MBVE
XIV. Konferencia – 2013. Siófok

A BIZTONSÁGI SZAKMA KÉRDÉSEI, AKTUALITÁSAI A MEGBÍZÓI ÉS A SZOLGÁLTATÓI OLDAL SZEMSZÖGÉBŐL

A Magyar Biztonsági Vezetők Egyesületének (MBVE) idei konferenciája is bebizonyította hogy nagy az igény a szakmai tájékozódásra, egyeztetésekre, a technikai-, szervezeti-, jogi-, oktatási változások fejlődésének követésére. Fialka György, az MBVE elnöke hangsúlyozta az egyesület nyitottságát a civil és hivatásos szervek felé, a partnerkapcsolati megállapodások fontosságát és a biztonsági képzésben való szerepvállalást. Kitűnő előadások hangzottak el többek közt a BRFK, a Kamara, a Montana Tudásmenedzsment Kft., az Óbudai Egyetem, a Justice Security, a Seawing Kft., a Nemzeti Bűnmegelőzési Tanács, a MOL, a Rendészeti Tudományos Társaság, a Magyar Bankszövetség, a Biztonságvédelmi Klaszter, a Nemzeti Biztonsági Felügyelet, és a NEC Eastern Europe Kft. előadói részéről.

Fialka György az MBVE elnöke *„Az MBVE szerepvállalása és lehetőségei 2013. évben”* előadásában hangsúlyozta, hogy szorosabb együttműködést lehet végezni azokkal a civil és hivatásos szervekkel, akik a biztonság kialakításáért felelősek, és így a biztonsági szakma sokkal erősebb és hatékonyabb lehet. A hivatásos „biztonságvédőknek”, a rendészeti dolgozóknak és a magánbiztonsági szféra szereplőinek érdekei azonosak, a biztonság védelme és biztosítása terén. Az MBVE nyitott a társadalmi kapcsolatok bővítésére a közszféra irányába. Ennek érdekében számos együttműködési megállapodást kötöttek, a közelmúltban.

- Partnereik között megtalálható a RTF Magánbiztonsági Tanszék, Bólyai (ZMNE) Biztonságtechnikai tanszék, melyet most Közszolgálati Egyetemként egyesítettek, az SZVMSZK, az Óbudai Egyetem, az MBF együttműködés, a Magánbiztonsági Klaszter, a BM OKTF, az NBT, a BRFK, a NBSZ, a HM EI RT és a REMOK.
- Az MBVE célja a biztonsági képzés területén magánbiztonsági tudásbázis, az intézményi háttér, és a tudományág megteremtése együttműködve e célból a mérvadó testületekkel SZVSZMK, MRTT, RTF, Zrínyi és az OBE.
- Tovább kell lépnünk, a közép és felsőszintű képzések tekintetében is. Ki kell dolgozni a ciklikus képzés kreditrendszerét.

Berár Iván rendőr ezredes BRFK Gazdaságvédelmi Főosztályvezető *„A rendőrség és a magánbiztonsági terület együttműködési formái”* című előadását hallgathatták meg az érdeklődők.

Az SZVMSZK elnöke ***dr. Német Ferenc*** *„A vagyonvédelmi kamara helyzete, a 2013-as kötelező oktatási feladatok”* címmel tartott színvonalas előadást

Preklet István, a Montana Tudásmenedzsment Kft. ügyvezető igazgatója mutatta be *Digisec rendszerük szolgáltatásait.*

➲ Elmondta, hogy a DIGISEC Rendszer a MONTANA Tudásmenedzsment Kft. által fejlesztett megfigyelő és eseményelemző intelligens biztonsági rendszer. Képes egy telephely, épület, országos kiterjedésű szervezet megfigyelési, biztonsági feladatainak támogatására. Akár a meglévő megfigyelőrendszer intelligens kiegészítéseként, akár önálló rendszerként képes a videók rögzítésére, tárolására, a videoképek folyamatos elemzésére, értékelésére, akár egyszerű (belép; kilép; túl gyors), akár összetett (ügyintézésre vár, de az ügyintéző nincs jelen; belépőkártyája nem a sajátja – nem egyezik a tárolt arckép a belépővel) események esetében is.

A rendszer az azonosított eseményeket tárolja, és fejlett visszakereső-rendszerének segítségével képes esemény alapon lejátszani a releváns videoszakaszt (leválogatja a tegnapi összes belépés eseményt, majd 1-1 kattintással visszajátszható a film).

Nyílt rendszerként képes tetszőleges intelligens IP vagy analóg kamerarendszerekkel is együttműködni, felhasználva akár a kamerák eseményelemzőit, vagy saját megoldásokkal „okosítja" az analóg kamerákat.

■ ***Kovács Tibor*** (Óbudai Egyetem, egyetemi docens, PhD/CSc) *„A biometria eszközei és azok sérülékenysége"* című előadásában elemezte, hogy a biometrikus azonosítók műszaki paraméterei mennyire erőteljesen függnek az adott eszköz alkalmazási körülményeitől.

Elmondta, hogy a gyártók által kiadott műszaki adatlapokon (data sheet) feltüntetettek a környezettől függően a gyakorlatban eltérhetnek a leírtaktól. Ez több okra vezethető vissza. A leglényegesebb üzemeltetési paraméterek (hőmérséklet, levegő-páratartalom és ezek stabilitása ott, ahol az eszköz felállításra került) alapvetőek a megfelelő működés szempontjából. Gyakran maguknak a felhasználóknak a nem optimális fizikai paraméterei (sérült vagy szennyezett ujj, kancsalság, stb.) vezetnek a sikertelen biometriai azonosításhoz. Néha az is megtörténik – különösen, ha a készülék a működési paramétereinek maximumához közel üzemel –, hogy a téves elutasítási értékek feltűnően leromlanak. Az előadásában négy különböző azonosítási elvű biometrikus eszköztípus (ujjnyomat, kézgeometria, ujj-, és tenyérerezet és írisz) működését elemezte, feltárta a tapasztalt problémákat és megoldásokat is javasolt.

■ ***Bene Krisztián***, a Justice Security értékesítési vezetője *„Aggodalom csillapító módszerek az információbiztonság területén"* című előadásában elemezte a Justice Security innovatív vagyonvédelmi partneri szerepét, amely célzott és hatékony megoldások segítségével megnyugtató értékvédelmet biztosít megbízói számára. Az előadás során nemcsak az aggodalomra gyakran okot adó biztonsági kockázatokat ismerhettek meg a hallgatók, de megoldási javaslatokat is kaptak…

Az emberi erőforráshoz kapcsolódó kockázatok egyik leghatékonyabb kezelési eszköze a magánnyomozás, amelynek eleme lehet az alkalmazotti megbízhatósági vizsgálat, a HR-nyomozás és -környezettanulmány, a betegállomány-ellenőrzés, az üzleti partnerek feltérképezése és a kockázatelemzés.

A gyártósorok magas selejtaránya, vagy a raktárak kiugró leltárhiánya komoly veszteséget jelent. Ilyenkor kiváló aggodalomcsillapító módszer a Justice Security által kifejlesztett POSeidon Control System. Ez az egyedi rendszer nemcsak kameraképre integrált blokkinformációt ad, de speciális nyomozati szoftvere segítségével automatikusan jelzi a gyanús tranzakciókat. A POSeidon Control System kiválóan működik ipari felhasználásoknál: például belső üzemanyagkutak, töltő és gyártósorok esetében, valamint a mérleghasználat területén is.

Az előadás harmadik témája a vezetői információk kijutásának megakadályozása, vagyis a lehallgatás-felderítés volt. Az előadó bemutatta, milyen olcsó és egyszerű ma lehallgató eszközhöz jutni, ami komoly veszély a cégek, illetve cégvezetők bizalmas információira

A megelőző intézkedéseken túl ma már komoly szerepe van a lehallgatóeszközök felderítésének. A technika fejlődésével a „poloskák" egyre kisebbek és hatékonyabbak

lettek, ezért ezek megtalálása ma már komoly emberi és technkiai apparátust igényel.
A lehallgatás-felderítés első lépése a fizikai és endoszkópos átvizsgálás. Ezt követi a teljes spektrumú pásztázóeszköz, majd a félvezetőkereső és a speciális hőkamera használata.
A prezentáció végén az előadó hangsúlyozta, hogy lehallgatásfelderítés csak hatósági engedély birtokában végezhető.

Dr. Horváth Sándor, az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karának dékánja *„Biztonságtechnikai mérnök képzésének tapasztalatai”* című előadását rövid történelmi visszatekintéssel kezdte.
Elmondta, hogy hasonló nevű egyetem már létezett a középkorban is, 1395. október 6-án adta ki IX. Bonifác pápa Luxemburgi Zsigmond magyar király kérésére az Óbudai Egyetem első alapítólevelét, amely az ország második, a főváros első egyeteme lett. Az egyetemet 1403-ban a király belpolitikai okok miatt bezáratta.
Zsigmond kérésére 1410. augusztus 1-jén a pápa aláírta az Óbudai Egyetem újjáalapítására vonatkozó bulláját, de 1419 után nincs adat az egyetem további működéséről.
A jelenlegi Óbudai Egyetem természetesen nem jogutódja a Zsigmond által alapítottaknak, de annak szellemiségét tovább kívánja vinni. Első jogelődjét a Budapesti Állami Közép-Ipartanodát 1879-ben alapították, az egyetemmé válás folyamatának főbb állomásai pedig: 1898 Magyar Királyi Állami Felső-ipariskola (ahol 1901-ben Galamb József befejezi tanulmányait), 1954 Bánki Donát nevének felvétele, 1962 Bánki Donát Felsőfokú Gépipari Technikum, 1969 Bánki Donát Gépipari Műszaki Főiskola, 1991 Bánki Donát Műszaki Főiskola, 2000 BMF Bánki Kar, 2010 Óbudai Egyetem Bánki Kar.
A jogelőd főiskolán éppen 20 évvel ezelőtt, 1993-ban kezdődött meg biztonságtechnikai mérnökök képzése.
A jelenlegi képzési kínálatban szerepel a 7 féléves alapképzés (BSc) és az arra épülő 4 féléves mesterképzés (MSc). A képzésekben az egyetem Kandó Kálmán Villamosmérnöki Kara is meghatározó szerepet vállal.
Az előadó a képzések erősségeként annak gyakorlatorientált jellegét, az erős humán, valamint infrastrukturális hátteret említette. Kiemelte a széles szakmai kapcsolatrendszer rendkívüli jelentőségét, a kiváló külső óraadókat, a szakmai szervezetekkel, kamarával kötött, és tartalommal megtöltött megállapodásokat. Hangsúlyozta a tehetséggondozás fontosságát, és elmondta, hogy ezen a területen még további előrelépésre látnak lehetőséget.
Mind az egyetem, mind pedig a szakma szempontjából rendkívüli jelentőségű, hogy 2012-ben megalapításra került a Biztonságtudományi Doktori Iskola, ami a biztonságvédelem területén tevékenykedő szakemberek számára lehetőséget kínál tudományos kutatásra, majd doktori fokozat megszerzésére.

„Beléptetés, biztonság és HR…” – ezzel a címmel tartott előadást a Magyar Biztonsági Vezetők Egyesületének XIV. konferenciáján a Seawing Kft. ügyvezető igazgatója **Pálffy Zoltán**. A siófoki prezentáció érdekessége abban rejlett, hogy rendhagyó módon, új megvilágításban nem a gyártó, hanem a vállalkozói és megrendelői preferenciák szemszögéből elemezte a beléptetőrendszerekkel kapcsolatos helyzetet.
Vajon biztonsági, ár, vagy cégstratégiai kérdésről beszélünk? Vajon melyik ebből a legfontosabb? – hangzott el a kérdés a hallgatóság irányába az előadás kezdetén. A kérdések megválaszolása a rendszer és rendszerszállító kiválasztásáért felelős jelenlévő biztonságtechnikai szakemberek számára is komoly kihívást jelent. Ezért a SEAWING ügyvezető elemezte, majd összefoglalta a cégek gazdaságos működéséhez hozzájáruló rendszerszolgáltatásokat. A prezentáció többek között kitért a beléptetőrendszer szerepére a rend fenntartásában, milyen megoldást adhat az erőforrások ellenőrzésére, gyakorlati alkalmazásokat mutatott be a beléptetőrendszer adatainak másodlagos felhasználására is. Az előadás keretében számos életből vett példa is elhangzott, amely bizonyította, az élet mindig produkál olyan helyzeteket, amelyet csak egy jól támogatott rendszerrel lehet megoldani. A jó beléptetőrendszer alkalmas a cég működésével összefüggő nem szigorúan csak biztonsági feladatok ellátására is, így a cég biztonsági vezetője a cég organikus működésében aktív részt vállalhat, támogatást nyújthat a cégen belüli problémák megoldásában.
Az Mt. trv. változása, a munkaügyi szabályok betartásának szigorúbb ellenőrzése kapcsán a beléptetőrendszer kitüntetett szerepet kaphat a cég életében. Az előadás második felében Pálffy Zoltán részletezte a beléptetőrendszerhez kapcsolódó, de funkciójában független munkaidőnyilvántartó-rendszer kialakításának módszertanát, a megoldás előnyeit.

Ezt követően **Dr. Hatala József** a Nemzeti Bűnmegelőzési Tanács elnöke *„A Duna stratégia magánbiztonsági lépései”* című előadását hallgathatták meg a konferencia résztvevői.

Dr. Dósa Imre előadása *a személyes adatok védelmének új aspektusaival foglalkozott.* Az adatvédelmi és a biztonsági érdekek hagyományosan ütköznek. Ezért a biztonsági szakemberek számára is fontos a szakmájukat érintő adatvédelmi szabályok, elvek, hatósági gyakorlat ismerete.
Az előadás két nagyobb területet érintett. A munkahelyi kamerázásról a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) a közelmúltban ajánlást bocsájtott ki. Az ajánlás megfogalmazza a munkahelyen alkalmazható elektronikus megfigyelőrendszer alkalmazhatósági körét, jogalapját, feltételeit. Az előadás bemutatta a munkahelyi kamerázás nyomán előálló alkotmányossági, törvényességi aggályokat. Ezekkel szembeállítva ismertette a hatóság által javasolt alkalmazhatósági feltételeket, tájékoztatási gyakorlatra vonatkozó ajánlásokat. Az előadás érzékeltette, hogy ➲

➲ egyszerűen megismerhető korlátok, tilalmak figyelembevétele mellett, a kamerázás gondos megtervezésével és felügyeletével, az adatkezelés hatósági bejelentésével teljesíthetők a törvény által előírt és a NAIH által értelmezett feltételek.

Az előadás második része az Európai Unióban formálódó adatvédelmi rendelet tervezetéről szólt. A tervezett – európai szinten egységes, közvetlenül érvényesülő – szabályozás több olyan rendelkezést tartalmaz, amely új adatvédelmi szemléletet igényel. A személyes adatok hordozhatóságának elve, vagy a tervezett bírságolási lehetőségek olyan megfelelési kötelezettséget vetítenek előre, melyekre érdemes már most felkészülni. Így gazdaságos keretek között biztosítható egy olyan adatvédelmi megfelelési szint, ami végső soron versenyelőnyt hoz a vállalkozásoknak.

■ ***Dr. Janza Frigyes*** vezérőrnagy, a Rendészeti Tudományos Társaság főtitkára *„A magánbiztonság rendészeti aspektusai, felsőfokú oktatása, tudományos bázisa"* című előadását hallgathatták meg az érdeklődők.

■ ***Jakab Péter***, MKB Bank ZRt. Bankbiztonság, ügyvezető igazgató, a Magyar Bankszövetség Bankbiztonsági Munkabizottság elnöke, az *„Információvédelem aktualitásai"* című előadásában elmondta, hogy egyre erősödő tendenciaként jelentkezik a hacker/cracker tevékenység, a bűnözés, a kémkedés, a terrorizmus, a hadviselés, a létfontosságú infrastruktúrák (SCADA) IT rendszerei elleni támadások területén.

Az informatikai rendszerekben tárolt információ mennyisége és értéke rohamosan növekszik. Az adatok megszerzéséhez, manipulálásához egyre komolyabb érdekek fűződnek, és jól kitapintható módon a szervezett bűnözés is jelen van és a technológia fejlődése a támadókat is „segíti".

A szolgáltatások kiesésének hatása egyre súlyosabb és a kritikus infrastruktúrák és az információtechnológiát alkalmazó szervezetek IT-függősége is egyre nagyobb.

Az előadó bemutatta az IT-fenyegetettség legjellemzőbb okait, egyebek között, a bonyolult rendszerek tesztelhetőségének korlátait, az alkalmazásfejlesztések nem megfelelő minőségét, a mobil kommunikáció és a vezeték nélküli hálózatok használata kockázatait, a megbízható azonosítás problematikáját, a globalizálódó és állandósuló támadások hatását, az IT rendszerek fizikai sérüléseinek kockázatait. Egyre nagyobb gond, hogy a támadások elleni intézkedések kidolgozására mind kevesebb idő van.

Az előadó említést tett a legjellemzőbb internetes támadásokról: mint a webhelyrongálás (pl. Anonymus group); a kliens oldali támadások (azonosítók megszerzése, adatforgalom megszerzése titkosítás előtt, gép memóriájában maradt adatok felhasználása); a kockázatos ügyfélmagatartás kihasználása – jelszókezelés, idegenkedés a tokenektől, gyenge biztonsági színvonalú PC-védelem (biztonsági frissítések, vírusvédelem, spamszűrés, kémprogramok elleni védelem hiánya, rosszul beállított tűzfalak); a rosszul megírt, gyenge bemenetszűrésű alkalmazások támadási lehetőségei, (SQL injekció, XSS, beégetett és tárolt jelszavak, gyenge kriptográfiai algoritmusok); és a manapság oly „divatos" sávszélességnek mint erőforrásnak az „elfogyasztásával operáló, szolgáltatást megtagadtató támadások – (DOS, DDOS) – valamint a kommunikáló felek közé beálló támadók un. közvetítéses támadásai. (MITM, MITB).

■ ***dr. Füzesy István***, az Első Magyar Polgári Biztonságvédelmi Klaszter elnöke, *„A magánbiztonsági klaszter kibontakozásának lehetőségei"* című előadásában bemutatta a 2010-ben Szegeden megalapított klasztert, melynek alapcéljai között szerepel a klasztertagok, a polgári biztonságvédelmi iparág tevékenységhez kapcsolódó vállalkozások gazdasági lehetőségeinek szélesítése és fejlődésének elősegítése, ami által várható a gazdasági válság hatá-

sainak csökkentése, az iparág fejlesztése, megrendelések – munkalehetőség –, generálása. Fontos célkitűzés a biztonsági iparág társadalmi elfogadottságának erősítése, a társadalmi biztonság fejlesztése.

A klasztermozgalom adta háttér új lehetőséget teremthet a polgári biztonsági terület ágazatai, vállalkozásai, és a megrendelők között. A többrétű cél hazai bázison projektgenerálással, pályázati lehetőségek felkutatásával, a megfelelés elősegítésével, valamint támogató K+F tevékenységgel valósítható meg. A klasztertagok kiegészíthetik egymás tevékenységét, közös szolgáltatást nyújthatnak, azonban egyéni érdekeltségeiket is fenntartják. A gazdaságfejlesztési, területfejlesztési, és társadalmi szervezetek, valamint szolgáltatásokat nyújtó cégek közti kapcsolat elmélyítése révén növelhetik a hatékonyságot, eredményességet.

A magyar biztonsági ipar egyik kitörési irányaként a nemzetközi együttműködés fejlesztését tartják célszerűnek. Ennek érdekében megkezdték a határon átnyúló gazdasági tevékenységekhez kapcsolódó nemzetközi elvárásoknak történő megfelelés kialakítását, támogatását. Nemzetközi szinten együttműködéseket kezdeményeznek, melyeket megállapodások formájában dokumentálnak Ausztria és Szerbia irányába. A külföldi partnerekkel történt közös jövőkép felvázolása alapján lehetőség mutatkozik arra, hogy az Unió ajánlásai és céljai figyelembevételével és az ehhez kapcsolódó támogatási rendszer felhasználásával több országot érintő projektekbe is bekapcsolódjanak, amelyre a Duna-stratégia is megfelelő keretet biztosít. A nemzetközi együttműködés együtt szolgálja a magyar biztonsági iparág céljait, valamint egyedi szinten az adott vállalkozásoknak az érdekeit az új lehetőségek megteremtésével.

A nemzetközi együttműködés keretében egységes alapú, tudáshátterű és színvonalú, transznacionális szintű tevékenység kialakítása a cél, amihez kapcsolódik a hazai és az adott országok cégeinek, munkavállalóinak tudásanyagának megfeleltetése is. Ennek konkrét megvalósítása nemzetközi oktatás, továbbképzés, egységes szabályozási rendszerek, best practice kialakítása révén lehetséges.

A klaszter célja az akkreditált cím elnyerése, ami további pályázati lehetőségeket nyithat meg.

Zala Mihály, a Nemzeti Biztonsági Felügyelet elnöke, az *„MBVE-NBF együttműködés lehetőségei, tartalma, várható eredményei”* című előadását a hazai szabályozási környezet átalakítása, a minősített adatvédelem 2009-es újraszabályozásának bemutatásával kezdte, amelyek a következők voltak: A nemzeti és a külföldi minősített adatok védelmére egységes követelmények meghatározása, a magasan minősített adatok számának radikális csökkentése, a minősítési eljárás modernizációja, a négyszintű, kockázat-, és káralapú minősítési rendszer teljes körű adaptálása a nemzeti minősített adatokra, az automatizmushoz vezető államtitokköri, illetve szolgálati titokköri jegyzékek megszüntetése és helyettük a „minősítéssel védhető közérdek” fogalmának bevezetése.

Elmondta, hogy a Nemzeti Biztonsági Felügyelet alapvető feladatai közé tartoznak a minősített adatok kezelésének hatósági felügyelete (valamennyi minősített adatot kezelő szervezet ellenőrzése, rendvédelmi szervek, gazdálkodó szervezetek, központi államigazgatási szervek stb.), a nemzeti iparbiztonsági hatósági feladatok ellátása (a nemzeti, NATO és EU telephely biztonsági tanúsítvány kiadása – valamennyi minősített adat felhasználásával járó projekt esetében); a minősített adat biztonsága megsértésének esetén a körülmények kivizsgálása – az elektronikus rendszerek használatba vételének engedélyezése és az engedélyben foglaltak betartásának ellenőrzése – mintegy 2000 helyszínt és 30 000 munkaállomást érint; a rejtjeltevékenység hatósági engedélyezése és felügyelete, az Országos Rejtjelfelügyelet korábbi tevékenységének ellátása révén; valamint végül, de nem utolsó sorban a TEMPEST hatósági feladatok (nóvum a magyar minősített adatvédelemben) elvégzése.

A Felügyelet megalakulása óta megfigyelhető folyamatos hatáskörbővülés eredményeként 2010. óta a felügyelet végzi felkérés esetén a kormányzati és létfontosságú információs rendszerek sérülékenység-vizsgálatát is.

Előadásában kitért a Felügyelet új feladataira és tervezett szolgáltatásaira is, mint amilyen például a hatósági termékajánlás és terméktanúsítás, valamint a proaktív és preventív kibervédelem kiépítése a közigazgatásban.

A Felügyelet tervei szerint a közeljövőben megkezdődik a hatósági terméktanúsítási tevékenység a fizikai- és információbiztonsági területen. A gazdálkodó szervezeteknél a terméktanúsítás piaci alapon működik majd. A hatósági terméktanúsítási tevékenység ezentúl kiterjed a biztonságtechnikai termékek (eszközök), információbiztonsági és IT-biztonsági termékek (eszközök, szoftverek, hardverek) tanúsítására is.

A széles körű partneri kapcsolatok kialakításához és elmélyítéséhez a Felügyelet több együttműködési megállapodást kötött, az SZVMSZK, az MBVMSZ és az MBVE szakmai szervezetekkel.

Előadásában az elnök bemutatta az NBF–MBVE közötti együttműködés lehetőségeit, tartalmát és várható előnyeit és kifejezte abbéli reményét, hogy a megállapodással az NBF erősíteni tudja kapcsolatát a biztonsági vezetőket és a biztonsági szakma megrendelői oldalát tömörítő szervezettel, az MBVE-vel.

Az együttműködés során a Felügyelet számít az MBVE szakértői kompetenciáira és figyelembe veszi azokat, véleményezési lehetőséget biztosít a jogszabály-alkotási és követelménymeghatározási folyamatok során.

Az MBVE építhet az NBF minősített adatok védelmével kapcsolatos tapasztalataira, szaktudására.

Az együttműködési keretmegállapodást számos kölcsönösen előnyös szakterületi, eseti megállapodással és közös projektekkel kívánják a felek kitölteni.

Lőrinczy Péter, NEC Eastern Europe Kft. üzletfejlesztési vezető, – *„Az ujjvéna elemzés, mint a személyazonosítás új eszköze”* című előadásában először néhány szóval bemutatta a céget ahol dolgozik. Az első Japán Amerikai közös vállalatot 1899-ben alapították, amelynek 150 országban jelenleg 115 840 alkalma- ➲

zottja van. Tizenkét kutatóközpontban 2,193 M USD-t költenek kutatásfejlesztésre, és több mint 40 000 szabadalommal rendelkeznek.

Elmondta, hogy az USA-ban a bűnügyi nyilvántartás ujjlenyomat-adatainak több, mint 50%-a az NEC rendszerein van.

Bemutatta az új hibrid érintésmentes ujjlenyomat-olvasójukat melynek előnyei a kettő az egyben kivitel, az érintésmentes kivitelezés, az egyidejű leolvasás, a kiváló leolvasási pontosság.

A leolvasó jól alkalmazható számos területen, mint például vállalati beléptetőrendszereknél (időmenedzsment, részmunkaidős alkalmazottak), kórházi adathozzáféréshez, banki alkalmazásoknál, határellenőrzéseknél a pontosabb személyazonosítás érdekében.

Fialka György (MBVE elnöke) *„A pénzintézetek biztonsági helyzete, lehetőségei 2012-ben"* című előadása elején beszélt a 2012-es év kihívásairól és kockázatairól, mint a bankellenességet okozó hangulati tényezőkről (gazdasági válság, árfolyamproblémák, eladósodás, munkanélküliség), a megszorításokat követő optimalizációkról (létszámcsökkentés, felgyorsult ütem, veszteségkezelés), és a humán kockázatokról (homless helyfoglalások, ügyféli indulatok kezelése).

- A banki kockázati területen növekedett az ATM eszközök támadása (kártyaadatlopásos nemzetközi akciók, reverzművelet-akadályozás),
- az elektronikus csatornák támadása (Anonymus, orosz vonal, netbank hacking),
- a megszemélyesítéses bűncselekmények (az ügyfél szerepének átvétele, adatszerzéssel, kiváló hamis okmányokkal),
- az alkalmazotti kör bizonytalanságai (belső korrupciós, vagy együttműködési hajlandóság, üzleti magatartás).
- Az előadó bemutatta a védekezés lehetséges forrásait, mint az intézményesült biztonsági szemléletmód fejlesztését, a pénzintézeti biztonsági vezetők közös elhárítási fórumait, a Bankszövetség mint közösítő, irányító testületet, a Rendőrség partnerfórumait, a minőségbiztosítás lehetőségeit és az utánpótlásképzést.

Elmondta, hogy a biztonságtechnika által biztosított új lehetőségek banki területeken is megjelentek

- a személyazonosítás új eszközei kerültek forgalomba (a biometria térhódítása),
- az intelligens szoftverek – (eseményalapú képkezelés),
- a rendkívüli események megakadályozása beavatkozó eszközökkel (füstágyú, vezérelt záróeszközök).

Beszélt az ellenőrzés jelentősége kapcsán a folyamatok végrehajtásának szabályozottságáról és ellenőrzéséről, a másodlagos kontrollok fontosságáról, a kikerülhetetlen technikai kontrollok alkalmazásáról, az „Ügyfélszokás"-ra épített szűrésről és a devianciafigyelésről…

Előadása végén az előadó kiemelte a pénzintézeti kapcsolati eredményeket, mind az Együttműködést a BM törvényalkotó fórumaival és a szerződés szerinti folyamatos munkacsoporti kapcsolatot az ORFK, BRFK szerveivel.

Zólyomi Zsolt, (MOL-csoport Biztonsági Igazgató) a *„Kríziskezelési stratégia"* című előadásában hangsúlyozta, hogy a MOL Társasági Biztonság küldetése az anyagi értékek (termékek, üzemegységek, csővezetékek, töltőállomások, irodaépületek, stb.), a humán értékek (munkavállalók, beszállítók, vásárlók, látogatók), szellemi értékek (tudásvagyon, technológiák, bizalmas üzleti információk) védelme.

Bemutatta a MOL csoport széles körű tevékenységét. Elmondta, 7 országban folyik kőolaj-kitermelés és kutatás 11 országban zajlik jelenleg.

A társaságnak 5 finomítója, 2 petrolkémiai üzeme van, és több mint 1600 töltőállomása működik a régióban. Kiterjedt a gázvezetékrendszerük és aktív szerepük van a gáztárolás és értékesítés területén. A MOL csoport több mint 31 000 munkavállalót alkalmaz.

MOL – Magyarország tevékenység része a Dunai Finomító, 364 benzinkút, 174 bányászati technológiai egység, 3 gázfeldolgozó,

5378 db olaj- és földgázkút, 132 termelőmező, 1 petrolkémiai üzem (TVK), 5800 km földgáz-távvezetékrendszer (FGSZ), 1,9 Mrd m^3 földgáztároló (MMBF).

Az előadó beszélt a MOL-Csoport Krízis Menedzsment Rendszer felépítéséről és kiemelte, hogy az üzletmenet-folytonosság általános célja krízishelyzet esetén, a visszatérés a normál operációhoz amint lehet a leghatékonyabban, a legkisebb ráfordítással, a lehető legrövidebb úton és idő alatt.

Ennek érdekében hatékony krízismenedzsment csoportot kell létrehozni minden fő terület képviseletével, meg kell határozni a megfelelő vezetői szinteket, és a megfelelő pozícióba a megfelelő személyeket kell delegálni.

▸ A krízismenedzsment feladatai: a Krízisközpontok létesítése – elsődleges központok, másodlagos központok (Alternatív helyszínen) – és karbantartása.

Krízisközpontok felszerelésének biztosítása: kommunikációs eszközök (rádió, telefon, LAN, stb.), alternatív áramforrás, tervrajzok, dokumentumok (munkavállalói adatok, elérhetőségek, tervek, stb.).

Adatbázisok karbantartása: csoporttagok frissítése (negyedévente), krízis Tervek teljes felülvizsgálata (évente), oktatások, gyakorlatok dokumentálása (évente).

Oktatások, gyakorlatok tervezése, végrehajtása: tűz, bombafenyegetés, természeti/ember okozta katasztrófa, polgári/politikai zavargás.

K. M.