ALVERAD
SECURITY TESTING LABORATORY

II. ALVERAD-BÁNKI

Nemzetközi Kiberbiztonsági Konferencia

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS
BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Budapest, 2024. október 15.

II. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencia

II. Alverad-Bánki International Cybersecurity Conference

Konferenciakötet - Book of abstracts

Kiadó / Publisher: Óbudai Egyetem, valamint az Alverad Technology Focus Kft. Kutatás, fejlesztés és innováció Üzletág

Felelős kiadó / Editor-in-Chief: Prof. Dr. Rajnai Zoltán

Szerkesztette / Edited by: Dr. Répás József

Műszaki szerkesztő / Technical Editor: Horváth Richárd

ISBN 978-963-449-372-3

Köszöntő

Az Alverad Technology Focus Kft. és az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Kara az Európai Kiberbiztonsági hónap keretében 2024. október 15-én második alkalommal rendezte meg hibrid formában nemzetközi tudományos konferenciáját.

A konferencia célja volt, az Európai és hazai kiberbiztonsági szabályozás feldolgozása és ismertetése, a legújabb hazai és nemzetközi kutatási eredmények elérhetővé tétele. Ezen túlmenően lehetőség biztosítása a kutatók, a PhD hallgatók számára a publikációs gyakorlat megszerzésére, valamint a társegyetemek oktatói és hallgatói, kollégáink tudományos kapcsolatai elmélyüljenek.

Az előadók névsora, a helyszín, a kísérőprogramok, valamint a szervezők elismertsége ismét garantálta a hiánypótló és hasznos rendezvényt. Az előadások témagazdagsága és sokszínűsége hűen tükrözi napjaink kiberbiztonsági kihívásokban gazdag időszakát, illetve a legújabb kutatási trendeket és irányokat.

Ezúton szeretnénk köszönetet mondani elsősorban az előadóknak, különös tekintettel azokra, akik a tavalyi alkalom után, idén is részt vettek konferenciánkon. Külön köszönet mindazoknak, akik részt vettek az esemény megvalósításában, támogatták, valamint ösztönzésükkel és segítségükkel nagyban hozzájárultak a konferencia sikeréhez és e kiadvány megjelenéséhez.

Budapest, 2024. december 20.

Hinkel Attila	Prof. Dr. Rajnai Zoltán
Ügyvezető	Dékán

Greetings

As part of the European Cyber Security Month, the Banki Donát Faculty of Mechanical and Safety Engineering (Óbuda University) and Alverad Technology Focus Ltd. organised their second international scientific conference in a hybrid format on 15 October 2024.

The aim of the programme was to analyse and present European and national cyber security legislation and to make available the latest national and international research results. It also provided an opportunity for researchers and PhD students to gain publication experience and to deepen academic contacts between teachers and students from the partner universities and our colleagues.

The list of speakers, the location, the supporting programmes and the reputation of the organisers once again guaranteed a gap-filling and useful occasion. The richness and variety of the presentations faithfully reflected the challenging times in cybersecurity today and the latest research trends and tendencies.

We would like to thank the lecturers, especially those returning after last year. A special appreciation goes to all those who were involved in organising and whose encouragement and support contributed greatly to the success of the event and the publication of this brochure.

Budapest, December 20, 2024.

Attila Hinkel
CEO

Prof. Dr. Zoltán Rajnai
Dean

Szervezőbizottság / Organizing Committee

Tiszteletbeli elnök / Honorary chair

Hinkel Attila (Alverad Technology Focus Kft.)

Általános elnök / General chair

Prof. Dr. Rajnai Zoltán (Óbudai Egyetem – ÓE BGK)

Általános társelnök / General co-chair

Dr. Számadó Róza (Óbudai Egyetem – ÓE BGK)

Tudományos bizottság elnöke / Scientific Committee chair

Prof. Dr. Berek Lajos (Óbudai Egyetem – ÓE BGK)

Tudományos bizottság / Scientific Committee

Dr. Kovács László, (Nemzeti Közszolgálati Egyetem / National University of Public Service – NKE)

Dr. Alexin Zoltán (Szegedi Tudományegyetem – SZTE)

Dr. Berek Tamás (Nemzeti Közszolgálati Egyetem / National University of Public Service – NKE)

Dr. Huszti Andrea (Debreceni Egyetem / Debrecen University – DE)

Dr. Hidvégi Timót (Széchenyi István Egyetem / Széchenyi István University – SZE)

Dr. Krasznay Csaba (Nemzeti Közszolgálati Egyetem – NKE)

Dr. Répás József (Nemzeti Közszolgálati Egyetem / National University of Public – NKE)

Dr. Török Árpád (Budapesti Műszaki Egyetem – BME)

Dr. Wersényi György (Széchenyi István Egyetem / Széchenyi István University – SZE)

Tartalomjegyzék / Contents

Plenáris szekció

Plenary session

Plenáris szekció

A NIS2 KÖZVETLEN HATÁSAI A KRITIKUS INFRASTRUKTÚRÁRA ÉS AZ ÁLLAMI SZEKTORRA

OROSHÁZI Dávid

Az előadás célja, hogy röviden bemutassa a kritikus infrastruktúra és az állami szektor vonatkozásában a Magyarországon hatályos és a NIS2 implementációját követő jövőbeli jogszabályi elvárásokat. A jelenlegi szabályok szerinti kritikus infrastruktúra fogalom értelmezési kereteit az Lrtv. szabja meg, az állami szektor fogalom pedig a Ibtv. hatályának vizsgálata alapján válik értelmezhetővé. Az érvényben lévő kiberbiztonsági elvárásrendszer alapjait az Ibtv. és a 41/2025. BM rendelet által megfogalmazott védelmi intézkedések jelentik a vizsgált szektorok vonatkozásában. A NIS2 transzpozícióját követően az elvárásrendszer átalakul, a keretszabályokat a Magyarország kiberbiztonságáról szóló törvény tartalmazza majd, a megvalósítandó konkrét védelmi intézkedéseket pedig a vizsgált szektorok vonatkozásában 2025. január 1-től a 7/2024. MK rendelet határozza meg.
A helyzetet árnyalja, hogy a Kibertantv. fokozatosan hatályba lépő, szintén a 7/2024. MK. rendeletre alapozott előírásai már most is érintik a kritikus infrastruktúra kiberbiztonságát.

Kulcsszavak:

Ibtv., 41/2015. BM rendelet., Kibertan törvény, 7/2024. MK rendelet, védelmi intézkedések

Plenary session

THE DIRECT IMPACT OF NIS2 ON CRITICAL INFRASTRUCTURE AND THE PUBLIC SECTOR

Dávid OROSHÁZI

The aim of the presentation is to briefly summarize the current and future legal requirements for critical infrastructure and the public sector in Hungary following the implementation of NIS2. The definition of critical infrastructure under the current legislation is derived from the Hungarian Critical Infrastructure law and the term public sector is based on the Information Security law (IBtv.). The security controls formulated by the Ibtv and the BM 41/2025 regulation are the basis of the current cybersecurity framework in the examined sectors. Following the adoption of NIS2, the requirements will change, the regulatory framework will be set out in the new Hungarian Cybersecurity Act, and the specific security controls will be defined in the Decree MK 7/2024 as of 1 January 2025 for the designated sectors.

The picture is further complicated by the fact that the Cybersecurity Certification Act provisions, which enter into force gradually and is also based on Decree MK 7/2024, already affect the cybersecurity of critical infrastructure.

Keywords:

NIS2, Cybersecurity Certification Act, Decree MK 7/2024, security controls

Plenáris szekció

KIBERBIZTONSÁG ÉS ADATVÉDELEM - INCIDENSEK A NAIH GYAKORLATÁBAN

ESZTERI Dániel

Az Európai Unió általános adatvédelmi rendelete, a GDPR egyik leggyakrabban hivatkozott jogintézmény-csoportja az adatvédelmi incidensekhez kapcsolódó kötelezettségeket és eljárásokat tartalmazza. Az előadás első fele az adatvédelmi incidensek, mint személyes adatokat érintő biztonsági események fogalmának a tisztázásával és az ehhez kapcsolódó adatkezelői kötelezettséggel indított, kitérve annak az adatkezelés biztonságával összefüggő szoros kapcsolatára. A fogalmi keretek tisztázása után a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (NAIH) bejelentett adatvédelmi incidensek eddigi statisztikái és az azokból kiolvasható trendek kerültek ismertetésre. Az előadás a második felében a NAIH adatvédelmi incidensekkel kapcsolatos eddigi hatósági gyakorlatából ismertetett néhány szakmai szempontból tanulságosabb esetet.

A fő konklúzió ezzel kapcsolatban, hogy a személyes adatok kezelésére használt rendszerek és környezet biztonságos kialakítása kulcsszerepet játszik az incidensek elkerülésében. A NAIH incidensekkel kapcsolatos hatósági felügyelete szempontjából az incidens megfelelő kezelésén és az esetleges biztonsági hiányosságok adatkezelői felülvizsgálatán és kijavításán van a hangsúly. Önmagában egy incidens bekövetkezése miatt még nem merül fel a GDPR megsértésének gyanúja, az adatkezeléshez használt rendszerek régóta elavult vagy hanyagul kezelt biztonsági komponensei már sokkal nagyobb problémát jelentenek és általában ezek szokták megalapozni egy-egy jogsértés és bírságolás alapját.

Keywords:
GDPR, adatbiztonság, adatvédelmi incidens, NAIH, hatósági gyakorlat

Plenary session

CYBERSECURITY AND DATA PROTECTION – DATA BREACHES IN THE PRACTICE OF THE HUNGARIAN DATA PROTECTION AUTHORITY

Dániel ESZTERI

One of the most frequently cited group of legal institutions in the European Union's General Data Protection Regulation (GDPR) contains obligations and procedures related to data breaches. The first part of the presentation started with the clarification of the concept of personal data breaches as security incidents affecting personal data and the related obligations of the data controller, including its close connection with the security of data processing. After clarifying the conceptual framework, the statistics of data breaches reported to the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) and the trends that can be gleaned from them were presented. In the second half of the presentation some of the most instructive cases from the practice of the NAIH related to data breaches were presented. The main conclusion was that the secure design of systems and environments used to process personal data plays a key role in avoiding incidents. From the point of view of NAIH's official supervision of data breaches, the emphasis is also on the proper handling of the breach and the correction of possible security deficiencies by the data controller. The mere occurrence of a data breach does not constitute the violation of the GDPR in itself. The long-outdated or negligently managed security components of systems used for data processing are a much bigger problem, and they usually form the basis for the established infringement and fine in a NAIH decision.

Kulcsszavak:

GDPR, data security, data breach, NAIH, official practice

Plenáris szekció

KIBERBIZTONSÁGI JOGSZABÁLYI KÖRNYEZET IPARBIZTONSÁGI HATÁSA

HINKEL Attila

A hazai kialakítás alatt lévő és új kiberbiztonsági követelményekkel kapcsolatban jellemzően az informatikai rendszerek, elektronikus információs rendszerek kerülnek górcső alá. Az érintett szervezetek azonban nem csupán IT rendszerekkel rendelkeznek, jellemzően használnak különböző ipari/gyártó rendszereket is, melyek kiberbiztonságáról szintén gondoskodni kell. Míg az IT rendszerek esetén a bizalmassági, sértetlenségi és rendelkezésre állási szempontok hangsúlyosak, ipari rendszerek esetén a bizalmasság mellett az üzembiztonság és a megbízhatóság a két legfontosabb szempont, ami jelentős különbséget eredményez a védelem kialakítása során. Egyes követelmények ipari rendszerek esetén nem értelmezhetőek/megvalósíthatóak, vagy rendszerre szabott módon, illetve helyettesítő kontrollok kialakításával lehetséges. Az előadás során összehasonlításra kerülnek az informatikai és ipari rendszerek, például az összetevők, működés, életciklus vagy biztonsági koncepció szempontjából. Emellett bemutatásra kerülnek a NIST 800-53 és 800-82 szabványok, melyek a hazai jogi szabályozás hátterét is adják.

Kulcsszavak:
NIS2, kiberbiztonság, 7/2024. MK rendelet, védelmi intézkedések

Plenary session

THE EFFECT OF THE CYBERSECURITY LEGAL ENVIRONMENT ON INDUSTRIAL SECURITY

Attila HINKEL

In relation to developing and new cybersecurity requirements at national level, the focus is typically on IT systems and electronic information systems. However, the organisations concerned do not only have IT systems, but also typically use various industrial/manufacturing systems, the cybersecurity of which also needs to be ensured. While for IT systems, confidentiality, integrity and availability are the most important factors, for industrial systems, in addition to confidentiality, operational security and reliability are the two most important aspects, which leads to a significant difference in the development of security. Some requirements cannot be interpreted / implemented in industrial systems or can be met by system-specific or compensating controls. The presentation will compare IT and industrial systems, e.g. in terms of components, operation, life cycle or security concepts. In addition, the NIST 800-53 and 800-82 standards will be introduced, which also provide the background for hungarian national legislation.

Keywords:
NIS2, cybersecurity, 7/2024. MK, security control

Kiberbiztonság - I. szekció – NIS2

Cybersecurity - session I.– NIS2

Kiberbiztonság - I. szekció – NIS2

KIBERMŰVELETEK ÉS A HONVÉDELEM

BALOGH Péter

A modern hadviselés egyre inkább digitális technológiákra és kibertérre épül, átformálva a honvédelem és nemzetbiztonság fogalmát. Az előadás bemutatja a kiberműveletek szerepét a honvédelemben, a kiberhadviselés stratégiáit, támadó és védekező műveleteit, valamint a kiberbiztonság fontos aspektusait a nemzetközi katonai együttműködésben. Kitér a jogi és etikai kérdésekre, valamint arra, hogy a kiberfenyegetések milyen új képességeket és képzési igényeket támasztanak a fegyveres erők számára. Végül, áttekinti a kiberhadviselés integrációját a hagyományos katonai műveletekbe és a jövőbeli trendeket.

Kulcsszavak:
kiber műveletek, kiberhadviselés, honvédelem, Magyar Honvédség

Cybersecurity - session I.– NIS2

CYBER OPERATIONS AND NATIONAL DEFENCE

Péter BALOGH

Modern warfare increasingly depends on digital technologies and cyberspace, reshaping defense and national security. This presentation will explore the role of cyber operations in defense, highlighting key challenges and opportunities. It will cover cyber warfare strategies, offensive and defensive operations, and crucial cybersecurity aspects in international military cooperation. Additionally, it will address the legal and ethical issues of cyber operations and the new skills and training needed for managing cyber threats. Lastly, the presentation will examine how cyber warfare integrates with traditional military operations and future trends in this evolving field.

Keywords:
cyber Operations, cyber warfare, national defence, Hungarian Defence Forces, multi domain

Kiberbiztonság - I. szekció – NIS2

A NIS 2 EURÓPAI UNIÓS IRÁNYELV ESETE A KIBERBIZTONSÁGI TUDATOSÍTÁSSAL

BOR Olivér

A szerző tanulmányában azt vizsgálja, hogy az Európai Unió NIS 2 irányelve és annak nemzeti végrehajtása kapcsán milyen összefüggések, feladatok várnak az érintett cégekre a kiberbiztonsági tudatosítás terén, illetve a közösségi média miként képes mindezt támogatni. A NIS 2 Európai Uniós irányelv célja az Unió kiberbiztonsági szintjének növelése, különösen az olyan ágazatokban, amelyek kritikusak a társadalom és a gazdaság működése szempontjából. A digitalizációval együtt járó kiberbiztonsági kihívásokra való felkészülés és a tudatosítás kiemelt fontossága mára már egyértelművé vált, mivel a kibertámadások száma és komplexitása az elmúlt években folyamatosan növekedett. A kiberbűnözők gyakran a technikai sebezhetőségek helyett azonban a felhasználók tudáshiányára, figyelmetlenségére építenek, ami azt jelenti, hogy az eredményes védekezésben kulcsszerep hárul az oktatásra és a tudatosításra. Az információbiztonság növelése érdekében az érintett szervezeteknek átfogó képzési programokat kell biztosítaniuk munkavállalóik számára, a tagállamok kiberbiztonság erősítéséért felelős állami szervezeteinek pedig szükségszerűen szerepet kell vállalniuk a tudatosító tevékenységben. Mindezek tekintetében a közösségi média jelentős szerepet játszhat a kiberbiztonsági tudatosításban, mivel széles körben és gyorsan képes elérni az embereket.

Kulcsszavak:
kiberbiztonság, NIS2, szabályozás, tudatosítás

Cybersecurity - session I.– NIS2

THE CASE OF NIS 2 EUROPEAN UNION DIRECTIVE WITH CYBER SECURITY AWARENESS

Olivér BOR

The author's study examines the implications and responsibilities that companies face in terms of cybersecurity awareness in light of the European Union's NIS 2 Directive and its national implementation, and how social media can support these efforts. The goal of the NIS 2 Directive is to enhance cybersecurity levels within the EU, particularly in sectors critical to the functioning of society and the economy. The importance of preparedness for cybersecurity challenges associated with digitalization, as well as awareness-raising, has become increasingly clear, as the number and complexity of cyberattacks have been steadily rising in recent years. Cybercriminals often exploit user ignorance and inattention rather than technical vulnerabilities, highlighting the critical role of education and awareness in effective defense. To enhance information security, organizations must provide comprehensive training programs for their employees, while state organizations responsible for strengthening national cybersecurity must play an active role in awareness-raising activities. In this context, social media can play a significant role in cybersecurity awareness, as it can quickly and widely reach a large audience.

Keywords:
cybersecurity, NIS2, regulation, awareness

Kiberbiztonság - I. szekció – NIS2

A FEJLESZTŐK LEGGYAKORIBB HIBÁI: HOGYAN NYITUNK AJTÓT A HACKEREKNEK?

KISS Tamás László

Az előadás során bemutatásra kerülnek a kiberbiztonság jogi keretrendszerének hiányosságai, melyek különösen veszélyesek, hiszen a biztonsági rések gyakran már a tervezési és fejlesztési szakaszban kialakulnak. Az elmúlt időszak nagyobb incidensei is rámutatnak, hogy biztonságos fejlesztési módszertanok alkalmazása nélkül, a fejlesztők biztonságtudatossági szintjének növelése nélkül kritikus biztonsági rések maradhatnak rendszereinekben. A technológiai fejlődés egyre összetettebb problémák elé állítja a fejlesztőket. A mesterséges intelligencia, a kvantumszámítógépek és az IoT-eszközök terjedése újfajta támadások megjelenését eredményezik, amelyeket csak innovatív, biztonságtudatos megoldásokkal lehet kezelni. A biztonsági problémák hatékony kezeléséhez alapvető, hogy a fejlesztők megfelelő képzésben részesüljenek. A sérülékenységvizsgálatok rendszeres elvégzése segíthet a biztonsági rések időben történő azonosításában. A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet térítésmentes sérülékenységvizsgálati szolgáltatása jól mutatja, hogy az állami és magánszféra együttműködése hogyan segítheti a rendszerek ellenállóbbá tételét. Az innovatív megoldások és az együttműködés az iparági szereplőkkel biztosíthatják, hogy a rendszerek lépést tartsanak a folyamatosan változó fenyegetésekkel.

Kulcsszavak:
sérülékenységvizsgálat, biztonságtudatos programozás, képzés, jogszabályi környezet.

Cybersecurity - session I.– NIS2

THE MOST COMMON MISTAKES DEVELOPERS MAKE, OR HOW DO WE OPEN THE DOOR TO HACKERS?

Tamás László KISS

The presentation will highlight the weaknesses in the legal framework for cybersecurity, which are particularly dangerous as vulnerabilities often arise at the design and development stage. Recent major incidents also show that without the use of secure development methodologies and without raising the level of security awareness among developers, critical vulnerabilities can remain in our systems. Technological advances pose increasingly complex problems for developers. The growth of artificial intelligence, quantum computing and IoT devices is leading to new types of attacks that can only be addressed with innovative, security-conscious solutions. To effectively address security issues, it is essential that developers are properly trained. Regular vulnerability scans can help identify vulnerabilities in a timely manner. The Special Service for National Security (SSNS) National Cyber-Security Center's free vulnerability assessment service demonstrates how public-private collaboration can help to make systems more resilient. Innovative solutions and collaboration with industry actors can ensure that systems keep up with the constantly changing threats.

Keywords:
vulnerability assessment, security-conscious programming, training, regulatory environment

Kiberbiztonság - I. szekció – NIS2

NIS2 FELKÉSZÜLÉS GYAKORLATI TAPASZTALATAI

SÁNDOR Zsolt András

A NIS2 irányelv az európai kiberbiztonság megerősítését célozza, növelve a kritikus szolgáltatások kiberbiztonsági követelményeit. A felkészülés során a szervezeteknek kockázatelemzést kell végezniük, és ki kell alakítaniuk egy átfogó kibervédelmi stratégiát. A tapasztalatok szerint az egyik legnagyobb kihívás a szabályozások értelmezése és a megfelelő technológiai megoldások integrálása. Fontos a folyamatos incidenskezelési terv kialakítása és a jelentési kötelezettségek betartása, hiszen a gyors reagálás kulcsfontosságú. A NIS2 felkészülés során kiemelt szerepet kap az emberi tényező, hiszen a munkatársak képzése és tudatossága alapvető a sikeres védelemhez. Az előadásban szó lesz arról, hol tartanak a magyar cégek, értékeljük és pozícionáljuk a 7/2024 MK rendeletet az cégek felkészültsége, az ISO 27001 elvárásai és az iparági good practis-hoz képest, összességében értékeljük mennyire lesz bevezethető a célcsoportba tartozó vállalkozásoknál. Bemutatjuk, egy -két példán keresztül a legnagyobb technikai, szervezési és szabályozási kihívást, továbbá megemlítjük a saját tapasztalat alapján a legnagyobb költséget jelentő elvárásokat. Bemutatjuk a felkészítő módszertanokat, azok előnyét és hátrányát, így mindenki el tudja majd dönteni, hogy milyen típusú támogató csapatot választ a felkészüléshez. Végezetül értékeljük a jelenleg ismert auditorokat és megosztjuk a hallgatósággal a feltételezéseinket és gondolatainkat a várható tanúsításokról.

Kulcsszavak:
NIS2 irányelv, kockázatkezelés, incidenskezelési terv, kiberbiztonság

Cybersecurity - session I.– NIS2

PRACTICAL EXPERIENCES OF NIS2 PREPARATION

Zsolt András SÁNDOR

The NIS2 Directive aims to strengthen European cybersecurity by increasing cybersecurity requirements for critical services. During the preparation, organizations must conduct risk assessments and develop a comprehensive cyber defense strategy. Experience shows that one of the biggest challenges is interpreting the regulations and integrating appropriate technological solutions. It is crucial to establish a continuous incident management plan and comply with reporting obligations, as rapid response is key. The human factor plays a prominent role in NIS2 preparation, as employee training and awareness are essential for successful protection. The presentation will discuss the current status of Hungarian companies, evaluate, and position the 7/2024 MK regulation in comparison to company preparedness, ISO 27001 expectations, and industry best practices. We will assess how implementable it will be for businesses within the target group. We will present, through one or two examples, the biggest technical, organizational, and regulatory challenges, as well as mention the most costly requirements based on our experience. We will introduce the preparation methodologies, highlighting their advantages and disadvantages, enabling everyone to decide what type of support team to choose for the preparation. Finally, we will evaluate the currently known auditors and share our assumptions and thoughts regarding the expected certifications.

Keywords:
NIS2 Directive, risk mamagement, incident management plan, cybersecurity

Kiberbiztonság - I. szekció – NIS2

NIS2 - AZ ÚJ KIBERSZABÁLYOZÁS

MARSI Tamás

A NIS2 irányelv -az Európai Unió új kiberbiztonsági szabályozása- célja az EU kiberbiztonsági szintjének emelése és a kritikus szektorok lefedése, mint például az energia, közlekedés, egészségügy, digitális infrastruktúra, valamint a pénzügyi és banki szektor. Az irányelv új alapvető és fontos ágazatokat határoz meg, szigorúbb követelményeket támaszt a kibervédelmi intézkedések, kockázatkezelési rendszerek, valamint az incidensjelentések terén.

A NIS2 szigorúbb jogi következményeket vezet be, például pénzbírságokat, felelősségre vonást, és fokozott ellenőrzéseket, miközben a kockázatalapú megközelítésre helyezi a hangsúlyt. Az ellátási lánc biztonsága kiemelt fontosságú, amely a beszállítói kockázatok kezelését és a harmadik felek kibervédelmi megfelelését is magában foglalja. Az EU-tagállamok közötti együttműködés és információmegosztás szintén kulcsfontosságú, amit a közös kockázatértékelések és a kötelező információmegosztás biztosítanak.

A törvény hatálya jelentősen bővült, új definíciókat és szereplőket vezetett be, például központi szolgáltatók és rendszerek, valamint többségi állami befolyás alatt álló szervezetek bevonásával. Az NIS2 továbbá szigorúbb felügyeletet és kötelező gyakorlatokat ír elő, beleértve az EU-CyCLONe válságkezelési mechanizmusát.

Kulcsszavak:
NIS2, kiberbiztonság, incidens jelentés, ellátási lánc biztonsága, kritikus szektorok, kritikus infrastruktúra

Cybersecurity - session I.– NIS2

NIS2 – THE NEW CYBERREGULATION

Tamás MARSI

The NIS2 Directive, the European Union's new cybersecurity regulation, aims to enhance the cybersecurity level across the EU by expanding its scope to cover critical sectors such as energy, transportation, healthcare, digital infrastructure, and the financial and banking sectors. The directive introduces a distinction between essential and important sectors and enforces stricter requirements for cybersecurity measures, risk management systems, and incident reporting.

NIS2 imposes stricter legal consequences, including fines, accountability measures, and enhanced oversight, while emphasizing a risk-based approach to cybersecurity. The directive highlights the importance of supply chain security, requiring management of supplier risks and compliance with cybersecurity standards across the entire supply chain. Collaboration and information sharing among EU Member States are prioritized through joint risk assessments and mandatory information-sharing protocols.

The directive's scope has significantly expanded to include new definitions and actors, such as central service providers, state-controlled organizations, and key infrastructure operators. Additionally, NIS2 mandates stricter oversight of cybersecurity developments, compulsory exercises, and integrates crisis management mechanisms like the EU-CyCLONe framework.

Keywords:

NIS2, cybersecurity, incident reporting, supply chain security, critical sectors, critical infrastructure

Kiberbiztonság - II. szekció – Kibervédelem I.

Cybersecurity - session II.– Cyber defence I.

Kiberbiztonság - II. szekció – Kibervédelem I.

EGY MERÉNYLETKÍSÉRLET NARRATÍV HÁLÓZATAI

BÁNYÁSZ-VÁCZI Kincső Boróka

A 2024 nyarán bekövetkezett Donald Trump elleni merénylet jelentős társadalmi reakciókat váltott ki, és számos összeesküvés-elmélet megjelenését eredményezte a közvélemény körében. Az eseményeket követően különböző politikai csoportok és ideológiai irányzatok különféle narratívákat alakítottak ki, gyakran saját politikai céljaik és érvrendszerük mentén torzítva a valóságot. A merénylet után nagyszámú videó jelent meg a YouTube platformján, amelyek eltérő elméleteket vázoltak fel a merénylet hátteréről. A kutatás célja e tartalmak elemzése, amely során a szerző a merénylethez kapcsolódó kulcsszavak alapján gyűjtött le több, mint 52.000 YouTube videókhoz fűzött kommentet. Ezeket a kommenteket tartalomelemzés, majd hálózatelemzés módszertanával vizsgálta a kommentelők közötti interakciókat és kapcsolatokat. A kutatás központi kérdése az volt, hogy milyen mintázatok és jellegzetességek azonosíthatóak a kommentek tartalmában és a felhasználók közötti hálózati struktúrákban.

Kulcsszavak:
Donald Trump, YouTube, tartalomelemzés, hálózatelemzés, merényletkísérlet

Cybersecurity - session II.– Cyber defence I.

NARRATIVE NETWORKS OF AN ASSASSINATION ATTEMPT

Kincső Boróka BÁNYÁSZ-VÁCZI

The attempted assassination of Donald Trump during the summer of 2024 sparked significant public controversy and gave rise to various conspiracy theories. In the aftermath, different political factions and belief systems constructed divergent narratives, often distorting reality to align with their particular agendas. Subsequent to the incident, a substantial number of videos emerged on the YouTube platform, each presenting distinct theories regarding the circumstances surrounding the assassination. This research aimed to scrutinize this content, encompassing an aggregation of over 52,000 comments from YouTube videos featuring keywords related to the assassination. Through the use of content analysis and network analysis methodologies, the comments were examined to explore the interactions and connections between commentators. The primary objective of the research was to discern patterns and attributes within the content of the comments and the network structures involving users.

Keywords:
Donald Trump, YouTube, content analysis, network analysis, assasination attempt

Kiberbiztonság - II. szekció – Kibervédelem I.

NEMZETI KIBERVÉDELEM TÁMOGATÁSA AUTOMATIZÁLT SÉRÜLÉKENYSÉGVIZSGÁLÓ RENDSZERREL

MILÁNOVICS Krisztián

A kiberbiztonság terén különösen fontos szerepet kap a rendszeres, megelőző sérülékenységvizsgálat, amelynek célja, hogy feltárja és kijavítsa a rendszer gyenge pontjait, mielőtt azok kihasználhatóvá válnának. A digitalizáció térhódításával egyre több szervezet szolgáltatása, de akár reputációja is függ a nyílt internetről elérhető szerverektől és alkalmazásoktól. Ezek a rendszerek felhasználóik részére hatalmas előnyöket biztosítanak, ugyanakkor nyílt támadási felületük által, számos kockázatot is hordoznak magukban.

Az ebből fakadó veszélyekre nem csak a magánszektorban, hanem állami szinten is hatékony, az igényeket támogató, ugyanakkor a kor műszaki- és jogszabályi környezetébe egyaránt illeszkedő megoldások kialakítása szükséges. Az előadás során áttekintésre kerülnek a nyílt internetes szolgáltatások üzemeltetésével kapcsolatos fő biztonsági problémák, bemutatva a Nemzeti Kibervédelmi Intézet szerepét és Automatizált Sérülékenységvizsgálati megoldását ügyfelei részére.

Kulcsszavak:

állami kibervédelem, sérülékenységvizsgálat, automatizált szolgáltatás, ASR

Cybersecurity - session II.– Cyber defence I.

SUPPORTING NATIONAL CYBER DEFENSE WITH AUTOMATED VULNERABILITY TESTING SYSTEMS

Krisztián MILÁNOVICS

In the field of cyber security, regular, preventive vulnerability testing plays a particularly important role, the purpose of which is to reveal and correct weak points in the system before they become exploitable. With the spread of digitalization, the services and even the reputation of more and more organizations depend on servers and applications available from the public Internet. These systems provide enormous benefits to their users, but at the same time, they also carry many risks due to their open attack surface!

To mitigate the resulting dangers, effective solutions need to be deployed not only in the private sector, but also at the state level, which at the same time should fit into the technical and legal environment. During the presentation, the main security problems related to the operation of open Internet services will be reviewed, while presenting the role of the National Cyber Security Center and its Automated Vulnerability Detection service created for its customers.

Keywords:

government cyber defense, vulnerability detection, automated service, ASR

Kiberbiztonság - II. szekció – Kibervédelem I.

BIZTONSÁGOSAN HASZNÁLHATÓK A HIVATÁSOS ÁLLOMÁNYBAN LEVŐK ÁLTAL A MŰKÖDÉSBEN LEVŐ PLATFORMOK?

AVORNICULUI Mihai-Constantin

A platformok felemelkedése egyértelműen összefüggésben van a digitalizációval, valamint az internet megjelenésével. Elmondhatjuk, hogy a közösségi platformok napjaink meghatározó kommunikációs eszközévé vált. Így a hivatásos állományban levő katonák és más rendvédelmi feladatokat ellátók rendelkeznek akár saját, akár munkahelyi mobil eszközzel, amelyen elérhetők bizonyos közösségi platformok (Telegram, WhatsApp, Viber, stb.), amelyek nincsenek letiltva. Emiatt vizsgálni kell, hogy ezek milyen körülmények között használhatók biztonságosan a mindennapi feladatvégzés során. A platformok biztonsága az ezekbe bekerülő, bennük létrehozott, tárolt, feldolgozott, továbbított stb. adatok és információk biztonságát kiterjeszti az azokat kezelő rendszerekre is. A platformok használata esetében fontos tárgyalni ezek biztonságát, ugyanis ez garantálja a rendszerben tárolt adatok és információk bizalmasságát, sértetlenségét és rendelkezésre állását. Tehát gyakorlatilag informatikai biztonságról van szó, amely a kiberbiztonság egy szegmese. A WhatsApp például a végponttól végpontig titkosított (E2EE) kommunikációt biztosítja, ahol a feladón és a címzetten kívül egyetlen fél sem tudja elolvasni vagy módosítani a küldött üzeneteket. Így azok a közösségi platformok, amelyek a végponttól végpontig titkosított kommunikációt biztosítják, biztonságosan használhatók a hivatásos állományban lévők által, hogyha betarják az adatvédelmet és a további hatályos speciális jogszabályokat, amelyek a tevékenységüket szabályozza.

Kulcsszavak:
közösségi platform, informatikai biztonság, végponttól-végpontig titkosítás, adatvédelem

Cybersecurity - session II.– Cyber defence I.

CAN THE PLATFORMS BE SECURELY USED BY MILITARY PERSONNEL?

Mihai-Constantin AVORNICULUI

The rise of platforms is clearly connected to digitalization and the rise of the internet. It can be said, that social platforms have become the defining communication tools of our time. As a result, military personnel and other law enforcement officials in active service may possess personal or work-related mobile devices that provide access to certain social platforms (Telegram, WhatsApp, Viber, etc.), which are not restricted. This necessitates an examination of the circumstances under which these platforms can be safely used during daily tasks. The security of platforms extends to the security of the data and information that is stored, processed or transmitted through them, which also impacts the systems managing these platforms. When discussing the use of platforms, their security must be a focal point, as this ensures the confidentiality, integrity, and availability of data and information stored within the system. Essentially, this involves IT security, which is a subset of cybersecurity. For example, WhatsApp provides end-to-end encryption (E2EE), ensuring that only the sender and the recipient can read or modify the messages sent, with no other parties able to do so. Therefore, social platforms that offer end-to-end encrypted communication can be used safely by professional personnel, in case they comply with data protection regulations and the other relevant legal frameworks that govern their activities.

Keywords:
social platform, IT security, end-to-end encryption, data protection

Kiberbiztonság - II. szekció – Kibervédelem I.

EGY PUBLIKUS FELHŐSZOLGÁLTATÁS BIZTONSÁGI KONTROLLJAI EGY PÉNZINTÉZETNÉL

OLÁH István György, MAGYAR Sándor

Napjainkban a felhő technológiával kialakított informatikai szolgáltatások rohamosan terjednek. Ennek alapvető okai az egyre gyorsuló innovációból származó folyamatosan növekvő igény az informatikai erőforrásokra, az egyre komplexebb tudást igénylő IT rendszerek. Egy szerver kiszolgálót beszerezni, üzemebe állítani, az üzemeltetési feladatokat kialakítani, a szakembereket kiképezni több hét, hónap is lehet saját telephelyen. Ezzel szemben ugyanazt az erőforrást üzemeltetéssel együtt a felhőszolgáltatás pár perc alatt biztosítja. Amennyiben egy szervezet igénybe vesz felhő szolgáltatást, akkor arra célszerű a rendelkezésre állási és biztonsági feltételeket is meghatározni, mert ezen informatikai elemek ugyanúgy részei a működési ökoszisztémának. Egy publikus felhőszolgáltató egy pénzintézet ellátási láncának része lehet. Ez a felfogás jelenik meg a 2023. januárban hatályba lépett CER-ben, NIS2-ben, valamint a DORA előírásokban. 2024-ben az informatikai rendszerekkel kapcsolatosan jelent meg, a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. MK rendelet. A publikáció fő témája az, hogy miként lehet alkalmazni az előírt kontrollokat egy publikus felhő szolgálatás estében egy pénzintézetnek. A hipotézisünk szerint igen, de ehhez a korábban megszokott bizonyosság-szerzési módszerek helyett más ellenőrzési módszereket szükséges alkalmazni.

Kulcsszavak:

NIS2, audit, publikus felhő, pénzintézet

Cybersecurity - session II.– Cyber defence I.

SECURITY CONTROLS FOR A PUBLIC CLOUD SERVICE AT A FINANCIAL INSTITUTION

István György OLÁH, Sándor MAGYAR

Today, IT services built with cloud technology are rapidly expanding. The fundamental reasons for this are the constantly growing demand for IT resources resulting from accelerating innovation and IT systems that require increasingly complex knowledge. It can take several weeks or months to procure a server, set it up, develop the operational requirements and train the staff on-site. In contrast, the same resources, including operation, can be provided by cloud services in a matter of minutes. If an organisation uses cloud services, it is also advisable to define the availability and security conditions, because these IT elements are also part of the operational ecosystem. A public cloud service provider can be part of the supply chain of a financial institution. This concept is reflected in the CER, NIS2 and the DORA regulations, which came into force in January 2023. In 2024, Decree No. 7 of 2024 (VI. 24.) of the Cabinet Office of the Prime Minister on the requirements for security classification and the specific protection measures to be applied for each security classification was published in relation to IT systems. The main topic of the publication is how to apply the required controls in the case of a public cloud service for a financial institution. Our hypothesis is that it can, but this requires the use of other control methods instead of the previously used assurance methods.

Keywords:
NIS2, audit, public cloud, financial institution

Kiberbiztonság - II. szekció – Kibervédelem I.

A NATO KATONAI LÉGISZÁLLÍTÁSI MŰVELETEINEK KIBERBIZTONSÁGI KIHÍVÁSAI

PARÁDA István, TÓTH András

A légiközlekedési ágazat egyre nagyobb mértékben támaszkodik a technológiára, ami aggodalomra ad okot az államilag támogatott kibertámadásokkal kapcsolatban, ami a katonai és polgári légiközlekedés számára is kihívást jelent a kiberbiztonság terén. Ez a cikk a NATO katonai légi teherszállítási képességeit és a kapcsolódó kiberbiztonsági kihívásokat, például az infrastruktúrák megzavarását és a biztonság veszélyeztetését vizsgálja. A kutatás a repülés kiberbiztonsági sebezhetőségeinek és fenyegetéseinek azonosítására, elemzésére és kezelésére összpontosít. A fejlett kiberbiztonsági protokollok és a személyzet folyamatos képzése kulcsfontosságú az informatikai infrastruktúra védelméhez. Mivel jelenleg nincs egységes nemzetközi kibervédelmi irányelv a légi közlekedésben, ezért a NATO-nak nagyon sürgősen védelmi stratégiákat kell kidolgoznia a katonai légi közlekedési képességek kibertámadásokkal szembeni védelmére. A biztonságos légiközlekedési rendszer biztosítása és a fejlődő kiberfenyegetések kezelése a kormányok, légitársaságok, repülőterek és gyártók közös felelőssége. A katonai légiközlekedési képességek védelme a kiberfenyegetésekkel szemben alapvető fontosságú, és átfogó kibervédelmi stratégiát igényel, amely magában foglalja a kockázatértékelést, a biztonságos hálózati architektúrát, az incidensekre való reagálás tervezését és a folyamatos nyomon követést.

Kulcsszavak:
katonai légi közlekedés, kiberbiztonsági kihívások, működésbiztonság, repülésbiztonság, kölcsönös függőség a polgári-katonai légi közlekedésben

Cybersecurity - session II.– Cyber defence I.

CYBER SECURITY CHALLENGES FOR NATO MILITARY AIR TRANSPORT OPERATIONS

István PARÁDA, András TÓTH

The aviation sector's increasing reliance on technology has raised concerns about state-sponsored cyberattacks, which pose cybersecurity challenges for both military and civil aviation. This article examines NATO's military air cargo capabilities and related cybersecurity challenges, such as disruption of infrastructure and security threats. The research focuses on identifying, analysing and addressing cybersecurity vulnerabilities and threats to aviation. Advanced cybersecurity protocols and continuous personnel training are key to protecting IT infrastructure. As there is currently no uniform international cyber defence policy for aviation, NATO urgently needs to develop defence strategies to protect military aviation capabilities against cyber attacks. Ensuring a secure aviation system and addressing evolving cyber threats are shared responsibilities of governments, airlines, airports, and manufacturers. Protecting military aviation capabilities from cyber threats requires a comprehensive cyber defense strategy that includes risk assessment, secure network architecture, incident response planning, and continuous monitoring.

Keywords:
military aviation, cyber security challenges, operational safety, aviation safety, interdependence in civil-military aviation

Kiberbiztonság - III. szekció – Oktatás és képzés

Cybersecurity - session III.– Education and training

Kiberbiztonság - III. szekció – Oktatás és képzés

SZAKIRÁNYÚ TOVÁBBKÉPZÉSI SZAKOK INDÍTÁSI LEHETŐSÉGEI A VÉDELMI SZFÉRÁBAN

KRIZSÁN Zoltán

Az alapképzésre vagy mesterképzésre épülő szakirányú továbbképzési szak, a magasabb vezetői betöltésekhez szükséges képzettséget és végzettséget adja meg. Az alapképzési szakok tárházából figyelembe vehető szakok első sorban a mérnöki, valamint a vezetői készséget adó szakok. Az alapszak és esetleges szakirányaik közvetlen csatlakozása a lényeg. A közvetlen csatlakozás jelentése az, hogy a jelzett alapképzési szakon, szakirányon, specializáción, modulon szerzett végzettség teljes kredit értékkel vehető figyelembe a szakirányú továbbképzési szakon.

Jelenleg két képzés dokumentumai készültek el és folyamatban van a biztonság védelmi szakirányú továbbképzési szak dokumentációinak elkészítése.

A tervezett tűzvédelmi felelő műszaki vezető és műszaki ellenőr szakirányú továbbképzési szak képzési struktúráját és oktatási feltételeit a Katasztrófavédelmi Intézet által működtetett tűzvédelmi mérnöki alapképzési szak ismeretanyaga és állománya képes biztosítani.

A kritikus infrastruktúra-védelmi biztonsági összekötő személy szakirányú továbbképzési szak célja olyan korszerű jogi és szakmai ismeretekkel rendelkező szakemberek képzése, akik komplex módon képesek a létfontosságú rendszerek és létesítmények védelmével kapcsolatos üzemeltetőt érintő biztonsági összekötői szakmai feladatok ellátására.

Kulcsszavak:

Szaklétesítés, szakindítás, kompetencia, tudás, képesség, attitűd

Cybersecurity - session III.– Education and training

POSSIBILITIES FOR LAUNCHING SPECIALIZED FURTHER TRAINING PROGRAMS IN THE DEFENSE SECTOR

Zoltán KRIZSÁN

The specialized further training program based on a bachelor's or master's degree provides the qualifications and credentials necessary for higher managerial positions. The fields of study that can be considered from the range of bachelor's programs primarily include engineering and managerial skills programs. The key point is the direct connection to the bachelor's program and any of its specializations. This direct connection means that the qualifications obtained in the indicated bachelor's program, specialization, or module are fully credited in the specialized further training program. Currently, the documentation for two training programs has been completed, and the documentation for the security defense specialized further training program is in progress.

The training structure and educational conditions of the planned fire safety officer and technical supervisor specialized further training program can be provided by the knowledge base and resources of the fire engineering bachelor's program operated by the Disaster Management Institute.

The aim of the specialized further training program for critical infrastructure protection security connectors is to train professionals with modern legal and professional knowledge who can comprehensively handle the security connector professional tasks related to the operation of vital systems and facilities. Graduates will be qualified to fill the security connector position related to the protection of vital systems and facilities.

Keywords:

program establishment, program launch, competence, knowledge, ability, attitude

Kiberbiztonság - III. szekció – Oktatás és képzés

AZ INFORMÁCIÓBIZTONSÁG ALAPJAI A SZLOVÁKIAI ALAP ÉS KÖZÉPISKOLÁS DIÁKOKNAK

PÁSZTOR Bence

Az okoseszközök szinte a mindennapi életünk részévé váltak. Az okostelefonok, okosórák és egyéb internethez kapcsolódó eszközök használata mára már mindennapossá vált, és egyre több diák használja őket. Ezzel párhuzamosan az adatvédelem fontossága is növekszik, mivel az eszközökön tárolt adatok, különösen a személyes adatok védelme, kiemelt figyelmet igényel, amit már iskolás korban el kell sajátítani.

A tanulmány bemutatja, milyen mértékben foglalkozik a szlovákiai államilag kiadott oktatási tanterv a jelszókezeléssel. Az általános iskolás és a középiskolás tanulóknak már korán meg kell tanítani a biztonságos jelszóhasználat alapjait, mivel a gyenge jelszavak, mint például a „123456” vagy a „password”, könnyen kitalálhatóak és feltörhetők. A jelszóválasztás megfelelő ismerete elengedhetetlen a diákok digitális biztonságának megőrzéséhez, hiszen a gyenge jelszavak komoly kockázatokat hordoznak, amelyek veszélyeztethetik a felhasználók adatait.

A publikáció rámutat arra is, hogy a jelszóválasztáson túl milyen további digitális biztonsági intézkedéseket érdemes alkalmazni annak érdekében, hogy fokozzuk a digitális biztonságunkat a jelszókezelők alkalmazásával és a kétfaktoros hitelesítés használatával.

Kulcsszavak:

információbiztonság, általános iskola, középiskola, jelszó, kétfaktoros hitelesítés

Cybersecurity - session III.– Education and training

INFORMATION SECURITY BASICS FOR PRIMARY AND SECONDARY SCHOOL STUDENTS IN SLOVAKIA

Bence PÁSZTOR

Smart devices have become almost part of our everyday lives. The use of smartphones, smartwatches, and other internet-connected devices have become ordinary items, and nowadays more and more students are using them. At the same time, the importance of data protection is also growing, as the protection of the data stored on these devices, especially personal data, requires special attention and needs to be learned from a young age.

This publication will show to what extent the Slovakian public education curriculum deals password management. Primary and secondary school students should be taught the basics of secure password use from an early age, as weak passwords such as "123456" number or the word "password" itself are easy to be find out and hacked. The proper knowledge of password selection is essential to keep students digitally safe, as weak passwords carry serious risks that can compromise users' data.

This publication also highlights additional digital security measures beyond password selection how to enhance digital security through the use of such password managers and two-factor authentication.

Keywords:

information security, primary school, secondary school, password, two-factor authentication

Kiberbiztonság - III. szekció – Oktatás és képzés

INFORMATIKAI OKTATÁSI TANANYAG MAGYARORSZÁGON ÉS SZERBIÁBAN

MANDIC Dorottya, KISS Gábor

Az informatikának fontos szerepe van az oktatásban, hiszen a felhasználói szintű informatikai ismeretek megszerzése egyre fontosabbá válik napjainkban. Több tanulmány is foglalkozik Magyarország és Szerbia informatikai oktatási tananyagával. Mivel napjainkban egyre több felhasználó használ különféle okoseszközöket ezért egyre fontosabbá válik, hogy a felhasználók megfelelő ismeretekkel rendelkezzenek ezen a téren is, illetve megfelelő körültekintéssel használhassák ezeket a személyes adataik védelmében. Várhatóan a jövőben még több okoseszköz lesz jelen, és a felhasználók közül sokan nem tudják, hogy hogyan kell biztonságosan használni az okoseszközeiket és sokan még csak alapvető ismeretekkel sem rendelkeznek. Fontos, hogy a felhasználók megfelelő ismeretekkel rendelkezzenek, és hogy tudatában legyenek azzal, hogy az okoseszközök használata milyen veszélyeket rejthet. Jelen tanulmány azt vizsgálja, hogy Magyarország és Szerbia informatikai oktatási tananyagában található-e információbiztonság tudatosság fejlesztése, valamint, hogy a két ország informatikai tananyaga között van-e különbség.

Kulcsszavak:

informatika, oktatás, információbiztonság, tudatosság, tananyag

Cybersecurity - session III.– Education and training

IT EDUCATION CURRICULUM IN HUNGARY AND SERBIA

Dorottya MANDIC, Gábor KISS

IT has an important role in education, as acquiring user-level IT knowledge is becoming more important nowadays. Several studies deal with the IT education curriculum of Hungary and Serbia. As more and more users are using various smart devices these days, it is becoming more important that they have the right knowledge in this area and that they can use it with the right amount of care to protect their personal data. It is expected that more smart devices will be present in the future and smart device users generally do not know how to use their smart devices safely and many users do not even have basic knowledge. It is important that they have adequate knowledge and are aware of the dangers that the use of smart devices can hide. This study examines whether information security awareness development can be found in the IT education curriculum of Hungary and Serbia and whether there is a difference between the IT curriculum of the two countries.

Keywords:
IT, education, information security, awareness, curriculum

Kiberbiztonság - III. szekció – Oktatás és képzés

ÚJ MEGKÖZELÍTÉSEK A SZOFTVERMÉRNÖKÖK OKTATÁSÁBAN A KIBERBIZTONSÁG TERÜLETÉN

ČOVIĆ Zlatko

Tanúi vagyunk annak, hogy minden nap hatalmas mennyiségű információ cserélődik weboldalakon és alkalmazásokon keresztül. Ez az információcsere kulcsszerepet játszik a modern digitális rendszerekben, és elengedhetetlen, hogy biztonságosan történjen. Az adatcserék biztonságának biztosítása mellett ugyanolyan fontos a rendszerek biztonságának garantálása is. Ahogy a kiberfenyegetések folyamatosan fejlődnek, egyre fontosabbá válik, hogy a szoftvermérnökök ne csak tisztában legyenek a potenciális biztonsági kockázatokkal, hanem rendelkezzenek a szükséges tudással és készségekkel e kockázatok hatékony kezeléséhez is. A sebezhetőségek megértése és a megfelelő technikák, eszközök és biztonsági módszerek alkalmazása alapvető ahhoz, hogy a mérnökök által fejlesztett termékek és rendszerek védettek maradjanak a rosszindulatú támadásokkal szemben. Ez a dolgozat innovatív megközelítéseket mutat be a szoftvermérnökök kiberbiztonság terén történő képzésére. Bár az elméleti tudás biztosítja az alapokat, a gyakorlati tudás és tapasztalat ugyanolyan fontos. A kiber támadások növekvő fenyegetéseivel szemben a hallgatóknak valódi szcenáriókhoz kell hozzáférniük. Ezek a szcenáriók szimulálják a gyakori kiberbiztonsági kihívásokat, lehetővé téve a hallgatók számára, hogy aktívan részt vegyenek a problémákban és alkalmazzák a megszerzett tudást.

Kulcsszavak:
kiberbiztonság, biztonsági kockázatok, szoftvermérnökök, gyakorlati oktatás, sebezhetőségi tesztelés

Cybersecurity - session III.– Education and training

NEW APPROACHES IN THE EDUCATION OF SOFTWARE ENGINEERS IN THE FIELD OF CYBERSECURITY

Zlatko ČOVIĆ

We are witnesses to the fact that every day, vast amounts of information are exchanged through websites and applications. This information exchange plays a crucial role in modern digital systems, and it is imperative that it is done securely. In addition to ensuring the security of the data being exchanged, it is equally important to guarantee the safety of the systems themselves. As cyber threats continue to evolve, it becomes increasingly vital for software engineers to not only be aware of potential security risks but also to possess the necessary knowledge and skills to mitigate these risks effectively. Understanding vulnerabilities and knowing how to implement appropriate techniques, tools, and security methods are fundamental to ensuring that the products and systems engineers develop remain safe from malicious attacks. This paper will present innovative approaches to educating software engineers specifically in the field of cybersecurity. While theoretical knowledge provides the foundation, practical knowledge and experience are equally important. To address the growing threat of cyber attacks, students must be exposed to real-world scenarios. These scenarios should simulate common cybersecurity challenges, allowing students to actively engage with the problems and apply the knowledge they have gained.

Keywords:
cybersecurity, security risks, software engineers, practical education, vulnerability testing

Kiberbiztonság - III. szekció – Oktatás és képzés

FIATALKORÚAK RADIKALIZÁLÓDÁSA A KÖZÖSSÉGI MÉDIÁBAN: HOGYAN TORZÍTJÁK AZ ALGORITMUSOK A NÉZETEKET

LACZI Szandra Anna, PÓSER Valéria

A kiskorúaknak a közösségi médián keresztül történő radikalizálódása egyre nagyobb aggodalomra ad okot, amelyet a szűrőbuborékokat létrehozó és a szélsőséges tartalmakat felerősítő algoritmusok vezérelnek. Ezek a felhasználói elkötelezettségre optimalizált algoritmusok gyakran teszik ki a fiatal felhasználókat olyan érzelmekkel teli, ideológiailag szűkszavú tartalmaknak, amelyek erősítik az előítéleteket és népszerűsítik a szélsőséges nézeteket. A kamaszok, akik az identitás és a hovatartozás keresése miatt különösen sebezhetőek, olyan online visszhangkamrákba kerülnek, amelyek normalizálják a radikális eszméket. Ez a tanulmány azt vizsgálja, hogy a közösségi médiaplatformok, a befolyásolók és a digitális terek anonimitása hogyan járulnak hozzá a fiatalok radikalizálódásához, hangsúlyozva, hogy sürgősen szükség van digitális műveltségre, algoritmikus átláthatóságra és proaktív beavatkozásokra a kiskorúak körében növekvő szélsőségesség kockázata ellen. Beavatkozás nélkül az e platformok által létrehozott elszigetelt környezetek továbbra is súlyosbítani fogják a társadalmi polarizációt és a szélsőségességet.

Kulcsszavak:
radikalizálódás, közösségi média algoritmusok, visszhangkamra, szűrőbuborék, kiberbiztonság

Cybersecurity - session III.– Education and training

YOUTH RADICALISATION ON SOCIAL MEDIA: HOW ALGORITHMS DISTORT VIEWS

Szandra Anna LACZI, Valéria PÓSER

The radicalization of minors through social media is an escalating concern, driven by algorithms that create filter bubbles and amplify extremist content. These algorithms, optimized for user engagement, often expose young users to emotionally charged, ideologically narrow content that reinforces biases and promotes extreme views. Adolescents, particularly vulnerable due to their search for identity and belonging, are drawn into online echo chambers that normalize radical ideas. This paper explores how social media platforms, influencers, and the anonymity of digital spaces contribute to youth radicalization, emphasizing the urgent need for digital literacy, algorithmic transparency, and proactive interventions to counter the growing risk of extremism among minors. Without intervention, the insular environments created by these platforms will continue to exacerbate societal polarization and extremism.

Keywords:
radicalization, social media algoritms, echo chamber, filter bubble, cybersecurity

Kiberbiztonság - IV. szekció – Kutatás, fejlesztés I.

Cybersecurity - session IV.– Research and development I.

Kiberbiztonság - IV. szekció – Kutatás, fejlesztés I.

INFOLAB KUTATÁSOK ÉS SZÉLESKÖRŰ HASZNOSULÁSUK

OROSZ Péter Pál

A napjainkban folyamatosan zajló információs forradalom meghatározó eleme, hogy az egyes leading edge technológiák fejlesztése – különös tekintettel az új generációs mobiltechnológiák (5G, 6G) / és az MI – egyre fokozódó egymásra hatása (szimbiotikus tovább fejlődése) elérhető közelségbe hozták a technológiai szingularitás megvalósulását. Biztonsággal kijelenthető, hogy az elkövetkezendő néhány évben olyan új megoldások látnak napvilágot, melyek felhasználása és alkalmazása mind a nemzetbiztonságban, rendvédelemben, mind a közigazgatásban előmozdítja olyan képességek és szolgáltatások megvalósulását, amelyek eredményesen járulnak hozzá az ágazati és nemzeti stratégiai célok megvalósulásához.

A Nemzetbiztonsági Szakszolgálat az InfoLab konzorcium vezetőjeként végzi kiber és további védelmi célú kutatásait. Ezek a kutatások és eredményeik közvetve, vagy közvetlenül a társadalom széles spektrumára van kihatással. A hatások az eredmények hasznosulásán keresztül reprezentálhatók leginkább, amely az előadás fő fókusza.

Az előadásban szó esik az 5G telekommunikációs ökoszisztémákról, valós idejű sérülékenységi szint megítélésének faktorairól, az Internetre kapcsolódó eszközök kiberbiztonsági fókusszal történő felmérhetőségéről, IoT eszközök biztonsági minősítéséről, a blockchain biztonsági alkalmazásáról, és a fotó alapú 3D modellezés megvalósításáról.

Kulcsszavak:

5G, kibervédelem, IoT, blockchain, 3D modellezés

Cybersecurity - session IV.– Research and development I.

INFOLAB RESEARCHES AND ITS WIDESPREAD APPLICATIONS

Péter Pál OROSZ

A defining element of the nowaday's ongoing information revolution is that the development of certain leading edge technologies – with particular regard to the new generation mobile technologies (5G, 6G) / and AI – and their increasing mutual influence (symbiotic further development) have brought the realization of the technological singularity within reach. It can be safely stated that in the next few years, new solutions will emerge, the use and application of which in both national security, law enforcement, and public administration will promote the realization of capabilities and services that effectively contribute to the realization of sectoral and national strategic goals.

The Special Service for National Security conducts its cyber and further defense research as the leader of the InfoLab consortium. These researches and their results have an indirect or direct impact on a wide spectrum of society. The effects can best be represented through the utilization of the results, which is the main focus of the presentation.

The presentation will discuss 5G telecommunications ecosystems, factors for assessing real-time vulnerability levels, the ability to assess Internet-connected devices with a cybersecurity focus, the security certification of IoT devices, the security application of blockchain, and the implementation of photo-based 3D modeling.

Keywords:

5G, cybersecurity, IoT, blockchain, 3D modeling

Kiberbiztonság - IV. szekció – Kutatás, fejlesztés I.

HAISQ-TÓL A SAM-IG, A BIZTONSÁGTUDATOSSÁG MÉRÉSÉNEK MODERNIZÁCIÓJA

RÉPÁS József, BEREK László, BAK Gerda, OLÁH Norbert, UJHEGYI Péter

A kiberbiztonság napjaink egyik legkritikusabb kihívása, amely folyamatos fejlődést és alkalmazkodást követel. A technológia exponenciális fejlődésével párhuzamosan a kibertámadások is egyre kifinomultabbá válnak, fokozva ezzel a veszélyt mind az egyénekre, mind a szervezetekre. Ebben a dinamikusan változó környezetben a biztonságtudatosság kulcsfontosságú., melynek mérése elengedhetetlen a hatékony védekezési stratégiák kialakításához és a fejlesztendő területek azonosításához.

A biztonságtudatosság mérésére számos eszköz áll rendelkezésre, melyek közül kiemelkedik a HAISQ (Human Aspects of Information Security Questionnaire) modell. Jelen kutatás egy új modellt, a SAM-ot (Security Awareness Model) mutatja be, amely a HAISQ modellre építve, de azt jelentősen kibővítve és modernizálva közelíti meg a biztonságtudatosság mérését. A SAM hét fő dimenziót vizsgál: autentikáció, internetes szolgáltatások használata, információkezelés, eszközhasználat, incidensmenedzsment, szabályozás és tudatosság.

A SAM modellre épülő kérdőív 120 kérdést tartalmaz, követve a KAB (Knowledge, Attitude, Behavior) modellt. Ez a komplex mérőeszköz lehetővé teszi a biztonságtudatosság részletes és sokoldalú felmérését, hozzájárulva ezzel a hatékonyabb kiberbiztonsági stratégiák kialakításához.

Kulcsszavak:

Security Awareness Model, SAM, kiberbiztonság, biztonságtudatosság, kvantitatív mérés

Cybersecurity - session IV.– Research and development I.

FROM HAISQ TO SAM, THE MODERNISATION OF SECURITY AWARENESS MEASUREMENT

József RÉPÁS, László BEREK, Gerda BAK, Norbert OLÁH, Péter UJHEGYI

Cybersecurity is one of the most critical challenges of our time, requiring continuous evolution and adaptation. As technology evolves exponentially, cyber-attacks become more sophisticated, increasing the threat to individuals and organisations. In this dynamically changing environment, security awareness is crucial, and its measurement is essential to developing effective protection strategies and identifying areas for improvement.

Several tools are available to measure security awareness, most notably the HAISQ (Human Aspects of Information Security Questionnaire) model. The present research proposes a new SAM (Security Awareness Model), which builds on the HAISQ model and significantly extends and modernises its approach to measuring security awareness. The SAM examines seven main dimensions: authentication, use of Internet services, information management, use of devices, incident management, regulation and human awareness.

The questionnaire based on the SAM model contains 120 questions, following the KAB (Knowledge, Attitude, Behavior) model. This complex measurement allows a detailed and multi-faceted security awareness assessment, contributing to the development of more effective cybersecurity strategies.

Keywords:

Security Awareness Model, SAM, cybersecurity, security awareness, quantitative measurement

Kiberbiztonság - IV. szekció – Kutatás, fejlesztés I.

GENERATÍV MESTERSÉGES INTELLIGENCIA: A FELSŐOKTATÁS ÉS A TUDOMÁNYOS KOMMUNIKÁCIÓ ÁTALAKULÁSA

BEREK László

A ChatGPT nagy nyilvánosság előtti megjelenését követően a mesterséges intelligencia egyre szélesebb körben terjed az élet minden területén. A generatív mesterséges intelligencia alkalmazásai gyors ütemben hódítanak teret a tudományos kommunikációban, az oktatásban és a publikációs folyamatokban. A technológiában óriási lehetőségek rejlenek a gépi fordítás, a beszédfelismerés, az oktatás vagy a tartalomkészítés területein is, de ezzel együtt aggodalmakat is felvet az esetleges visszaélések, az etikus alkalmazás és a plágium egyes kérdései kapcsán.

Ahogy a generatív mesterséges intelligencia alkalmazásai folyamatosan fejlődnek, a piacon elérhető detektáló eszközöknek is igyekezniük kell lépést tartani. Ez a tanulmány a Scopus és a Web of Science adatbázisok adatait felhasználva térképezi fel az AI által generált szövegdetektorok jelenlegi használhatóságát a felsőoktatás és a tudomány területein, valamint bepillantást ad a tudományetikai vonatkozásokba is.

Kulcsszavak:

mesterséges intelligencia, MI által generált szöveg detektálása, tudományos integritás, plágium, felsőoktatás

Cybersecurity - session IV.– Research and development I.

GENERATIVE ARTIFICIAL INTELLIGENCE: TRANSFORMING HIGHER EDUCATION AND SCIENTIFIC COMMUNICATION

László BEREK

Since the launch of ChatGPT, artificial intelligence is becoming increasingly pervasive in all walks of life. Generative AI applications are rapidly gaining ground in scientific communication, education, and publishing. This technology holds significant promise for machine translation, speech recognition, and content creation, but also raises concerns about bias, manipulation, and plagiarism.

As generative AI applications evolve, detection tools need to keep pace. This paper analyzes data from Scopus and Web of Science to map the usability of AI-generated text detectors in higher education and science. Additionally, it explores the ethical considerations surrounding such detection tools.

Keywords:

artificial intelligence, AI-generated text detector, academic integrity, plagiarism, higher education

Kiberbiztonság - IV. szekció – Kutatás, fejlesztés I.

A LOKÁLIS MÚZEUMI KIÁLLÍTÁS ÉS RAKTÁROZÁS KIHÍVÁSAI

LŐRINCZI László

A tanulmány célja a kisebb lokális múzeumok raktározási lehetőségeinek és a műtárgyak védelmének vizsgálata, különös tekintettel a műtárgyak hosszú távú megőrzésére és biztonságára. A publikáció arra fókuszál, hogy milyen raktározási megoldások felelnek meg legjobban a lokális múzeumok igényeinek és erőforrásainak, valamint a fenntartható tárolási módszerek azonosítására.

A kutatás során elsősorban interjúkat és esettanulmányokat alkalmazok a helyi múzeumok tapasztalatainak és kihívásainak feltérképezésére. A kisebb intézmények esetében különösen fontos feltárni, hogy miként birkóznak meg az erőforráshiánnyal, és hogyan igyekeznek fenntartható megoldásokat alkalmazni a műtárgyak hosszú távú megőrzésére.

Az eredmények révén a tanulmány arra törekszik, hogy nyújtson javaslatokat a lokális múzeumok raktározási gyakorlataira, figyelembe véve a hosszú távú fenntarthatóságot, a műtárgyak biztonságát és a gazdaságos energiagazdálkodást. A cél egy olyan keretrendszer kidolgozása, amely segíti a magyar helyi múzeumokat abban, hogy hatékonyabb és fenntarthatóbb raktározási megoldásokat alkalmazzanak.

Kulcsszavak:
műtárgyvédelem, közgyűjtemény, raktározás, lokális múzeum erőforrások

Cybersecurity - session IV.– Research and development I.

CHALLENGES OF LOCAL MUSEUM EXHIBITION AND STORAGE

László LŐRINCZI

The aim of this study is to examine the storage options and ArtWork Protection in smaller local museums, with particular attention to the long-term preservation and security of these artifacts. The publication focuses on identifying which storage solutions best meet the needs and resources of local museums, as well as determining sustainable storage methods.

The research primarily employs interviews and case studies to map the experiences and challenges faced by local museums. In the case of smaller institutions, it is particularly important to explore how they cope with resource limitations and strive to apply sustainable solutions for the long-term preservation of their collections.

The study aims to provide recommendations for the storage practices of local museums, taking into account long-term sustainability, artwork security, and efficient energy management. The goal is to develop a framework that supports Hungarian local museums in adopting more efficient and sustainable storage solutions.

Keywords:

artwork protection, public collection, storage, local museum, resources

Kiberbiztonság - IV. szekció – Kutatás, fejlesztés I.

AZ AUTONÓM KÖZÚTI GÉPJÁRMŰVEK TÁRSADALMI MEGÍTÉLÉSE ÉS KIHÍVÁSAI

KATONA Gergő

A téma fontosságát és aktualitását jól mutatják a szektor piaci mutatói is. Az autonóm járművek globális piacának mérete 2022-ben 1 500,3 milliárd USD volt, és az előrejelzések szerint 2030-ra 13 632,4 milliárd USD-re fog nőni. Tehát egy olyan pénzügyileg folyamatos növekedést mutató ágazat jelenik meg, amelynek a technológiai és társadalmi háttere kevésbé ismert. Az autonóm közúti gépjárművek tásdalami megítélése kiemelten fontos tényező, ezen technológia elterjedésében. Fontos azt felmérni, hogy milyen tényezők befolyásolják a társadalmat az önvezető járművek használatával kapcsolatban. A társadalmi kérdéskörök mellett fontos ezen technológia biztonsági aspektusát is az elejétől kezdve vizsgálni és értékelni annak érdekében, hogy az önvezető járművek egy biztonságos és valós közlekedési alternatíva legyen.

Kulcsszavak:

önvezetés, autonóm gépjárművek, kiberbiztonság, knight rider

Cybersecurity - session IV.– Research and development I.

SOCIAL PERCEPTION AND CHALLENGES OF AUTONOMOUS ROAD VEHICLES

Gergő KATONA

The importance and timeliness of the topic is also reflected in the market indicators for the sector. The global market for autonomous vehicles was worth USD 1 500.3 billion in 2022 and is forecast to grow to USD 13 632.4 billion by 2030. This is a financially steadily growing sector whose technological and social background is less well understood. The perception of autonomous road vehicles in the context of the economic and social environment is a key factor in the uptake of this technology. It is important to assess what factors influence society's perception of the use of self-driving vehicles. In addition to societal issues, it is also important to investigate and evaluate the safety aspects of this technology from the outset in order to make autonomous vehicles a safe and realistic transport alternative.

Keywords:
self-driving, autonomous vehicles, cybersecurity, knight rider

Kiberbiztonság - V. szekció –

Digital Forensics I.

Cybersecurity - session V.– Digital Forensics I.

Kiberbiztonság - V. szekció – Digital Forensics I.

A FELÜGYELETI LÁNC DIGITALIZÁLÁSÁNAK LEHETŐSÉGEI

KREITZ Zsuzsanna

A felügyeleti lánc, chain of custody (továbbiakban: CoC) folyamata elengedhetetlen az igazságügyi bizonyítékok kezelésében, biztosítva, hogy a bizonyítékok eredete, integritása és kezelése nyomon követhető és hiteles legyen. A digitalizáció gyors fejlődése lehetőséget kínál arra, hogy a hagyományosan papíralapú és manuálisan vezetett CoC folyamatok hatékonyabbak és megbízhatóbbak legyenek. A digitális megoldások alkalmazása, mint például a blokklánc technológia, RFID chipek és intelligens szerződések, jelentősen növelheti a folyamatok átláthatóságát és megbízhatóságát, miközben csökkentheti az emberi hibákból és csalásokból, kijátszásokból, tévedésekből eredő kockázatokat. E tanulmány célja a CoC digitalizálás lehetőségeinek feltárása, különös tekintettel a jogi, technológiai és adatbiztonsági szempontokra. A kutatás továbbá bemutatja a digitális CoC bevezetésének kihívásait, például az adatvédelmi szabályozásokhoz való illeszkedést, valamint a meglévő rendszerek integrációjának problémáit. Összességében a digitális CoC megoldások jelentős előrelépést hozhatnak a bizonyítékkezelés pontosságában és gyorsaságában, de bevezetésük alapos jogi és technológiai elemzést igényel.

Kulcsszavak:
felügyeleti lánc, blokklánc, RFID, bizonyíték

Cybersecurity - session V.– Digital Forensics I.

OPPORTUNITIES FOR DIGITIZING THE CHAIN OF CUSTODY

KREITZ Zsuzsanna

The chain of custody (CoC) process is essential in the management of forensic evidence, ensuring that the origin, integrity and handling of evidence can be traced and authenticated. Rapid advances in digitalisation offer the opportunity to make traditionally paper-based and manually managed chain of custody processes more efficient and reliable. The use of digital solutions, such as blockchain technology, RFID chips and smart contracts, can significantly increase the transparency and reliability of processes, while reducing the risks from human error and fraud, evasion and mistakes. The aim of this paper is to explore the opportunities for CoC digitisation, with a focus on legal, technological and data security aspects. It also describes the challenges of implementing a digital CoC, such as compliance with data protection regulations and the problems of integrating existing systems. Overall, digital chain of custody solutions can bring significant improvements in the accuracy and speed of evidence management, but their implementation requires a thorough legal and technological analysis.

Keywords:
chain of custody, blockchain, RFID, evidence

Kiberbiztonság - V. szekció – Digital Forensics I.

TERRORCSELEKMÉNY HELYSZÍNÉN A DIGITÁLIS JEGYZŐKÖNYVEZÉS PROBLÉMÁI

PAPP Kornél

Rendvédelmi szakmai berkekben sosem az a kérdés elképzelhető-e terroresemény bekövetkezése, csupán a mikor a kérdőjeles. Magyarország terrorfenyegetettsége rendkívül alacsony (2024 okt.) de ezt pillanatok alatt megváltozhat, így folyamatosan készen kell állnunk a megfelelő reagálásra. Ennek egyik aspektusa, hogy a terrorcselekmény helyszínén a bűnügyi helyszínelés szakszerű dokumentálására – a jelenleg általánosan használt komplex elektronikus szemle jegyzőkönyv mellett vagy helyett – a speciális körülményekre (CBRN, jammer, multiszektorok, időfaktor, stb.) tekintettel alternatív forgatókönyveket kidolgozása szükséges.
A cikkben a bizonyítékok láncolatának töretlenségéhez elengedhetetlen helyszíni dokumentáció összetettségére kívánok röviden rávilágítani, valamint lehetséges válaszokat bemutatni a felmerülő jegyzőkönyvezési kihívásokra.

Kulcsszavak:
bűnügyi helyszín, terror, bizonyíték, digitális adat, CBRN

Cybersecurity - session V.– Digital Forensics I.

PROBLEMS WITH DIGITAL REPORT AT THE SCENE OF A TERRORIST ATTACK

Kornél PAPP

In law enforcement professional circles, the question is never whether a terrorist event is conceivable, only when. Hungary's terror threat is extremely low (Oct 2024) but this can change in a matter of moments, so we must be constantly ready to respond. One aspect of this is the need to develop alternative scenarios for the professional documentation of the crime scene at the scene of a terrorist incident, in addition to or instead of the complex electronic inspection protocol currently in common use, taking into account the specific circumstances (CBRN, jammers, multi-sectors, time factor, etc.).

In this article, I will briefly highlight the complexity of on-site documentation, which is essential for the integrity of the chain of evidence, and present possible responses to the logging challenges that arise.

Keywords:

crime scene, terror, evidence, digital data, CBRN

Kiberbiztonság - V. szekció – Digital Forensics I.

LEHETŐSÉGEK A ROBBANTÁSSAL ELKÖVETETT TERRORCSELEKMÉNYEK HELYSZÍNI ADATAINAK DIGITÁLIS RÖGZÍTÉSÉRE ÉS ÉRTÉKELÉSÉRE

VOLARICS József

Tanulmányom témája a robbantással elkövetett terrorcselekmények helyszíni adatainak digitális rögzítésére és értékelésére szolgáló eszközök és módszerek, valamint ezek integrált rendszerbe foglalásának lehetőségei. A bevezető részben a NATO és a kriminológia által alkalmazott definíciók segítségével meghatározom a terrorizmus fogalmának saját szempontrendszerem szerinti lényegi elemeit, illetve röviden bemutatom a fizikai elkövetett terrorista támadások során leggyakrabban alkalmazott módszereket. Összefoglalom a robbantással elkövetett terrorcselekmények sajátosságait, az ilyen cselekményeket követő elsődleges feladatokat, a szemle során beszerezhető adatok jelentőségét.

Részleteiben tárgyalom a szemle feladatait az alkalmazott robbanóeszköz vonatkozásában, így hatásának dokumentálása, az az abból származó tárgytöredékek, anyagmaradványok összegyűjtése tekintetében. Bemutatásra kerülnek a vizuális adatok digitalizálásának alkalmazási lehetőségei a helyszíni dokumentáció elkészítése során, kiemelve a 3D technológiák előnyeit. Ismertetem a robbanó eszközből származó tárgytöredékek, illetve a robbanóanyagból származó anyagmaradványok detektálására alkalmas digitális eszközöket. Az összegzésben felvázolom a bemutatott technológiák integrált alkalmazásának lehetőségét, a rendszerként történő alkalmazás előnyeit.

Kulcsszavak:

terrorcselekmény, robbantás, helyszíni szemle, digitalizáció, 3D detektálás

Cybersecurity - session V.– Digital Forensics I.

POSSIBILITIES FOR DIGITAL RECORDING AND EVALUATION OF ON-SCENE DATA OF A TERRORIST ATTACK BY BOMBING.

József VOLARICS

The topic of my study is the equipment and methods for recording and evaluating on-scene data of terrorist attacks committed by Improvised Explosive Devices, and the possibilities of including them in an integrated system. In the introduction, I define the essential elements of the concept of terrorism according to my criteria using the definitions used by NATO and criminology. I briefly present the methods most frequently used during physical terrorist attacks. I summarize the characteristics of terrorist attacks committed by IEDs, the primary tasks following perpetration, and the significance of the data that can be obtained during the investigation.

I discuss in detail the investigation tasks from the perspective of the explosive device used, such as documenting its effect and collecting object fragments and material residues. I present the possibilities of digitizing visual data while preparing on-scene documentation, with the advantages of 3D technology. I will describe the digital devices suitable for detecting the fragments from explosive devices and explosives residues.

In the summary, I will outline the possibility of integrated application of the presented technologies and the advantages of applying them as a system.

Keywords:

terrorist attack, bombing, crime scene investigation, digitization, 3D detection

Kiberbiztonság - V. szekció – Digital Forensics I.

DIGITÁLIS ADATOK BEGYŰJTÉSE CBRN HELYSZÍNEKEN

KAKUJA Izabella

Napjainkban a társadalom nagy részének van hozzáférési lehetősége az online térhez. Vagyis a felhasználó online jelenléte után maradnak/maradhatnak digitális nyomok, amelyekből következtetni lehet az online térben végzett tevékenységére. Emiatt a digitális nyomokat és azok követését egy bűnüldöző szervezet sem hagyhatja figyelmen kívül. A bűnügyi helyszínen jelen lévő digitális nyomok, digitális adathordozók bizonyítékként történő rögzítésére tehát kiemelt figyelmet kell fordítani. Ugyanakkor, ha ez a helyszín CBRN anyaggal van szennyezve, akkor az egészség védelme érdekében speciális védőeszközöket kell használni. Továbbá az adathordozók szennyezettsége esetén további speciális eljárásokra van szükség. Jelen tanulmányban ezen tevékenységek végzéséhez és összehangolásához kívánok néhány alternatívát felvázolni.

Kulcsszavak:

bűnügyi helyszín, CBRN, bizonyíték, digitális adat

Cybersecurity - session V.– Digital Forensics I.

DIGITAL DATA COLLECTION AT CBRN CRIME SCENE

Izabella KAKUJA

Today, a large part of society has access to the online space. In other words, after the user's online presence, digital traces remain/may remain, from which it is possible to infer his activities in the online space. For this reason, digital traces and their tracking cannot be ignored by any law enforcement organization. Special attention must therefore be paid to the recording of digital traces and digital data carriers present at the crime scene as evidence. However, if this site is contaminated with CBRN material, special protective equipment must be used to protect health. Furthermore, additional special procedures are required in case of contamination of the data carriers. In this article, I would like to outline some alternatives for carrying out and coordinating these activities.

Keywords:
crime scene, CBRN, evidence, digital data

Kiberbiztonság - V. szekció – Digital Forensics I.

COMPUTER FORENSICS MÓDSZERTAN ALKALMAZÁSÁNAK VIZSGÁLATA MAGAS AUTOMATIZÁLTSÁGÚ JÁRMŰVEK SZAKÉRTŐI VIZSGÁLATÁBAN

RÉPÁS József

A magas automatizáltságú közúti közlekedési járművek és maga a közlekedés és közlekedési rendszerek is folyamatos fejlődésen mennek keresztül. Az összekapcsolt járművek polgári és katonai szférában is egyre népszerűbbek. A járművek által kezelt, gyűjtött, feldolgozott, továbbított adatok, mint digitális nyomok az utólagos szakértői vizsgálatok értékes és nélkülözhetetlen elemeivé váltak. Mind a balesetekben, terrorcselekményekben, gyilkosságokban, csempészetben résztvevő, mind a katonai műveletekben alkalmazott járművek nagy mennyiségben tartalmaznak digitális adatokat, melyek kinyerése és vizsgálata a rendelkezésre álló szakértői módszertanokkal nem, vagy nem teljeskörűen végezhető el. Jelen tanulmány célja a számítógépek szakértői vizsgálati módszertanának vizsgálata a modern járművek speciális vizsgálati szempontjait figyelembe véve. A computer forensics módszertanok, a Kamarai módszertani levelek nem terjednek ki a digitális járművek vizsgálati módjaira és lehetőségeire. Kutatásom célja olyan szakértői módszertan kidolgozása, ami alkalmazható a modern járművek belső adattárolóinak, azok adattartalmának vizsgálatára.

Kulcsszavak:
járművek szakértői vizsgálata, modern járművek, digitális nyomok, számítógépek szakértői vizsgálata

Cybersecurity - session V.– Digital Forensics I.

EXAMINATION OF THE APPLICATION OF COMPUTER FORENSICS METHODOLOGY OF THE HIGHLY AUTOMATED VEHICLES

József RÉPÁS

Highly automated transport vehicles and the transport systems themselves are constantly evolving. Connected vehicles are becoming increasingly popular in both civilian and military usage. Data managed, collected, processed, and transmitted by vehicles, as digital evidence, have become valuable and indispensable elements of digital forensics examinations. The vehicles involved in accidents, terrorist acts, murders, smuggling, and military operations can contain a large amount of digital data. The extraction and examination of these cannot be carried out or cannot be fully carried out with the available expert methodologies. This study aims to look at the computer forensics methodology taking into account the special examination aspects of modern vehicles. Computer forensics methodologies and the Hungarian Chamber of Juridical Experts methodological letters do not cover the methods and possibilities of examining digital vehicles. The aim of my research is to develop a digital vehicle forensics methodology that can be applied to the examination of the internal data storage devices of modern vehicles and their data content.

Keywords:
vehicle forensics, modern vehicles, digital evidence, computer forensics

Kiberbiztonság - VI. szekció – Kibervédelem II.

Cybersecurity - session VI.– Cyber defence II.

Kiberbiztonság - VI. szekció – Kibervédelem II.

YANAC – LÉGY NAPRAKÉSZ!

BIRÓ Péter

Míg a nemzetközi írott sajtóban szinte naponta jelennek meg kiberbiztonsággal, kibervédelemmel, vagy támadásokkal kapcsolatos információk, a magyar szakirodalom ezeket a híreket egyáltalán nem, vagy csak késéssel veszi át. Az ismertebb szakmai oldalak (PCW, HWSW, ICTGlobal) jellemzően csak az igazán nagy port felkavaró, kiemelt híreket veszik át, illetve saját tartalmat is jellemzően csak nagy horderejű esetekről, eseményekről írnak.

A globális kibertér magyar nyelvű szegletében, kiberbiztonsággal foglalkozó, magyar nyelvű híreket csak elvétve lehet találni, a kutatók többnyire a nagy nemzetközi szakmai oldalakra támaszkodva tudnak tájékozódni az aktualitásokról, trendekről.

A YANAC (Yet Another News Aggregator Channel) célja, hogy kiválogassa a nemzetközi sajtóban megjelent érdekesebb, fontosabb híreket, és azokat tömören összefoglalva adja tovább az érdeklődőknek. Az oldalon minden érdeklődő a saját szájízlése szerint tud keresni az összegyűjtött angol- és idegen nyelvű híranyagok között, illetve a szerkesztők a legrelevánsabb híreket magyar nyelven is összefoglalják és megjelenítik.

Kulcsszavak:
CTI, YANAC, hírek, információgyűjtés, OSINT

Cybersecurity - session VI.– Cyber defence II.

YANAC – KEEP ME UPDATED

Péter BIRÓ

Although topics like cybersecurity, cyber defense, and cyberattacks frequently appear in the international press, the Hungarian literature either lags behind or barely addresses these issues. Well-known Hungarian professional sites, such as PCW, HWSW, and ICTGlobal, generally focus on high-profile stories or major incidents, while in-depth coverage of ongoing trends is rare.

In the Hungarian-language segment of the global cyberspace, cybersecurity news in Hungarian is scarce, leaving researchers to depend on international sources for updates and developments. To address this gap, YANAC (Yet Another News Aggregator Channel) curates and summarizes key international cybersecurity news. The platform allows users to browse English and other foreign-language articles in their preferred language, while its editors provide concise summaries of the most relevant content in Hungarian.

Keywords:

CTI, YANAC, news, intelligence, OSINT

Kiberbiztonság - VI. szekció – Kibervédelem II.

CYBERRANGE - A KIBEREDZŐTEREM AHOL A SZAKEMBEREKBŐL PROFIK LESZNEK

CSORDÁS Szilárd

Az IT-biztonsági technológiák rohamléptekkel fejlődnek, egyre hatékonyabban detektálva és blokkolva a támadók aktivitását. De mi van, ha a támadó kreatív és kitartó? És higgyük el, ilyen szervezetek léteznek. Egyértelmű, hogy a technológia önmagában nem elég – szükség van emberekre, jó szakemberekre, akik a védekezést a következő szintre emelik.

A CyberRange épp ezt kínálja: egy virtuális edzőtermet, ahol az IT-szakemberekből valódi profik válnak. Valósághű szimulációk, szakértői tudásbázis, és izgalmas wargame-ek – ez a tökéletes recept, hogy a csapatod ne csak reagáljon, hanem dominálj on is a kiberharcmezőn.

Legyél kezdő, haladó vagy akár profi, a CyberRange-en mindenki megtalálja a számára megfelelő szintet, hogy fejlődhessen. Egyszerű egyszemélyes feladatoktól a komplex csapatjátékokig, egyedül is képezheted magad, vagy összemérhetitek az erőtöket csapatban. Ráadásul, ha eddig csak a védekező kék sapkát viselted, most lehetőséged van lecserélni azt a támadó pirosra, hogy a másik oldalon is kipróbáld magad. Így lesz teljes a kép, és így válik a szakemberből valódi profi.

Kulcsszavak:

kiberbiztonság, cyberrange, red team, blue team

Cybersecurity - session VI.– Cyber defence II.

CYBERRANGE – THE CYBER GYM WHERE EXPERTS BECOME PROS

Szilárd CSORDÁS

IT security technologies are advancing at a rapid pace, becoming increasingly effective at detecting and blocking attackers' activities. But what happens when an attacker is creative and persistent? And believe us, such organizations do exist. It's clear that technology alone is not enough — skilled professionals are needed to take defense to the next level.

This is exactly what CyberRange offers: a virtual training ground where IT specialists can become true professionals. With realistic simulations, expert knowledge bases, and exciting war games, it's the perfect recipe for ensuring your team not only reacts but dominates on the cyber battlefield.

Whether you're a beginner, advanced, or already a pro, CyberRange has something for everyone to help them grow. From simple solo tasks to complex team challenges, you can train on your own or test your strength in group settings. Moreover, if you've only worn the defensive blue hat so far, now you have the chance to switch to the offensive red one and experience the attacker's role. This comprehensive approach completes the picture, transforming a specialist into a true professional.

Keywords:

cybersecurity, cyberrange, red team, blue team

Kiberbiztonság - VI. szekció – Kibervédelem II.

CSAPDARENDSZEREK FELHASZNÁLÁSA A KÖZIGAZGATÁSI SZEKTROBAN

GONDA Ábel

A közigazgatás önmagában egy egyedi jellemzőkkel ellátott szektor, amely különleges szükségleteket igényel, ha kiberbiztonságról beszélünk. 2018 óta a Nemzeti Kibervédelmi Intézet szolgáltatási palettájában megtalálható a Honeypot azaz Csapdarendszer is. Ez a különleges rendszer képes egyedülálló megoldásokkal eltéríteni a behatolókat, az általuk visszahagyott adatokat pedig felhasználni kiberhírszerzési és trend elemzési folyamatokban. Az előadás során a hallgatóság egy rövid betekintést nyerhet a Honeypotok világába és ezen rendszerek stratégiai felhasználásában az NKI által.

Kulcsszavak:
csapdarendszerek, közigazgatás, Nemzeti Kibervédelmi Intézet, kiberhírszerzés

Cybersecurity - session VI.– Cyber defence II.

THE USECASE OF HONEYPOTS IN THE PUBLIC ADMINISTRATION SECTOR

Ábel GONDA

The public administration by itself contains many unique features, which certainly demands special needs in the world of cybersecurity. Since 2018 the National Cyber Security Center (NCSC) Hungary has Honeypots in their range of services. This specialized network security system uses some unique ways to keep intruders busy and utilize interaction data for cyber intelligence and trends analyzis. In this session the audience will be able to get a quick glance into the world of Honeypot and their strategic use by the National Cyber Security Center.

Keywords:
honeypot, public administration, National Cyber Security Center, cyber intelligence

Kiberbiztonság - VI. szekció – Kibervédelem II.

CYBER THREAT INTELLIGENCE FELHASZNÁLÁSI LEHETŐSÉGEI A KIBERVÉDELEMBEN

MARSI Tamás, ARADI Zoltán

A Cyber Threat Intelligence (CTI) a kibervédelmi stratégia alapvető eleme, amely elősegíti a fenyegetések azonosítását, a kockázatok csökkentését és a gyors reagálást. A CTI több szinten működik, a technikai részletektől kezdve – például IP-címek és domain nevek azonosítása – egészen a stratégiai szintű elemzésekig, amelyek üzleti döntések előkészítését támogatják. Az előadás bemutatja a CTI szintek közötti különbségeket, a fenyegetési szereplők tevékenységének elemzéséhez alkalmazott keretrendszereket (pl. Mitre ATT&CK), valamint a CTI alkalmazásával járó hazai kihívásokat, mint az automatizáció, az interoperabilitás és az érzékeny adatok védelme. A hazai CTI-képességek jelentős fejlődésen mentek keresztül az elmúlt években. Példaként említhető a Nemzeti Kibervédelmi Intézet által fejlesztett fenyegetéselemző platformok, a dark web feedek figyelése és a nemzeti CSIRT által biztosított adatcsere-mechanizmusok. A CTI alkalmazása nemcsak a fenyegetések elleni hatékony védekezést segíti, hanem a döntéshozatali folyamatokat is támogatja, különös tekintettel az incidensmenedzsmentre és a kockázatcsökkentésre. Az előadás kiemeli a bizalomépítés és az információmegosztás fontosságát, miközben megoldási javaslatokat kínál az interoperabilitás és az automatizáció terén felmerülő problémákra.

Kulcsszavak:
cyber threat intelligence, CTI, kibervédelem, fenyegetéselemzés, információmegosztás

Cybersecurity - session VI.– Cyber defence II.

APPLICATIONS OF CYBER THREAT INTELLIGENCE IN CYBER DEFENSE

Tamás MARSI, Zoltán ARADI

Cyber Threat Intelligence (CTI) is a fundamental element of cybersecurity strategy, facilitating the identification of threats, risk mitigation, and rapid response. CTI operates on multiple levels, ranging from technical details – such as identifying IP addresses and domain names – to strategic analyses that support business decision-making. This presentation highlights the distinctions between CTI levels, the frameworks used for analyzing threat actors' activities (e.g., Mitre ATT&CK), and the domestic challenges associated with CTI implementation, such as automation, interoperability, and the protection of sensitive data.

In recent years, domestic CTI capabilities have undergone significant development. Examples include threat analysis platforms developed by the National Cybersecurity Center, monitoring dark web feeds, and data exchange mechanisms provided by the national CSIRT.

The application of CTI not only supports effective defense against threats but also aids decision-making processes, particularly in incident management and risk reduction. The presentation emphasizes the importance of trust-building and information sharing, while also offering solutions to challenges in interoperability and automation.

Keywords:

cyber threat intelligence, CTI, cybersecurity, threat analysis, information sharing

Kiberbiztonság - VI. szekció – Kibervédelem II.

RENDSZERMEMÓRIA ELLENI TERHELÉSES TÁMADÁS HATÉKONY DETEKTÁLÁSA

HORCSIN Bálint

Sok x86-64 utasításkészletű processzor memória elérése sérülékeny terheléses támadásokkal szemben. Jelen dolgozatomban tárgyalt módszer már korábban is ismert volt, és úgy csökkentették a processzor számítási teljesítményét, hogy több cache line-t érintő atomi utasításokat hajtottak végre egymás után, amelyekkel bus lock-okat váltottak ki, amely drasztikusan csökkentette a processzor számítási teljesítményét. Ez a támadás olyan esetben is sikeres volt, hogyha a támadó kód hardveresen gyorsított virtuális gépen futott. Egyes újabb processzorokon beállítható, hogy védett legyen ilyen típusú támadás ellen. Ugyanakkor sok processzor továbbra is üzemben van, amelyek esetén nincs ismert megoldás a sérülékenység elhárítására. Annak érdekében, hogy egy támadásra lehessen reagálni, képesnek kell lenni detektálni, amikor ezt a sérülékenységet kihasználják. Több kutatás is foglalkozott azzal, hogy miképpen detektálható egy folyamatban lévő támadás. Ezek 1-30 mp alatt adtak eredményt, amely az esetek 5-30%-ban téves volt. Korábbiaktól eltérő mérési és statisztikai módszerrel átlagosan 80 µs alatt tudtam elvetni a támadás tényét, ha nem volt támadás alatt a számítógép; és átlagosan 1-3 ms alatt tudtam érzékelni egy aktív támadást, lényegében hiba nélkül. A támadás detektálásában elért új eredmények demonstrálása céljából rejtett kommunikációs csatornát alakítottam ki két virtuális gép között, amelyen 832 bit/mp sebességgel voltam képes adatot továbbítani.

Kulcsszavak:

processzor, virtualizáció, rejtett kommunikáció, memória

Cybersecurity - session VI.– Cyber defence II.

EFFICIENTLY DETECTING DENIAL OF SERVICE ATTACKS AGAINST SYSTEM MEMORY

Bálint HORCSIN

Many x86-64 processors are susceptible to denial-of-service attacks due to the way they access system memory. The method discussed in this paper was already known, which executes unaligned atomic instructions on the processor. These instructions trigger bus locks, and they drastically degrade the compute performance of the given processor. The attack is also successful when it is performed on a virtual machine thanks to hardware-accelerated virtualization. Some newer processors can be set to be resilient against this kind of denial-of-service attack. But many processors that are still in operation cannot be protected against such attacks using any known methods. In these cases, the only way of mitigating this threat is by detecting an ongoing attack and react accordingly.

Multiple papers were published on how an ongoing attack can be detected. These solutions have typically been able to detect such an attack in 1-30 seconds with an error rate of 5-30%. By using other measurement and statistical methods, I was able to reject that the computer was being attacked in 80 µs on average, and I was able to detect an ongoing attack in 1-3 ms with almost perfect accuracy. To demonstrate my results in attack detection, I established a covert communication channel between two virtual machines with a data rate of 832 bits/sec.

Keywords:

processor, virtualization, memory, covert communication, bus lock

Kiberbiztonság - VII. szekció – Mesterséges intelligencia és blokklánc

Cybersecurity - session VII.– Artificial intelligence and blockchain

Kiberbiztonság - VII. szekció – Mesterséges intelligencia és blokklánc

A KVANTUM TECHNOLÓGIA ÜNNEPI ÉVE ELÉ

NAGY Zoltán András

Jövőre lesz egy évszázada lesz annak, hogy Erwin Schrödinger kifejlesztette a hullámmechanikát, Werner Heisenberg, Max Born és Pascual Jordan pedig a mátrixmechanikát. Ez az apropó az ürügy arra, hogy az ENSZ 2025-öt a Kvantum Tudomány és Technológia nemzetközi évének nyilvánította.
Ennek ismeretében és ehhez kapcsolódva a Világgazdasági Fórum idén januárban a kvantumgazdaság lehetőségeit vizsgálandó Blueprintet bocsátott ki.
Ez a dokumentum gyakorlatilag egy ütemtervet irányoz elő az államok számára, amelynek elemei a kvantumgazdaságra felkészülés folyamatában a kvantumkockázatok megértése és az átállásra felkészülés, az akadémiai, a gyakorlati és az oktatási szféra együttműködése, a tudás más országokkal való megosztásának szükségessége.
Az előadás e dokumentum alaptételeiből kiindulva a kiberbiztonság kutatása és oktatása során szerzett tapasztalatokkal kiegészítve szól a közeljövő technológiai fejlődésének együtt hatásáról köszöntve a kvantumtechnológia 2025-ös ünnepi évét.

Kulcsszavak:
kvantum technológia, kvantum gazdaság, ENSZ, Világgazdasági Fórum

Cybersecurity - session VII.– Artificial intelligence and blockchain

BEFORE THE FESTIVE YEAR OF QUANTUM TECHNOLOGY

Zoltán András NAGY

Next year it will be a century since Erwin Schrödinger developed wave mechanics and Werner Heisenberg, Max Born and Pascual Jordan developed matrix mechanics. This is the reason why the UN has declared 2025 the International Year of Quantum Science and Technology.

Knowing this and in connection with this, the World Economic Forum issued a Blueprint to examine the possibilities of the quantum economy in January this year. This document practically foresees a roadmap for the states, the elements of which in the process of preparing for the quantum economy are the understanding of quantum risks and preparation for the transition, the cooperation of the academic, practical and educational spheres, and the need to share knowledge with other countries.

Starting from the basic tenets of this document, supplemented by experiences gained during cyber security research and education, the presentation talks about the combined effect of the technological development of the near future, greeting the 2025 festive year of quantum technology.

Keywords:
quantum technology, quantum economy, UN, World Economic Forum

Kiberbiztonság - VII. szekció – Mesterséges intelligencia és blokklánc

AZ EURÓPAI UNIÓ, AZ AMERIKAI EGYESÜLT ÁLLAMOK ÉS A KÍNAI NÉPKÖZTÁRSASÁG MESTERSÉGES INTELLIGENCIA JOGI SZABÁLYOZÁSÁNAK ÖSSZEHASONLÍTÓ ÁTTEKINTÉSE

SIPOS Sándor Zsolt

Az MI fejlődésének fontosabb nem technikai állomásai: Alan Turing - Computing Machinery and Intelligence, Logic Theorist program, MI telek, Global Partnership on AI kezdeményzés, Interregionális Bűnügyi és Igazságügyi Kutatóintézet.

Az MI rövid jogi fejlődéstörténete az EU-ban: EU GDPR, EU DSA, EU DMA, Európai Bizottság: Fehér Könyv a Mesterséges Intelligenciáról.

Az MI rövid jogi fejlődéstörténete az Egyesült Államokban: AI Bill of Rights tervezet, útmutató MI alkalmazások szabályozásához, Elnöki rendeletek.

Az MI rövid jogi fejlődéstörténete Kínában: intézkedés tervezetek a generatív MI-hoz, átmeneti intézkedések a generatív MI-hoz, Kínai Kibertér Ügynökség.

Koncepcionális különbségek az EU, az USA és Kína MI szabályozásában: szabályozási filozófiák, szabályozó intézményi keretek.

Koncepcionális hasonlóságok az EU, az USA és Kína MI szabályozásában: globális vezető szerep, US Chief AI Officer és EU AI Office, White House AI Council, European AI Board, Bletchley Nyilatkozat, UNESCO: Ajánlások az MI Etikára, a kiszabható bírságok rendszere.

Kulcsszavak:

Európai Unió, Egyesült Államok, Kína, mesterséges intelligencia, jogi összehasonlítás

Cybersecurity - session VII.– Artificial intelligence and blockchain

A COMPARATIVE OVERVIEW OF THE AI REGULATION OF THE EUROPEAN UNION, THE UNITED STATES OF AMERICA AND THE PEOPLE'S REPUBLIC OF CHINA

Sándor Zsolt SIPOS

The most important non-technical milestones in the development of AI: Alan Turing on Computing Machinery and Intelligence, Logic Theorist program, AI winters, Global Partnership on AI, Interregional Crime and Justice Research Institute.
A brief history of the legal development of AI in the European Union: EU GDPR, EU DSA, EU DMA, European Commission: White Paper on AI.
A brief history of the legal development of AI in the USA: Blueprint for an AI Bill of Rights, Guidance for Regulation of AI Applications, Executive Orders.
A brief history of the legal development of AI in the People's Republic of China: draft measures on Generative AI, interim measures on Generative AI, Cyberspace Administration of China.
Conceptual approach differences in EU, US and Chinese AI regulation: regulatory philosophies, regulatory institutional frameworks.
Similarities in conceptual approach in EU, US and Chinese AI regulation: globális vezető szerep, US Chief AI Officer és EU AI Office, US White House Artificial Council, European Artificial Intelligence Board, Bletchley Declaration, UNESCO "Recommendation on the Ethics of AI", system of the applicable fines.

Keywords:
European Union, USA, China, artificial intelligence, legal comparison

Kiberbiztonság - VII. szekció – Mesterséges intelligencia és blokklánc

NEM INTERAKTÍV NULLAISMERETŰ KRIPTOGRÁFIAI PRIMITÍV ALKALMAZÁSA BLOKKLÁNC KÖRNYEZETBEN

NAGY Csaba Norbert, OLÁH Norbert

Manapság a blokklánc technológia jelentős figyelmet kap a tudományos irodalomban és a piaci szektorokban egyaránt. A blokkláncnak széleskörű alkalmazási területei vannak, a pénzügyi szektortól kezdve egészen a digitális művészetekig. Ezen területek közül egyik népszerű téma az ingatlanok tokenizálása és az ingatlanvagyonok felosztása. A mindennapi használatban jelentős kihívásokkal kell szembenézni, mint például egy tokenizált társasház közös döntéseinek menedzselése, vagy a tulajdonjogok és a kapcsolódó bevételek pontos elosztása a tulajdonosok között. A nem interaktív nullaismeretű kriptográfiai (NIZK) primitívek alkalmazása lehetővé teszik az adatok biztonságos ellenőrzését anélkül, hogy azokat felfednék a jogosulatlan felhasználók előtt. Ezzel párhuzamosan a Chameleon hash kontrollált módosítási lehetőséget biztosít a tranzakciók számára, egy előre meghatározott titkos kulcs segítségével, anélkül, hogy sérülne a blokklánc kriptográfiai integritása. Ez a rugalmasság lehetőséget ad a hibák korrigálására vagy megegyezések módosítására anélkül, hogy hamisítási kockázatot jelentsen az eredeti tranzakcióra nézve. Ezek a kriptográfiai megoldások növelik a rendszer biztonságát és kiber-ellenálló képességét, miközben biztosítják az átláthatóságot és megbízhatóságot, így elősegítve az ingatlan tokenizáció hatékonyabb és biztonságosabb működését.

Kulcsszavak:

blokklánc, ethereum, tokenizáció, NIZK, kaméleon hash

Cybersecurity - session VII.– Artificial intelligence and blockchain

APPLICATION OF NON-INTERACTIVE ZERO-KNOWLEDGE CRYPTOGRAPHIC PRIMITIVES IN BLOCKCHAIN ENVIRONMENT

Csaba Norbert NAGY, Norbert OLÁH

Nowadays, blockchain technology is receiving significant attention in both academic literature and the market sectors. Blockchain has a wide range of applications, from the financial sector to digital arts. Among these areas, one popular topic is the tokenization of real estate and the fractional ownership of property. In everyday use, significant challenges arise, such as managing collective decisions in a tokenized condominium or the precise distribution of ownership rights and related revenues among the owners. The application of non-interactive zero-knowledge (NIZK) cryptographic primitives allows for the secure verification of data without revealing it to unauthorized users. Simultaneously, the Chameleon hash provides a controlled modification option for transactions, using a pre-determined secret key, without compromising the cryptographic integrity of the blockchain. This flexibility enables the correction of errors or the modification of agreements without posing a risk of forgery to the original transaction. These cryptographic solutions enhance the system's security and cyber-resilience while ensuring transparency and trustworthiness, thereby promoting the more efficient and secure functioning of real estate tokenization.

Keywords:
GDPR, healthcare, healthcare IT, artificial intelligence

Kiberbiztonság - VII. szekció – Mesterséges intelligencia és blokklánc

AJA PROJEKT-A MESTERSÉGES ÉRZELMI INTELLIGENCIA ÉS A MENTÁLIS EGÉSZSÉG KAPCSOLATA

SOÓS Georgina

A mesterséges intelligencia (MI) alkalmazása a mentális egészségügyben jelentős potenciállal bír a diagnosztika, a kezelés és a betegek jólétének javítása terén. Az MI-alapú chatbotok, hangulatkövető rendszerek és személyre szabott beavatkozások révén az AI lehetővé teszi a mentális állapot folyamatos monitorozását, személyre szabott támogatást nyújtva. Az MI természetes nyelvfeldolgozási és gépi tanulási képességei elősegítik a mentális problémák azonosítását, az ellátáshoz való hozzáférés javítását, valamint az egészségügyi költségek csökkentését. Az MI alkalmazása azonban etikai aggályokat vet fel, például a magánélet védelme, az adatbiztonság és a potenciális elfogultságok kapcsán. A tanulmány TAP modell alkalmazása mellett az érzelmi mesterséges intelligencia (EMI) klinikai felhasználásait vizsgálja, és feltárja, hogyan növelhető az EMI segítségével a terápiás beavatkozások hatékonysága, különösen a szövegalapú rendszerek révén, amelyek személyre szabott, valós idejű érzelmi támogatást és interakciót biztosítanak a betegek számára, hozzájárulva a mentális egészségügyi ellátás javításához.

Kulcsszavak:
mesterséges intelligencia, mentális egészségügy, MI-alapú chatbotok, természetes nyelvfeldolgozás, etikai aggályok

Cybersecurity - session VII.– Artificial intelligence and blockchain

PROJECT AJA-THE LINK BETWEEN ARTIFICIAL EMOTIONAL INTELLIGENCE AND MENTAL HEALTH

Georgina SOÓS

The integration of Artificial Intelligence (AI) into mental health care offers significant opportunities to enhance diagnostics, treatment, and patient well-being through innovative tools like AI-enabled chatbots, mood tracking systems, and personalized interventions. AI's capabilities in natural language processing, machine learning, and data analysis can provide tailored mental health support, improve access to care, and potentially lower healthcare costs. However, the deployment of AI in mental health also presents challenges, including ethical concerns around privacy, data security, potential biases, and the risk of dehumanization in care. There is a critical need for balanced implementation strategies that prioritize transparency, accountability, and alignment with ethical standards, ensuring that AI supplements rather than supplants human expertise in mental health services. Overall, while AI holds transformative potential in mental health, its use must be carefully managed to protect patient welfare and promote equitable, effective care. The study explores the clinical applications of Emotional Artificial Intelligence (EMI) using the TAP model and explores how EMI can be used to increase the effectiveness of therapeutic interventions, particularly through text-based systems that provide personalised, real-time emotional support and interaction with patients, contributing to improved mental health care.

Keywords:
artificial intelligence, mental health, AI-based chatbots, natural language processing, ethical concerns

Kiberbiztonság - VII. szekció – Mesterséges intelligencia és blokklánc

PRÉMIUM BORÁSZATI TERMÉKEK VÉDELME BLOKKLÁNC ALKALMAZÁSÁVAL

OLÁH Norbert

Napjainkban a borkereskedelem egy nagy befolyással rendelkező piac, ahol hektoliterek cserélnek gazdát. Azonban ez a terület sem mentes a csalásoktól, valamint a hamisításoktól és az időről időre napvilágra kerülő botrányok alapjaiban rengetik meg a bor világát.

A megoldási javaslatban az ellenőrizhetőség, a nyomonkövethetőség és a termékhez kapcsolódó adatok hitelességének és integritásának védelmét a blokklánc technológia biztosítja. Miután az adatok rendelkezésre állnak a blokkláncon fontos, hogy megtörténjen a prémium bor digitális azonosítójának összekapcsolása a fizikai palack dugójával. A fizikailag nem klónozható függvények (PUF) a hardverbiztonság egyik fontos eleme, ahol az eszköz egyedi fizikai sajátosságain alapulva egy adott bemenetre a függvény nem klónozható, egyedi eszközválaszt hoz létre. A PUF kimenete egy olyan titkos érték lenne, amely bizonyítaná, hogy a termék nem hamisított. Mivel fontos, hogy a PUF érték titkos legyen és ne szivárogjon ki semmilyen részinformáció erről az értékről ezért nullaismeretű protokollt kell alkalmaznunk. A nullaismeretű protokolloknak három kritériumnak kell megfelelniük: teljesség, megbízhatóság és nulla ismeret. A nullaismeretű protokollok segítségével a dugóban lévő NFC chip képes bizonyítani a titkos érték helyességét úgy, hogy más információt nem ad ki.

Kulcsszavak:

prémium bor termékek, blokklánc, nullaismeretű protokollok, fizikailag nem klónozható függvények

Cybersecurity - session VII.– Artificial intelligence and blockchain

PROTECTING PREMIUM WINE PRODUCTS USING BLOCKCHAIN

Norbert OLÁH

Today, the wine trade is an influential market where hectolitres change hands. However, it is not without fraud and counterfeiting, and scandals that come to light from time to time shake the wine world to its foundations.

The proposed solution is to use blockchain technology to protect the verifiability, traceability, authenticity and integrity of the data linked to the product. Once the data is available on the blockchain, it is essential to link the digital identifier of the premium wine to the physical bottle cork. Physically Unclonable Functions (PUF) are an important element of hardware security, where a function generates an unclonable, unique device response based on the unique physical characteristics of the device for a given input. The output of a PUF would be a secret value that would prove that the product is not counterfeit. Since it is vital that the PUF value is hidden and that no partial information about it is leaked, we must use a zero-knowledge protocol. Zero-knowledge protocols must meet three criteria: completeness, soundness and zero-knowledge. Zero-knowledge protocols allow the NFC chip in the plug-in to prove the correctness of the secret value without outputting any other information.

Keywords:

premium wine products, blockchain, zero-knowledge protocols, physically unclonable functions

Kiberbiztonság - VIII. szekció - Egészségügy

Cybersecurity - session VIII. - Healthcare

Kiberbiztonság - VIII. szekció - Egészségügy

EGÉSZSÉGÜGYI KIBERBIZTONSÁG 2023-BAN: HUNEX KIBERVÉDELMI GYAKORLAT TAPASZTALATOK

MARSI Tamás, ARADI Zoltán

2023-ban az egészségügyi szektor kiemelt célpontja volt a kiberbűnözők számára, amit az év során bekövetkezett támadások – például a KillNet DDoS támadásai vagy a barcelonai klinikát érintő incidensek – is igazolnak. A HunEx program keretében 2023-ban és 2024 elején két nagyszabású kibervédelmi gyakorlatot hajtottak végre, amelyeken 26 szervezet több mint 160 tagja vett részt. A gyakorlatok elsődleges célja az incidenskezelési és kommunikációs képességek mérése, a kiberbiztonsági együttműködés erősítése, valamint a nemzetközi jó gyakorlatok adaptálása volt.

A HunEx gyakorlatok keretében a résztvevők számára nem tartozott a feladatokba a kibertámadások során érintett rendszerek teljes körű helyreállítása vagy a mélyreható hálózati elemzés, ehelyett a gyakorlat a valós idejű döntéshozatali folyamatok, a kommunikációs stratégiák és a jogszabályi kötelezettségek teljesítésének tesztelésére fókuszált.

Az eredmények rávilágítottak az egészségügyi szektor gyenge pontjaira, például a hatósági bejelentések és a kommunikáció terén. Ugyanakkor számos pozitívum is azonosításra került, például a felsővezetés megfelelő tájékoztatása. Az előadás összegzi a gyakorlatok tanulságait, és javaslatokat tesz a kiberbiztonsági együttműködés javítására.

Kulcsszavak:

kiberbiztonság, egészségügy, incidenskezelés, HunEx, nemzetközi gyakorlatok

Cybersecurity - session VIII. - Healthcare

CYBERSECURITY IN THE HEALTHCARE SECTOR IN 2023 – INSIGHTS FROM THE HUNEX EXERCISES

Tamás MARSI, Zoltán ARADI

In 2023, the healthcare sector became a prime target for cybercriminals, as demonstrated by significant incidents such as the KillNet DDoS attacks and the breach affecting a clinic in Barcelona. Within the framework of the HunEx program, two large-scale cybersecurity exercises were conducted in 2023 and early 2024, involving more than 160 participants from 26 organizations. The primary objectives of these exercises included assessing incident management and communication capabilities, strengthening cybersecurity cooperation, and adapting international best practices.

The tasks within the HunEx exercises did not include the comprehensive restoration of systems affected by cyberattacks or in-depth network analysis. Instead, the focus was placed on testing real-time decision-making processes, communication strategies, and compliance with legal obligations.

The findings highlighted several vulnerabilities in the healthcare sector, particularly in the areas of authority reporting and communication. At the same time, numerous positive aspects were identified, such as effective communication with senior management. This presentation summarizes the lessons learned from the exercises and provides recommendations to enhance cybersecurity collaboration.

Keywords:

cybersecurity, healthcare, incident management, HunEx, international best practices

Kiberbiztonság - VIII. szekció - Egészségügy

LEHETSÉGES BIZTONSÁGI INCIDENSEK EGY EGÉSZSÉGÜGYI INTÉZMÉNYBEN

ALEXIN Zoltán

Az egészségügyi ellátás digitalizálása az ezredforduló körül indult el egye gyorsuló ütemben. Mára az intézményekben nagyjából 25 évnyi ellátási adatmennyiség gyűlt össze. Ennek biztonságos kezelése jelentős feladat, amelynek során különböző súlyú incidensek is előfordulhatnak.

Egy nagyobb intézményben egészségügyi adatok nem kizárólag egyetlen nagy HIS rendszerben találhatók. További informatikai rendszerek látnak el kisegítő feladatokat, pl. vezérlik a különböző automatákat, orvosi képeket készítenek és dolgoznak fel. Az időpont foglalások egy része, valamint a dolgozók kommunikációja egy belső elektronikus levelezőrendszerben történik. Az intézményekben még mindig sok papír alapú irat, dokumentáció keletkezik.

A szerző szeretné példákon keresztül bemutatni, hogy milyen külső és belső támadások érhetnek egy intézményt. Kitérne arra is, hogy a gondatlanság, vagy az informatikai képzettség hiánya milyen károkat okozhat. Felhívná a figyelmet a harmadik országban található adatfeldolgozók problémájára, illetve a jövő évtől minden járó- és fekvőbeteg ellátó intézményekben telepítendő szoftver kockázataira.

Kulcsszavak:

egészségügyi adat, bizalmasság, biztonsági incidens, külső és belső támadások

Cybersecurity - session VIII. - Healthcare

SECURITY INCIDENTS THAT MAY HAPPEN IN A MEDICAL INSTITUTION

Zoltán ALEXIN

The digitization of health care started around the millennium at an accelerating pace. To date, approximately care data for 25 years have been accumulated in the institutions. Ensuring the security of the data processing is a significant task, during which incidents of varying severity may occur.

In a larger institution, health data are not exclusively stored in one large HIS system. Other IT systems perform additional tasks, e.g. they control various automata, take and/or process medical images. Appointment bookings partly, as well as employee communication, are done in an internal electronic mail system. Institutions still create a large amount of paper-based documentation.

The author would like to cite examples to show what kind of external and internal attacks can befall an institution. He would also address the damage that carelessness or a lack of IT training may cause. He would draw attention to the problem of data processors located in third countries, as well as the risks of the software to be deployed in all outpatient and inpatient care institutions from next year.

Keywords:

health data, confidentiality, security incident, external and internal attacks

Kiberbiztonság - VIII. szekció - Egészségügy

ÚTMUTATÓ A NIS 2 KIBERBIZTONSÁGI IRÁNYELV INTÉZMÉNYI BEVEZETÉSÉHEZ

NAGY István, RÉPÁS József

A szervezeteknek kellő gondossággal kell kezelniük az információbiztonsági és adatvédelmi kockázatokat egy átfogó kockázatkezelési program létrehozásával. Rendszerek biztonsági osztályba sorolása: Az információs rendszerek osztályozása az alapján, hogy milyen hatással lenne a szervezetre, ha azok sérülnének.
Védelmi intézkedések kiválasztása és végrehajtása: Azoknak a biztonsági és adatvédelmi ellenőrzéseknek a kiválasztása és alkalmazása, amelyek megfelelnek a szervezet küldetésének és üzleti igényeinek.
A védelmi intézkedések hatékonyságának értékelése: A védelmi intézkedések teljesítményének értékelése annak biztosítására, hogy azok a kívánt védelmet nyújtsák.
Rendszerek engedélyezése: A rendszerek hivatalos jóváhagyása az üzemeltetésre, biztosítva, hogy megfeleljenek a biztonsági és adatvédelmi követelményeknek.
Folyamatos felügyelet: Állandó felügyelet fenntartása az újonnan felmerülő fenyegetés és sebezhetőségek észlelése és kezelése érdekében.

Kulcsszavak:
kibererbiztontonság, NIS 2, NIST, kibertér, kockázatkezelés, biztonsági osztály

Cybersecurity - session VIII. - Healthcare

GUIDE TO THE INSTITUTIONAL INTRODUCTION OF NIS 2 DIRECTIVE

István NAGY, József RÉPÁS

Organizations have to handle the information security risks and privacy risks with sufficient care by creating a comprehensive risk management program.

Sorting of the Systems into the adequate security classes: Classification of information systems based on their affects to the organization in of their damage.

Selection and implementation of security controls: Selecting and applying of those security and data protection controls, which meet the organization's mission and business needs.

Evaluation of the efficiency of the protection measures: Evaluation of the protection measures' efficiency to ensure the required protection.

Authorization of the systems: Official approval of the systems' operation, ensuring that they meet the security and data protection requirements.

Continuous monitoring: Maintaining a permanent supervision to detect and manage the newly arisen threats and vulnerabilities.

Keywords:

cyber security, NIS 2, NIST, cyberspace, risk management, security class

Kiberbiztonság - VIII. szekció - Egészségügy

A MESTERSÉGES INTELLIGENCIA FEJLŐDÉSÉNEK TRENDJE AZ EGÉSZSÉGÜGYI ELLÁTÓ FOLYAMATOKBAN

TISÓCZKI József

A hazai egészségügyi ellátó szektorban is egyre inkább megfigyelhető a mesterséges intelligencia (AI) informatikai megoldások térnyerése. Kiemelkedő a diagnosztikus és tervező (3D) informatikai szoftverek térnyerése. Tanulmányomban szakirodalmi módszertani elemzéssel egymás mellé állítom a magyarországi, valamint több Európai Uniós országban, az elmúlt években megvalósult egészségügyi mesterséges intelligencia alkalmazások fejlődési trendjeit. Vizsgálatom tárgya a következő évek fejlődésének trendje, annak a betegbiztonságra, a morbiditásra és mortalitásra gyakorolt hatása. Az egészségügyben bevezetésre kerülő mesterséges intelligencia megoldások (AI) döntő hányada, szignifikáns módon a diagnosztikus szakmaterületeken kerül bevezetésre. Ugyanakkor az alkalmazott technológiai megoldások tervezése, bevezetése, majd azok mindennapi alkalmazása során kiemelt figyelmet szükséges fordítani az AI megoldások folyamatmodelljeiben megjelenő, felhőtechnológiát (cloud) érintő kiberbiztonsági trendekre is.

Kulcsszavak:

mesterséges intelligencia, egészségügy, cloud, kiberbiztonság

Cybersecurity - session VIII. - Healthcare

TRENDS IN THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE IN HEALTHCARE PROCESSES

József TISÓCZKI

The healthcare sector in Hungary is also witnessing the increasing use of artificial intelligence (AI) IT solutions. The rise of diagnostic and design (3D) informatics software is prominent. In my study, I present a methodological analysis of the literature to compare the development trends of health artificial intelligence applications in Hungary and several European Union countries in recent years. My study's subject is the following year's development trend and its impact on patient safety, morbidity and mortality. Most AI solutions in the healthcare sector will be implemented significantly in the diagnostic specialities. At the same time, the technology solutions' design, deployment and day-to-day use must pay particular attention to the cybersecurity trends in the cloud reflected in AI solutions' process models.

Keywords:
artificial intelligence, cloud, healthcare, cybersecurity

Kiberbiztonság - VIII. szekció - Egészségügy

A DIGITÁLIS EGÉSZSÉGÜGYI INFRASTRUKTÚRA KIBERVÉDELMI KIHÍVÁSAI: KOCKÁZATELEMZÉS AZ INTERNETRE CSATLAKOZTATHATÓ ORVOSI ESZKÖZÖK

GULYÁS László

A modern egészségügyi rendszer egyre inkább függ az internetre csatlakoztatható orvosi eszközöktől, amelyek egyszerre biztosítanak gyors és hatékony betegellátást, miközben növelik a kibertámadások kockázatát is. A dolgozat célja, hogy feltárja a digitális egészségügyi infrastruktúra főbb kiberbiztonsági kihívásait, különös tekintettel a kritikus internetre kapcsolódó orvosi eszközök, mint például pacemakerek, defibrillátorok és vérnyomásmérők sérülékenységét. A kutatás a kiberbiztonsági fenyegetéseket két modell, a SecRam és az Octave módszertan alapján elemzi, hogy megérthessük ezek alkalmazhatóságát a sebezhetőségek és a kockázatok kezelésében. A dolgozat hipotézisei között szerepel, hogy képes-e a kockázatelemzés hatékonyan csökkenteni a kibervédelem sérülékenységét az egészségügyi szektorban, illetve ez a módszertan hozzájárulhat-e a betegadatok és rendszerek biztonságos működéséhez. Az eredmények rávilágítanak a kiberfenyegetések jelentőségére, valamint arra, hogy a kockázatkezelési stratégiák fejlesztése kulcsfontosságú a jövő egészségügyi szolgáltatásainak védelmében. Az eredmények hangsúlyozzák az intézkedések szükségességét, melyek nélkülözhetetlenek a modern egészségügyi ellátás biztonságos működéséhez.

Kulcsszavak:

kockázatelemzés, kiberbiztonság, IoMT, OCTAVE, egészségügy

Cybersecurity - session VIII. - Healthcare

CYBERSECURITY CHALLENGES IN DIGITAL HEALTH INFRASTRUCTURE: RISK ANALYSIS OF INTERNET-CONNECTED MEDICAL DEVICES

László GULYÁS

The modern healthcare system increasingly relies on internet-connected medical devices, which provide fast and efficient patient care while also increasing the risk of cyberattacks. The aim of this paper is to explore the major cybersecurity challenges in digital healthcare infrastructure, with a particular focus on the vulnerabilities of critical internet-connected medical devices such as pacemakers, defibrillators, and blood pressure monitors. The research analyzes cybersecurity threats through two models, the SecRam and Octave methodologies, to understand their applicability in managing vulnerabilities and risks. The paper's hypotheses include whether risk analysis can effectively reduce cybersecurity vulnerabilities in the healthcare sector and whether this methodology contributes to the safe operation of patient data and systems. The findings highlight the significance of cybersecurity threats and the importance of developing risk management strategies that are essential for protecting future healthcare services. The results emphasize the need for cybersecurity measures that are indispensable for the safe operation of modern healthcare services.

Keywords:
cybersecurity, risk analysis, IoMT, Octave, healthcare

Kiberbiztonság - IX. szekció – Digital forensics II.

Cybersecurity - session IX.– Digital forensics II.

Kiberbiztonság - IX. szekció - Digital forensics II.

DIGITÁLIS NYOMOK KINYERÉSE ÉS FELHASZNÁLÁSA A PILÓTA NÉLKÜLI LÉGIJÁRMŰVEK ESETÉN

RIPSZÁM Dóra, RÉPÁS József

A pilóta nélküli légijármű-rendszerek technológiai fejlődése az elmúlt időszakban rohamos fejlődésen ment keresztül. Ezek az eszközök bizonyos bűncselekmények körülményeinek tisztázása szempontjából kiemelkedő jelentőségű video- és fényképfelvételeket, valamint repülési adatokat (pl.: földrajzi koordináták, sebesség, magassági adatok). A polgári (nem katonai) felhasználásban lévő pilóta nélküli légijárművek (UAV) általában nem különböznek nagyban a távirányítású repülő- vagy helikopter modellektől. Kisméretű fedélzeti számítógépet és adattárolót tartalmaznak, emellett általában kamerát. Működtethetők vezetéknélküli hálózaton keresztül pl.: Wi-Fi-n keresztül okos telefonról, tabletről vagy kifejezetten erre készített távirányítóról is. Ezen eszközök és maga az UAV is tartalmaz digitális adatokat, melyek kinyerés után felhasználhatóak utólagos szakértői vizsgálatok során.

A büntetőjog követi a technológiai fejlődési irányokat, ennek megfelelően, valamint a büntető eljárásjog bevezette az „elektronikus adat” fogalmát, így a jogszabály külön nevesíti a digitális eszközökkel és módszerekkel kinyerhető, feldolgozható és megjeleníthető adatokat, amelyek az eljárás során bizonyítékként használhatóak fel.

Kulcsszavak:

UAV, digitális nyomok, elektronikus adat, szakértői vizsgálatok

Cybersecurity - session IX.– Digital forensics II.

EXTRACTING AND USING DIGITAL EVIDENCE FROM UNMANNED AERIAL VEHICLES

Dóra RIPSZÁM, József RÉPÁS

The technological development of unmanned aircraft systems has undergone rapid development recently. These devices can help clarify the circumstances of certain crimes, with video and photograph recordings and flight data (e.g. geographical coordinates, speed, altitude data). Unmanned aerial vehicles (UAVs) in civilian (non-military) use are generally not much different from remotely piloted aircraft or helicopter models. They contain a small onboard computer and data storage, and usually one or more cameras. They can be operated via a wireless network, e.g. via Wi-Fi from a smartphone, tablet, or specific remote control device. These devices and the UAV itself contain digital data. These after extraction, can be used in digital forensics examinations.

Criminal law follows technological developments accordingly, and criminal procedure introduced the concept of "electronic data", so the law specifically mentions data that can be obtained, processed and displayed by digital means and methods, which can be used as evidence during proceedings.

Keywords:

UAV, digital evidence, digital data, digital forensics

Kiberbiztonság - IX. szekció - Digital forensics II.

IGAZSÁGÜGYI INFORMATIKAI SZAKÉRTŐI TEVÉKENYSÉG KIHÍVÁSAI

SCHMIDT Miklós

Az informatika egésze az elmúlt évtizedekben hatalmas fejlődésen ment keresztül, amely a mai napig tart. A korunkban megjelenő mesterséges intelligencia fejlődésével, széles körű elterjedésével ez a fejlődés újabb és újabb területeket sző át. Az informatika, a számítógépek és a mobil kommunikációs eszközök széleskörű elterjedése az emberek mindennapi életére komoly kihatással van az élet minden területét átalakítja, beleértve az igazságszolgáltatást is. Az igazságügyi informatikai szakértői tevékenység kulcsfontosságú szerepet játszik a digitális bizonyítékok kezelésében, a különböző informatikai rendszerek elemzésében és az adatok hitelességének megállapításában. Az ilyen szakértői tevékenység azonban számos kihívással néz szembe, amelyek mind technológiai, mind jogi és etikai tényezőkből fakadnak. Az igazságügyi informatikai szakértő feladatai közé tartozik a digitális bizonyítékok gyűjtése, azok elemzése és a megállapítások dokumentálása. E tevékenység során a szakértőknek különösen nagy figyelmet kell fordítaniuk az adatok hitelességére és integritására, hiszen a jogi eljárásokban ezek alapvető fontosságúak. Az olyan innovációk, mint a blockchain, az Internet of Things (IoT) és a mesterséges intelligencia újabb és újabb feladatok elé állítják az igazságügyi informatikai szakértőket. A technológiai kihívásokon túl az igazságügyi informatikai szakértőknek megfelelően kell alkalmazkodniuk a jogi és szabályozási környezethez is.

Kulcsszavak:

szakértői vizsgálatok, informatika, igazságügyi szakértő, digitális nyomok

Cybersecurity - session IX.– Digital forensics II.

CHALLENGES OF COMPUTER FORENSICS ACTIVITY

Miklós SCHMIDT

Information technology has undergone tremendous development in recent decades, which continues nowadays. With the development and spread of artificial intelligence appearing in our time, this development weaves through more and more new areas. The widespread use of information technology, computers, and mobile communication devices has a profound impact on people's daily lives, transforming all areas of life, including the judiciary. Computer forensics plays a key role in managing digital evidence, analyzing different IT systems, and establishing the authenticity of data. However, such expertise faces several challenges stemming from technological, legal, and ethical factors. The tasks of computer forensics include collecting digital evidence, analyzing it, and documenting evidence. In carrying out this activity, experts should pay particular attention to the authenticity and integrity of data, which are essential in legal processes. Innovations such as blockchain, the Internet of Things (IoT), and artificial intelligence are constantly challenging forensics experts. In addition to technological challenges, the experts also need to adapt appropriately to the legal and regulatory environment.

Keywords:
computer forensics, informatics, forensics expert, digital evidence

Kiberbiztonság - IX. szekció - Digital forensics II.

MODERN JÁRMŰVEK FOLYAMATSZEMLÉLETŰ UTÓLAGOS SZAKÉRTŐI VIZSGÁLATA

SCHMIDT Miklós, RÉPÁS József

A modern járművek kiberbiztonsága mind a gyártói és fejlesztői, mind a felhasználói oldalon fontos szempont. A gyártási folyamatokba épített és a járművek működéséhez kapcsolódó biztonsági követelmények hozzájárulnak a biztonságos közlekedéshez, megalapozzák az intelligens közlekedési rendszereket.

A fejlett vezetéstámogató rendszerek működéséhez nagy mennyiségű, gyors, minőségi és pontos információk szükségesek. Az információk gyűjtése, tárolása és feldolgozása a gyártói oldal által meghatározott folyamatok mentén történik. A járművekben a feldolgozás után is megőrzésre kerülnek olyan adatok, melyek utólagos szakértői vizsgálata hozzájárul a járműhöz kapcsolódó események pontos megismeréséhez. Legyen szó balesetről, kibertámadásról és hasonlókról.

A jelenlegi szakértői folyamatok nem, vagy jelentős módosítással alkalmasak a modern járművek vizsgálatára. Az adatgyűjtési és megőrzési fázist a bekövetkezett eseményhez mielőbb meg kell kezdeni, amiben kiemelt szerepe lehet a rendőrségnek. Jelen tanulmány célja az adatkinyeréshez kapcsolódó folyamatok illesztése a hatósági és szakértői munkához.

Kulcsszavak:

utólagos szakértői vizsgálatok, modern járművek, baleset vizsgálat, szakértői módszertan

Cybersecurity - session IX.– Digital forensics II.

PROCESS-BASED FORENSIC EXAMINATION OF MODERN VEHICLES

Miklós SCHMIDT, József RÉPÁS

The cybersecurity of modern vehicles is an important issue for manufacturers, developers, and users. The security requirements built into the production processes and related to the operation of vehicles contribute to safe transport and lay the foundations for intelligent transport systems. Advanced driver assistance systems require a large amount of fast, high-quality, and accurate information. The information is collected, stored, and processed according to processes defined by the manufacturer. Even after processing, the data is retained in the vehicle, and forensic examination of the data can provide accurate knowledge of what happened to the vehicle. Be it an accident, a cyber attack, or the like.

The current forensics processes are unsuitable for examining modern vehicles, or just with significant modifications. The data collection and acquisition phase must start as soon as possible after the event has occurred, where the police can play a key role. This study aims to adapt the data extraction processes to the work of the police and experts.

Keywords:
digital forensics, modern vehicles, accident investigation, forensics methodologies

Kiberbiztonság - IX. szekció - Digital forensics II.

LIVE FORENSICS FOLYAMATA, MÓDSZEREI ÉS ESZKÖZEI

POGÁNY Viktor

Az tanulmányom fő témája a digitális forensics egy feltörekvő részterülete a live forensics, amely futó rendszereken végez szakértői vizsgálatokat. A komplex digitális szakértői vizsgálat három részterületre osztható fel, amely alapján a szakértői vizsgálat lehet élő, proaktív és reaktív. Az élő szakértői vizsgálat során aktív rendszereken végezhetünk el elemzéseket.

A live forensics előnye, hogy további információkat biztosít, amelyek nem állnak rendelkezésre a képfájlokon, azaz olyan adatokhoz is hozzájuthatunk, amelyekhez egy hagyományos szakértői vizsgálat során nem feltétlenül tudnánk.

Az élő szakértői vizsgálat az incidensekre adott válaszadási folyamat fontos részévé válhat minden üzleti szervezetben, ahol olyan szerverekről van szó, amelyek kritikusak az üzletmenet szempontjából, és nem lehet leállítani vagy minimalizálni kell a kritikus folyamatok megszakítását az incidens kivizsgálása közben.

Tanulmányomban kitérek a live forensics technikáira, melyek közé tartozik a volatilis memória elemzése, a fordított szteganográfia és sztochasztikus elemzés is. Rövid leírást adok az alkalmazott eszközökről is, továbbá az élő szakértői vizsgálat előnyeiről, mely többek közt a magasabb idő- és költséghatékonyság, megbízhatóbb bizonyítékok, az illékony memóriaadatok megfelelő beszerzése és elemzése.

A tanulmány végén említést teszek a live forensics kihívásairól is melyekhez sorolhatjuk az anti-forensics eszközök használatát a futó rendszereken, vagy az adatkonzisztencia kihívásait is.

Kulcsszavak:

élő szakértői vizsgálat, live forensic, illékony memória, futó rendszerek

Cybersecurity - session IX.– Digital forensics II.

LIVE FORENSICS PROCESS, TECHNIQUES AND TOOLS

Viktor POGÁNY

The main topic of my study is an emerging subfield of digital forensics, live forensics, which performs forensic investigations on running systems. Complex digital forensics can be divided into three sub-fields, based on which forensic investigations can be classified as live, proactive and reactive. Live forensic investigations allow us to perform analysis on active systems. The advantage of live forensics is that it provides additional information that is not available on image files, i.e. we can access data that we would not necessarily be able to access during a traditional forensic examination. Live Forensic Investigation can become an important part of the incident response process for any organisation that has servers that are critical to business operations and cannot be shut down, or that needs to minimise disruption to critical processes while the incident is being investigated. In my study, I will discuss live forensic techniques that include volatile memory analysis, reverse steganography and stochastic analysis. I will also briefly describe the tools used and the benefits of live forensics, including increased time and cost efficiency, more reliable evidence, and proper acquisition and analysis of volatile memory data. At the end of the study I will also mention the challenges of live forensics, including the use of anti-forensic tools on running systems or the challenges of data consistency.

The purpose of this study is to provide a brief introduction to the process, benefits, tools and challenges of this field, and to give an insight into this exciting area of digital forensics.

Keywords:

forensic examination, live forensics, volatile memory, running systems

Kiberbiztonság - X. szekció - Média

Cybersecurity - session X.– Media

Kiberbiztonság - X. szekció - Média

SECURITY AWARENESS MEASUREMENT (SAM) - AZ INFORMÁCIÓBIZTONSÁG-TUDATOSSÁG MÉRÉSÉNEK ÚJ MEGKÖZELÍTÉSE

RÉPÁS József, LASKA Pál, BAK Gerda, BEREK László, OLÁH Norbert, UJHEGYI Péter, VINOGRADOV Szergej

A digitalizáció elterjedésével egyre nagyobb az információbiztonság jelentősége és ezen belül az egyének biztonságtudatossága. Az új és készülő kiberbiztonsági jogszabályok nagy hangsúlyt fektetnek a biztonsági szint növelésére. Kutatásunk során áttekintettük a nemzetközi kutatásokban alkalmazott különböző mérési módszereket, amelyekkel az egyének információbiztonsági tudatossági szintjét lehet mérni. A nemzetközi szakirodalomban végzett, kiterjedt irodalomkutatás során elemeztük a releváns tanulmányokat, előre definiált szempontok szerint. Ennek eredményeképp megállapíthatjuk, hogy a kérdőív a leggyakrabban alkalmazott mérőeszköz, azonban a kutatásokban jelentős eltérések figyelhetők meg a kérdőívek felépítésében és tartalmában. A leggyakrabban alkalmazott nevesített felmérés a HAIS-Q volt, amely átalakítása és továbbfejlesztése volt a kutatócsoportunk soron következő feladata.
Jelen publikációnkban a SAM (Security Awareness Measurement) kialakításának folyamatát mutatjuk be, kitérve a legfontosabb változások indoklására.

Kulcsszavak:

Security Awareness Model, kiberbiztonság, biztonságtudatosság, kérdőív, kvantitatív mérés

Cybersecurity - session X.– Media

SECURITY AWARENESS MEASUREMENT (SAM) - A NEW APPROACH TO MEASURING THE INFORMATION SECURITY AWARENESS

József RÉPÁS, Pál LASKA, Gerda BAK, László BEREK, Norbert OLÁH, Péter UJHEGYI, Szergej VINOGRADOV

With the spread of digitalization, the importance of information security and, within that, the security awareness of individuals is increasing. New and upcoming cybersecurity legislation emphasizes the importance of enhancing security levels. In our research, we reviewed the various measurement methods used in international studies to measure the level of information security awareness of individuals. We analyzed relevant studies through extensive literature research in the international literature, according to predefined criteria. As a result, we can conclude that the questionnaire is the most frequently used measurement tool; however, there are significant differences in the structure and content of the questionnaires used in the research. The most frequently used named survey was the HAIS-Q, the modification and further development of which was the next task of our research team.

In this publication, we present the process of developing the SAM, explaining the reasons for the most important changes.

Keywords:

Security Awareness Model, cybersecurity, security awareness, questionnaire, quantitative measurement

Kiberbiztonság - X. szekció - Média

ONLINE ZAKLATÁS ÉS MENTÁLIS EGÉSZSÉG: A KPOP RAJONGÓK KIHÍVÁSAI A DIGITÁLIS KÖZEGBEN

PILBÁT Jácinta-Orsolya

A K-pop, Dél-Korea zenei iparának globális sikere nemcsak műfaj, hanem kulturális mozgalom is, amely milliókat vonz világszerte. A rajongói közösségek, az úgynevezett „fandomok”, szenvedélyesek és elkötelezettek, de online jelenlétük gyakran megosztóvá válik. A K-pop rajongók nemcsak idoljaik védelmezői, hanem könnyen az online zaklatás célpontjaivá is válhatnak, legyen szó rivalizáló fandomok támadásairól vagy személyes támadásokról. Ez a folyamatos online zaklatás jelentős hatással lehet a rajongók mentális egészségére, akik nap mint nap kritikával és konfliktusokkal szembesülnek a digitális platformokon.

A kutatás célja, hogy kérdőíves felméréssel feltárja, hogyan befolyásolja az online zaklatás a K-pop rajongók mentális állapotát. A felmérés az ECIPQ (Emotional and Cognitive Impact of Online Harassment Questionnaire) modellt használja, amely a zaklatás különböző aspektusait értékeli. Az összegyűjtött adatokat statisztikai módszerek segítségével elemzi ki a szerző, hogy részletes képet nyújtson a jelenség súlyosságáról és annak pszichológiai hatásairól.

Kulcsszavak:

kpop, online zaklatás, mentális egészség, rajongó, fandom

Cybersecurity - session X.– Media

ONLINE HARASSMENT AND MENTAL HEALTH: K-POP FANS' CHALLENGES IN THE DIGITAL SPACE

Jácinta-Orsolya PILBÁT

K-pop, the global success of South Korea's music industry, is not merely a genre but a significant cultural phenomenon that captivates millions of fans around the world. The fan communities, known as "fandoms," are characterized by their intense passion and dedication. However, their presence online often becomes controversial and divisive. K-pop fans, while ardently defending their idols, frequently become targets of online harassment, which can come from rival fandoms or involve personal attacks. This relentless online harassment can have a profound impact on the mental health of fans, who are exposed to constant criticism and conflicts on various digital platforms.

This study aims to investigate how online harassment affects the mental well-being of K-pop fans through a comprehensive survey. The survey utilizes the ECIPQ (Emotional and Cognitive Impact of Online Harassment Questionnaire) model to assess various dimensions of harassment. The collected data will be analyzed using statistical methods to provide an in-depth understanding of the severity of the issue and its psychological effects. This analysis will offer valuable insights into the challenges faced by K-pop fans and contribute to a better understanding of the impact of online harassment on their mental health.

Keywords:

kpop, cyberbullying, fans, fandom, mental health

Kiberbiztonság - X. szekció - Média

A DIGITÁLIS GYERMEKVÉDELEM SZEREPE A GYERMEKKERESKEDELEM MEGELŐZÉSBEN

RIPSZÁM Dóra

Az emberkereskedelem áldozatainak számtalan esetben van internet-hozzáférése és sokan aktív résztvevőik a közösségi médiának.

A gyermekkereskedelem toborzásának módjai a közösségi média térnyerésével párhuzamosan jelentős fejlődésen mentek keresztül. A gyermekek internet – és elsősorban közösségi média – használatát az online tudatosság igen csekély mértékben jellemzi. A gyermekkereskedők számára könnyen megismerhetővé válik a gyermek napi rutinja, tartózkodási helye, szokásai, kedvelt dolgai.

Magyarország Digitális Gyermekvédelmi Stratégiájának kiemelt célja a tudatos, internethasználat támogatása mellett, hogy az eddigieknél hangsúlyosabban érvényesüljenek a gyermekek védelmét biztosító szabályok és intézkedések. Ennek érdekében elengedhetetlen az internethasználat során a gyermekekre leselkedő veszélyek, kockázatok azonosítása, valamint azok kiküszöbölése. Ezáltal a káros hatások megelőzése, illetve azok csökkentése.

Kulcsszavak:

gyermekkereskedelem, emberkereskedelem és kényszermunka, digitális gyermekvédelem, Magyarország Digitális Gyermekvédelmi Stratégiája

Cybersecurity - session X.– Media

THE ROLE OF DIGITAL CHILD PROTECTION IN THE PREVENTION OF CHILD TRAFFICKING

Dóra RIPSZÁM

In many cases, victims of human trafficking have access to the Internet and many are active on social media.

The methods of recruiting child trafficking victims have evolved significantly alongside the rise of social media. Children's use of the Internet - and especially social media - is often marked by a lack of online awareness. Child traffickers can easily get to know the child's daily routine, place of residence, habits, and favorite things.

In addition to promoting conscious Internet use, the main goal of Hungary's Digital Child Protection Strategy is to ensure that the rules and measures protecting children are enforced more effectively than before. To this end, it is essential to identify and eliminate the dangers and risks children face when using the Internet. This will help prevent and reduce harmful effects.

Keywords:

child trafficking, trafficking in human beings and forced labour, digital child protection, Hungary's Digital Child Protection Strategy

Kiberbiztonság - X. szekció - Média

CAN FORGALOM VIZSGÁLATA MACHINEL LEARNING SEGÍTSÉGÉVEL

HIDVÉGI Timót

A CAN (Controller Area Network) protokoll nagyon elterjedt, sok helyen alkalmazzák. Használják a gépjárműveknél, illetve az ipari hálózatoknál is. Ezt a protokollt széles körben használják, noha sok sérülékenységgel rendelkezik. Különböző támadási módok jelentek meg, amelyek sikeresen alkalmazhatók a CAN protokollnál. Ilyenek például: flooding, spoofing, fuzzing, replay, impersonation.

Ezek a támadások veszélyesek, mert a gépjárművek felett átvehető az irányítás, amely a környezetet is veszélyezteti (V2X). A védekezés nem egyszerű, mert például a CAN protokollnak nincsen küldője és címzettje. Nehéz tehát valós időben megkülönböztetni a korrekt frame-eket a támadástól.

A CAN buszon nagysebességű adatforgalom van, ezért célszerű alkalmazni a Mesterséges Intelligenciát. A Machine Learning-nél több algoritmus és modell található, amelyek talán sikeresen alkalmazhatók a védekezésben. A kutatásban a regresszió került részletes vizsgálat alá.

A kutatás miatt készíteni kellett egy fejlesztői környezetet. A fejlesztőkörnyezetben mikrovezérlők, CAN shield-ek és egy Infotainment (Android Automative OS) található.

Kulcsszavak:

CAN, gépi Tanulás, mesterséges Intelligencia, V2X, android OS, infotainment

Cybersecurity - session X.– Media

CAN TRAFFIC ANALYSIS USING MACHINE LEARNING

Timót HIDVÉGI

The CAN (Controller Area Network) protocol is very widespread and used in many places. It is also used in automotive and industrial networks (Operational Techjnology, OT). This protocol is widely used, although it has many vulnerabilities. Various attack methods have emerged that can be successfully applied to the CAN protocol. For Example: flooding, spoofing, fuzzing. replay, impersonation.

These attacks are dangerous because they can take control of vehicles, which can also endanger the environment (V2X). The defence is not easy because, for example, the CAN protocol has no sender and receiver. Therefore, it is difficult to distinguish in real time between correct frames and attacks.

The CAN bus has high-speed data traffic, so it is advisable to use Artificial Intelligence. Machine Learning has several algorithms and models that may be successfully applied in the defence. In this research, regression has been studied in detail.

A development environment had to be created for this research. The development environment contains microcontrollers, CAN shields and an infotainment (Android Automative OS). Large data flows were created and Machine Learning algorithms were tested on them.

Keywords:

CAN, machine learning, artificial intelligence, V2X, android automative OS, infotainment

Kiberbiztonság - XI. szekció - Új technológiák

Cybersecurity - session XI.– New technologies

Kiberbiztonság - XI. szekció – Új technológiák

KATASZTRÓFAVÉDELMI CÉLÚ PRECÍZIÓS TÉRKÉPI ÚTVONALTERVEZÉS DRÓNOK SZÁMÁRA

HAJDÚ Edina, PÁL Márton, PATZELT Miklós, JUNG András

Napjainkban a drónos rendszerek egyre fontosabb szerepet játszanak a különböző katasztrófavédelmi beavatkozásokban, védelemben. A MOL Dunai Finomítója szeretne újításokat bevezetni a kritikus infrastruktúra védelmének érdekében. A százhalombattai finomító területén felmerült a drónos légi útvonalak igénye. Mivel kritikus infrastruktúráról van szó, minimalizálni kell a légi jármű lezuhanásával járó károkat. Ehhez a lehető legnagyobb pontosságú geodéziai GPS-mérések szükségesek. Minden esetben az utak középvonalát, töréspontjait, kereszteződéseket, valamint a fontosabb beavatkozási pontokat mértük fel.

Ezt követően elkészült egy vektoros útvonaladatbázis. Egy esetleges vészhelyzet bekövetkeztekor a tűzoltók híradós tisztje kiválasztja a megfelelő útvonalat, amin a drón automatikusan elindul. Repülés közben vizuális felderítést végez az eszköz, egy időben több képmegjelenítő eszközön is nyomon lehet követni az élő közvetítést. Így a beavatkozásban résztvevők és az irányításért felelősök a helyszínre érkezés előtt megkezdhetik az oltási terv kialakítását.

Az eredményeket és a nemzetközi trendeket figyelembe véve a drónok bevetése a katasztrófavédelembe előremutató kutatási és fejlesztési cél hazánkban is.

Kulcsszavak:

UAS, vektoradatbázis, MOL Magyarország, kritikus infrastruktúra, RTK műszer

Cybersecurity - session XI.– New technologies

PRECISION MAP ROUTE PLANNING FOR DISASTER MANAGEMENT

Edina HAJDÚ, Márton PÁL, Miklós PATZELT, András JUNG

Nowadays, drones play an increasingly important role in various disaster management interventions and protection. The MOL Danube Refinery would like to introduce innovations to protect critical infrastructure. The need for air routes for drones has been raised at the refinery in Százhalombatta. As it is critical infrastructure, the damage caused by an aircraft crash should be minimised. To achieve this, we wanted to be as accurate as possible when designing the routes. We used a geodetic RTK GPS in the field. In each case, we surveyed the centre line of the roads, breakpoints, intersections, and major intervention points.

A vector route geodatabase has been created. In an emergency, the fire brigade's communications officer selects the appropriate route, which the drone automatically follows. During the flight, the device performs visual reconnaissance, and the live video can be viewed simultaneously on several devices. In this way, those involved in the intervention and those in charge of management can start formulating an emergency plan before arriving on site.

Given the results and international trends, using drones in disaster management could also be a forward-looking research and development objective in our country.

Keywords:

UAS, vector database, MOL Hungary, critical infrastructure, RTK instrument

Kiberbiztonság - XI. szekció – Új technológiák

AZ ELEKTROMOBILITÁSI ESZKÖZÖK KIBERBIZTONSÁGI KOCKÁZATAI, KÜLÖNÖS TEKINTETTEL AZ E-ROLLEREKRE

HARANGOZÓ Valentin

A kutatás célja az volt, hogy alaposan vizsgálja az elektromobilitási eszközök kiberbiztonsági vonatkozásait, azonosítva a lehetséges kockázatokat és veszélyforrásokat, valamint feltárja a felhasználók és az elektromos járművek kiberbiztonsága közötti összefüggéseket.

A kutatás során részletesen elemeztem az eszközök potenciális sebezhetőségeit, beleértve az adatbiztonsági kockázatokat, a fizikai biztonság kérdéseit és a vezérlőrendszer sebezhetőségeit. Megvizsgáltam az elektromobilitási eszközöket felhasználók technológia elfogadási hajlandóságát a TAP-modell alkalmazásával összeállított kérdőíves kutatás alapján. Továbbá bemutatom a közvetlen tapasztalataimat egy elektromos roller sebezhetőségeiről az általam elvégzett biztonsági tesztelés alapján.

A kutatási eredmények fontos következtetéseket vonnak maguk után. A felhasználók, a szolgáltatók és a gyártók közötti együttműködés elengedhetetlen a kiberbiztonság növelése érdekében. A proaktív intézkedések elősegíthetik, hogy az elektromobilitási járművek és azok felhasználói biztonságosabb környezetben vehessék igénybe ezeket az innovatív közlekedési eszközöket, ezzel hozzájárulva: egy fenntartható, biztonságos és technológiailag fejlett közlekedési jövőért.

Kulcsszavak:

elektromobilitás, kiberbiztonság, elektromos járművek, adatbiztonság

Cybersecurity - session XI.– New technologies

CYBERSECURITY RISKS OF ELECTROMOBILITY VEHICLES, WITH SPECIAL FOCUS ON E-SCOOTERS

Valentin HARANGOZÓ

The aim of the research was to thoroughly examine the cybersecurity aspects of electromobility devices, identifying potential risks and threats, as well as exploring the relationship between user and electric vehicle cybersecurity.

During the research, I analyzed in detail the potential vulnerabilities of the devices, including data security risks, physical safety issues, and control system vulnerabilities. I examined users' willingness to adopt electromobility devices using a questionnaire-based study designed with the Technology Acceptance Model (TAM). Furthermore, I present my direct experiences regarding the vulnerabilities of an electric scooter based on security testing I conducted.

The research findings lead to important conclusions. Collaboration between users, service providers, and manufacturers is essential to enhance cybersecurity. Proactive measures can help ensure that users of electromobility vehicles can utilize these innovative transportation tools in a safer environment, thereby contributing to a sustainable, secure, and technologically advanced future of transportation.

Keywords:

electromobility, cybersecurity, electric vehicles, data security

Kiberbiztonság - XI. szekció – Új technológiák

IOT ESZKÖZÖK AZ OKOSOTTHONOKBAN

HANKÓ Viktória

Az IoT (Internet of Things) eszközök otthoni alkalmazása napjainkban egyre elterjedtebb, köszönhetően a különböző SmartHome megoldásoknak. A kényelmet előnyben részesítő megoldások, mint például a hangasszisztensek, az okos villanykapcsolók vagy az intelligens belépést támogató kamerák számos előnnyel járnak a háztartásoknak, azonban megannyi kockázatot hordoznak magukban.

Rengeteg olcsó eszköz kerül a forgalomba, melyet a fogyasztó előnyben részesít, azonban ezek az eszközök jellemzően minimálisan vagy egyáltalán nem rendelkeznek biztonsági funkciókkal. Emellett az alapvető biztonsági intézkedések, mint például az eszközök szoftvereinek rendszeres frissítése, a gyári jelszavak megváltoztatása és a hálózati forgalom monitorozása elengedhetetlenek a biztonságos működéshez. A felhasználóknak meg kell érteniük a kockázatokat és proaktívan lépéseket kell tenniük a biztonság érdekében.

Ebből fakadóan az előadás középpontjában az állampolgári tudatosság fejlesztése áll, különös tekintettel az IoT eszközök mindennapi használatára. A téma célja, hogy felhívja a figyelmet a technológiai eszközök tudatos alkalmazásának fontosságára és azok társadalmi hatásaira.

Kulcsszavak:

IoT, okosotthon, kiberbiztonság, tudatosság

Cybersecurity - session XI.– New technologies

IOT DEVICES IN SMARTHOMES

Viktória HANKÓ

The use of IoT (Internet of Things) devices at homes is becoming more and more widespread today, thanks to the various SmartHome solutions. Solutions that benefit convenience, such as voice assistants, smart light switches or smart entry cameras, bring many benefits to households, but also many risks.

Many low-cost devices are marketed and preferred by consumers, but these devices typically do not have any, or have minimal security features. In addition, basic security measures such as regularly updating device software, changing factory passwords and monitoring network traffic are essential for secure operation. Users need to understand the risks and take proactive steps to ensure security.

Hence, the focus of this presentation is on developing citizen awareness, with a special focus on the everyday use of IoT devices. The aim is to raise awareness of the importance of the conscious use of technological tools and their impact on society.

Keywords:

IoT, smart home, cybersecurity, awareness

Kiberbiztonság - XI. szekció – Új technológiák

IOT ESZKÖZÖK KIBERBIZTONSÁGI KIHÍVÁSAI AZ OKOS OTTHONOK VILÁGÁBAN

CSEPREGI Lili

Kutatásom az IoT eszközök kiberbiztonsági kihívásait vizsgálja az okos otthonok kontextusában. Az IoT, vagyis a dolgok internete, olyan eszközök hálózatát jelenti, amelyek csatlakoznak az internetre, adatokat gyűjtenek, és gyors adatcserére képesek egymás között. Az eszközök okos technológiával történő felruházása egyre inkább elterjed otthonainkban, azonban a felhasználók gyakran figyelmen kívül hagyják az ezekkel járó biztonsági kockázatokat. Az IoT eszközök alkalmazása tudatos felhasználást és felelős vásárlói hozzáállást igényel, de egyben a gyártók felelőssége a megfelelő védelem alapkövének letétele.

A kutatás célja az, hogy átfogó elemzést adjon az IoT technológia biztonsági kockázatairól, különösen az okos otthonokban jelentkező biztonsági incidensekről. Továbbá bemutatja az USA-ban és az EU-ban érvényes IoT szabályozásokat, valamint a legjellemzőbb sérülékenységeket és támadási típusokat, kiegészítve a megelőzési stratégiákkal. A kutatás a magyar felhasználók IoT eszközökhöz fűződő viszonyát is elemzi.

Kulcsszavak:

IoT, okos otthon, kiberbiztonság, sérülékenység, biztonságtudatosság

Cybersecurity - session XI.– New technologies

CYBERSECURITY CHALLENGES OF IOT DEVICES IN THE WORLD OF SMART HOMES

Lili CSEPREGI

This research examines the cybersecurity challenges of IoT devices in the context of smart homes. IoT (Internet of Things) refers to a network of devices that connect to the Internet, collect data, and can rapidly exchange data between each other. Equipping devices with smart technology is becoming more and more common in our homes as well, but users often ignore the security risks of these devices. The use of IoT devices requires consciousness and a responsible consumer attitude, but it is also the responsibility of manufacturers to lay the foundations for adequate protection.
The aim of this research is to provide a comprehensive analysis of the security risks of IoT technology, in particular security incidents in smart homes. It also presents the IoT regulations in the US and EU, as well as the most common vulnerabilities and attack types, complemented by prevention strategies. The research also analyses the attitude of Hungarian users towards IoT devices.

Keywords:
IoT, smart home, cybersecurity, vulnerability, security awareness

Kiberbiztonság - XII. szekció – Kutatás, fejlesztés II.

Cybersecurity - session XII.– Research and development II.

Kiberbiztonság - XII. szekció – Kutatás, fejlesztés II.

SÖTÉT HÁLÓZATOK ÉS SÖTÉT SZEMÉLYISÉGEK- A KIBERBIZTONSÁGI KOCKÁZATOK ÉS A PSZICHOLÓGIA ÖSSZEFÜGGÉSEI

LASKA Pál

A modern kiberbiztonság kihívásai nem csupán technológiai, hanem pszichológiai dimenziókat is magukban foglalnak. A kutatás a Dark Triad személyiségmodell – melynek komponensei a nárcizmus, machiavellizmus és pszichopátia – és a kiberbiztonsági fenyegetések közötti összefüggéseket vizsgálja. Az elérendő cél, hogy megtudjuk, milyen mértékben járulhatnak hozzá ezek a személyiségjegyek a rosszindulatú online viselkedéshez, például a hacking, a social engineering és egyéb kiberbűnözői tevékenységekhez. A módszertan a pszichológiai jellemzők vizsgálatán túl leíró statisztikai módszereket is alkalmaz. Az eredmények betekintést nyújtanak abba, hogyan használhatók pszichológiai profilok a kiberfenyegetések előrejelzésére és kezelésére, ezáltal segítve a hatékonyabb védekezési stratégiák kialakítását.

Kulcsszavak:

kiberbiztonság, pszichológia, személyiségjegyek, tudatosság-fejlesztés

Cybersecurity - session XII.– Research and development II.

DARK NETWORKS AND DARK PERSONALITIES – THE INTERSECTION OF CYBERSECURITY RISKS AND PSYCHOLOGY

Pál LASKA

Modern cybersecurity challenges encompass not only technological aspects but also psychological dimensions. This study explores the relationship between the Dark Triad personality model—comprising narcissism, Machiavellianism, and psychopathy—and cybersecurity threats. The primary objective is to determine the extent to which these personality traits contribute to malicious online behaviors, such as hacking, social engineering, and other cybercriminal activities. The methodology integrates both psychological profiling and descriptive statistical analyses to assess these associations. The findings provide insight into how psychological profiles can be leveraged to predict and mitigate cyber threats, ultimately aiding in the development of more effective defensive strategies.

Keywords:
cybersecurity, psychology, personality traits, awareness

Kiberbiztonság - XII. szekció – Kutatás, fejlesztés II.

A KIBERBIZTONSÁGI STRATÉGIALKOTÁS AKTUÁLIS KIHÍVÁSAI

SZABÓ Zsolt Mihály

A stratégia alapvetően meghatározza a vállalat fejlődését és irányítását. Hosszú távon csak azok a vállalatok lehetnek sikeresek, amelyek tudják, hogy hova akarnak eljutni, és hogy mit kell ezért megtenniük.

A stratégiaalkotás olyan folyamat, amely kiemelt szerepet játszik a vállalat életében, kijelöli az utat a jelenlegi helyzettől a kívánt jövőbe. A stratégiaalkotás nem csupán egy feladat, hanem egy folyamatosan alkalmazkodó és innovatív vállalati kultúra része, amely hosszú távon segíti a vállalatokat a siker elérésében és fenntartásában.

A kiberbiztonság napjainkban kritikus fontosságúvá vált minden vállalat számára. A legjobb kiberbiztonsági stratégiák általában négy közös tényezővel rendelkeznek: hatékony incidens- és válságkezelési terv; erős irányítás; megbízható védelem a fenyegetések ellen; valamint folyamatos biztonsági felügyelet. Az egyes tényezők szinergikusan együttműködve és egymást erősítve megbízható kiberbiztonsági védelmet teremtenek a szervezet számára.

A kiberbiztonsági stratégia négy részének, illetve ezek egymásra gyakorolt hatásának megértésével könnyebben felismerhetők a kiberfenyegetések, és lényegesen erősödhet a szervezet általános kiberbiztonsági felkészültsége.

Kulcsszavak:
Kiberbiztonsági stratégia, incidens- és válságkezelési terv, irányítás, fenyegetésvédelmi technológia, biztonsági felügyelet

Cybersecurity - session XII.– Research and development II.

THE CURRENT CHALLENGES OF CREATING A CYBER SECURITY STRATEGY

Zsolt Mihály SZABÓ

The strategy basically determines the development and management of the company. Only companies that know where they want to go and what they need to do to get there can be successful in the long run.

Strategy creation is a process that plays a prominent role in the life of the company, marking the path from the current situation to the desired future. Strategizing is not just a task, but part of a constantly adapting and innovative corporate culture that helps companies achieve and maintain success in the long term. Cyber security has become critical for every company these days. The best cybersecurity strategies generally have four factors in common: an effective incident and crisis management plan; strong governance; reliable protection against threats; and continuous security monitoring. The individual factors cooperate synergistically and reinforce each other to create reliable cyber security protection for the organization.

By understanding the four parts of the cyber security strategy and their impact on each other, cyber threats can be recognized more easily and the organization's overall cyber security preparedness can be significantly strengthened.

Keywords:

cybersecurity strategy, incident and crisis management plan, management, threat protection technology, security monitoring

Kiberbiztonság - XII. szekció – Kutatás, fejlesztés II.

A FELHŐBIZTONSÁG JELENTŐSÉGE A KKV-K SZÁMÁRA

BAK Gerda

A felhőszolgáltatások használata a kis- és középvállalkozások (kkv-k) körében egyre népszerűbb a rugalmassága, skálázhatósága és költséghatékonysága miatt. Ugyanakkor a felhő bevezetése jelentős információbiztonsági kockázatokat is felvet. A kkv-k, amelyek gyakran nem rendelkeznek megfelelő IT-infrastruktúrával és szakértelemmel, fokozottan ki vannak téve adatlopásnak, rosszindulatú programoknak és kibertámadásoknak. A főbb biztonsági kockázatok közé tartozik az elégtelen adattitkosítás, a hozzáférés-ellenőrzés hiánya, valamint a felhőszolgáltató infrastruktúrájának sebezhetőségei. Másfelől a felhőszolgáltatók általában fejlett biztonsági megoldásokat kínálnak, mint például titkosítás, hitelesítés és rendszeres biztonsági frissítések, amelyek segíthetnek a kockázatok csökkentésében.

A kkv-k számára alapvető fontosságú egy megbízható felhőszolgáltató kiválasztása, amely erős biztonsági intézkedéseket alkalmaz, és megfelel az adatvédelmi előírásoknak (pl.: GDPR). Összességében a felhő számos előnyt kínál, de a kkv-knak proaktívan kell kezelniük az információbiztonságot, ennek kapcsán jelen kutatás ezen proaktív hozzáállást vizsgálja a kkv-k körében.

A kutatás alapvető fontosságú a kkv-k számára, hogy megértsék a felhőbiztonsági intézkedések jelentőségét, amelyek nélkülözhetetlenek az érzékeny adatok védelméhez és az üzletmenet folytonosságának biztosításához.

Kulcsszavak:

információbiztonság, felhő, kkv, proaktivitás, kockázatok

Cybersecurity - session XII.– Research and development II.

THE IMPORTANCE OF CLOUD SECURITY FOR SMES

Gerda BAK

The use of cloud services among small and medium-sized enterprises (SMEs) is increasingly popular due to its flexibility, scalability, and cost-effectiveness. However, cloud adoption also raises significant concerns regarding information security. SMEs, often lacking extensive IT infrastructure and expertise, are more vulnerable to data breaches, malware, and cyber-attacks. Key security risks include insufficient data encryption, lack of access control, and vulnerabilities in the cloud service provider's infrastructure. On the other hand, cloud providers typically offer advanced security solutions, including encryption, authentication, and regular security updates, which can help mitigate these risks.

For SMEs, selecting a reliable cloud provider with strong security measures and complying with data protection regulations (GDPR in EU) are crucial steps. Overall, while the cloud offers significant benefits, SMEs must adopt a proactive approach to information security. This research explores this proactive attitude among SMEs.

This research is crucial in helping SMEs understand the importance of robust cloud security measures, which are essential for safeguarding sensitive data and maintaining business continuity.

Keywords:

information security, SME, cloud service, proactive attitude, risks

Kiberbiztonság - XII. szekció – Kutatás, fejlesztés II.

A BIOMETRIKUS AZONOSÍTÁS ELTERJEDÉSÉNEK ELEMZŐ VIZSGÁLATA

UJHEGYI Péter

Kutatásom során a Maslow féle motivációelméletre alapulva a szükségletek hierarchikus rangsorolását figyelembe véve szoros kapcsolatot mutattam ki a biztonság, mint alapszükséglet, az egyén, valamint a biometrikus azonosítás között. Megvizsgáltam a biometria, a biometrikus adat, a biometrikus azonosítás definícióját és fejlődését és kimutattam, hogy a definíció nem követi le a technika fejlődését, mert nem tartalmazza a pszichológiai vagy érzelmi állapot, elemzett következtetett jellemzőire épülő valószínűsítő eljárás alapú azonosítási módszereket. Ennek hatására új definíciót alkottam. Kutatásom további részében összegeztem az azonosító eljárásokat és az elterjedésükkel összefüggő tényezőket és rámutattam, hogy a kockázatai mennyire erősen függenek össze a biometriával és annak elterjedésével, ezzel kutatásom hozzájárul a kockázatok jobb megértéséhez és kezeléséhez. Kutattam a személyes adatokkal, a biometriával és a biometrikus azonosítással összefüggő uniós és a hazai jogszabályokat, tematikusan rendeztem ezeket.

Kulcsszavak:
biometria, biometrikus azonosítás kockázatelemzése, mesterséges intelligenciával

Cybersecurity - session XII.– Research and development II.

ANALYTICAL STUDY OF THE SPREAD OF BIOMETRIC IDENTIFICATION

Péter UJHEGYI

In my research, based on Maslow's theory of motivation and considering the hierarchical ranking of needs, I demonstrated a close relationship between security, as a fundamental need, the individual, and biometric identification. I examined the definitions and development of biometrics, biometric data, and biometric identification, and I found that the definitions do not reflect the advancements in technology, as they fail to incorporate psychological or emotional states, as well as probabilistic identification methods based on analyzed inferred characteristics. Consequently, I developed a new definition. In the subsequent part of my research, I summarized the identification procedures and the factors associated with their proliferation, highlighting how the associated risks are closely tied to biometrics and its spread. This contribution enhances the understanding and management of these risks. I also investigated the EU and domestic regulations related to personal data, biometrics, and biometric identification, organizing them thematically.

Keywords:
biometrics, biometric identification risk analysis, artificial intelligence

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

BÁNKI DONÁT GÉPÉSZ ÉS
BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

BÁNKI DONÁT FACULTY OF MECHANICAL
AND SAFETY ENGINEERING

cyber
islands

E-mail:

konferencia@alverad.hu

Web:

https://bgk.uni-obuda.hu/alverad-banki-kiberkonferencia-2024/

https://bgk.uni-obuda.hu/en/alverad-banki-cyber-security-conference/

The conference is organized by

Óbuda University Donát Bánki Faculty of Mechanical and Safety Engineering

Alverad Technology Focus R&D&I Business Unit