HÍRKÖZLÉSI ÉS INFORMATIKAI
TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI
SZAKOSZTÁLY

HÍRLEVÉL

Tisztelt EIV! Kedves EIV Okosan Klub tag!

Az EIVOK 5. szakmai rendezvény 2018. május 31-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 5. EIVOK találkozó. A meghirdetett előadások előtt egy közlemény került kihirdetésre, amely szerint az információbiztonsági szakértői közösség szervezeti hátterének megteremtése érdekében az EIVOK Szervező Bizottsága kezdeményezte a Hírközlési és Informatikai Tudományos Egyesület (a továbbiakban: HTE) vezetősége felé az információbiztonsági szakosztály megalakítását. Az elnökség jóváhagyását követően 2018. május 28-án 11 taggal megalapításra került a HTE Információbiztonsági Szakosztály – EIVOK (a további részletek, a belépés feltételei megtalálhatók a HTE honlapján: www.hte.hu, www.hte.hu/informaciobiztonsagi-szakosztaly-eivok)

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.

A közlemény bejelentését örömmel fogadta a HTE elnöke **Dr. Magyar Gábor**, aki tájékoztatta a jelenlévőket az Egyesület munkájáról. **Dr. Bartolits István** a szakmai közösségi területért felelős elnökségi tag pedig röviden összefoglalta a szakmai közösségek munkáját a szervezeten belül, amelyben kiemelte azok önállóságát is.

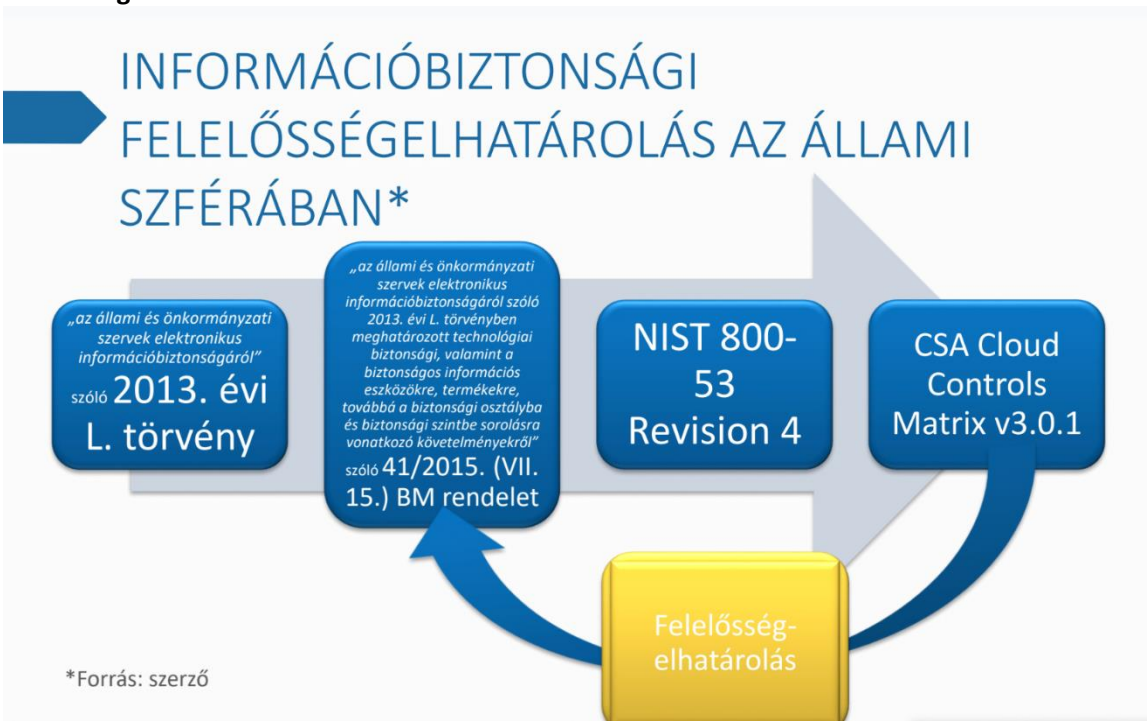
Az első előadást **Dr. Kovács Zoltán PhD.** a NISZ Zrt. Elektronikus Információbiztonsági Igazgatóság, igazgatója a *SOC, incidenskezelés közigazgatási kitekintéssel* témában tartotta.

A Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: NISZ Zrt.) fő tevékenysége teljes körű infokommunikációs szolgáltatások nyújtása az állami és a kormányzati szervek számára.

A 2013. évi L. törvény és a 41/2015. BM rendelet megadja, hogy milyen információbiztonsági kontrolokat kell beépíteni a meghatározott rendszerekbe. A NISZ Zrt., minden állami szervezetnek szolgáltat, ugyanakkor, mint szolgáltató magába az adatokba – mivel nem az övé – nem nézhet bele, ezzel együtt kell garantálnia az információbiztonság megvalósulását. A SOC – Security Operation Center – magyarul Biztonsági Műveleti Központot jelent. A kormányzati szervek különösen kitettek támadásoknak. Központosított szolgáltatóként a NISZ Zrt. került kijelölésre, amely a különböző szervezetek, minisztériumok, önkormányzatok informatikai rendszereit üzemelteti, továbbá az infrastruktúra jelentős részét biztosítja.

A NISZ Zrt. tevékenységének jelentős részében felhő alapú szolgáltatást nyújt az arra jogosultak számára, így az adott elektronikus információs rendszerek üzemeltetése és információbiztonsági feladatai is megoszlanak közte és az adott szervezet között. Ennek problematikájáról a feladat és felelősségi körök elosztásának, biztonság, mint szolgáltatás bevezetésének lehetőségéről szólt az előadás.

Előadó kiemelte, hogy a 41/2015 BM rendeletet visszabontva, meg kellett valósítani a felelősség elhatárolását üzemeltetés területével. A jogszabályi keretek **Adatgazdáról, Adatkezelőről és Adatfeldolgozóról** beszél, miközben a **Szolgáltató és a Felhasználó** azonosított esetünkben.



Forrás: Dr. Kovács Zoltán PhD, EIVOK prezentáció 2018.05.31.

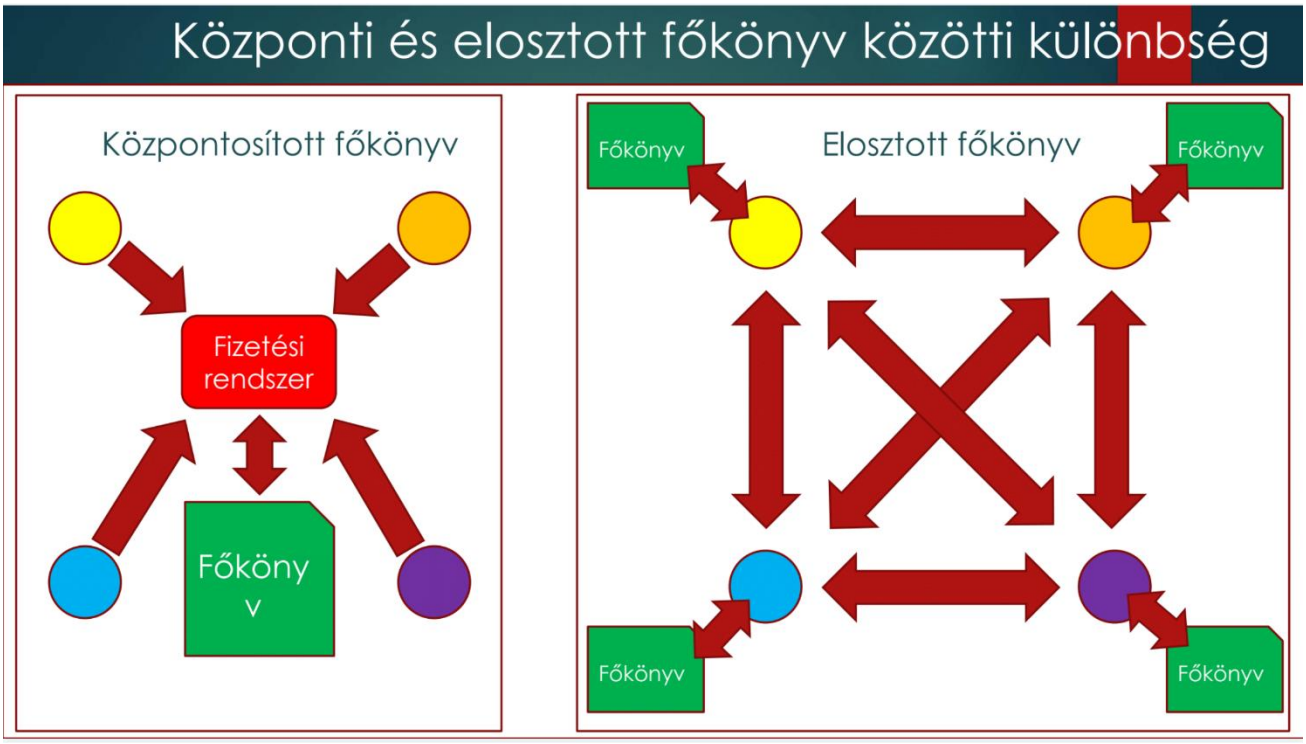
Előadó részletezte a Biztonsági Műveleti Központ (SOC) kialakítását, a SOC által nyújtott szolgáltatások: elektronikus információbiztonsági monitoring; SOC ügyfélszolgálat és előfeldolgozás; elektronikus információbiztonsági incidensek menedzsmentje és válasz intézkedések; sebezhetőség és sérülékenység menedzsment (felderítés és koordináció); fenyegetettségi információk (ThreatIntel –TI) begyűjtése és megosztása; elemzés, vadászat (hunting) és nyomozás; viselkedés alapú elemzés; igazságügyi nyomszakértői (forensics) tevékenység; detektálási képességek javítása és ami mára elengedhetetlen a mesterséges intelligencia és a gépi tanulás. RSA konferencia, mesterséges intelligencia alapú fejlesztett technológiák bemutatásra kerültek. SOC tervezésénél nélkülözhetetlen figyelembe venni a folyamatokat, a szükséges erőforrást és kompetenciát, valamint a technológiát. *„Vállalatra szabott és finomított rendszereket kell kialakítani és megfelelő riasztásokat generálni”.*

Zoltán kitekintést adott, hogy manapság – 2017. évi konferencia felmérése alapján – ki mit mond a támadásokról és a védelemről. Amire a biztonsági szakemberek fókuszálnak az a DDoS, az IDS/IPS jelzések, az APT, az SQL injection, a Phising, a hozzáférés megszerzése, a Malware. A vezetők pedig a következő kérdéskörökre fókuszálnak, például, hogy milyen rossz a támadás/kockázat, ki a támadó, hová jutottak be, mit vittek el, mi a jogi hatás, kontroll alatt lehet-e tartani, mi a kár?

Kihangsúlyozásra került, hogy a jól felkészült támadók ellen a hagyományos védelmi megoldások nem lesznek elegendőek. Felmérés alapján még mindig nagyobb mint 80% jelzi, hogy az ember felelős azért, hogy sikeres támadást tudnak végrehajtani a támadók. Ebből az következik, hogy a tudatosítás, az oktatás nem kihagyható egyetlen rendszerből sem.

Második előadó **Sík Zoltán Nándor** volt, aki sokak által ismeretlen téma bemutatását vállalta „*A blockchain filozófiája*” címmel.

Az előadás első részében átfogó képet mutatott be a technológia matematikai alapjairól, az alkalmazott technológiákról. Történeti áttekintésben mutatta be az eddig technikatörténet fontosabb lépéseit. A műszaki megoldásokon túl nyílt és elosztott FŐKÖNYV és az BIZALMI elvek ismertetése következett, valamint az ezeken alapuló pénzrendszereket kiemelve a bitcoint. A bemutatás során a különféle „kriptovaluták” keletkezésének, használatának eseteit számos gyakorlati példán keresztül ismertette.



Ábra forrása: Sík Zoltán Nándor, EIVOK prezentáció 2018.05.31

A jelenleg kialakulóban lévő társadalmi hatások, felhasználási lehetőségek, IT és adatbiztonsági kérdések áttekintése során számos kérdés érkezett a hallgatóságtól is. A szakmai kérdések is rámutattak arra, hogy ezzel az „új” világgal kapcsolatban, milyen IT és adatbiztonsági kérdéseket szükséges megoldani, milyen lehetséges alkalmazások lehetnek még a jövő társadalmasítási folyamatában. Az előadáson túl Sík Zoltán Nándor úr E-Közigazgatásban megjelent alábbi publikációja is megtalálható a dropboxban, amely segít megérteni a témakört.

E-KÖZIGAZGATÁS

SÍK ZOLTÁN NÁNDOR
ALELNÖK
NEMZETI HÍRKÖZLÉSI ÉS INFORMATIKAI TANÁCS

A blockchain filozófiája, avagy a fennálló társadalmi rendek felülvizsgálatának kényszere

Csak egy forradalmi innováció a sok közül?

Blockchain – jobb fordítás híján magyarul blokklánc[1]. A blockchain egy olyan információtechnológiai innováció, amely nevének már csak a hallatán is minden vezető állam, államszövetség politikai és gazdasági vezetőinek megremeg a szája széle. A jelen cikk írásának idejére gyakorlatilag a világ minden vezető hatalma tett már valamilyen nyilatkozatot blockchain „ügyben".

Kim[12] a Világbank vezetője, Mario Draghi[13], az Európai Központi Bank elnöke. Ugyanígy megszólaltak más banki és pénzintézeti vezetők, mint pl. Jamie Dimon[14] a JPMorgan vezetője, vagy a nagy multicégek vezetői, mint pl. Bill Gates[15], és sorolhatnánk. Sőt, a blockchain még a politika középpontjába is került.[16] Naponta születnek nyilatkozatok, vélemények, állásfoglalások, leginkább abban a tekintetben, hogy hogyan lehet a blockchain-t kordában tartani, az erre alapuló megoldásokat szabályozni.

Forrása: Sík Zoltán Nándor, EIVOK prezentáció 2018.05.31.

A kerekasztal beszélgetést **Németh Imre** vezette le „*Adataink története a Facebook-n*" címmel. Az előadó már a felvezetésében felhívta a figyelmet arra, hogy a személyes adatok összegyűjtése pontos profilok szerint történik. Létezik egy sor olyan tulajdonság, amely mérhető és amely felhasználási profillal – például életkorral, nemmel, elhelyezkedéssel stb. – van összefüggésben. A legnagyobb social média szolgáltató, becslések szerint több, mint 52 000 személyes tulajdonságot használt fel az emberek érdekeinek és attribútumainak osztályozására. A statisztikai módszereket ezután analitikus információk előállítására, vagy jövőbeni magatartásformálásra, vagy fejlesztésre használják fel. Hosszas beszélgetés alakult ki arról, hogyan használják fel az adatainkat és a manipulálás eszközeit, miként alkalmazzák azokat különféle célokra.
Amennyiben kíváncsi vagy rá, hogy ki nézte meg a Facebook oldaladat, akkor használd a „Initialchatfriendslist"-et. Imre továbbá ajánlott irodalomként megosztotta velünk a Facebooks_Revised_Policies_and_Terms_v1.3, érdemes elolvasni.

Az előadás anyagok elérhetőek az EIVOK Dropbox felületén.

Az EIVOK Klub legközelebb **2018.10.04-én** 17:00 órakor lesz.

Váruk szeretettel a következő alkalommal is.

EIVOK Szakosztályi Vezetőség