HÍRKÖZLÉSI ÉS INFORMATIKAI
TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI
SZAKOSZTÁLY

HÍRLEVÉL

Tisztelt EIV! Kedves EIV Okosan Klub tag!

Az EIVOK 6. szakmai rendezvény 2018. október 4-én került megrendezésre a Nemzeti Közszolgálati Egyetem (a továbbiakban: NKE) új oktatási épületében az Üllői út 82 szám alatt.

Hrucsár Mária nyitó szavaival kezdődött az 6. EIVOK találkozó. A 2018. évi kiberhónap kampány partnereiről szóló poszteren és előadássorozatban az EIVOK szerepet kapott.

Mária röviden felvezette, hogy miként jutott el a Nemzeti Közszolgálati Egyetem Elektronikus Információbiztonsági Vezető szakirányú továbbképzési szakon 2016/17-es évfolyamában végzett hallgatók 2017. szeptember 15-én megrendezett első találkozója a jelenleg több mint 130 főt számláló közösséghez.

A Szakosztály fő céljai: egy aktív információbiztonsági szakmai közösség működtetése; az információbiztonsági kihívások áttekintése, megvitatása, tapasztalatcsere útján; tudásmegosztás által a napi információbiztonsági munka támogatása szervezeti, nemzeti és nemzetközi szinten egyaránt. Együttműködés a HTE többi szakosztályával, a rendezvényeken és konferenciákon érdemi szakmai képviselet. Elősegíteni az HTE-NKE közötti megállapodást, valamint a HTE kapcsolatrendszerének fejlesztése az NKE-n.

Az első előadást **Prof. Dr. Kovács László** ezredes Úr, a Nemzeti Közszolgálati Egyetem egyetemi tanára a *Kibertámadások, kiberelrettentés* címmel tartotta meg előadását.

Professzor úr előadásában a kiberelrettentés szerepéről és fontosságáról beszélt, elengedhetetlen az elrettentés és a védelmi képességekbe való beruházás, amelybe beletartozik a kibertámadásokkal szembeni rugalmas, gyors és hatékony reagálási képességek kialakítása. Ennek egyik kiemelt eleme a „Cyber Espionage”, azaz a kiberfelderítés. Kiemelte, hogy demontstrálni kell a kibervédelmi képességeket stratégia szinten, ahhoz, hogy a kiberelrettentésnek legyen ereje viszontválaszok szükségesek.

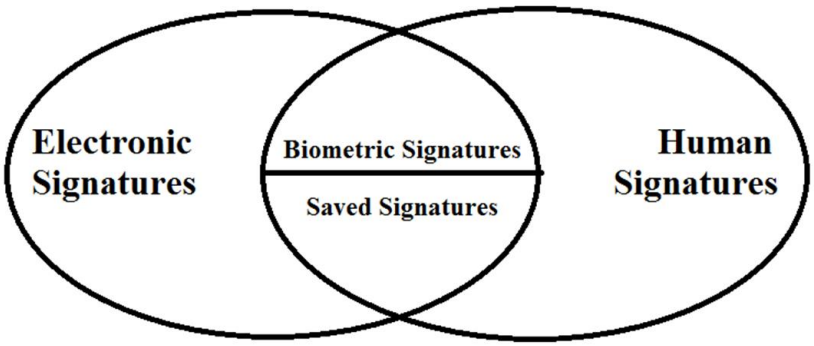
A kibertámadások hatásaival kapcsolatosan tette fel a kérdést, hogy vajon megtörténhetnek-e? Mi történik akkor, ha villamos energiaellátást például 3 hétre blokkolják (hackelik). Ugyanis annak ellenére, hogy sokat foglalkozik a lehetőséggel a szakma, tisztán informatikai eszközökkel elkövetett komplex, komolynak nevezhető támadást még nem tapasztaltunk meg. Ismerjük az elektronikus információs rendszereinktől való függésünket, van elképzelésünk arról, milyen hatással járna ezek támadása – gondoljunk a Digitális Mohács tanulmányban leírtakra -, de ezeket a hatásokat eddig csak elszigetelten és legtöbbször nem szándékos incidens kapcsán tapasztalhattuk meg.

Napjainkban jól elkülöníthető a kiberfenyegetések négy fajtája. Ezek a kiberbűnözés, a hacktivizmus és kiberterrorizmus, a kiberkémkedés és a kiberhadviselés. A kiberbűnözés célja az informatikai eszközökön keresztüli haszonszerzés, elsősorban a hagyományos szervezett bűnözői csoportokhoz köthető. A hacktivizmus és a kiberterrorizmus ugyan fogalmilag különálló cselekmény, de közös bennük, hogy elsősorban kisebb, decentralizált csoportok hajtják végre azokat az informatikai bűncselekményeket, melyek célja az, hogy minél szélesebb tömegek lássák a csoport által képviselt ideológiai véleményt. Hatásuk elenyésző, ugyanis azt a fajta szervezettséget nem tudják felmutatni, mely egy hatékony kibertámadáshoz szükséges lenne. A médiahatásuk azonban igen komoly. A kiberkémkedés az államok és nagyvállalatok által szervezett, elektronikus információs rendszerekből származó adatokat érintő információszerzést jelenti. A kiberhadviselés az államok közötti konfliktusokban jelenik meg, melynek során a felek informatikai eszközöket vetnek be egymás elektronikus információs rendszereinek befolyásolásának céljából.

A kiberhadviselés azonban komoly, egyre növekvő lehetőség, mellyel a hagyományos, fegyveres konfliktusok kísérőjeként már napjainkban is számolni kell. Az intelligens fegyverek kiterjedt használata szükségszerűen magával hozza az ezeket irányító informatikai rendszerek ellehetetlenítésének igényét. Ha ezt a képességet egy ország kifejleszti, automatikusan készen áll a polgári célpontok támadására is, hiszen a fegyverzeteket irányító szoftverrendszerek nem sokban vagy egyáltalán nem különböznek a polgári kritikus információs infrastruktúráktól. A Nato elrettentő doktrinája az erőben rejlő megfélemlítésre alapoz. Nemzetközi kitekintés keretében választ kaptunk az előadáson, hogy működik-e a kiberelrettentés az Egyesült Királyságban, Franciaországban a Fehér könyv az irányadó, Lengyelországban pedig a kibertér a fegyveres küzdelem dimenziójává vált. Magyarország a NATO és EU kötelékén belül elkötelezett, hogy a kiberelrettentési képességeit kialakítsa és annak legyen ereje.

Második előadónk, **Erdősi Péter Máté** a Nemzeti Közszolgálati Egyetem, Közigazgatás-tudományi Doktori Iskola, Doktoranduszaka a „*PKI-megoldás az aláírópadokon a gyakorlatban*” címmel adott át új ismereteket a hallgatóságnak. Az elektronikus rendszerben megvalósuló hitelesség alapvető fontossággal bír a digitális világnak, az adatok, dokumentumok megbízható és biztonságos tárolásának, továbbításának. *„Az elektronikus aláírás használatának elsajátítása azonban szükséges az elektronikus hitelesség értő és megfelelő megvalósításához, ezért az elektronikus aláírás tudásának elterjesztésére hite szerint szükség van egész Magyarországon gyártó- és platformfüggetlen módon. Ennek következtében megjelenhet a hiteles elektronikus információ minden társadalmi folyamatban, az összes gazdasági, jogi és társadalmi következményével együtt.”*

A biometrikus aláírás és a biometrikus hitelesítés



Forrása: Erdősi Péter Máté, EIVOK prezentáció 2018.10.04. /Erdősi Péter Máté, Bartók Sándor P.: May the advanced biometric electronic signature be applicable in Public Administration?/

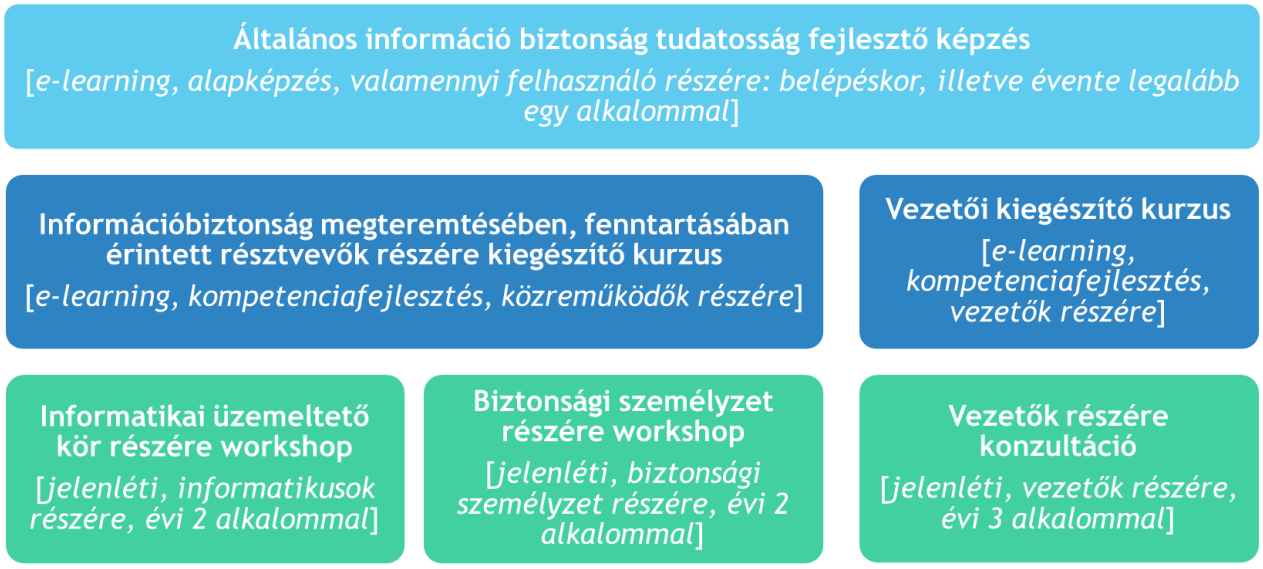
Az előadás a szakszavak és a jogi fogalomtárák bemutatásának keresztezésében hangzott el. Péter kiemelte, hogy kutatási területén meg kell különböztetni, hogy amerikai vagy azon kívüli joganyag hatályosak; mivel a szabályozási kör eltérő! Mindkét esetben azonban a cél ugyanaz; a küldő eredetét, a dokumentum sértetlenségét szükséges biztosítani. Kiemelte, hogy minden elektronikus aláírás fokozott biztonságú elektronikus aláírás. A fokozott biztonságú elektronikus aláírásnak a következő követelményeknek kell megfelelnie: kizárólag az aláíróhoz köthető; alkalmas az aláíró azonosítására; olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat; olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

Péter előadásában az új személyazonosító okmány és annak egy jövőben lehetséges használati módozataival kapcsolatban végnélküli kérdéshalmaz érkezett.

Harmadik előadásunkat egy virtuális kerekasztal beszélgetés formájában **Bubán Márton** vezette le „Információbiztonsági tudatosság szerepe” címmel. Márton kiemelte, hogy a tudatosság vizsgálatával több értekezésen keresztül dolgozott és akár amit az egyik szakdolgozatában állított, a másikban pontosan cáfolatot tudott adni ugyanarra. Ezzel a kezdőgondolattal nagy figyelem övezte az előadást – amelyben csak néha-néha mert a közönség bekapcsolódni. Márton tapasztalatai azonban többünket ráébresztett, hogy az általa felemlített, a munkahelyi környezetében megszerzett élmények – mindenki élménye. Mert ismerjük a szabályozó- szabályalkotó munkavállalókat és a technikai működésűeket is. Egy hivatal, egy társaság esetében is belátható, hogy a ’ONE MAN SHOW’ kerülendő. Csoportban kell a humán faktor szabadjogúsága/önfejűsége/nem akarása/érdektelensége ellen fellépni.

Márton előadásában nagy vonalakban egy szervezet információbiztonsági kultúrájának fejlesztését vázolta, alábbi ábrája pedig hasznos ajánlásokat nyújt az általa kidolgozott „learningek” rendszerére.

Információbiztonság tudatosság Képzési rendszere – Forma



Forrása: Bubán Márton, EIVOK prezentáció 2018.10.04.

HÍRKÖZLÉSI ÉS INFORMATIKAI
TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI
SZAKOSZTÁLY

A EIVOK 6. szakmai rendezvény a 2018. kiberhónap eseménysorozat része volt.

https://kiberhonap.hu/
https://www.facebook.com/kiberhonap/

Az előadás anyagok megtalálhatóak a Dropboxban, illetve a HTE honlapján is.

Az EIVOKlub következő időpontja: **2018.11.29 17 óra!**

Váruk szeretettel a következő alkalommal is.

EIVOK Szakosztályi Vezetőség