Kiberhónap tudatosító kampány összegzés 2016. október

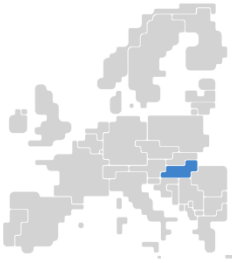
NEMZETI KIBERVÉDELMI INTÉZET

Tartalom

EUROPEAN CYBER SECURITY MONTH

2016 CYBER SECURITY ACTIVITIES BY COUNTRY

HUNGARY



MOTTO:
Cyber Security is a Shared Responsibility

LEADING ACTIVITY:
Cooperation between Agencies, raising awareness, facilitate the network and information security of governmental agencies

NEMZETI KIBERVÉDELMI INTÉZET

Security Tips

1. Do not connect to unknown, unsecure wireless network (for example: hotel wifi)
2. Protect your personal data online, check your security and privacy settings
3. Dont click on unfamiliar links or unexpected attachments.
4. Keep your system updated, always install the official software update.
5. Do not use your private device for business issues

Country Activities Map

CYBERSEC2016.HU

This 2 days conference will be the opening of the hungarian cyber security campaign. The conference is organised by the Cyber coordinator for the public and private sector representatives. The aim is to facilitate the PPP cooperation and discuss the main trends and challenges in cyber.

THEMATIC LANDSCAPE
regulation, implementation, technical questions, NIS Directive

1

VENUE
Teréz Körút, 43 H-1067 Budapest Hungary

FIND OUT MORE
http://www.cert-hungary.hu/cybersec2016.hu

IN GATEWAY OF SCIENCE – POSTER CONTEST AND EXHIBITION

For years the National University of Public Service organize the "In Gateway of Science" - Poster Contest and Exhibition, which aims to provide a publication surface for students who are interested in science. The Poster Contest and Exhibition in this year organize a subsection for cyber security issues

THEMATIC LANDSCAPE
academia, exhibition

2

VENUE
1118 Budapest, Ménesi út 5. Hungary

FIND OUT MORE
https://www.facebook.com/events/1610455912581230/

Activities Implemented

22

Public, Private, NGOS and Regulatory Bodies Stakeholders Involved

21

Achievements & Metrics

CYBER SECURITY QUIZ

1171

In 51 days 1171 people filled in the online quiz of the National Cyber Security Center. This quiz was made for the governmental organizations to evaluate the general cyber security knowledge of the administrative staff.

Generally we got the correct answers for the questions in our quiz in 76%.

TRAINING FOR ELECTRONIC INFORMATION SECURITY MANAGERS

100

In compliance with the Hungarian IT security regulation (called: Ibtv.), the National University of Public Service (NKE) has launched a vocational training programme in 2014 to train Electronic Information Security Managers. Students enrolled in the program could begin the fourth year of their studies in 2016. Unit now, more than 100 professionals enrolled in the programme.

E-TRAINING LINKS
goo.gl/4bEpx2 | www.cyberk id.gr
@cyberaler tGR | @CyberccGR

#eskills #eEducation #enisa JOIN#CyberSecMonth

The European Cyber Security Month (ECSM) is an EU advocacy campaign. It promotes cyber security among citizens and advocates for change in the perception of cyber-threats, by promoting data and information security, education, sharing of good practices and competitions. Supported by ENISA and EC DG CONNECT.

CYBER SECURITY IS A SHARED RESPONSIBILITY!

enisa

The EU cyber security agency

www.enisa.europa.eu |
For more information info@enisa.europa.eu
www.cybersecuritymonth.eu | #CyberSecMonth

IN PARTNERSHIP WITH

Bevezetés

A Nemzeti Kibervédelmi Intézetnek (NKI) az egyik feladata a törvényben meghatározottak szerint, hogy elősegítse az állami és önkormányzati szervek biztonságtudatosságát, oktatási anyagokat dolgozzon ki, tréningeket tartson, felvilágosító és szemléletformáló kampányokat szervezzen.

Ezen tudatosító tevékenységhez illeszkedik az Európai Hálózatbiztonsági Ügynökség (ENISA) által 2012. óta minden év októberében megszervezésre kerülő Európai Kiberbiztonsági Hónap (**European Cyber Security Month** – ECSM) elnevezésű nemzetközi kampánysorozat, amelynek célja a lakosság kiberbiztonsági tudatosságának növelése, valamint a kibertérben megjelenő fenyegetések széles körben történő megismertetése. Az ECSM keretében képzéseket, tudatosító előadásokat tartanak az Európai Uniós tagországok intézményei, ezek koordinálását az ENISA ügynökség végzi.

Az ENISA Ügynökség 2016. május 4-én kezdte meg a 2016. évi kampány előkészületeit és megtartotta a az ECSM kampány tagállami koordinátorai számára az első tervezői munkacsoportülést Brüsszelben (Belgium). Magyarország részéről a Nemzeti Kibervédelmi Intézet látta el az ECSM kampányban a koordináló és kapcsolattartó feladatokat, így a májusi tervezői ülésen és az azt követő tervezői telefonos konferencia egyeztetéseken is az NKI képviselte Magyarországot.

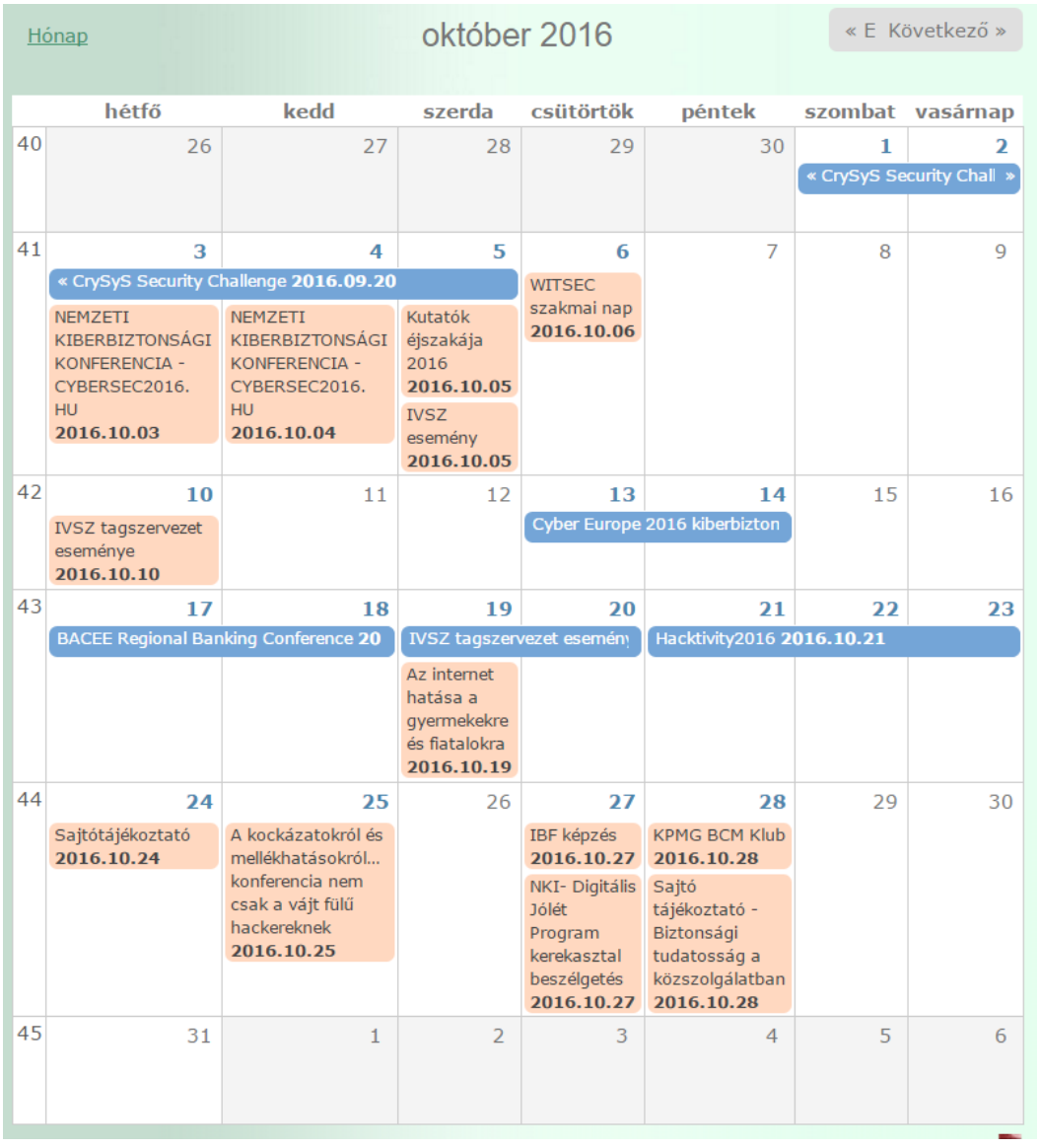
Az NKI június 3-án ECSM reggeli címmel munkamegbeszélést tartott a tudatosító kampány iránt érdeklődő szervezetek részére. Ezt követően számos egyeztetésen munakcsoportülés került megszervezésre az októberi kampány magyarországi programjának és elemeinek kidolgozása érdekében, amelynek eredményeként **21 állami és gazdasági szervezet** összesen 22 rendezvény lebonyolítását vállalta a kiberbiztonsági hónaphoz csatlakozva.

A kampánysorozat mottója: „**A kiberbiztonság közös felelősség**”, amelynek szellemében az alábbi biztonsági tippeket kívánjuk a felhasználók figyelmébe ajánlani:

1. **Ne kapcsolódjon** ismeretlen, nem biztonságos vezeték nélküli hálózatokhoz (pl. hotel wifi)!

2. **Védje** személyes adatait elektronikusan, ellenőrizze a biztonsági és személyes beállításait!
3. Ne kattintson ismeretlen linkekre, ne nyisson meg nem várt csatolmányokat!
4. Folyamatosan **frissítse** a rendszerét, de mindig csak a gyártói frissítéseket telepítse fel eszközeire!
5. Ne személyes használatú eszközén intézze munkaügyeit!

Az ECSM kampány keretében Magyarországon megszervezett események:



Az ECSM kampányról és az októberi eseményekről az előző oldali poszteren, illetve az alábbi hivatkozásokon olvashat bővebben:

- http://cybersecuritymonth.eu
- http://govcert.hu/ecsm

Cybersec2016.hu

Magyarországon a kiberhónap tudatosító kampány nyitó eseménye a 2016. október 3-4-én **Magyarország Kiberkoordinátora által** megrendezésre került Nemzeti Kiberbiztonsági Konferencia (CYBERSEC2016.HU) volt.
A két napos konferencia célja az volt, hogy elősegítse, előre mozdítsa az információbiztonságban érintett kormányzati és piaci szereplők közötti együttműködést.

Az esemény remek alkalmat biztosított arra, hogy feltárjuk a kormányzati szféra információbiztonságának megvalósításával kapcsolatos problémákat, valamint felhívjuk a piaci szereplők figyelmét is arra, hogy az idén hatályba lépett európai Hálózat- és Információbiztonsági (NIS) Irányelvnek köszönhetően milyen új előírásoknak kell megfelelniük a jövőben.

A CYBERSEC2016.hu konferenciára 79 állami és gazdasági szereplő képviseletében összesen 147 fő látogatott el a másfél nap során.

Az első nap **során** plenáris ülés keretében előadás**ok**ra került sor kormányzati és nem kormányzati **szereplők** a részéről egyaránt.

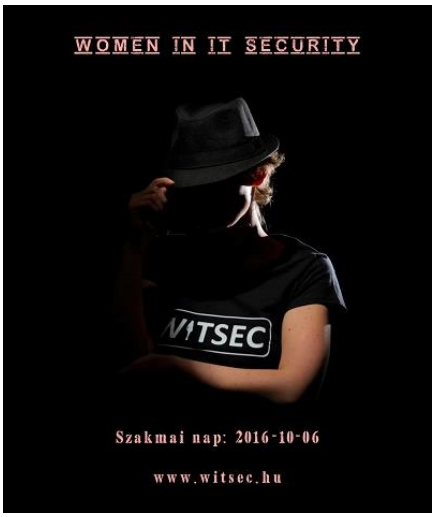
A második nap két kerekasztal beszélgetés keretében vitatták meg a részt vevők az aktuális kiberbiztonsági kihívásokat, a hallgatóság aktív bevonásával. Az első kerekasztal Kormányzati és piaci szereplők együttműködésének lehetőségeire a PPP együttműködés megvalósítására koncentrált. **A szekcióbeszélgetés során a beszélgetésben részt vevő fe4lek megvitatták, hogy mely területeken látják fontosságát és lehetőségét az együttműködésnek, illetve, milyen módon segítheti elő ezen együttműködéseket a Kiberkoordinátor munkája (Kiber Fórum összehívása, munkacsoportok átgondolása, egyeztetés a NIS irányelv végrehajtásáról), valamint az új EU-s szerződésen alapuló PPP együttműködés lehetőségeiről is szó esett.**
A kerekasztal beszélgetés moderátora prof. Rajnai Zoltán, Magyarország kiberkoordinátora volt. A kerekasztal beszélgtésben résztvevők Gasparetz András (elnök, Hétpecsét Egyesület), Hódy Árpád (Microsoft Hungary), Keleti Arthur (elnök, Önkéntes Kibervédelmi Összefogás), Pölcz Péter Attila (CODEL Kft., ügyvezető igazgató).

A másik kerekasztal az úgynevezett Alapvető szolgáltatók és /vagy Kritikus infrastruktúrák az IT biztonságtükrében. címet kapta. A kerekasztalbeszélgetés moderátora dr. Bencsik Balázs, az NKI igazgatója volt. A kerekasztal beszélgetésben részt vevők Bauer Miklós (Nemzeti Útdíjfizetési Szolgáltató Zrt.), Dr. Bognár Balázs (BM OKF), Dr. Kovács Zoltán (NISZ Zrt.), Varjas Gábor (MOL Nyrt.) voltak.

A szekcióbeszélgetés során a résztvevők megvitatták, hogy az új EU-s sabályozás a Hálózat és információbiztonsági irányelv végrehajtása milyen lehetőségeket, nehézségeket, kihívásokat jelenthet a kormányzat és a szabályozás hatálya **alá tartozó szervezetek számára, illetve hogy milyen együttműködés útján lehetne ezt a leghatékonyabban és legsikeresebben átültetni a magyar jogszabályokba és a hétköznapi munkánkba, együttműködéseinkbe.**

WITSEC szakmai nap

Október 6-án a Nők az Informatikában (WITSEC) egyesület megszervezte az első WITSEC szakmai napot az Óbudai Egyetemen.



A rendezvényen megközelítőleg 150 fő vett részt. A hallgatóság összetétele nagyon változatos képet mutatott, hiszen az egyetemista hallgatók, az IT biztonsági szakemberek, valamint egyetemi oktatók is részt vettek.

A szakmai napon a WITSEC bemutatásán, céljainak eredményeinek bemutatásán túl, az elektronikus aláírásról szóló EU-s szabályozásról, az Európai Unió hálózat és információbiztonsági irányelvéről, IT biztonsági tudatosításról-oktatásról, a napjainkban tapasztalható trendekről, kihívásokról, illetve konkrét sérülékenységekről (pl: Shadow Brokers incidens) hallhattak előadásokat a szakmai különböző területein dolgozó szakemberektől.

A szakmai nap lehetőséget adott arra is, hogy a WITSEC-en kívül a hallgatók, látogatók más IT biztonsági szervezet tevékenységével is megismerkedhessenek egy külön kiállító teremben. Itt a Nemzeti Kibervédelmi Intézet is megtalálható és megismerhető volt.

Cyber Europe 2016

Az ECSM keretében 2016. október elején az ENISA immár negyedik alkalommal rendezte meg a **Cyber Europe 2016 pán-európai kiberbiztonsági gyakorlat**ot.[1]

Az idei gyakorlat az IT, a telekommunikáció és az információbiztonsági iparágakra terjedt ki, amely nem csupán stratégiai és kommunikációs elemeket tartalmazott, hanem különböző, elemzendő technikai incidensekkel (malware, forensics, mobil fertőzés, DDoS, OSINT, drónok, stb.) is ellátta a résztvevőket.

Az incidensek jellegéből adódóan szervezeti, helyi, nemzeti és európai szintű krízis-koordináció gyakorlására is lehetőség nyílt.

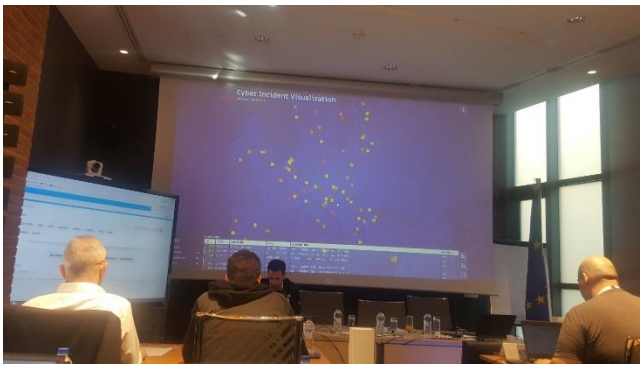
[1] https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2016

Az idei gyakorlat két szakaszban valósult meg.Az első szakaszban (mely májustól szeptemberig tartott) a gyakorlatra való felkészítésre, online tréningekre koncentrált. Ebben a szakaszban a gyakorlathoz kapcsolódó különböző témájú és nehézségű feladatokat kellett megoldaniuk a játékosoknak, illetve megismerkednek a gyakorlat platformjával és annak működésével.

Ez a szakasz a feladatok által, a támadásokat megelőző a válság kialakulását volt hivatott szimulálni.

A második szakasz tekinthető az éles gyakorlatnak, melyre 2016. október 13-14-én (reggel 9-től délután 6 óráig) kerül sor.

A gyakorlaton összesen 31 ország 948 játékossal vett részt.



Magyarország részéről a nemzeti Kibervédelmi Intézet vett részt a gyakorlat előkészületeiben, tervezésében, valamint a magyar csapat összeállítását, felkészítését illetve a gyakorlat során a nemzeti koordinátori feladatokat is a Nemzeti Kibervédelmi Intézet látta el.

Magyarország az egyik legnagyobb csapattal, a GovCERT vezetésével összesen nyolc szervezettel – az Invitel Zrt., a Magyar Telekom Nyrt., a NISZ Zrt., a Hun-CERT, a honvédelmi ágazat szereplői a honvédelmi ágazati eseménykezelő központ koordinálásával, az Országos Katasztrófavédelmi Főigazgatóság, a Nemzeti Média és Hírközlési Hatóság – vett részt a gyakorlaton.

A hazai csapatot – mint a három legaktívabb, leggyorsabban reagáló csapat egyikét – az ENISA szervezőbizottsága **dicséretben részesítette.**

Együttműködési megállapodás

A tudatosító kampány keretében a Nemzeti kibervédelmi Intézet együttműködés kialakításába kezdett az Invitel Csoporttal az üzleti és egyéni ügyfeleik informatikai biztonsága növelése érdekében. A Nemzeti Kibervédelmi Intézet és az Invitel Csoport, mint Magyarország egyik vezető távközlési és informatikai szolgáltatója 2016 október 18-án Együttműködési megállapodást írt alá, melyne értelmében a felek együttműködnek az internetes biztonság területén. A dokumentumot David Blunck, a cégcsoport vezérigazgatója, és Dr. Bencsik Balázs, az NKI igazgatója írta alá. Az együttműködés elsődlegesen az informatikai biztonságot növelő műszaki- technológiai megoldásokra, az üzleti, és egyéni ügyfelei informatikai biztonság tudatosságának növelésére, illetve a szervezetek közötti hatékony kapcsolattartásra terjed ki.

A megállapodásban foglaltak szerint a Nemzeti Kibervédelmi Intézet megosztja a nemzetközi kibervédelmi együttműködésből származó információkat az Invitel Csoporttal a védelmi intézkedések hatékonyságának növelése érdekében.

Az együttműködés előremozdítását bizonyítja az is, hogy a kiberhónap kampány egyéb eseményeibe is együttműködött a szolgáltató a Nemzeti Kibervédelmi Intézettel, mégpedig részt vettek a Cybersec2016.hu Konferencián és előadásukban bemutatták, hogy ők milyen típusú feladatokkal és kihívásokkal néznek szembe információbiztonsági területen. Ezen felül részt vettek a 2016. október 13-14-én megrendezett Cyber Europe európai szintű kibervédelmi gyakorlatban is.

Mobil biztonság kampány

Az ECSM tudatosító kampányhoz csatlakozva az Europol Kiberbűnözés Elleni Központ (EUROPOL) a tagállamok közreműködésével készített egy mobilbiztonságról szóló tudatosító kampány csomagot. A projekt által életre hívott kampányban összesen 24 ország vesz részt – többek között - Horvátország, Hollandia, Ausztria, Írország, Franciaország, Németország, Lettország, Litvánia, Portugália, Románia, Szlovénia, Spanyolország, Nagy-Britannia, Kolumbia.

A kampány kidolgozásában Magyarország képviseletében a Nemzeti Nyomozó Iroda (NNI) közreműködött. A kampány célja, hogy felhívja az állampolgárok figyelmét a mobil bankolás, a mobil alkalmazások stb. veszélyeire, illetve javasolatokat fogalmaz meg ezen alkalmazások helyes és biztonságos használatára is.

A projekt eredményeként elkészítésre került egy másfél perces videó, öt darab egy-három másodperc időtartamú mozgókép valamint négy darab infógrafika

A projekt keretében elkészült anyagok felhívják a figyelmet a mobileszközök veszélyeire általánosságban, mint például adathalászat, internetes böngészés illetve fájlok letöltése. Az elkészült anyagok felhívják figyelmet arra, hogy a visszaélések elkerülése érdekében csak megbízható forrásból származó alkalmazásokat telepítsünk a mobil eszközünkre, a telepítés előtt ellenőrizzük le, hogy milyen adatokhoz kér hozzáférést az alkalmazás, valamint hogy megoszthatja-e azokat külső féllel.

A kampány egyik kiemelt témája a mobilbakolás veszélyei, hiszen a mobilbakolási lehetőségeket kihasználó kártevő szoftverek célja az eszközön tárolt, a pénzforgalommal kapcsolatos adatok megszerzése (ez személyi hitelesítő adatok megszerzésével vagy akár pénzfelvétellel is járhat). A biztonságos mobilbakoláshoz tippeket, javaslatokat fogalmaz meg (pl: WI-FI hálózaton ne használjuk a netbankot, ne adjuk meg vagy mentsük le a felhasználó adatainkat és jelszavunkat, ne állítsuk be automatikus bejelentkezésre az alkalmazást, biztonsági program alkalmazása az eszközön).

A kampány a vállalkozások mobileszközeinek biztosítására vonatkozó főbb tanácsokat is ki emeli, mint például, hogy fontos a munkatársak tájékoztatása a mobileszközök használatának veszélyeiről, elengedhetetlen a saját eszközök használatát szabályozó irányelvek bevezetése, javasolt a nyilvános WI-FI hálózat használatának mellőzése céges eszközök estén, kiemeli az operációs rendszer és az alkalmazások frissítésének fontosságát, számba veszi a felhő technológia hátrányai, továbbá javasolt a biztonsági alkalmazások használata.

Napjainkban egyre többet találkozunk a zsaroló vírusok (ransomvare) okozta nehézségekkel. Ez a mobil eszközök esetében is valós fenyegetést jelent, ezért a kampány a zsaroló vírusok veszélyeire is felhívja az emberek figyelmét.

2016. október 24-én a Nemzeti Nyomozó Iroda és az Nemzeti Kibervédelmi Intézet közösen bemutatta az elkészült mobilbiztonsági kampány anyagot az ORFK által szervezett sajtó tájékoztatón. A sajtótájékoztatón dr. Bencsik Balázs, a Nemzeti Kibervédelmi Intézet Igazgatója a 2016. évi Európai Kiberbiztonsági tudatosító kampányról, illetve a tudatosítás fontosságáról beszélt, Szongoth Richárd a Nemzeti Nyomozó Iroda munkatársa pedig bemutatta a mobilbiztonságról szóló kampány elemeit.

A mobilbiztonságról készült magyar nyelvű kampány anyag elérhető az alábbi linken:

http://www.cert-hungary.hu/node/329

Az NJSZT és a Nemzeti Kibervédelmi Intézet konferenciája „kockázatokról és mellékhatásokról”

Az október 25-én, Szegeden, az NJSZT Informatika Történeti Kiállításának is helyet adó Szent-Györgyi Albert Agora dísztermében tartott tanácskozás tartalmas volt – hat előadó tartott magas színvonalú ismeretterjesztő előadást. A konferencia moderátora, Bőgel György – az NJSZT alelnöke – helyesen állapította meg, hogy ezek a gondolatébresztő előadások a pályaorientációt is szolgálták.

Alföldi István bevezetőjében hangsúlyozta, hogy az exponenciális fejlődésre kapcsoló infokommunikáció világában a felhasználói tudatosság nem nélkülözhető. Az infokommunikáció számos előnye, az általa biztosított kényelmesebb, élhetőbb mindennapok mellett az egyéni és közösségi életünk sérülékenységére is oda kell figyelnünk. Ennek jegyében lépett szövetségre a Társaság a Nemzeti Kibervédelmi Intézettel.

Az intézet tevékenységeit Bencsik Balázs igazgató mutatta be. Megismerhettük Magyarország nemzeti kiberbiztonsági stratégiájának kereteit és a számítógépes incidenskezelés a magyar államot védő struktúráját. Bencsik Balázs előadásában számos példát említett a biztonsági fenyegetések formáira, amelyek webes tartalmak böngészése, elektronikus levelezés, a közösségi háló használata vagy akár felhőalapú tárhelyek igénybevétele közben is érhetnek minket. A túlterheléses támadásoktól kezdve a kiberbűnözés egyéb formáiig – ma már nagyon komolyan veendő károkat okoz, ha nem helyezünk elég hangsúlyt intézményeink biztonságára.

Egy műszaki terméket mindig egy adott célra hoznak létre. Az internet nem arra készült, hogy ennyi helyen használják – hívta fel a figyelmet Molnár Bálint egyetemi docens (ELTE). Az eleinte a kutatók kiszolgálására létrejött – és egy atomháború esetén is elérhető – hálózatot ma már több milliárdan használják kereskedelmi és egyéb célokra is.

A Digitális Mohácsot, azaz egy Magyarországot térdre kényszerítő katasztrófa rémképét is felvázolta – egyébként rendkívül dinamikus és humoros előadásában – Hirsch Gábor (Fortinet). Az alapvetően az ipari irányítási rendszerek biztonsági kérdéseit taglaló előadás olyan veszélyekre hívta fel a figyelmet, amelyekbe még John McLane, az akcióhős is belepirulna. Prezentációjából megismerhettük a fenyegetések evolúcióját, amely a felhasználói hibákkal indult, a „script kiddies", azaz a kihívást kereső tinédzserek próbálkozásain át vezet a hacktivizmusig, sőt a szervezett bűnözésig és az egyes kormányzatok által támogatott kibertámadásokig. Ma már több olyan ország is van, amely ezerfős „kiberhadsereget" tart fenn. Az amerikai elnökválasztási kampányban is felmerült a vád, hogy orosz hackerek is beleszólnak a jelöltek küzdelmébe. Az előadó és Bőgel György levezető elnök is hangsúlyozta: ma már az IoT („dolgok internete") eszközök is támadhatnak. Komikus kép, de nem teljesen irreális: „egy kávéfőző megtámadta az Amerikai Egyesült Államokat".

„Az informatikai világban nem előfeltétel a paranoia. Előbb-utóbb úgyis kialakul." – fogalmazott Erdősi Péter Máté, az NJSZT információbiztonsági szakértője, aki az elektronikus hitelesség jelentéseit járta körül a digitális korban. Az alapos elméleti hátteret adó előadás a bizalom különböző szintjeit, a hitelesítés és hitelesség kérdéseit világította meg.

„A biztonság csak egy állapot. A be nem következett veszteség – nyereség." – ezt az aforizmát már Rajnai Zoltántól, a magyarországi kiberkoordinátortól hallhattuk, aki kibervédelem és a kibervédelmi stratégia kapcsolatáról, a megvalósítás szervezeti kereteiről beszélt. Megismerhettük a kibervédelem össztársadalmi funkciórendszerét és kormányzati struktúráját. A kiberbiztonsági munkacsoportok között többek között az energiabiztonság, az E-közigazgatás, a gyermekvédelem kérdéseinek is fontos szerep jut.

Magyarország Digitális Gyermekvédelmi Stratégiája és az információbiztonság szerepe

Október 27-én a Nemzeti Kibervédelmi Intézet és a Digitális Jólét Program irodája megtartotta a Magyarország Digitális Gyermekvédelmi Stratégiája és az információbiztonság szerepe című kerekasztal beszélgetést.

A Digitális Jólét Program ernyője alatt nemrég elkészült Magyarország Digitális Gyermekvédelmi Stratégiájának célja, hogy az eddigieknél hangsúlyosabban érvényesüljenek a gyermekek védelmét szolgáló szabályok és intézkedések, mivel a gyermekek tájékozottsága, tudatossága az internetes kommunikációban fontosabb, mint valaha. A Stratégia, akárcsak a Kiberbiztonsági Hónap fókuszában a tudatosítás, a képzés áll.

Dr. Krasznay Csaba moderátor segédletével, dr. Bencsik Balázs, a Kibervédelmi Intézet elnöke, Dr. Farkas Attila Erik, a DJP állandó szakértője, Prof. Rajnai Zoltán Magyarország Kiberkoordinátora valamint, Szongoth Richárd a Nemzeti Nyomozó Iroda munkatársa megvitatták a tudatosítás, az oktatás jelentőségére vonatkozó kérdéseket, illetve a Stratégia és az információbiztonság lehetséges kapcsolódási pontjait.

Sajtó Tájékoztató- Biztonság tudatosság a közszolgálatban

Az Európai Kiberbiztonsági Hónap tudatosító kampány Magyarországon szervezett programok lezárására október 28-án került sor a Nemzeti Közszolgálati Egyetem Államtudományi és Közigazgatási Karon szervezett kutatói beszámolón és sajtótájékoztatón, amelyen Dr. Bencsik Balázs, a Nemzeti Kibervédelmi Intézet vezetője értékelte az Európai Kiberbiztonsági Hónap magyarországi kampánysorozatát, valamint Dr. Krasznay Csaba ismertette a NKE által szervezett rendezvényeket, illetve az Elektronikus Közszolgálati Intézetben zajló oktatói-kutatói tevékenységet.

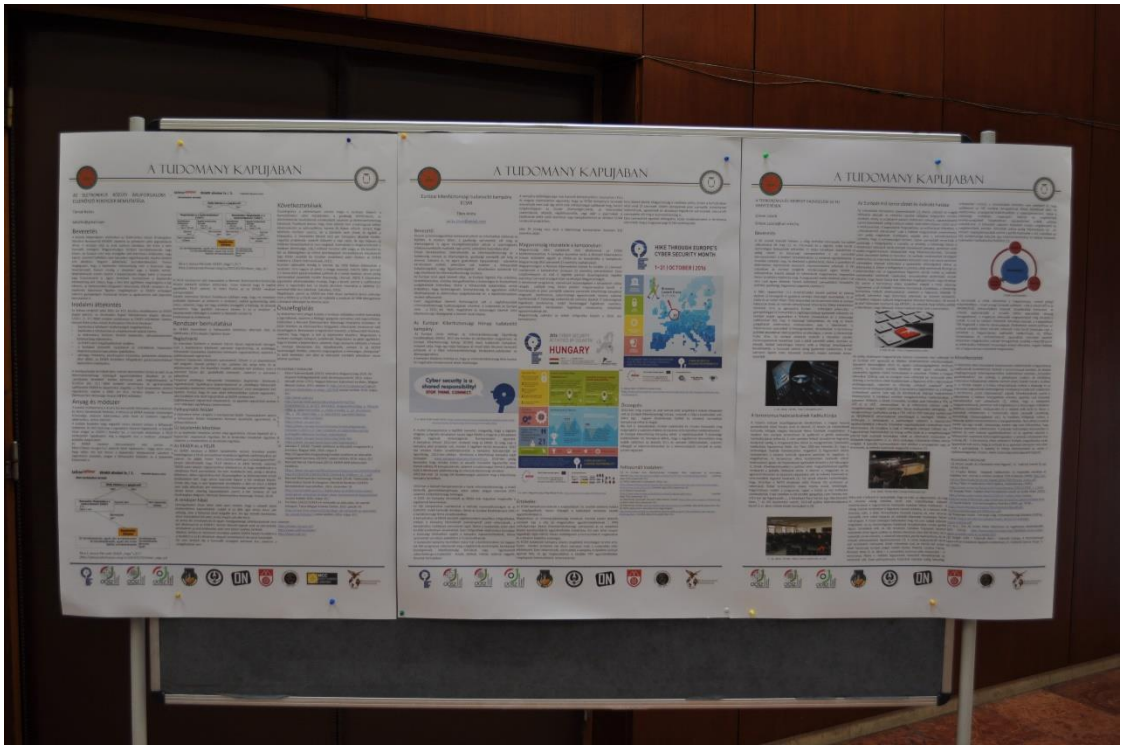
Krasznay Csaba elmondta, hogy Nemzeti Közszolgálati Egyetem az idén Magyarországon is megszervezett Kiberbiztonsági Hónaphoz rögtön hat rendezvénnyel csatlakozott. Az, hogy az NKE ilyen erősen megjelenik a kampányban, nem véletlen, hiszen a közszféra minden területe kötődik a kibertérhez, illetve legyen szó bármely hivatásnem képviselőiről, azáltal, hogy az állam szolgálatába álltak, sokkal értékesebb célpontnak számítanak a támadóknak, hiszen általuk rendkívül értékes információkhoz férhetnek hozzá.

A rendezvénysorozat első elemét a szeptember 30-án, a Kutatók Éjszakáján Bányász Péter, az Elektronikus Közszolgálati Intézet oktatójának előadása jelentette, amelyben a közösségi média és a big data jelentette kockázatokat mutatta be a hallgatóságnak.

A hivatásnemek együttműködésének szellemében került sor október 5-én a Ludovika Campus Zrínyi termében az Elektronikus Közszolgálati Intézet szervezésében egy kerekasztal beszélgetésre „Kiberbiztonság a közszférában” címmel, amelynek legfontosabb gondolata egy olyan, karok közti együttműködés megerősítése volt, amelyben az egyes hivatás nemek a közszolgálati életpályamodell részeként a kiberbiztonsággal kapcsolatos aktuális problémákra közösen keresik a választ. Az eseményen Prof. Dr. Nemeslaki András, az Elektronikus Közszolgálati Intézet vezetője és Bányász Péter, az Intézet oktatója, Szabó András főhadnagy, a Hadtudományi és Honvédtisztképző Kar oktatója, dr. Simon Béla, a Rendészettudományi Kar oktatója, valamint Berzsenyi Dániel doktorandusz, a Stratégiai Védelmi Kutató Központ munkatársa mutatták be az Egyetemen zajló, kiberbiztonsággal kapcsolatos kutatásokat és oktatási tevékenységet, illetve felidézték, melyek azok a területek, amelyek további kutatásokat- fejlesztéseket igényelnek, valamint bemutatták az erre vonatkozó főbb kutatási pontokat.

Október 10-én Dr. Krasznay Csaba, az Elektronikus Közszolgálati Intézet oktatója tartott előadást a Ludovika Campuson a kibertér jelentette aktuális fenyegetettségekről. Bár maga a rendezvény alapképzésben résztvevő hallgatók számára volt meghirdetve, rajtuk kívül egyéb érdeklődők is jelen voltak. Az előadásban a hallgatóság megismerhette a kibertérben végbement trendváltozásokat, illetve azokat az új típusú kihívásokat, amelyek a kibertérből származnak. Az eseményen az amerikai elnökválasztás példáján keresztül bepillantást nyertek az érdeklődők, hogy a kiberbiztonság milyen komoly következményekkel járhat nem csak az egyének, de az államok szempontjából egyaránt.

A rendezvények közül az egyik kiemelt esemény a Nemzeti Közszolgálati Egyetemen lassan hagyományosnak tekinthető, a „Tudomány Kapujában poszterverseny és kiállítás” volt, amelynek megnyitójára október 12-én került sor az Államtudományi és Közigazgatási Karon. Az idén második alkalommal megrendezett poszterverseny egy külön, kiberbiztonsággal foglalkozó szekcióval csatlakozott a kampányhoz.



Az októberi poszter versenyt a Nemzeti Közszolgálati Egyetem Doktorandusz Önkormányzata az Egyetem Szakkollégiumaival, Magyar Hadtudományi Társaság Kápolnai Pauer István Ifjúsági Klubjával, a Doktoranduszok Országos Szövetségének Hadtudományi, Műszaki-, és Közigazgatás-tudományi Osztályaival közösen szervezte. Az idén második alkalommal megrendezett poszter verseny és kiállítás megtartotta nemzetközi jellegét, több pályamunka érkezett be Erdélyből, Kárpátaljáról és Ausztriából.

Az NKE-n megszervezett események másik kiemelt rendezvényére október 27-én került sor Ludovika Campus Hunyadi termében „Magyarország digitális gyermekvédelmi stratégiája és az információbiztonság szerepe” címen.

Kapcsolat

Nemzeti Kibervédelmi Intézet (NKI)

E-mail: titkarsag@govcert.hu
Telefon: +36 (1) 336 4840
Fax: +36 (1) 336 4886

Posta: 1399 Budapest,
62. Pf. 710.

NKI – Kormányzati Eseménykezelő Központ (GovCERT)

Web: http://govcert.hu
E-mail: team@govcert.hu
Incidens-bejelentés: cert@govcert.hu
PGP: 0x1D16DFE7

0-24h ügyelet: +36 (1) 336 4833

NKI – Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH)

Web: http://neih.gov.hu
E-mail: info@neih.gov.hu
PGP: 0x2938F849

Telefon: +36 (1) 206-9320
Fax: +36 (1) 206-9329

Hivatali Kapu: NEIH

Borítógrafika: Fir0002, Wikimedia Commons