom. A köz- és magánügyek távolból történő intézésének társadalma. Magasabb technikai és tudásszínvonalú társadalmi életmód, életforma. Az információs társadalom digitálisan, informatízáltan működik.

Az információ és az infokommunikáció vezérli a hálózatközpontú rendszerlogisztikát. Tudásalapon szervezett több tudományág közös tevékenysége

[4] Dr. Estók Sándor(2015):Előadás: XXI. század kihívása a Hálózatközpontú Rendszerlogisztika, Óbudai Egyetem Biztonságtudományi Doktori Iskola 2017. nov.(felett tárgy,)

révén éveken keresztül formálódott, úgy a logisztikai rendszerek vonatkozásában, mint az infokommunikáció kapcsolat rendszerével együtt. A kialakított nagy intenzitású szervezett hálózatok tovább fejlesztik működőképességüket. Az új alkalmazás erősítette a rendszerlogisztikai verseny, profit növelését. Ez az együttműködés logisztikára hangolt, a klasszikus értékteremtés elméletét és gyakorlatát erősíti a modern innováció rendszerbe építésével.

Nem hagyható figyelmen kívül az a tény, hogy a legmeghatározóbb a megszervezett információ, de ezzel együtt több információ áramlás is jelen van és eddig még nem ismert, amely hatalmas jelentőséggel bír.

Ezek következőképp valósultak meg és került rendszerszinten nyugvópontra.

- A hálózatok szervezett rendszerré alakítása azonnali megoldást igényelt,
- Az információ minden szinten és szervezetben középpontba került,
- A menedzsmentek, az információ központba kerültek több új feladattal – amely az egész rendszert érinti,
- Az információ áramlás rendszerének védetté tétele, valós, egyidejű, kép, hang, adat, digitális jel áramoltatása, kialakítása kulcsfeladat,
- Valós idejű egyfajta információ áramoltatás minden rendszerben.
- Az anyagáramlást a fizikai és virtuális térben egyaránt működőképessé tenni,
- A hálózatok menedzsmentjeinek az adatok hálózatba felvitele, és onnan letöltése, belépése csak személy szerinti jogosultság alapján történhet meg.
- A szinergia menedzsment működése minden rendszerben követelmény és tervezetten szükséges a jelenléte minden logisztikai szintnek megfelelően.
- Az infokommunikáció hálózataiban minden szinten új elemekkel erősítsék meg az informatikai infrastruktúrájukat, digitális képességeiket helyezzék előtérbe és alkalmazásukat tegyék valóssá.
- Minden szinten előtérbe szükséges helyezni az interaktív és okos infokommunikációs megoldásokat,

- Az új korszak adta minden kihívásra reagálni szükséges és a lehető legrövidebb idő alatt alkalmazni az új lehetőséget a rendszerbe helyező cégnél a tesztelt jó eredmények alapján, majd kiterjesztése annak más rendszerekre is.

Új szemlélet, gondolkodás, világlátás és észjárás vette kezdetét logisztikai környezetben, előtérbe került a rendszerszemlélet, a rendszerben való gondolkodás. Kiemelkedő szerepet kap a logisztikai szervezet mikro, makro szinten egyaránt, de a horizontális logisztikai hálózatok vertikálissá tétele is előtérbe kerül. Fontos a hálózatközpontú rendszer eredményeit illetően a globális együttműködés és verseny mellett a profitnövelés, az integrált interdiszciplináris interaktív ellátási láncok, hálók, cégek a külső kapcsolatok. A termelő, ellátó, szolgáltató rendszerek megbízható partneri kapcsolatok is. Cél mindenképpen az hogy a felsorolt kapcsolatokat alkalmassá tenni a hálózatközpontú rendszer tagjává tudjon válni. Ezen kívül fontos a célokhoz, üzleti érdekekhez, a partnerek képességeihez, és vevői igényekhez igazított stratégiát hozzárendelni.

Az infokommunikációs tudás, technológia, a technika fejlettsége a modern 21. század szintjén van, amellyel együtt a hálózatközpontú rendszerlogisztika működni képes. Kialakult az infokommunikációs Just in Time **dinamikus eleme** és mozgató rugója a **Rendszerlogisztikának.** Az információ önálló és szervezett időben és térben, valamint mozgásban a virtuális, valós és fizikai környezetben. Mindezeken túl a rendszerlogisztika minden jogosult részes tagja szervezi, alakítja, használja a nap 24 órájában igény szerint bármelyik hálózati elemet. A virtuális interaktív tér kialakítása az infokommunikációs rendszer, az információ Just in Time, az információ áramoltatás révén érhető el.

Változás a Hálózatközpontú rendszeren belüli és a külső kapcsolatokban.

Az utóbbi néhány évben a hálózatközpontú rendszer is jelentős változáson ment keresztül. Első változatként **a Hálózatközpontú logisztika kialakítását végeztem el**, majd **a logisztikai együttműködést az Infokommunikációs rendszerekkel** ezt követően **az interdiszciplináris biztonságtechnikai együttműködés volt meghatározó.** Itt a fejlesztés nem áll meg és következett **a Hálózatközpontú Infokommunikációs és Interdiszciplináris interaktív, virtuális-valós hálózati Rendszerlogisztika.** Több tudományterület rendszerei tud egymáshoz illeszkedni. Közösen nagy eredményekre képesek. A tudomány bázisán és kapcsolataival kifejleszthető olyan vállalat, vállalkozás, ahol a logisztikai rendszerek szolgálják az adott interdiszciplináris kapcsolatot. Egyértelművé vált az a tény, hogy napjainkra kevés olyan szervezet, ellátási lánc, hálózat van, ahol a logisztika bármilyen szinten kikerülhető lenne. A leírtak alapján egyetértek Barabási A. L. abban,

„A valóságban a piac nem más, mint egy irányított hálózat, vállalatok, vállalatcsoportok, pénzügyi intézmények, a gazdaság minden lehetséges szereplője ennek a hálózatnak egy – egy pontja. A kapcsolatok ezen intézmények egymás közötti kapcsolatait mutatják ebbe beleértendők a beszerzések, eladások, közös kutatási és piacszerzési programok és minden más is.” [5]

A hálózatok hosszútávra szóló kapcsolatot, elkötelezettséget és bizalmat építenek fel, ez a kapcsolat partneri, hosszú időre szól és a cégek a stabilitás miatt a fő tevékenységükre koncentrálnak. Napjainkban olyan gazdaság kialakulásának vagyunk szemtanúi, ahol a stratégiai szövetségek és kapcsolatok hosszú távra szerveződnek és biztonságot adnak a túlélésnek. A linkek és a kapcsolatok egyre

[5] Barabási Albert-László:(2008 Behálózva, A Hálózatok új tudománya, Helikon Kiadó, 2008, 225-256 o.

nagyobb szerepet kapnak, kialakul az újszerű gazdaság, úgy kicsiben, mint nagyban és érinti a társadalom és a gazdaság teljes vertikumát.

A **Hálózatközpontú Hálózati- Rendszerlogisztika** annak ellenére, hogy hatalmas rendszer, tud rugalmas és alkalmazkodó lenni, nem elsősorban a piachoz, mivel az is egy rendszerelem a kapcsolatokban, elsősorban a vevői igényekre és a biztonságra alapozott. Valamint az együttműködésre azokkal, akik a logisztikát és a biztonságot akarják. Természetesen az egész rendszer az igényekhez igazodó és részükre **„testre szabott**" Így tagjai lehetnek a **Hálózatközpontú Rendszerlogisztikának**. (HKR)

A rendszerben a logisztikával együttesen az információnak és az infó kommunikációnak is jelentős szerepe van. A rendszerek és az információ titkosított, virtuális, valós és interaktív. Ha szükséges az egész tér is virtuális és valós, valamint a fizikai tér is egyszerre képes jelen lenni a rendszer minden elemében. A hálózatközpontú rendszer intelligens, rugalmas, dinamikus, innovatív az Információ Just in Time közreműködésével.

A vállalkozások, vállalatok a HKR rendszerben nem csak gazdasági, logisztikai kapcsolatban vannak egymással, többféle kapcsolat van közöttük, mint partneri, stratégiai együttműködési, de kialakulhat akár baráti kapcsolat is. A hálózati kapcsolatok a HKR minden rendszere, valós információt kap, több információ csatornán keresztül. Az együttműködő partnerek önállóan vállalattal vagy több vállalattal lehet egyszerre kapcsolatban. Személyre szóló információt is kaphat bármelyik hálózatból. Egy - egy hálózatnak akár tíz menedzsmentje is lehet bent az információ központban.

A Hálózati rendszerlogisztika hálózatai különbözőek, nem központosítottak, viszont kulcsszerepük megnövekedett, központi csomóponttal nem rendelkeznek. Minden kapcsolat így a hálózat is önmagától szerveződik, kiterjedésük grandiózus, de működésük látványos, szinte elképzelhetetlen. A hálók ismérve hasonlítanak

egymáshoz, viszont különféle rendszerekhez tartoznak. Ugyanakkor a HKR mögött bonyolult együttműködési háló húzódik meg. A hálózatok összetett rendszerre engednek következtetni, amelyek a felsoroltak alapján a komplexitás alapjait is magukban hordozzák. A csomópontok, kapcsolatok sokasága behálózzák a hálózatközpontú rendszerlogisztikát.

Napjainkban már egyértelműen kimondható, hogy a logisztikai hálózatok a legkisebbtől a globális hálózatokig néhány középpont tartja össze sok kapcsolattal, számos önálló funkcionális modul csomóponttal összeköttetésben. A modulok nem elszigeteltek de nevezhető skálafüggetlennek. A Hálózatközpontú rendszer bonyolult, sok összetett hálózattal. Ebben **a rendszerlogisztikában is a komplexitás ott kezdődik, ahol a hálózat bonyolulttá válik. A gazdasági, logisztikai folyamatok megjósolhatatlansága, a kiszámíthatatlan piac mögötti ismeretlen kapcsolati hálóban gyökerezik**. **Így a hálózatok nélkülözhetetlen előfeltétele bármilyen komplex rendszer leírásának. „A komplexitás elmélet elkerülhetetlenül a hálózatelmélet vállán kell hogy nyugodjék." (Barabási A. László)**

A Hálózatközpontú Infókommunikáció vezérlésű Rendszerlogisztika négy tudományterület szerves részét képezi. Így megnevezhető **a logisztikatudomány**, az **Információs társadalom** több **Interdiszciplináris tudomány területét érintő tudományok** főleg azok, **akik a rendszerlogisztika szolgáltatását partnerként** igénybe veszik.

Összegzés

Az új tudományos hálózatok olyan felfedezéssel gazdagították századunk társadalmi gazdasági környezetét, kapcsolatait, úgy a világhálón mint az üzleti életben jelen levő sikereinkben és eredményeinkben. Napjaink egyértelműen sok kapcsolattal,

számos önálló hálózatok rendszereit tartják összeköttetésben modulokkal, csomópontokon, és más hálózati rendszereken keresztül. A hálózatok mindenütt jelen vannak, átszőve világunk civilizációi, regionális és globális tereit. Ezt a formációt már komplex, heroikus hálózatként lehet értelmezni, természetesen ennek megfelelően csak így lehet megérteni.

A tudásbázisa az informatikára, az infókommunikációra, a hálózatok fejlődésére, az új tudományok által feltárt eredményekre alapozott. Saját rendszerét alakította ki, megszervezte azokat és új virtuális, interaktív interdiszciplináris korszakot nyitott, ha szükséges akkor valós-virtuális, vagy virtuális-valós, ha a fizikai térben levő logisztikai informatikai műveletek felgyorsításra van szükség, akkor vertikálissá és virtuális valósággá formálható,

A hálózatok matematikai hatványfüggvények által meghatározottak, valamint az önszerveződés a rendezetlenből a rendezetté, renddé alakítás, ez a formálás folytatódik az egyszerűbb logisztikai megoldástól a bonyolult hálózatokig. Mindezek a logisztikatudomány tudásbázisán és a hálózatok új tudománya által feltárt eredmények alapján valósul meg.

Irodalom jegyzék

1. Barabási Albert-László:(2008 Behálózva, A Hálózatok új tudománya, Helikon Kiadó, 2008,
2. Barabási Albert-László: 2008 Behálózva, Helikon Kiadó
3. Estók Sándor:((2015) XXI. század logisztikai kihívásai, trendjei és lehetőségei LOGISZTIKA TRENDEK ÉS LEGJOBB GYAKORLATOK 1(1) pp.35-38
4. Estók Sándor: (2009) Hálózatközpontú integrált interdiszciplináris logisztika BOLYAI SZEMLE XVIII (3) pp.23-33 (2009)
5. Barabási Albert-László:(2010) Villanások a jövő kiszámítható

Darázs Tamás: Hálózati eszközök sérülékenysége

Absztrakt

Az internet napjainkban végtelen számú lehetőséget szolgáltat számunkra, ehhez azonban, egyéni felhasználóként szükséges felcsatlakoznunk a hálózatok hálózatára. Ez a csatlakozás különböző hálózati eszközöket igényel, melyek rendszerét megfelelően kell kiépítenünk és megvédenünk. Ugyanis az esetleges illetéktelen személyek számos privát információt szerezhetnek meg, ha a hálózatunkat és a benne foglalt hálózati eszközeinket nem tesszük védetté és biztonságossá. Ezen cikk bemutat néhány alapvető támadási formát és az ezek elleni védekezés lehetőségeit.

Kulcsszavak *hálózat, hálózati eszközök, védettség, támadás, biztonság*

Bevezetés

„Az információ hatalom”. Az ember történelmében és jelenében az információ mindig meghatározó volt. Az ősember is a létfontosságú információ birtokában kezelte a körülötte lévő történéseket. Információ birtoklásával ejtette el zsákmányát, szerzett vizet, gyújtott tüzet. Az idő múltával az információnak napról napra jelentősebb szerepe lett. Bonaparte Napóleon idézete is az, hogy „a háború kilencven százalékban információ”. Valószínűleg ez a kijelentés napjainkban még inkább helyénvaló. Minden a hiteles és a számunkra hasznos információ birtoklásáról szól. Ebbe beleérthetjük a háborús körülmények információit vagy az üzleti versenyben lévő információbirtoklást vagy csak szimplán a mindennapi élet megkönnyítéséhez szükséges tudás, azaz információ megszerzését is. Az informatika és még inkább az internet megjelenésével az adatok áramlása, mozgása, cseréje rohamos mértékben felgyorsult és ennek megfelelően birtoklása is még fontosabbá vált. Az ember saját életének megkönnyítése, az információhoz való

gyorsabb hozzáférés érdekében alkotta meg azokat a rendszereket, amelyeknek a valós idejű információ csere nagy távolságok leküzdésénél sem okoz problémát. Gondolhatunk itt a postagalamboktól kezdve a rádiókon, telefonokon keresztül egészen az internet megjelenéséig. Ahhoz, hogy az interneten keresztül keressünk és elérjünk adatokat, információkat szükség van egy úgynevezett hálózat kiépítéséhez, amihez elengedhetetlen a hálózatot felépítő és működtető eszközök és rendszerek összessége. Ebből a napjaink felhasználója csak annyit tapasztal, hogy van Wifi jel, amire rácsatlakozik és képes elérni adatait az Interneten keresztül. Természetesen a hálózat kiépítéséhez szükség van végberendezésekre (számítógép, laptop, táblagép, mobiltelefon); közvetítő hálózati eszközökre (kapcsolók, vezeték nélküli hozzáférési pontok, forgalomirányítók, tűzfalak); és hálózati átviteli közegre (fémvezetékek, optikai kábelek, vezeték nélküli átviteli közeg).

A hálózati eszközök biztonságától általánosan

A hálózatot fenyegető veszélyek

„A biztonság egy objektum állandóan fennálló, komplex védelme. Ez az objektum lehet egy személy, egy épület, vagy például egy számítógépes rendszer.”[1] Amint már említettem az információ hatalom. Természetesen ezt a hatalmat megszerezhetjük törvényes úton és törvénytelen eszközökkel egyaránt. A vezeték nélküli vagy vezetékes hálózatok mindennapi életünk szerves részei. A különféle szervezetek, mind a közszférában mind pedig az üzleti versenyszférában és természetesen a magánszemélyek is függenek a számítógépektől és a hálózatoktól. A hálózatok megtámadása komoly anyagi és információs károkat okozhat mind a szervezeteknek, mind a magánszemélyeknek. Az illetéktelen személyek a szoftver sebezhető pontjain keresztül, a hardverek elleni támadással vagy egy felhasználó

nevének és jelszavának ellopásával szerezhetnek hozzáférést a hálózathoz. Hardver elleni támadás lehet például az is, hogy az illetéktelenek hozzáférnek a számítógépeink vagy telefonjaink web kameráihoz, úgynevezett „webcam hack-el”. [2] Ezeket az illetéktelen személyeket, akik a fent említett módszerekkel próbálnak meg hozzáférni a hálózathoz és valamilyen módon olyan tevékenységet folytatnak, melyek kárt okozhatnak, általában hackereknek nevezzük.

A hacker hozzáférése a hálózathoz az alábbi fenyegetéseket jelentheti:

- Információlopás
- Azonosító lopás
- Adatvesztés és manipuláció
- Szolgáltatás megszakítása

Fizikai biztonság

Egy hálózat, hálózati eszközök vagy számítógép sebezhetőségét vizsgálva általában a szoftveres gyengeségeken alapuló támadásokra gondolunk. Hajlamosak vagyunk megfeledkezni az eszközök fizikai biztonságáról, pedig ez is legalább ugyanannyira fontos, mint a szoftveres sebezhetőségek. Egy esetleges hacker megakadályozhatja a hálózati erőforrások használatát, ha azokat fizikailag képes veszélyeztetni.

A fizikai fenyegetések az alábbiak lehetnek:

- Hardverfenyegetések: kapcsolók, forgalomirányítók, szerverek, munkaállomások, kábelezés fizikai megrongálása
- Környezeti hatások: szélsőséges hőmérséklet, szélsőséges páratartalom
- Elektromos veszélyek: áramszünet, zaj, feszültségesés
- Karbantartási veszélyek: hibás kábelezés, elektrosztatikus feltöltődés, kritikus alkatrészek hiánya

Hálózatbiztonsági tényezők

Sebezhetőség: A gyengeség fokmérője, mely minden hálózati eszközben eredendően benne van.
Fenyegetés: Azok az illetéktelen személyek, akik érdekeltek és kellőképpen képzettek is a biztonsági rések kihasználására.
Támadás: Azok a fenyegetések, amelyek különféle segédeszközök és programok formájában alkalmasak a hálózat és a hálózati eszközök megtámadására.
A három elsődleges sebezhetőségi pont a technológiai, konfiguráció és a biztonsági házirend.

Hálózati támadások típusai

Vírusok, trójai lovak, férgek

Azok a számítógépes programok, amelyek adatvesztést vagy sérülést képesek okozni a hálózatban, a rosszindulatú kód támadások csoportjába tartoznak. Ezek lehetnek vírusok, trójai lovak vagy pedig férgek.

A vírus egy olyan rosszindulatú szoftver, amely más programokba beágyazódva nemkívánatos hatást okoz egy munkaállomáson. Például a vírus egy program formájában beágyazódhat a Windows rendszerek elsődleges parancsértelmezőjébe és ott letörölhet vagy megfertőzhet fájlokat, adatokat.

A trójai ló annyiban különbözik a vírustól, hogy az alkalmazás teljesen másnak tetteti magát, mint ami valójában. Ez például lehet egy játék. Miközben a felhasználó játszik a trójai ló elküldi a saját másolatát a játékossal összeköttetésben lévő összes felhasználó számára, ezt megcsinálja ezen felhasználók összeköttetésében lévő felhasználókkal is és a folyamat így megy tovább.

A férgek önálló programok, amelyek megtámadják a rendszert és megpróbálják kihasználni annak a sebezhető pontjait. A féreg abban különbözik a vírustól, hogy a vírus továbbterjedéséhez emberi közreműködés kell a féreg pedig önálló.

2. ábra [3]

Felderítéses támadások

Egy esetleges külső támadó internetes eszközöket használva, különböző segédprogramok segítségével meg tudja állapítani egy adott szervezet IP-címtartományát. Ezután a támadónak már csak ki kell választani az aktív állomásokat, amit a tartomány publikus IP címeinek a megpingelésével tud elérni. Ezt meg tudja csinálni egy ping pásztázó segédprogrammal, ami szisztematikusan végigpingeli az összes címet egy hálózaton vagy tartományon belül.

Hozzáférési támadások

A támadó személy célja, hogy számára titkos adatokhoz jusson hozzá jogosulatlanul. A hozzáférési támadások a hitelesítési, FTP és web szolgáltatások ismert sebezhetőségi pontjait használják ki a bejelentkezési adatok és bizalmas információk

megszerzéséhez. A hozzáférési támadásokat négy csoportba sorolhatjuk. A jelszó elleni támadások; megismételt bejelentkezési próbálkozások; ismétléses támadások; és a nyers erő támadások.

DoS támadások

A DoS rövidítés a Denial of Service-re utal, ami a szolgáltatás megtagadását jelenti. Ez talán a legismertebb és a legnehezebben kiküszöbölhető támadási forma, azonban végrehajtása nagyon csekély erőfeszítésbe kerül. „A NATO 2007 óta kiemelten kezeli a kibervédelem és kiberhadviselés kérdéskörét. Számos adat van a 2007-ben Észtország ellen indított kiberműveletekről, amikor meghatározó jelentőségű szolgáltatásmegtagadást kiváltó támadássorozat történt.” [4] Sokféle DoS-támadás létezik, de a végeredménye mindegyiknek ugyanaz, mégpedig az, hogy a jogosult felhasználókat megakadályozzuk a szolgáltatás használatában a rendszer erőforrásainak felemésztésével. [5]

Hálózati támadások elhárítása

Hálózati eszközök biztonságossá tétele

Napjainkban egyre nagyobb mértékben terjednek el az úgynevezett IoT (Internet of Things) eszközök, melyek védelme az illetéktelen behatolások ellen még gyerekcipőben jár. A hálózatbiztonság akkor valósul meg, ha a hálózati eszközöket beleértve a végberendezéseket is biztonságossá tettük. Amikor beüzemelünk egy új eszközt szükséges telepítenünk rá operációs rendszert, melynek biztonsági beállítási az alapértelmezett értéket veszik fel, amely számunkra a védelem szempontjából nem megfelelő. Szükséges tehát néhány beállítást alkalmaznunk. [6]

- Az alapértelmezett felhasználónevek és jelszavak megváltoztatása
- A rendszer erőforrásaihoz való hozzáférés csak az arra jogosult személyek részére történő engedélyezése
- Szükségtelen vagy felesleges szolgáltatások és alkalmazások kikapcsolása vagy törlése.

Az eszközök esetenként több időt is eltölthettek raktárakban várakozva, így a szükséges biztonsági frissítések telepítése célszerű.

Biztonsági mentés, frissítés

A vírusirtó szoftverek működhetnek helyi felhasználói vagy hálózati szinten is, melyek megakadályozhatják a legtöbb vírus és trójai ló szétterjedését a hálózatban. A legfrissebb fejlesztések alkalmazása eredményesebb védekezést tehet lehetővé e támadások ellen. A féregtámadások is jelentős veszélyt rejtenek, ezért a védekezés javasolt lépései a következők:

- Elszigetelés: a férek terjedésének megakadályozása a fertőzésmentes részek leválasztásával.
- Immunizálás: Hibajavító csomagok telepítése és sebezhetőségi pontok keresése.
- Karantén: A fertőzött gépek azonosítása majd leválasztása a hálózatról.
- Mentesítés: A fertőzött rendszerek tisztítása és javítása.

A féregtámadások elkerülésének leghatékonyabb módja az operációs rendszer biztonsági frissítéseinek telepítése és a sebezhető rendszerek hibajavítása.

Tűzfalak

A tűzfal az egyik leghatékonyabb biztonsági eszköz, amely a belső hálózati felhasználók külső veszélyektől való megvédésére szolgál, mégpedig a hálózatba beérkező és az onnan kimenő forgalom ellenőrzésével. A tűzfal két vagy több hálózat között helyezkedik el, ellenőrzi a köztes forgalmat, és véd a jogosulatlan hozzáféréstől is különböző (alábbi) módszerek alkalmazásával.

- Csomagszűrés: Tiltja vagy engedélyezi a hozzáférést IP-cím vagy MAC-cím alapján.
- Alkalmazásszűrés: Tiltja vagy engedélyezi a hozzáférést bizonyos alkalmazások számára portszámuk alapján.
- URL-szűrés: Tiltja vagy engedélyezi weboldalak elérését adott URL alapján.
- Állapot alapú csomagszűrés: A bejövő csomagok csak a belső hálózat állomásairól kezdeményezett kérések válaszcsomagjai lehetnek.

A tűzfalak az alábbi formákban kerülhetnek forgalomba:

- Eszköz alapú tűzfalak: Olyan biztonsági berendezés, melybe a tűzfal célhardverként van beépítve.
- Szerver alapú tűzfalak: A hálózati operációs rendszeren fut egy speciális alkalmazást tartalmazva.
- Integrált tűzfalak: Az integrált tűzfal egy meglévő eszköz, például egy forgalomirányító tűzfalszolgáltatással kiegészítve.

Személyes tűzfalak: Személyes tűzfal a munkaállomásokon található és nem a LAN védelmére tervezték.

Jelszavak

A hálózati eszközök védelme érdekében célszerű az erős jelszavak használata, melyek megadásában fontos néhány alapelvet követnünk.

- Minél hosszabb egy jelszó, annál biztonságosabb. Használjunk tehát minimum 8 karakterből álló jelszavakat.
- A jelszavak legyenek bonyolultak, például tartalmazzanak kis- és nagybetűt, számot, szóközt, egyéb karaktereket.
- A jelszavakban kerülni kell az ismétlődéseket, számsorozatokat, gyakori szavakat, rokonok vagy háziállatok neveit, születési dátumokat, azonosító számokat vagy bármely könnyen azonosítható információt.
- Cseréljük gyakran a jelszavakat.
- Ne hagyjuk a leírt jelszavakat látható helyen

Az erős jelszavakat titokban is kell tartanunk, ha el akarjuk velük érni a kívánt hatást. A következő lépések segíthetik a jelszavak titokban tartását. Az eszközön globális konfigurációs módban megadva a következő parancsokat:

- service password-encryption: a parancs titkósítja az összes kódolatlan jelszót.
- security password min-length: a jelszavak minimális hosszát határozza meg.
- login block-for 90 attempts 3 within 30: letiltja a bejelentkezést 90 másodperc időtartamra, ha 3 sikertelen kísérletet érzékel 30 másodpercen belül.

Következtetések

Láthatjuk, hogy a hálózatunkat számos veszély fenyegeti, illetve a privát adatainkat szükséges valamilyen formában védenünk az illetéktelen hozzáféréssel szemben. Ezen cikkben csak néhány alapvető és napjainkban is használatos támadási forma

került bemutatásra, azonban az idő múlásával és a technológia fejlődésével a támadási formák száma egyre növekszik. Szerencsére az ellenük való védekezés is hasonlóképpen frissül és fejlődik.

Felhasznált irodalom

[1] Szanyi Sándor – Jobbágy Szabolcs – Pándi Erik: A minden a hálón biztonsági aspektusai: Hírvillám – Signal Badge 2015/1. szám

[2] Paráda István hadnagy: WEBKAMERA HACK - PENETRATION TESZT Hadmérnök: XII. Évfolyam 1. különszám – 2017. július

[3]https://www.dcicontracts.com/resource-centre/defence-blog/three-lessons-nhs-cyber-attack/ (letöltve: 2017.11.2.)

[4] Paráda István hadnagy: A NATO KIBERVÉDELMI IRÁNYELVEINEK FEJLŐDÉSE Honvédségi Szemle 2018/3. szám

[5] Tóth András: INTERNATIONAL INFORMATION SECURITY IN HUNGARY, 8. medzinárodná vedecká konferencia: "NATIONAL AND INTERNATIONAL SECURITY 2017, pp. 548-557.

[6] Tóth András: A jövő információbiztonsági fenyegetései a védelmi szférában – Hadtudományi Szemle 2017. X. évfolyam 4. szám

Oláh Dániel: A felhasználói viselkedés, mint belső veszélyforrás

Absztrakt

A korszerű vállalati környezetek alapvető komponensei az infokommunikációs hálózatok. Ezek a hálózatok a vállalatok struktúrájának minden szegmensében megtalálhatók, és nemcsak az alkalmazottakat (felhasználókat) kötik össze egymással, hanem felhő alapú szolgáltatásokkal a hatékonyabb munkavégzést is biztosítják. Segítségével valós időben dolgozhatnak együtt egy projekten a munkacsoportok, a megosztott meghajtóknak és az azonnali üzenetküldő szolgáltatásoknak köszönhetően az információáramlás soha nem látott sebességgel történik, a megosztott erőforrások használatával költséghatékonyabb a vállalatok működése.

A STUXNET [1] felfedezése óta tudjuk, hogy mekkora potenciál van a kiberhadviselésben, és hogy kellő technikai tudás birtokában még a legbiztonságosabbnak hitt hálózatokat, rendszereket is el tudjuk érni. Napjainkban a hálózatok biztonságáért felelős személyek kiemelt figyelmet fordítanak a külső fenyegetések megelőzésére és elhárítására, azonban vállalati környezetben nagyobb valószínűséggel fordulnak elő olyan biztonsági incidensek, amelyek belső forrásból származnak.

Kulcsszavak: *belső fenyegetés ~ insider threats, adatszivárgás*[1]*~ data leakage, biztonsági házirend ~ security policy, felhasználói viselkedés ~ user behaviour*

[1] Az adatszivárgás egy biztonsággal kapcsolatos információs technológiai kifejezés, amelyet olyan esetekben használnak, amikor védett, bizalmas adatok valamilyen módon kijutnak, „kiszivárognak” a védett környezetből. (forrás: https://hu.wikipedia.org/wiki/Data_Loss_Prevention, letöltve: 2016.10.27.)

Bevezetés

Vállalati környezetben az alkalmazottak különböző típusú végponti eszközökön keresztül érik el a munkahelyi hálózatot, és sok esetben azon keresztül az egész világot összekapcsoló hálózatot, az internetet is. A hálózat adta lehetőségek kihasználásával egyre gyorsabbá és hatékonyabbá válik a munkavégzés. A felhasználóknak lehetőségük van kommunikálni egymással, összedolgozni és a munkavégzéshez szükséges különböző minőségű és formátumú adatokat elérni. Napjainkban elmosódni látszanak az iroda – mint a munkavégzés helye – határai. A mobil eszközökkel (laptopok, okostelefonok, tabletek) szinte bárhonnan végezhető a munka, a felhasználók nincsenek helyhez kötve, mindössze a munkahelyi hálózathoz való csatlakozás lehetőségét kell biztosítani számukra.

Az információs társadalom [2] kialakulásával a szellemi termék [2] egyre nagyobb értékkel bír a vállalatok számára. A munkahelyi hálózatok egyre több ilyen jellegű adatot tartalmaznak, így azok tervezése és üzemeltetése során számolni kell azzal a ténnyel, hogy ezekhez az adatokhoz illetéktelen személyek próbálnak meg hozzájutni haszonszerzés céljából. A hackerek 3 különböző módszerek felhasználásával, kívülről próbálják elérni a hálózatot és annak elemeit.

A hálózatok tekintetében a másik – és nem kevésbé jelentős – fenyegetést a belső veszélyforrások, vagyis maguk a felhasználók jelentik. A felhasználók

[2] A szellemi termékek: olyan tartós, nem anyagi javak, amelyek felhasználásával (alkalmazásával) hasznosítható anyagi javak és/vagy nem anyagi javak állíthatók elő. (forrás: http://www.econom.hu/szellemi-termekek, letöltve: 2016.10.27.)

[3] A klasszikus terminológiában a kivételes ismerettekkel és problémamegoldó készséggel rendelkező szakember, aki váratlan helyzetekben ill. nem szokványos módokon is képes a felmerülő problémák azonnali kezelésére. Napjainkban a "hacker" szót inkább a tudását negatív módon felhasználó, azzal visszaélő, tipikusan számítógépes rendszereket feltörő szakemberek jelölésére szokás használni. A jóindulatú hackereket "fehérkalapos hacker", míg a rosszindulatúakat "feketekalapos hacker" néven is szokás nevezni. (forrás: http://pcforum.hu/szotar/hekker, letöltve: 2016.10.27.)

gyakran figyelmen kívül hagyják a biztonsági szabályzókban foglaltakat, így veszélybe kerülnek a vállalat számára fontos adatok. Sok esetben a felhasználói mulasztás sokkal nagyobb kárt képes okozni, mint a kívülről érkező támadások. [3] Érthető tehát, hogy sok IT[4] szakember jobban aggódik a belső veszélyforrások miatt, mint a külső fenyegetések miatt.

Az adatszivárgás kapcsán felmerülő anyagi kárt lehetetlen meghatározni, hiszen adott esetben a vállalat hírnevének romlását; a vállalat piaci és/vagy technológiai előnyének elvesztését; az ügyfelek személyiségi jogainak sérülését (személyes adatok kiszivárgását) eredményezheti.

A felhasználók viselkedése és az adatszivárgás kapcsolata

A felhasználók viselkedése nagyban befolyásolja az adatszivárgás kockázatát. A rossz szokások olyan biztonsági réseket nyitnak meg, ahol szinte észrevétlenül juthatnak illetéktelen személyek érzékeny információkhoz.

Az érintettek gyakran nincsenek tisztában azzal, hogy amit tesznek, mekkora kockázatot jelent a vállalat számára, azonban van olyan eset is, hogy annak ellenére cselekszenek, hogy tudják a cselekedet szabálytalan mivoltát.

[4] Information technology

Felhasználói szokásokat vizsgáló felmérés és annak eredménye[5]

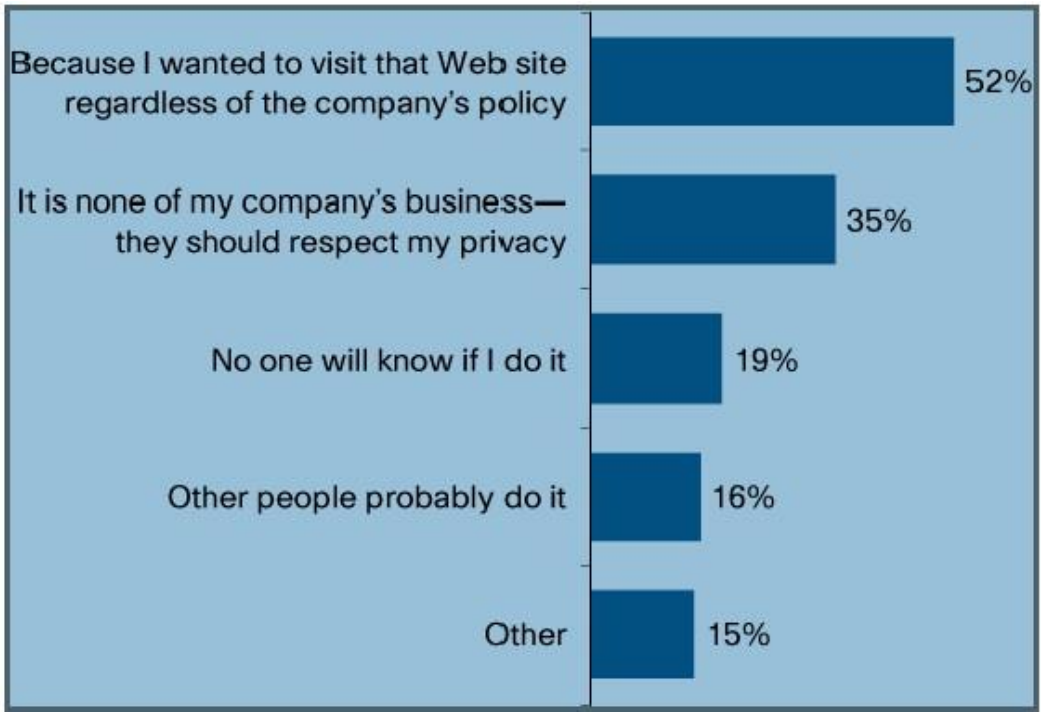
A felhasználói szokásokat vizsgáló felmérés számos meglepő eredmény tárt a nyilvánosság elé, amelyekből kiderül, hogy a belső veszélyforrások előfordulási valószínűsége nagyon magas, valamint az ilyen jellegű fenyegetések hatalmas kárt okozhatnak a vállalatoknak. Fontos megjegyezni, hogy a legtöbb felhasználói hiba – jellegét tekintve – viszonylag egyszerű és könnyen orvosolható, mégis nehézséget okoz a hálózatok biztonságért felelős személyeknek.

Az következő részben kiemelem a legnagyobb előfordulási eséllyel bíró kockázatokat.

Belső fenyegetések jellege [3][4][5][6]

A megkérdezett IT szakemberek több, mint kétharmada meg van győződve róla, hogy az adatszivárgás felét a meg nem engedett alkalmazások és programok használata okozza. A felhasználók képesek módosítani az eszközök biztonsági megoldásait még akkor is, ha tudják, hogy ez szabályokba ütközik, csak hogy azokat személyes céljaikra használhassák fel.

[5] CISCO System, Inc. A hálózati eszközöket tervező, gyártó és forgalmazó vállalat az InsightExpress céget bízta meg a felhasználói szokásokat vizsgáló piackutatással. A kutatásban résztvevő cégek összesen 1000 alkalmazottját és 1000 informatikai szakemberét kérdezték meg a világ 10 országából.



1. ábra: A beállítások módosításának okai (forrás: www.cisco.com, letöltve: 2016.10.27.)

A felhasználók nyolcvanhárom százaléka használja személyes célokra a munkahelyi számítógépét. Az illegális tartalomelérés repertoárjában szerepel zeneletöltés, online vásárlás, számlafizetés és egyéb banki tranzakciók, de szerencsejáték és pornográf tartalom is.

A munkahelyi eszközökkel történő visszaélés másik területe, amikor illetéktelenek részére adják át azokat szándékosan, vagy akaratlanul. A megkérdezettek negyvennégy százaléka osztozik a számítógépén más alkalmazottakkal, és majdnem egyötödük a jelszavát is megosztja másokkal. Az eszközök jelszavas védelme az egyik legrégebbi és legegyszerűbb módja az illetéktelen hozzáférés kiküszöbölésének, ennek ellenére sok felhasználó (a résztvevők egyharmada) hagyja úgy el a munkahelyét, hogy nem jelentkezik ki a számítógépéből, így teret adva az adatlopásnak. A jelszavak kezelésében is találunk

fatális hibákat: sok esetben (a résztvevők) húsz százaléka az asztalán hagyja a leírt jelszavát, vagy a monitorra ragasztja azt. Néhányan ezt úgy teszik, hogy az iroda nyitott, illetve többen használják a helyiséget. Sajnálatos módon előfordul az is, hogy a banki adataikkal teszik ugyanezt, amiből kiderül, hogy a biztonsági tudatosság6 messze nem éri el a kívánt szintet.

További veszélyforrást jelent, hogy a vállalatok nem ellenőrzik a munkaterületre való ki- és belépést, illetéktelen személyek kíséret nélküli közlekedését engedélyezik. Ez azt eredményezheti, hogy a vállalat vagyontárgyait eltulajdonítják (akár adathordozókat is), vagy végponti eszközökön keresztül hozzáférhetnek a bizalmas információkhoz.

A távmunka is potenciális veszélyforrás. Adatszivárgásnak minősül az is, ha az alkalmazott hangosan beszél telefonon – vállalati adatokat közölve –, vagy engedi, hogy számítógépének kijelzőjét mások is lássák munka közben, így juttatva őket érzékeny információkhoz. Gyakran a családjuknak, barátaiknak, sőt, ismeretleneknek is beszélnek érzékeny adatokról, mert úgy érzik, ötleteiket meg kell osztaniuk másokkal (44%). Sajnos csaknem egyharmaduk nem is érzi, hogy amit tesz, az károsan befolyásolja az adatbiztonságot. A távmunkával együtt jár a tény, hogy a vállalati információk a felhasználók otthoni számítógépére is átkerülnek, így a biztonságos környezet helyett egy olyan számítógépen válnak elérhetővé, amely nem felel meg a biztonsági szabályzóknak. Gyakran előfordul a vállalati adatokat tartalmazó eszközök elvesztése, vagy eltulajdonítása harmadik fél által. Ebben a válaszadók kilenc százaléka érintett. Ennél a résznél érdemes megemlíteni, hogy a nyilvános (nem megbízható) hálózatokra történő csatlakozás tovább rontja a helyzetet.

Haszonszerzés céljából elkövetett gondatlanság vagy szándékos cselekedet is állhat az adatszivárgás hátterében. Az alkalmazottak hatvan százaléka otthon is

[6] Security Awareness – a biztonsággal kapcsolatos tudás és hozzáállás

használja a vállalattól kapott számítógépet, így akaratlanul is veszélyes környezetnek teszi ki az információkat. Mégis a legnagyobb kockázatot az elégedetlen, csalódott emberek jelentik, akik bosszúvágyból vagy anyagi haszonszerzés céljából szivárogtatják ki az információkat vagy lopják el a vállalati eszközöket. A felhasználók tizenegy százaléka számolt be arról, hogy adott el (vagy valamelyik kollégája) profitszerzés céljából vállalati adatokat, vagy lopott el munkahelyi eszközöket.

Biztonsági szabályzók[7] hatékonysága [5]

A hálózatok és rendszerek biztonságos üzemeltetésének és használatának módját leíró szabályzók az esetek többségében nem képesek ellátni a feladatukat, nem biztosítják az adatokat az elvárt mértékben.

A felmérésen résztvevő informatikai állományból huszonhárom százalék dolgozik olyan vállalatnál, amelynél egyáltalán nincs – az informatikai területre vonatkozó – biztonsági házirend. Ezekben az esetekben gyakorlatilag semmi nem áll az adatszivárgás útjában. Ez egy fatális hiba. Azt gondolnánk, hogy egy ilyen típusú dokumentum a hálózat üzemeltetésének természetes velejárója, mégis a vállalatok negyedénél hiányzik. A maradék résznél pedig található szabályzás, de később be fogjuk látni, hogy ott sem túl hatékony.

Sajnos ezeknek a dokumentumoknak nem csak a tartalmáról, de a létezéséről sem tud az alkalmazottak negyven százaléka. Gondoljunk bele, hogy milyen hatékonyan szolgálja az adatbiztonságot az a szabályzó, aminek a létezéséről sem tud az, akinek az abban foglaltak alapján kellene tevékenykednie a napi munkavégzése során. Talán a felmérés legmeglepőbb adata, hogy az informatikai

[7] Security Policy – Biztonsági Házirend mint biztonságot szabályozó előírás, szervezeti biztonságpolitika (EIBSZ, IBSZ)

területen dolgozó szakemberek húsz százaléka sem tudott ilyen dokumentum létezéséről!

A szakemberek huszonhét százaléka bevallottan nem ismeri az DLP[8]-t érintő trendeket, nem követi figyelemmel azok változását évek óta. Ha nem rendelkeznek naprakész információkkal a témát illetően, akkor a házirendek frissítését sem tudják hatékonyan megoldani.

Érdekes adat, hogy míg az oktatásért felelős személyek több, mint fele állítja azt, hogy az új alkalmazottak részesülnek biztonsági felkészítésen, addig maguk az alkalmazottak harminckét százaléka állítja csak, hogy részt vett ilyenen. Ez a példa elég jól szemlélteti a biztonságért felelős szakemberek elképzelései és a valóság közötti különbséget. Mindemellett a felhasználók csaknem fele, a szakemberek több, mint háromnegyede úgy gondolja, hogy a munkahelyükön szükség van a szabályok frissítésére.

A fent tárgyalt tények megmutatják, hogy sok helyen nem létezik IBSZ; ahol létezik, ott is kevesen tudnak róla; ahol minkét feltétel teljesül, ott pedig sokan elavultnak tartják. Azonban a felhasználók maradék kisebbsége olyan helyen dolgozik, ahol minden adott ahhoz, hogy viszonylagos biztonságban tartsák a vállalat adatait. Bár a feltételek adottak, a felhasználók mégsem veszik figyelembe a dokumentumok iránymutatásait.

A szabályzók be nem tatásának okai [3][4][5]

- Az alkalmazottak nem tudják, hogy létezik biztonsági házirend.
- Nem ismerik a szabályzókban foglaltakat.
- Nem érzik azt, hogy a vállalatra negatív hatással van az, amit tesznek.
- Okozhatja figyelmetlenség, hanyagság.

[8] Data Loss Prevention — adatszivárgás megelőzése (adatvesztés megelőzése)

- Úgy gondolják, hogy amit tesznek, az magánéleti kérdés.
- Úgy gondolják, hogy amit tesznek, az soha nem derül ki.
- Úgy gondolják, hogy ha valami bajt okoznak, az soha nem derül ki.
- Tudatában vannak annak, hogy helytelen dolgot tesznek, de nem érdekli őket.
- Csak azért csinálják, mert másoktól ezt a példát látják.
- Anyagi haszonszerzés céljából.
- Bosszúból.
- Mert nem marad energiájuk eleget tenni a követelményeknek. Feszítettebb a munkatempó, mint bármikor ezelőtt.
- Azt hiszik, hogy a szabályok betartása a munkavégzés hatékonyságának csökkenésével jár.
- Úgy gondolják, ha hibát okoznak, akkor a szakemberek segítenek elhárítani azt, és ennek nem lesz semmilyen következménye.
- A szabályzók megszegése pusztán személyes haszonszerzés céljából.

	IT Decision Makers										
	Total (n=776)	US (n=76)	BRA (n=85)	UKV (n=71)	FRA (n=75)	DEU (n=83)	ITA (n=77)	CHN (n=92)	JPN (n=61)	IND (n=77)	AUS (n=79)
They do not think there is enough risk to be concerned	47%	51%	44%	44%	41%	52%	38%	59%	49%	51%	39%
They think IT is there to protect them if something goes wrong	41%	39%	36%	39%	33%	41%	38%	47%	38%	52%	44%
Security is just not top-of-mind for them	39%	34%	29%	45%	31%	33%	31%	77%	25%	38%	39%
They do not care	38%	38%	21%	34%	57%	37%	31%	34%	49%	39%	41%
They do not know about or understand the policy	34%	30%	35%	31%	43%	29%	25%	45%	41%	35%	29%
They do not know that security is a concern for IT	33%	28%	22%	23%	24%	41%	29%	59%	30%	36%	35%
They are in a hurry	25%	29%	24%	24%	27%	40%	12%	17%	13%	38%	23%
We need to create or improve our employee education and training programs	22%	21%	27%	11%	5%	14%	12%	40%	30%	44%	14%
Other	2%	1%	0%	8%	1%	1%	1%	1%	2%	0%	4%
Don't know/not sure	2%	4%	1%	3%	3%	1%	6%	0%	0%	0%	3%

2. ábra: a szabályzók megsértésének okai (forrás: www.cisco.com, letöltve: 2016.10.27.)

Összegzés

A fentiek alapján elmondhatjuk, hogy a felhasználók számos okból nem tartják be a biztonsági szabályzatot. Sajnos még akkor is nehéz kialakítani és fenntartani a hálózatbiztonságot, ha minden körülmény adott. Sokszor a siker útjában az áll, hogy a szakemberek részéről észlelt információk – amikből tapasztalatokat vonnak le – szöges ellentétben állnak a valós veszélyforrásokkal.

A legalapvetőbb hiba, amit ki kell küszöbölni, a biztonsági szabályzók létrehozása olyan módon, hogy annak léte mindenki (felhasználó és szakember) számára egyértelmű legyen. Az így kialakított szabályzatot naprakészen kell tartani a legújabb trendeknek megfelelően. A kialakítás során figyelembe kell venni a hálózat minden paraméterét, a vállalat érdekeit, valamint a felhasználói szokásokat. A dokumentum megfogalmazása úgy kell, hogy történjen, hogy az a nem szakavatott alkalmazottak számára is érthető legyen. Terjedelmét tekintve ne legyen hosszú, és könnyen elsajátítható legyen. Minden alkalmazott számára tartsunk oktatást, különös tekintettel a vállalat új alkalmazottjaira. Az új információkat személyesen közöljük, a levélben történő adatközlés hatástalan. Kezeljük a belső veszélyforrásokat egyenlő szinten a külső fenyegetésekkel.

Ezen alapelvek betartásával hatékonyabban alakítható ki olyan szabályrendszer, ami a vállalati érzékeny adatok védelmét hivatott elérni. De a legfontosabb annak elérése, hogy a felhasználók megértsék, a vállalati adatok megvédése közös cél, és ennek a célnak az elérésében ők is nagy szerepet játszanak.

Irodalomjegyzék

[1] Gyebrovszki Tamás: STUXNET - MINT AZ ELSŐ ALKALMAZOTT KIBERFEGYVER - A TALLINNI KÉZIKÖNYV SZABÁLYRENDSZERE

SZEMPONTJÁBÓL, Hadmérnök, IX. Évfolyam 1. szám - 2014. március, in: http://hadmernok.hu/141_16_gyebrovszkyt.pdf, letöltve: 2016.10.27.

[2] Tattay Levente: A tudás alapú társadalom és a szerzői jogból mint tudásgazdaságból eredő jövedelem, in: http://epa.oszk.hu/01900/01963/00037/pdf/EPA01963_informacios_tarsadalom_2012_2_090-104.pdf (letöltve: 2016.10.27.)

[3] Data Leakage Worldwide: The High Cost of Insider Threats, in: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.html, letöltve: 2016.10.27.

[4] Data Leakage Worldwide: Common Risks and Mistakes Employees Make, in: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html, letöltve: 2016.10.27.

[5] Data Leakage Worldwide: The Effectiveness of Security Policies, in: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-503131.html, letöltve: 2016.10.27.

[6] Tóth András: Future Information Security Threats to the Defense Sector, HADTUDOMÁNYI SZEMLE X. évfolyam 4. szám: pp. 246-257. (2017)

Farkas Tibor, Tóth András: Csapatgyakorlat végrehajtása a Magyar Honvédség Összhaderőnemi Parancsnokság alakulatainál

Absztrakt

A Nemzeti Közszolgálati Egyetem képzési rendszerében törvényi előírás a honvéd tisztjelöltek részére csapatgyakorlat végrehajtása a Magyar Honvédség különböző szervezeteinél. 2018. májusában a végzős hallgatói állomány tervezett első tiszti beosztásuk helyszínén Budapest helyőrségben három hét időtartamban hajtotta végre feladatait. Lehetőségük nyílt beosztásuk és leendő kollégáik megismerésére, a szolgálati és munkafeladataik behatóbb tanulmányozására, a szükséges alapok elsajátítására.

Kulcsszavak: *csapatgyakorlat, honvéd tisztjelölt, MH 12. Arrabona Légvédelmi Rakétaezred, MH 54. Veszprém Radarezred, MH 59 Szentgyörgyi Dezső Repülőbázis, MH 5. Bocskai István Lövész Dandár*

A Nemzeti Közszolgálati Egyetem Híradó Tanszékének honvéd tisztjelölt állománya a 282/2016. (IX. 21.) Korm. rendelet az államtudományi képzési terület alap- és mesterképzési szakjainak meghatározásáról és azok képzési és kimeneti követelményeiről, valamint az azzal összefüggő kormányrendeletek módosításáról, 2. melléklet Az alapképzési szakok képzési és kimeneti követelményei 11.9. pontjában foglaltak szerint *„A honvéd tisztjelöltek az első szakmai gyakorlatot az alapképzésben a 6. szemeszterben, 2 hetes időtartamban, a Magyar Honvédség kijelölt katonai szervezeteinél, választott szaknak, illetve specializációnak megfelelő feladattal hajtják végre. A második szakmai gyakorlat az alapképzés 8. szemeszterében történik. Ez egybefüggő 4 hetes szakmai gyakorlatot jelent, amely az első tiszti beosztásra való felkészítést is jelenti egyben.”* Ennek megfelelően

tanszékünk hallgatói állománya csapatgyakorlatot hajtott végre három hét időtartamban 2018. májusában a Magyar Honvédség különböző alakulatainál. A negyedik évfolyamos hallgatók első tiszti beosztásuk helyszínén – ennek megfelelően egy fő az MH 12. Arrabona Légvédelmi Rakétaezrednél, egy fő az MH 5. Bocskai István Lövész Dandárnál, egy fő az MH 54. Veszprém Radarezrednél, egy fő az MH 59. Szentgyörgyi Dezső Repülő Bázison – teljesítettek szolgálatot.

A szakmai gyakorlat szerves részét képezi az oktatásnak, ennek megfelelően a Nemeztei Közszolgálati Egyetem Tanulmányi és vizsgaszabályzatában a következő pontok kerültek meghatározásra ezzel összefüggésben:

- A szakmai gyakorlat időtartamát az ajánlott tantervek határozzák meg.
- A szakmai gyakorlat teljesítése feltétele a záróvizsgára bocsátásnak.
- A hallgató a Neptun.Net rendszerben köteles felvenni a szakmai gyakorlat tárgyat.
- A szakmai gyakorlat megszervezésének, a jelentkezés és a gyakorlat teljesítésének részletes rendjét a karok, illetve a karhoz nem tartozó intézet által gondozott képzések esetében az intézetek szakspecifikusan szabályozzák.

MH 12. Arrabona Légvédelmi Rakétaezred

Az MH 12. Arrabona Légvédelmi Rakétaezred esetében hallgatónk az ezredtörzs híradó és informatikai részlegén teljesített szolgálatot és vet részt a mindennapi életben. Az ezred hírfőnökének közreműködésével bemutatkozott az ezred parancsnokainak, illetve körbe lett vezetve a törzs különböző részlegein, mint például személyügy, logisztika, hadművelet, felderítés. Ezt követően a laktanyán belül került körbevezetve és megismerhette a fontosabb objektumok helyszíneit. Az első héten az ideje nagy részét híradó és informatika részlegen töltötte az

informatikai rendszerfenntartó tisztekkel, akik megmutatták számára, hogy hogyan működnek a laktanyában használt informatikai rendszerek, mint például a belső levelező szerver, a beléptetések, a különböző jogosultságok a mágneskártyákkal kapcsolatosan, illetve az IP és ISDN telefonhálózatok.

A következő héten már a leendő beosztásával ismerkedhetett meg a vezetési zászlóalj, tűztámogató század, híradó szakaszán belül. Megismerkedett a zászlóalj megbízott parancsnokával, a leendő századparancsnokával, illetve a századon és a szakaszon belüli leendő kollégáival. Becsatlakozott a szakasz mindennapi életébe, segédkezett a szakasz adott napi feladataiban, melyek nagyon változatosak voltak és rengeteg szakmai kihívással rendelkeztek. A feladatok közt többek között szerepelt a külső körlet rendezés, anyag felvétel és leadás, adminisztrációs feladatok, illetve testnevelés foglalkozás. Minden nap nagy hangsúlyt fektetett az ismeretségi köröm bővítésére, a szakmai ismeretei bővítésére, illetve a rendszeres testedzés végrehajtására.

Az utolsó héten hallgatónk az előző hetekhez hasonlóan változatos és kihívásokkal teli feladatokkal nézett szembe. Ilyen feladat volt többek között a „Tobruq Legacy” nemzetközi légvédelmi gyakorlatra való felkészülés, melyben a vezetési zászlóalj, és azon belül a híradó szakasz néhány tagja is érintett volt. További feladat volt a felkészülés a május 21-e, a Magyar Honvédelem Napja alkalmából tartott nyíltnapra is. Ezek a feladatok különféle pakolási, illetve készletezési feladatokban merültek ki. Végül, de nem utolsó sorban részt vett a havonta megrendezett Levendula híradó rendszergyakorlaton, melynek keretén belül feladat volt az összeköttetés felvétele a székesfehérvári ÖHP-vel, az R-142-es rádióállomásban található R-130-as rövidhullámú rádiókészülékkel. Az összeköttetést sikeresen felvette a szakasz, továbbá számos más ÖHP alárendelt alakulat bejelentkezését is hallották. Hallgatónk megítélése alapján szakmai

csapatgyakorlata győri szakasza sikeresen zárult és új szakmai ismeretekkel és élményekben gazdagon tért vissza Budapestre.

MH 54. Veszprém Radarezred

Egy fő honvéd tisztjelöltünk a részére meghatározott időszakban az MH 54. Veszprém Radarezrednél teljesítette csapatgyakorlatát, ahol első tiszti beosztása helyszínén nyerhetett bepillantást a híradó zászlóalj, híradó század, rádió relé szakasz, szakaszparancsnoki beosztás feladataiba. Az első napokban a század megbízott parancsnoka volt a segítségére. Megismerhette a század és a zászlóalj felépítését, valamint vezetését, továbbá a század napi életének rendjét. Megismerkedett az ezrednél található technikai eszközökkel (VSAT, R-1406 rádió relé állomás) és a laktanyában található objektumokkal (parancsnoki épület, személyügy, telephely). Előnyére szolgált, hogy a jövőbeli beosztottjai nagyon segítőkészen álltak hozzá, rengeteg segítséget kapott tőlük, így az első benyomás és az ismerkedés is megfelelően alakult. Az étkezést és a szállást is az ezred biztosította, mely jó minőségű volt, ott tartózkodása ideje alatt nem merült fel semmilyen probléma.

MH 59 Szentgyörgyi Dezső Repülőbázis

Egy fő honvéd tisztjelöltünk az MH 59 Szentgyörgyi Dezső Repülőbázis Híradó és FRISZ századnál teljesítette a részére meghatározott csapatgyakorlati követelményeket. Az első hét során körbevezették a bázis területén, megismerkedett a nyolcórás munkarendben dolgozó állománnyal. Részt vett az újonnan megalakult zászlóalj (Repülő Harcbiztosító és Üzemeltető Zászlóalj) sorakozóján, ahol ismertették a zászlóalj előtt álló feladatokat a kettős felhasználású repülőtér,

valamint az amerikai egységek fogadásával kapcsolatban. A sorakozó után megismerhette a zászlóalj vezetését, törzsét, valamint bemutatták neki a század által kezelt dokumentumokat, valamint a század felépítését, a repülőtér FRISZ eszközeit, valamint részletesen bemutatták a váltásos munkarendben dolgozó katonák feladatait, eszközeit, valamint járműveit. Szintén részt vett a bázis logisztikai főnöke által vezetett nyári igénybevételre való felkészítés szemléjén.

Következő héten Iskolások Napja került lebonyolításra, így a századra hárult a hangosítás feladata. Minden nap végrehajtották azok kiépítését és bontását. Hallgatónk szintén részt vett a Levendula rendszergyakorkatban a századnál rendszeresített R-130-as rövidhullámú rádiójával.

Összességében hallgatónk a két hét folyamán megismerhette a század állományát és mindennapi feladataikat, valamint eszközeit és dokumentumait.

MH 5. Bocskai István Lövész Dandár

Egy fő honvd tisztjelöltünk csapatgyakorlatotát az MH 5.Bocskai István Lövész Dandárnál Debrecenben, a Kossuth laktanyában hajtotta végre. Hallgatónk az első és második héten a zászlóalj törzsébe nyerhetett betekintést, majd az utolsó héten lehetősége nyílt betekintést nyerni a törzstámogató század mindennapi életébe, és ott felkészülni az első tiszti beosztására, mint híradó szakaszparancsnok. Sajnálatos módon a századhoz csak egy-egy foglalkozás erejéig tudott lemenni, mert a zászlóalj misszióra való felkészülése már kezdetét vette. Megalakultak az IKBK és KFOR századai, aminek köszönhetően az állománytáblák teljesen átrendeződtek, így nem maradt szakasz, akivel dolgozhatott volna. A csapatgyakorlat során hallgatónk megismerhette leendő beosztottjait, illetve a híradó raktárakat és a rejtjelző szobát, a zászlóalj felépítését és feladat körét. Szintén bemutatásra került számára a zászlóalj törzse úgy, mint a személyügy, pénzügy, lakásügy és a logisztika. A híradó és

informatikai részleg részlegvezető helyettese az S6 parancsnoki munkájába nyújtott számára betekintést. Részt vehetett a KFOR missziós felkészítés parancsnoki gyűlésén, ahol a zászlóalj parancsok, a megalakult KFOR századainak a parancsnokai és a részlegvezetők vettek részt. Ismertette a KFOR feladatát, annak felépítését és az arra való felkészülés menetét. A beosztott zászlós a feladatok gyakorlati oldalát mutatta meg, a „hogyanokat" és „miérteket". Tapasztalat átadás során sok esetelemzést taglaltak és így hallgatónk az egyetemen tanult ismereteit gyakorlati körben is alkalmazhatta, azokat bővíthette.

A mindennapi élet reggeli testneveléssel kezdődött a laktanyában lévő sportcsarnokban vagy a laktanya mellett elhelyezkedő „B" típusú sportkomplexumban. A reggeli testnevelés követően, ha kellett parancsnoki értekezletre menni, akkor az volt az első, utána a kötelező ellenőrzések, valamint a kapott napi feladatok kerültek végrehajtásra. Minden pénteken délelőtt ellenőrzésre kerültek a Közúti Szállítású Készenléti Szakasz híradó felszerelései és okmányai.

Második héten hallgatónknak lehetősége nyílt kimenni Hajdúhadházra a dandár híradó századához és megnézhette a gépjárműparkot és a haditechnikai eszközöket. Az akkor zajló nyári időszakra való felkészítésbe is betekinthetett. A gépjárműparkban parkoló parancsnoki BTR-ekbe beülhetett és részt vett az azokról szóló foglalkozáson. Meglátogatta a Hajdúhadháznál lévő lőteret is, ahol a logisztikai század éppen lövészetet hajtott végre.

Összefoglalva hallgatónk a csapatgyakorlatról pozitív élményekkel tért vissza Budapestre.

Felhasznált irodalom

- 282/2016. (IX. 21.) Korm. rendelet az államtudományi képzési terület alap- és mesterképzési szakjainak meghatározásáról és azok képzési és kimeneti

követelményeiről, valamint az azzal összefüggő kormányrendeletek módosításáról

- Nemzeti Közszolgálati Egyetem Tanulmányi és vizsgaszabályzat, Budapest, 2012
- http://felveteli.uni-nke.hu/hhk/alapkepzes/katonai-uzemeltetes/
- 9/2013. (VIII. 12.) HM rendelet a honvédek jogállásáról szóló 2012. évi CCV. törvény egyes rendelkezéseinek végrehajtásáról
- 2012. évi CCV. törvény a honvédek jogállásáról
- Dr. Szekendi Gyöngyvér: A hivatásos és a szerződéses katonák jogállása, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel, ISBN 978-615-5491-14-6, Nemzeti Közszolgálati Egyetem, Budapest, 2014
- Csikos Christopher: Csapatgyakorlat jelentés, 2018
- Czető Bálint: Csapatgyakorlat jelentés, 2018
- Darázs Tamás: Csapatgyakorlat jelentés, 2018
- Nagy Szabolcs: Csapatgyakorlat jelentés, 2018

Farkas Tibor, Tóth András: Csapatgyakorlat végrehajtása a Magyar Honvédség 43. Nagysándor József Híradó és Vezetéstámogató Ezrednél

Absztrakt

A Nemzeti Közszolgálati Egyetem képzési rendszerében törvényi előírás a honvéd tisztjelöltek részére csapatgyakorlat végrehajtása a Magyar Honvédség különböző szervezeteinél. 2018. májusában a végzős hallgatói állomány tervezett első tiszti beosztásuk helyszínén az MH Összhaderőnemi Parancsnokság vidéki alakulatainál három hét időtartamban hajtotta végre feladatait. Lehetőségük nyílt beosztásuk és leendő kollégáik megismerésére, a szolgálati és munkafeladataik behatóbb tanulmányozására, a szükséges alapok elsajátítására.

Kulcsszavak: *csapatgyakorlat, honvéd tisztjelölt, MH Összhaderőnemi Parancsnokság, MH 43. Nagysándor József Híradó és Vezetéstámogató Ezred,*

A Nemzeti Közszolgálati Egyetem Híradó Tanszékének honvéd tisztjelölt állománya a 282/2016. (IX. 21.) Korm. rendelet az államtudományi képzési terület alap- és mesterképzési szakjainak meghatározásáról és azok képzési és kimeneti követelményeiről, valamint az azzal összefüggő kormányrendeletek módosításáról, 2. melléklet Az alapképzési szakok képzési és kimeneti követelményei 11.9. pontjában foglaltak szerint *„A honvéd tisztjelöltek az első szakmai gyakorlatot az alapképzésben a 6. szemeszterben, 2 hetes időtartamban, a Magyar Honvédség kijelölt katonai szervezeteinél, választott szaknak, illetve specializációnak megfelelő feladattal hajtják végre. A második szakmai gyakorlat az alapképzés 8. szemeszterében történik. Ez egybefüggő 4 hetes szakmai gyakorlatot jelent, amely az első tiszti beosztásra való felkészítést is jelenti egyben.”* Ennek megfelelően tanszékünk hallgatói állománya csapatgyakorlatot hajtott végre három hét

időtartamban 2018. májusában a Magyar Honvédség különböző alakulatainál. A harmadik évfolyamos hallgatók az MH 43. Nagysándor József Híradó és Vezetéstámogató Ezrednél teljesítettek szolgálatot.

A szakmai gyakorlat szerves részét képezi az oktatásnak, ennek megfelelően a Nemeztei Közszolgálati Egyetem Tanulmányi és vizsgaszabályzatában a következő pontok kerültek meghatározásra ezzel összefüggésben:

- A szakmai gyakorlat időtartamát az ajánlott tantervek határozzák meg.
- A szakmai gyakorlat teljesítése feltétele a záróvizsgára bocsátásnak.
- A hallgató a Neptun.Net rendszerben köteles felvenni a szakmai gyakorlat tárgyat.
- A szakmai gyakorlat megszervezésének, a jelentkezés és a gyakorlat teljesítésének részletes rendjét a karok, illetve a karhoz nem tartozó intézet által gondozott képzések esetében az intézetek szakspecifikusan szabályozzák.

MH 43. Nagysándor József Híradó és Vezetéstámogató Ezred

Harmadéves honvéd tisztjelöltjeink 2018. május 22. -25. között a jogszabályban meghatározottak és a megküldött feladatlap alapján szakmai csapatgyakorlatot hajtottak végre az MH 43. Nagysándor József Híradó és Vezetéstámogató Ezrednél, Székesfehérvár helyőrségben.

A gyakorlaton az elméleti felkészítés keretében megismerkedtek az alakulat felépítésével, feladatkörével, a betölthető kezdő tiszti beosztásokkal, azok munkaköri leírásával, és az azokhoz tartozó általános napi rutinnal és feladatokkal. Ezen felül bemutatták számukra a végrehajtó alegységek műszaki-technikai felszereltségét, az eszközök működésének elméleti hátterét, továbbá az

infokommunikációs és komplex információbiztonsági rendszereket és azokkal kapcsolatos előírásokat.

Gyakorlati felkészítés keretében bemutatásra kerültek az alkalmazott haditechnikai eszközök, rendszerek és ezekkel kapcsolatos eljárások. Továbbá a különböző a Magyar Honvédség által a mindennapokban alkalmazott polgári rendszerek, ezek gyakorlati felhasználása és a civil szolgáltatókkal, partnerekkel való kapcsolattartás rendszerét is megismerhették.

Az első napon az adminisztratív teendők, belépési engedélyek, élelmezési átjelentő elintézésével kezdődött. Ezt követően hallgatóink körbe lettek vezetve az Alba Regia és a Nagysándor József laktanyákban és ismertetésre kerültek a különböző épületekben települt alegységek. A délelőtt maradék részében az alakulat történetét és főbb feladatait, általános békeidőbeli és gyakorlatok során való tevékenységet ismertették velük egy rövid előadás keretein belül, ahol még szóba kerültek a számukra lehetséges kezdő beosztások és azokhoz tartozó feladatkörök. Nem utolsó sorban szó esett magáról a városról és általánosságban a helyőrség sajátosságairól, pl. lakhatás. A hét hátra lévő részében törekedtek arra, hogy az összes alegységet bemutassák számukra.

A második napon hallgatóinknak lehetősége nyílt a Dunántúli Híradó és Informatikai Központ híradó és informatikai felügyelet altiszti és legénységi állományú katonáival a várpalotai gyakorlótéren megrendezett „Tobruq Legacy 2018” gyakorlatra kilátogatni. Fő feladatuk a vezetési ponton belül és környékén lévő telefonhálózat kiépítése volt, a készülékek elhelyezése, a hozzájuk tartozó vezetékek lemérése és méretre vágása, illetve megfejelése RJ11-es és 45-ös fejekkel. Később pedig bemutatták számukra a várpalotai lőtéren található mikrohullámú átjátszó állomás és hálózat működését.

A csütörtöki napon a hírközpont rádióvevő vezérlőtermének személyzete mutatta be számukra a náluk található technikai berendezéseket, illetve hallhattak

több kapcsolatfelvételt, köztük egyet a jelenleg szolgálatot teljesítő KFOR kontingenssel, és a rendszer működésének tesztelését. Ezután az Iridium és Bgan műholdas telefonokkal kapcsolatos tudni valókat és ezek rendszerét ismertették velük. A nap végén a Dunántúli Híradó és Informatikai Központ híradó és informatikai ügyelet teendőit és általános feladatait ismertették meg velük, továbbá az ottani szolgálatot és annak tevékenységét nagy vonalakban. Ezenfelül megtekinthették a szervertermet, ahol az ott található berendezések működéséről is esett szó.

Az utolsó napon a híradózászlóalj egy századának napirendjét ismerhették meg, illetve az aznapi feladatokba hallgatóinkat is bevonták. A feladatuk főként a másnapi nyíltnapra való felkészülés volt, a tisztjelöltek is segítettek a kijelölt állománynak a sátorépítő munkálatokban és megismerhették egy híradó század, szakaszparancsnok tevékenységét egy feladat végrehajtása során általánosságban.

Hallgatóink véleménye szerint a gyakorlat hasznos volt mindannyiuk számára. Megismerhették mind a lehetséges beosztásokat, mind az ezekkel járó kihívásokat és motiváló tényezőket. Ezenfelül az ott eltöltött idő rövidsége ellenére hozzájárult szakmai tudásuk elmélyítéséhez, továbbá lehetőséget adott egy kevés gyakorlati tapasztalat szerzésére is.

Összefoglalás

A hallgatói beszámolók alapján összességében elmondható, hogy az alakulatnál eltöltött 1 hét lehetőséget adott arra, hogy a honvéd tisztjelöltek megismerkedjenek az alakulattal. Ezek mellett új technikai eszközöket ismerhettek meg, valamint az itt szolgáló katonák, az évek alatt szerzett tapasztalataikat is megosztották velük. Szabadidejükben lehetőségük nyílt a sportlétesítmények használatára, vagy a város felfedezésére, megismerésére.

Felhasznált irodalom

- 282/2016. (IX. 21.) Korm. rendelet az államtudományi képzési terület alap- és mesterképzési szakjainak meghatározásáról és azok képzési és kimeneti követelményeiről, valamint az azzal összefüggő kormányrendeletek módosításáról
- Nemzeti Közszolgálati Egyetem Tanulmányi és vizsgaszabályzat, Budapest, 2012
- http://felveteli.uni-nke.hu/hhk/alapkepzes/katonai-uzemeltetes/
- 9/2013. (VIII. 12.) HM rendelet a honvédek jogállásáról szóló 2012. évi CCV. törvény egyes rendelkezéseinek végrehajtásáról
- 2012. évi CCV. törvény a honvédek jogállásáról
- Dr. Szekendi Gyöngyvér: A hivatásos és a szerződéses katonák jogállása, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel, ISBN 978-615-5491-14-6, Nemzeti Közszolgálati Egyetem, Budapest, 2014
- Nagy Dávid Tamás: Csapatgyakorlat jelentés, 2018
- Szűcs Gábor: Csapatgyakorlat jelentés, 2018
- Major Márk: Csapatgyakorlat jelentés, 2018

Tóth András: Az Amerikai Egyesült Államok Védelmi Minisztériumának felhő koncepciója

Absztrakt

Jelen cikkben célom volt bemutatni az Amerikai Védelmi Minisztérium által 2017-ben megfogalmazott új felhőszolgáltatásokon alapuló koncepció alapjait. A kutatásaim során megvizsgáltam és elemeztem a jelenleg rendelkezésre álló elektronikus forrásokat, a kapcsolódó dokumentumokat, jelentéseket. Ezek alapján készítettem egy értékelő, elemző cikket, amely bemutatja a koncepcióval szemben támasztott követelményeket, a kialakításának alapelveit, lehetséges irányelveit, továbbá a pozitív és negatív oldalakat.

Kulcsszavak: *felhőinformatika, felhőszolgáltatás, védelmi informatika, C4ISR*

2017-ben az Amerikai Egyesült Államok Védelmi Minisztérium bejelentette, hogy egy új katonai felhőszolgáltatást nyújtó projekt elindítását. A projekt a Joint Enterprise Defense Infrastructure (továbbiakban: JEDI) nevet kapta. A cél egy olyan cég megbízása, amely képes egy olyan egyedi felhőszolgáltatás nyújtására, ami alkalmas az egyes feladatok, küldetések szempontjából fontos munkafolyamatok és katonai titkok tárolására, ezáltal képes a nyílt és minősített információk megosztására a világ bármely pontján feladatot teljesítő katonák számára. Ezen képesség egyéb technológiákkal való közös alkalmazása vitathatatlanul hozzájárulhat az információs fölény kialakításához, mivel egy gyorsabb és hatékonyabb elemzést érhetnek el a megnövekedett adatmennyiségek halmazában, melyek az alkalmazott szenzorok, kamerák és egyéb felderítő és megfigyelő

eszközöktől érkezhetnek. Ennek megfelelően egy olyan közösségi felhő létrehozását tervezik, amely a fenti eszközrendszereket egy hálózatba integrálja, és hozzáférést biztosít minden a megfelelő jogosultságokkal rendelkező felhasználó számára. A National Institute of Standards and Technology (NIST) alapján a számítási felhők kialakításának négy alaptípusát különböztethetjük meg, melyek a következők: magán-, A közösségi felhő a National Institute of Standards and Technology (NIST) szervezet alapján egy olyan számítási felhő, melyet adott közösség, vállalkozások vagy szervezetek egy csoportja használ, akiket valamilyen közös érdek köt össze. [1]

Ezt a koncepciót mutatja be Denis Mercier francia tábornok következő gondolata: „A jövő harci rendszere nem egy harci repülőgép, hanem egy felhőalapú azonosítással rendelkező C4ISR1 (rendszer), melyet egy ember vezette vagy pilóta nélküli platformon helyeznek. És nekünk képesnek kell lennünk ehhez kapcsolódni. Ez az, amit a jövőnk érdekében ki kell építenünk, de még ma el kell kezdenünk.” [2]

Az amerikai hadsereg jelenleg is használ felhőszolgáltatásokat, a Defense Information Systems Agency (továbbiakban: DISA) által üzemeltetett katonai felhő alkalmazási modellt, amelyben számos szervezet vesz részt, és felöleli a missziós-, politikai-, biztonsági-, minőségbiztosítási területeket is. Az egyik legjelentősebb szolgáltatás, amelyet a DISA használ a Védelmi Online Kapcsolat (Defense Connect Online, DCO), amely biztosítja a katonák és parancsnokaik számára, hogy együttműködhessenek a világ bármely részéről. [3]

[1] C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance: Vezetés, Irányítás, Kommunikáció és Számítástechnika, Hírszerzés, Megfigyelés és Felderítés

A JEDI alapelv

2017. szeptember 13-án Patrick Shahan helyettes védelmi miniszter megfogalmazott egy jelentést, melyben egy a kereskedelmi megoldásokon alapuló felhő alapú architektúrák, infrastruktúrák és platformszolgáltatások alkalmazását hangsúlyozta a minisztérium szolgáltatásainak körében. A cél egy olyan környezet kialakítása, amely:

- világszerte elérhető, exponenciálisan terjedő, biztonságos, rugalmas felhőalapú számítási és tárolási környezet, ami zavartalanul képes működni a hazai hátvéd területektől egészen a műletek színtereiig;

- olyan többfunkciós járművek létrehozása, melyek folyamatos rendelkezésre állást biztosítanak, továbbá teszik a felhőalapú számítástechnikai és tárolási szolgáltatások automatizált, önálló kiépítését, üzemeltetését;

- folyamatosan a legfrissebb kereskedelmi védelmi technológiákat alkalmazza;

- lehetővé teszi az új alkalmazások és speciális funkciók és képességek azonnali kiépítését és üzembe helyezését;

- kereskedelmi felhőszolgáltatások felhasználásával átalakíthatja a védelmi minisztérium adatainak rögzítését, feldolgozását, megértését és kiaknázását, ezzel biztosítva a speciális képességeket, melyek lehetővé teszik a valós idejű döntéshozatalt és támogatják az összhaderőnemi műveleteket.

Beszerzési stratégia:

- egy teljes és nyílt versenytárgyalási eljárás keretében kerül meghatározásra az egyszemélyes nyertes, azonban a mennyiségi és szállítási adatok még nem kerültek meghatározásra;
- egyetlen felhőszolgáltató cég, aki szállítja és biztosítja a szükséges felhő informatikai infrastruktúrát és platformszolgáltatásokat;
- 10 éves rendelési idő;
- a szerződés kiterjed az alkalmazás-migrációs támogatásra, alkalmazás-modernizációs támogatásra, a változáskezelésre, valamint a képzésre.

Bevezetési stratégia:

- minden a védelmi minisztérium alárendeltségébe tartozó szervezetnek lesz hozzáférése a felhő környezethez, továbbá képes lesz saját maga rendszereket integrálni a szolgáltatáshoz, ott beállításokat és saját szolgáltatásokat létrehozni;
- a minisztérium felügyeli a kiválasztott projektek migrációját az új szerződés- és kiépítési folyamatok érvényesítése érdekében.

A fentieket figyelembe véve elmondható, hogy a jelentés célja volt bemutatni, hogy a védelmi minisztérium rendszereinek és szolgáltatásainak körében szükséges egy komoly modernizáció és felülvizsgálat, amely kiterjed az informatikai szabályozásokra, hozzájárul az információbiztonság növeléséhez, illetve megszűnteti az esetleges interoperabilitási, kompatibilitási problémákat az egyes

szervezetek között. Az elkészült szerződésben meghatározásra kerülnek azok a követelmények, melyek szükségesek lesznek a kulcsfontosságú partnerekkel történő együttműködések során. A program célja az ipar bevonása a támogatási folyamatokba. [4]

A JEDI pozitív és negatív oldala

Az amerikai katonai szervezetek esetében (szárazföldi erők, légierő, haditengerészet, tengerészgyalogság) elmondható, hogy adataikat az esetek döntő többségében felhőkben tárolják, lényegében olyan központosított szervereken, melyek a többszörös hozzáférések érdekében védett hálózatokon keresztül érhetőek el. Azonban probléma, hogy minden egyes szervezet más és más felhőbe helyezte az általa készített, kezelt és felhasznált adatokat, különböző adatformátumokkal, hozzáférési eljárásokkal és hozzáférésre jogosult felhasználókkal. Ennek megfelelően a Védelmi Minisztérium évente rengeteg pénzt költ körülbelül ötszáz különböző felhőalapú szerződésre. Mindezeket figyelembe véve nagyon pozitív vonzata lenne a JEDI kialakításának, hogy egyetlen, közös „vállalati" felhőben tudná automatikusan megosztani az adatokat a különféle felhasználók között, nem is beszélve a kiberbiztonsági javítások és az új szoftverek automatikus terjesztéséről. Ezzel elérhetővé válna egy olyan képesség, ami támogatja a többdimenziós műveleteket , és ez által ötvözné az űr-, kiber-, elrettentő, szállítási, elektromágneses spektrum-műveleteket, a rakétavédelmet és egyéb globális képességeket a konfliktusok minden szintjén.

A pozitív oldal mellett a negatív oldal meglepő módon a lehetséges beszállítók oldalán jelent meg először. A legnagyobb technikai cégek, mint a Google, Amazon, IBM, Oracle alkalmazottai egyre többször tiltakoznak a cégjeik által kialakított és

üzemeltetett szolgáltatások rendvédelmi szervekkel történő megosztása ellen. A fenti cégek esetében legalább egy alkalommal történt már olyan nyílt petíciók benyújtása, melyek valamelyik szolgáltatásuk vagy termékük védelmi célú alkalmazása ellen irányult. Például a Google esetében komoly felháborodást váltott ki, hogy a cég a védelmi minisztériummal együttműködve olyan dolgok előállításán munkálkodik, amelyek egyrészt az emberéletek kioltását, másrészt a kémkedést teszik könnyebbé. [5] A legnagyobb problémát az jelenti a dolgozók szemszögéből, hogy az előállított szolgáltatások és rendszerek nagy valószínűséggel mesterséges intelligenciát fognak alkalmazni, amelyek komoly aggályokat jelentenek véleményük szerint, mivel nem tudhatják, hogy ez hosszú távon milyen képességeket fog adni a fegyveres erők kezébe. Ennek megfelelően nagyon nagy szükség mutatkozik megfelelőn, jól átgondolt etikai előírások és intézkedések kidolgozására.

Összefoglalás

Az Amerikai Egyesült Államok Védelmi Minisztériuma felismerte, hogy a jelenleg alkalmazott információmegosztási képességek nem támogatják teljes mértékben a vezetés-irányítást, a megszerzett információk nem jutnak el valós időben a döntéshozókhoz, ezért a döntéshozatali folyamatok nem biztos, hogy a legmegfelelőbb eredményt fogják meghozni. 2017. szeptemberében arra az elhatározásra jutottak, hogy szükséges egy olyan platform kialakítása, ami támogatja az azonnali információmegosztást. Ehhez létrehozták a Joint Enterprise Defense Infrastructure projektet, melynek célja egy közös számítási felhő létrehozása, melyhez a minisztérium alárendeltségébe tartozó összes szervezet és katonai erő hozzáférne, a megfelelő jogosultságokkal adatokat lennének képesek megosztani egymással védett hálózatokon valós időben. A projekt nyertesének

tervezett kihirdetése 2018. negyedik negyedévére várható, az első adatok migrálása az új védelmi felhőbe 2019. első negyedévére várható.

Felhasznált irodalom

[1] Peter Mell, Timothy Grance: The NIST Definition of Cloud Computing, National Institute of Standards and Technology, NIST honlap, 2011. Forrás: csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (letöltve: 2018. 05. 14.)

[2] Aaron Mehta: For NATO, a Cloudy Future, https://www.defensenews.com/air/2015/05/23/for-nato-a-cloudy-future/ (leöltve: 2018. 05. 15.)

[3] Tibenszkyné Fórika Krisztina: A katonai felhő békés villámai: a honvédelmi célú számítási felhő létrehozásának lehetőségei és veszélyei, Hadmérnök, VI. Évfolyam 4. szám - 2011. december, pp.: 250-261

[4] US Department of Defense: Joint Enterprise Defense Infrastructure (JEDI), https://www.nextgov.com/media/gbc/docs/pdfs_edit/121217fk1ng.pdf (letöltve: 2018. 05. 15.)

[5] Az Amazon-dolgozók is a sarkukra álltak, https://bitport.hu/az-amazon-dolgozok-is-a-sarkukra-alltak (letöltve: 2018. 06. 25.)

Tóth András: A mesterséges intelligencia és az IoT összekapcsolásának lehetőségei

Absztrakt

Jelen cikkben célom volt bemutatni a mesterséges intelligencia és a dolgok internete elven működő eszközök és szolgáltatások összekapcsolásának lehetőségeit. A kutatásaim során megvizsgáltam és elemeztem a jelenleg rendelkezésre álló elektronikus forrásokat, a kapcsolódó dokumentumokat. Ezek alapján felállítottam azon területeknek a listáját, melyek alkalmazhatják az integrációval létrejövő képességeik előnyeit. Megvizsgáltam, hogy az egyes rétegek milyen módon járulhatnak hozzá a koncepció kialakításához, és ezek milyen előnyökkel járhatnak az egyes alkalmazói területeken.

Kulcsszavak: *mesterséges intelligencia, IoT, felhőinformatika, edge informatika, fog informatika*

A mesterséges intelligencia (Artificial Intelligence, továbbiakban: AI) és a dolgok internete (Internet of Things, továbbiakban: IoT) használatával a digitális átalakulás olyan területeken valósulhat meg, mint a munkakörülmények átalakítása, a beszerzési lánc átalakítása, a szervezetek és az ökoszisztémák átalakítása, valamint általuk új működési modellek alakulhatnak ki. Az IoT egy eszköz, amely felhasználható a valós világgal való kapcsolatok létrehozására. Az AI olyan eszköz, amely felhasználható a valós világból gyűjtött adatok gyors és kifinomult elemzésére. Ezek a technológiák új értékek létrehozására használhatók azáltal, hogy begyűjtik, megjelenítik és elemzik a rendelkezésre álló adatokat, majd azonosítják a hasznos és értékes információkat, és visszajuttatják azokat a valós világhoz.

A munkamódszer átalakításának területén a szokásokra és tapasztalatokra alapozott eljárásmódokról átváltunk a valós adatok és elemzések alapján végrehajtott műveletekre. Ez új értékek megteremtését eredményezheti olyan formában, mint stabil működés, explicit tudás és munkastílus létrehozása és megosztása a hely vagy az idő korlátozása nélkül.

A beszerzési lánc átalakítása területén egy olyan új módszer kerülhet kialakításra, amely során egy olyan fogyasztóközpontú struktúrárát alkalmazunk, amelyet a hatékonyabb termék- és termelési tervezés és termékfejlesztés jellemez, megfelel a kor igényeknek, és teljesen megújuló vásárlási és felhasználói élményt nyújt.

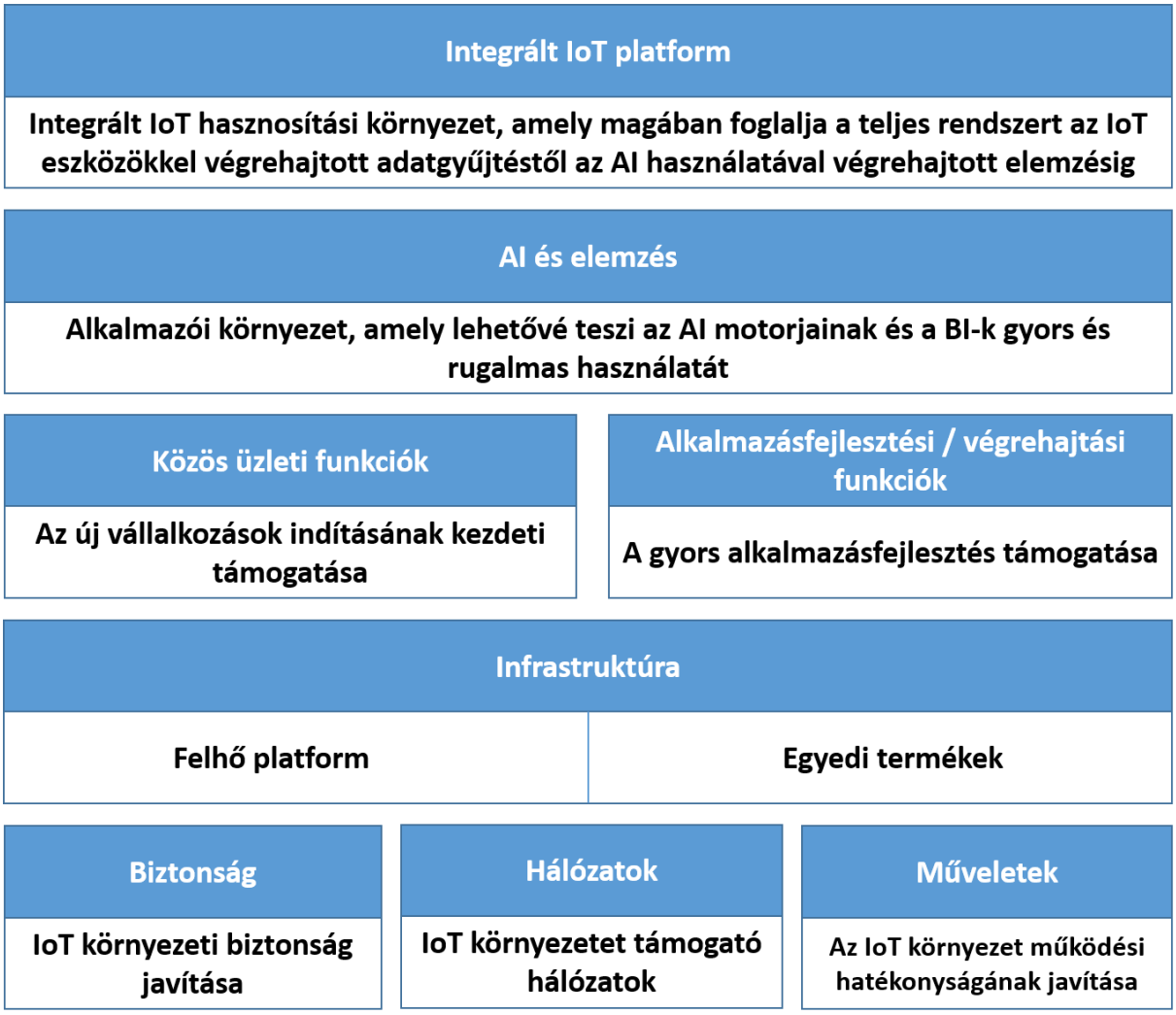
A szervezetek és az ökoszisztémák átalakításának területén az informatika, a marketing, a fejlesztés és a támogatás területén működő különféle osztályok összekapcsolásával általános optimalizálást érhetünk el, és új értéket teremthetünk, ha elmozdulunk a helyi optimalizálástól és átalakítjuk a szervezeteket és az ökoszisztémákat a fogyasztókra, partnerekre és lakosokra összpontosító rendszerekre.

Az alkalmazott műveleti modellek átalakítása területén digitálisan csatlakoztatott termékeket és szolgáltatásokat fogunk felhasználni az operatív hatékonyság növelése és az innováció előállítása érdekében, alkalmazva például az üzleti intelligencia (Business Intelligence, továbbiakban: BI) modelleket.

A széles IoT platform

Az AI technológia és az IoT integrálásával egy olyan széles IoT platformot tudunk létrehozni, ami rendkívül hatékony adatgyűjtési infrastruktúrát és olyan rendszerelemeket biztosít, amelyek lehetővé teszik a rendszer gyors kialakítását, telepítését és összekapcsolását a tervezéstől egészen a termelésig, ezzel lehetővé téve biztonságos és robusztus rendszerek rövid időn belüli felépítését. Ezen kívül teljes támogatást nyújtanak az infrastruktúrákhoz, a fejlesztési / végrehajtási

környezetekhez, a felhőhasználati környezetekhez, a hálózatokhoz, a biztonsághoz és a műveletekhez, a különféle iparágakban termelt üzleti know-how-tól az értéket biztosító közös üzleti tevékenységekig, továbbá a vállalati üzleti tevékenységeket támogató általános alkalmazásokig. [1]



1. számú ábra: A széles IoT platform
Készítette: a szerző

Az 1. számú ábrán látható, hogy az IoT és AI integrációjából olyan támogató platformokat tudunk létrehozni, melyek hozzájárulnak a kezdeti infrastruktúrák és

hálózatok gyors kialakításához, támogatják a gyors alkalmazásfejlesztést. Ezek segítségével javul a működési hatékonyság, és támogatja a környezeti biztonság javítását. A fő karakterisztikái a széles IoT platformnak a következők:

- Nagyon hatékony adatgyűjtő platform és élvonalbeli AI technológiák

  Az IoT adatgyűjtő platform hatékonyan gyűjt adatokat különféle szenzoroktól és eszközökről. A különféle formátumokban gyűjtött adatokat a legmodernebb AI technológiák, motorok elemezik és jelenítik meg. Az AI lehetővé teszi az adatok nagy sebességű hatékony gyűjtését és feldolgozását.

- Az alkotóelemek lehetővé teszik a rendszer zökkenőmentes felépítését és a tesztelésről a termelésre való áttérést

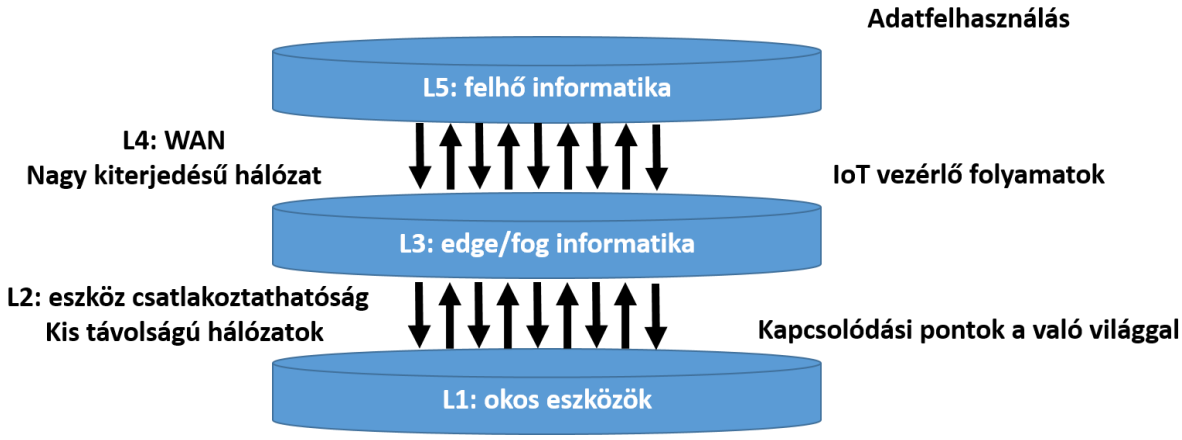
  Ez az egyszerű architektúra rugalmasan alkalmazkodik a rendszer kiegészítéseihez vagy változásaihoz, összhangban az ügyfél üzleti növekedésével, függetlenül attól, hogy csak egy kisméretű rendszerrel kezdődött a kiépítés vagy a méretezés. Az IoT rendszer elemei biztosítják a szerepeket (szoftver, AI motor, szolgáltatások, API[2] stb.). Ezek az elemek szabadon választhatók a felhasználó igényei szerint, és L1, L3 vagy L5 rétegekbe helyezhetők. Lehetőség van arra is, hogy több szolgáltatáson keresztül kapcsolódhasson a platformokhoz, például egy partner felhőn keresztül.

- Biztonságos és robusztus rendszer felépítés

  A szolgáltató biztonságosan koordinálja az egész rendszert L1-től L5-ig, és kiberbiztonsági intézkedéseket biztosít, ideértve a sebezhetőségi manővert

[2] application programming interface: alkalmazásprogramozási interfész

és a rosszindulatú programok elleni intézkedéseket is. Biztonságos környezetet kínálnak azon partnervállalatok számára is, amelyek az IoT rendszerhez csatlakoztatott berendezéseket fejlesztik. [2]



2. számú ábra: Az IoT architektúra modell
Készítette: a szerző

A 2. számú ábrán látható architektúra modell esetében a felhő informatika mutatja azt a szintet, ahol erőforrásokat vásárlunk egy szolgáltatóktól, és az így rendelkezésünkre álló felhőbe feltölthetjük az adatokat tárolás, rendelkezésre állás és elemzés céljából. Itt történik az adatfeldolgozás.

Az edge informatika esetében az IoT eszközök (kamerák, szenzorok, egyéb információgyűjtő berendezések, rendszerek) közvetlenül adatfeldolgozó eszközökhöz kapcsolódnak. Ezek az eszközök egyszerűbb műveleteket végeznek a bejövő adatokon, mint például átalakítás, aggregálás vagy egyéb, kevésbé számítás igényes algoritmusok futtatása. Ezt a technológiát főként azokban az esetekben használják, amikor a beérkező adat digitálisan fel nem ismerhető formában érhető el az eszközök számára. Ebben az esetben az edge csomópontok digitálissá transzformálják a beérkező adatokat és továbbítják azokat a „fog réteg” felé,

további elemzésre. Az edge rétegben alapvetően a következő elemek találhatóak meg:

- IoT átjárók;
- ipari számítógépek;
- beágyazott rendszerek;
- szenzorok, vezérlők.

A fog informatika tartalmazza a felhő megoldások minden előnyét a rendelkezésre állásra, skálázhatóság, megbízhatóságra vonatkozóan, ugyanakkor miután nem a felhőben működik, hanem a felhasználóknál, így kiküszöböli a felhő két legnagyobb hiányosságát: a kapcsolati bizonytalanságot és késleltetést. Alkalmazása csökkenti a hálózati torlódásokat, mivel a fog csomópontok az IoT-eszközök és a felhő között helyezkednek el, és a fog informatikai számítások végrehajtása csökkenti a hálózati torlódásokat a felhőn. Mivel a begyűjtött és rendelkezésre álló adatok formátuma többféle is lehet így szintén előnyös, hogy a fog informatikai számítások rétegelt architektúrája javítja az elemzés minőségét, és így hozzájárul a döntéshozatali folyamatok támogatásához, az eredményesebb döntések meghozatalához. Szintén nagy előnye, hogy a fog csomópontok nagyon közel vannak a végfelhasználóhoz, és elvégzik a feldolgozást, így a csomópontok munkaterhelése a helyüknek megfelelő, ezáltal csökkenti a feldolgozási késleltetést, továbbá ha a rendszerünk bármilyen azonnali beavatkozást igényel, a helyben elhelyezett eszközök miatt a reagálás akár pillanatokon belül megtörténhet. A fog informatika tulajdonképpen arról szól, hogy az edge csomópontok által gyűjtött adatokon nagy számításigényű, komplex algoritmusokat futtassunk. A fog informatika által elérhető szolgáltatások:

- komplex eseményfeldolgozás;
- nagy mennyiségű valós idejű adatfeldolgozás;

- alkalmazott gépi tanulás;
- az előzetes adatok megjelenítése. [3]

Az AI és IoT összekapcsolásának előnyei

Az AI legnagyobb előnye ebben az összefüggésben az a képessége, hogy gyorsan és pontosan képes a kapott adatokból használható eredmények származtatására. A gépi tanulás, egy AI-technológia, lehetővé teszi az minták automatikus azonosítását és az intelligens érzékelők és eszközök által generált adatok rendellenességeinek észlelését - például hőmérséklet, nyomás, páratartalom, levegőminőség, rezgés és hang. Az AI-alapú IoT hozzájárulhat a működési hatékonyság javításához. Csakúgy, mint a gépi tanulás előre jelezheti a berendezés meghibásodását, az üzemi körülményeket és azonosíthatja azokat az paramétereket, amelyeket menet közben meg kell változtatni az ideális eredmények megőrzése érdekében, és képes felismerni az emberi szem számára láthatatlan és az egyszerű mérőeszközökön nem látható mintákat. Más AI technológiák, például a beszédfelismerés és a virtuális képi azonosítás, segíthetnek azonnali döntést hozni azon adatokból, amelyeknél az emberi felülvizsgálatot korábban megkövetelték.

Az IoT fejlesztése a mesterséges intelligenciával közvetlenül új termékeket és szolgáltatásokat is létrehozhat. A természetes nyelvfeldolgozás (Natural Language Processing: NLP) egyre kiforrottabb, és napjainkban már lehetővé teszi, hogy az emberek már egyes esetekben gépekkel beszéljenek, ahelyett, hogy emberi operátort igényelnének meg az adott szolgáltatások. Az AI által vezérelt drónok és robotok - amelyek képesek olyan helyekre is eljutni, ahova az emberek nem tudnának - teljesen új lehetőségeket kínálnak a megfigyelésre és ellenőrzésre, amelyek korábban egyszerűen nem voltak megvalósíthatóak.

Számos alkalmazás, amely párosítja az IoT-t és a mesterséges intelligenciát, segíti a szervezeteket a különféle kockázatok megértésében és előrejelzésében, valamint automatizálja a gyors reagálást, lehetővé téve számukra a munkavállalók biztonságának, a pénzügyi veszteségeknek és az internetes fenyegetéseknek a jobb kezelését.

Az okos otthoni kivitelezésekben a különféle eszközök és rendszerek, beleértve a hűtőket, a váltóáramot, a sütőt, a vízellátást, az áramellátást és az otthoni érzékelőkkel felszerelt biztonsági rendszereket, IoT alkalmazásokhoz kapcsolódó okos eszközök. Az AI itt automatikusan működő adatgyűjtő, -elemző és döntéshozó rendszerként működik. Csakúgy, mint az okos otthon koncepciója, az okos városok esetében is vitathatatlan az IoT és az AI technológiák alkalmazása. Mindkét technológia támogatja a vízgazdálkodást, a hulladékgazdálkodást, a vízelvezető rendszert, a szállítási rendszert, a parkolási rendszert, az elektromos hálózatokat, a közúti és vasúti kezelést, az egész város biztonsági és védelmi megoldásait stb.

Az egészségügy hatalmas mennyiségű hasznos adatot generál, és ezek egy jelentős részét az IoT eszközök szolgáltatják. Az AI folyamatosan hozzáfér és kezeli a rendelkezésre álló adatokat, és segítséget nyújt a személyügyi munkákban, a valós idejű döntéshozatalban, a készletgazdálkodásban, a kapcsolódó gyógyszertári szolgáltatásokban, valamint az előrejelzésekben. [4]

Összefoglaló

Az IoT és AI együttes alkalmazása már jelenleg is nagyon sok helyen és területen előfordul a világon. Hamarosan azonban csak nagyon ritkán fordul majd elő olyan IoT megvalósítás, amely nem használja az AI-t. Az International Data Corp. azt jósolja, hogy 2019-re az AI támogatni fogja az „összes hatékony” IoT tevékenységet, és AI nélkül a telepítésekből származó adatok „korlátozott értékkel bírnak” majd. Ez azt jelenti, hogy a hatalmas mennyiségű adat, amit az alkalmazott IoT eszközök és

rendszerek begyűjtenek a jövőben, hogy az az AI alkalmazása nélkül elemezhetetlen, ezáltal használhatatlan lesz. Ennek megfelelően a mindennapi életünk részeit képező okos eszközök nagyon nagy valószínűséggel a következő évtizedben mesterséges intelligenciákat fognak alkalmazni, melyek lényegesen gyorsabb és pontosabb adatfeldolgozást fognak eredményezni. Véleményem szerint a legnagyobb problémát az fogja jelenteni, hogy ez által az adataink egy mesterséges intelligencia által elemzésre, összegzésre, feldolgozásra kerülnek, így még szenzitívebb információkat kapunk, melyek a napjainkban is jellemző adatszivárogtatásoknak köszönhetően még nagyobb veszélyt jelenthetnek a privát, az üzleti és minden egyéb szférára, mely az adott adatokhoz kapcsolható. Ennek megfelelően a bizalmatlanság lehet az, ami a legnagyobb akadályt fogja gördíteni ezen képességek teljeskörű kiaknázását illetően.

Felhasznált irodalom

[1] NEC Corporation: Information Security Report 2018, July 2018

[2] NEC the WISE IoT Platform, https://www.nec.com/en/global/solutions/iot/iotplatform/index.html (letöltve: 2018. 07. 10.)

[3] Garima Joshi Assistant, Pooja Deshpande, Prasun Joshi: A Layered Architecture for Fog Computing for an Effective Real Time Data Processing, International Journal of Computer Applications (0975 – 8887) Volume 180 – No.36, April 2018

[4] i-Scoop: The interaction and convergence of IoT and AI at work, https://www.i-scoop.eu/internet-of-things-guide/iot-and-ai/ (letöltve: 2018. 07. 12.)

Szerzőink figyelmébe

Kiadványunk lehetőséget biztosít max. 40 ezer leütés (egy szerzői ív) terjedelemben – *elsősorban: távközlés, híradás, informatika, információvédelem, illetőleg hadtudományi és természettudományi témakörökben* – tanulmányok, szakcikkek magyar és idegen nyelvű megjelentetésére.

A cikknek tartalmaznia kell egy 2-5 soros absztraktot magyar és/vagy idegen nyelven.

A cikkek beküldése e-mailen a hhk_hirado_szakcsoport@uni-nke.hu címre lehetséges. A cikkek leadási határideje: folyamatos (megjelenés évente kétszer).

A megjelentetésre szánt cikkek csak a szerző(k) eddig máshol még meg nem jelent, saját önálló (társszerzők esetében közös) írásműve(i) lehetnek. Az írásművekben lévő idézeteknek meg kell felelniük a szerzői jogról szóló hatályos jogszabályoknak. A megjelentetésre szánt írásművek csak nyílt (nem minősített) információkat és adatokat tartalmazhatnak. Ezek minősített voltát a szerkesztőbizottság nem vizsgálja, ennek felelőssége a cikk szerzőjét terheli.

A szerkesztőbizottság a megjelentetésre szánt írásműveket lektoráltatja. A szerkesztőbizottság fenntartja a jogot, hogy a megjelentetésre szánt és megküldött írásművet – *külön indoklás nélkül* - megjelenésre alkalmatlannak ítélje. Az ilyen cikkeket nem küldi vissza, és nem őrzi meg.

A kiadványban lehetőség van idegen nyelvű cikkek megjelentetésére. Az idegen nyelven megjelentetésre szánt írásművek nyelvi lektorálása a szerzőt terheli.

Minden kézirathoz elektronikusan is mellékelni kell egy kitöltött "Kéziratbeküldési űrlap"-ot, és egy "Copyright átruházási űrlap"-ot. Mindkét űrlapot ki kell nyomtatni

és alá kell írni (többszerzős cikk esetében minden szerzőnek!), majd a kinyomtatott és aláírt űrlapokat faxon (fax szám: +36-1-432-9025), vagy postai úton levélben (levélcím: Hírvillám Szerkesztőség, 1581. Budapest Pf.: 15.) is meg kell küldeni a szerkesztőségnek. Ezek hiányában a cikkeket a szerkesztőség nem lektoráltatja és nem jelenteti meg!

Az űrlapok a szerkesztőségnél szerezhetők be.

Felelős kiadó: Dr. Fekete Károly mk. alezredes
Megjelent az NKE HHK Híradó Tanszék gondozásában, 10 példányban, illetve elektronikusan:

www.comconf.hu
www.puskashirbaje.hu

HU ISSN 2061-9499

***

NKE HHK Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf. 15.
+36 1 432 9000 (29-407 mellék)
hhk_hirado_szakcsoport@uni-nke.hu