IT security 2015

2015. június 9., Budapest, Gundel étterem

IIR

„Informatikai rendszerekbe betörni olyan egyszerű, mint egy telefonhívást lebonyolítani"

Kevin Mitnick, a világ legismertebb hackere

A rendezvény fő témái

- **Third-party** együttműködés **kockázatai** és kezelésük - céges megközelítésbe
- **SCADA veszélyek** – a Stuxnet esetről dióhéjban
- **Adathalászat** – a naivitás és tudatlanság vámszedői
- **Cyber** security
- **Cloud** biztonság
- **APT** – védelem az összetett támadások ellen
- A **távmunka információbiztonság**i aspektusai

www.iir-hungary.hu fax +36 1 459 7301 conference@iir-hungary.hu

Szakembereink

Balogh Viktor
CISM, Certified FireEye Engineer

Bus László
IT manager, belső projektek felügyelete

Horváth Gergely Krisztián
CISA CISM, elnökségi tag

Jakab Péter
Ügyvezető igazgató

Kocsis Tamás
Enterprise Sales Strategist

Dr. Krasznay Csaba
IT biztonsági szakértő

Niklai Norbert
Information Security Officer

Pávlicz György
Chief Information Security Officer

Solymos Ákos
CISM, CRISC információbiztonsági szakértő

2015. június 9. kedd

IT security

8:30 Érkezés, regisztráció

8:50 Köszöntő az IIR és az elnök részéről

A nap levezető elnöke: Horváth Gergely Krisztián CISA, CISM, elnökségi tag, ISACA-HU

9:00 Cyber security

- Tisztázzuk az alapokat: információbiztonság, cyber security
- Hogyan lehet hatékonyan védekezni az APT támadások ellen?
- Mely cégek, szektorok állnak a támadások középpontjában? Milyen támadások érik őket? Mik a tapasztalatok?
- Hogyan lehet az APT támadás ellen védekezni, milyen eszközökkel? Hogyan lehet egészséges védelmet kialakítani?
- Hogyan lehet a felhasználói tudatosságot növelni?
- Milyen good practice-ek vannak? Hogyan lehet az APT támadások ellen fellépni globálisan, lokálisan?

Előadó: Jakab Péter, ügyvezető igazgató, MKB BANK Zrt.

9:40 Cloud biztonság

- A modern nagyvállalatoknál a felhő alapú megoldások megállíthatatlanul törnek előre. Legyen az privát vagy publikus cloud, szoftver vagy infrastruktúra szolgáltatás, az információbiztonsággal kapcsolatos kérdéseket mindenki felteszi, a válaszok azonban még nem túl megnyugtatóak.
- Az előadás áttekinti azokat a főbb kihívásokat, melyeket napjainkban a felhőbiztonsággal kapcsolatban a szakma érzékel, egyben bemutat néhány olyan jótanácsot, melyet üzemeltetőként és felhasználóként érdemes ebben a környezetben megfontolni.

Előadó: Dr. Krasznay Csaba, IT biztonsági szakértő, BalaBit IT Security Kft.

10:10 Mobile Device Management

- Android, IOS, Windows phone, Blackberry – melyik az üdvözítő, melyik biztonságosabb ? Mi nyújtja a legmagasabb védelmet?
- Milyen új kockázatok jelennek meg és az eddigi zárt hálózatoknál hogyan lehet védekezni ezek ellen?
- Milyen adatvédelmi és adatszolgáltatási kötelezettsgek vannak?
- Hogyan teremthető meg a szoftver oldali védelem?
- Hogyan alakítható ki egy védelmi blokkoló szegmens?
- Milyen biztonsági intézkedéseket szükséges bevezetni?
- Meddig terjed a felhasználó és szolgáltató felelőssége az adatvédelem területén? Ki a felelős, ha feltörik az eszközt? Hogyan kezelem ezt a kockázatot?
- Hogyan válasszuk el a privát és üzleti típusú adatokat?
- Hogyan kivitelezhető technológiailag az adott eszköz és szervezet védett hálózata közötti kommunikáció, adatátvitel?
- Sandbox technológia: mit tekintünk kritikus adatnak?

Előadó: Kocsis Tamás, Enterprise Sales Strategist, biztributor Kft.

10:40 Tesztvezetéssel egybekötött kávészünet a NISSAN támogatásával

BŐVEBB INFORMÁCIÓ: Papp Martina
+36 1 459 7326 +36 70 419 8623 +36 1 459 7301
martina.papp@iir-hungary.hu

Rendezvényünk szólni kíván

közép- és nagyvállalatok

➔ IT biztonsági szakembereit, igazgatóit, vezetőit, szakértőit
➔ CSO ➔ CISO ➔ CTO
➔ Risk Manager
➔ Infra-structure Manager
➔ Network Manager ➔ Head of Compliance and Governance
➔ Business Continuity Manager
➔ Data Security Analysts ➔ Heads of Security Architecture
➔ Head of IT Strategy

Várjuk továbbá az IT security megoldásokat kínáló **beszállító és tanácsadó cégek** képviselőit is.

Miért érdemes részt venni?

➔ **Malware fenyegetések** – tudjon meg többet az **APT támadások** elleni védekezésről
➔ Ismerje meg a **távmunka** információbiztonsági aspektusait a Ricoh Magyarország **esettanulmány**a keretében
➔ **Adathalászat**, a naivitás és tudatlanság vámszedői: számos **hazai példán keresztül** megismerheti az adathalászat veszélyeit és az ilyen támadások ellen való védekezés módjait

2015. június 9. kedd

IT security

11[25] APT – védelem az összetett támadások ellen

- Hogyan, milyen megoldások nyújtanak segítséget a Zero day fenyegetettségekkel szemben?
- Miben különbözik ez a védelem más megoldásoktól? Biztonságos-e a rendszerem?
- Milyen típusú viselkedésmintákra épít ez a rendszer?
- Nevezhetők-e kockázatarányosnak az APT elleni védekezésre használt rendszerek?
- Mekkora a beruházási és működtetési költsége?

Előadó: Balogh Viktor, CISM, Certified FireEye Engineer, TMSI Kft.

12[05] 2013. L. törvény követelményeinek értelmezése, és teljesítése NIST SP 800-53 r4 és MSZ ISO/IEC 27001:2013 alapokon

- Milyen irányba változott a törvény?
- Tudatosan foglalkoznak a szervezetek az információbiztonság irányításával, vagy csak a jogszabályi követelményeket akarják „kipipálni”?
- Milyen nehézségek tapasztalhatóak a rendelet követelményeinek teljesítésekor?
- Hogyan lehetséges a nemzetközi bevált gyakorlatokat és szabványokat felhasználnunk?
- Milyen előnyökkel járhat a tanúsított információbiztonság irányítási rendszerbevezetés és a jogszabályi megfelelés egy/párhuzamos projektként kezelése?

Előadó: Horváth Gergely Krisztián CISA CISM, elnökségi tag, ISACA-HU

12[40] Ebédszünet

14[00] Third-party együttműködés kockázatai és kezelésük – céges megközelítésben!

- A biztonsági aspektusai, felelősségek az együttműködés kapcsán
- A kockázatfeltárás, kockázatkezelés alapvető fontossága
- Mi minden legyen az együttműködési megállapodásban? Mire elég valójában a titoktartási megállapodás és az SLA?
- A harmadik fél kiválasztásának biztonsági szempontjai – referenciák, biztonsági megfelelés vizsgálata, információbiztonsági audit
- Biztonsági kontrollok az együttműködés során – jelentési kötelezettség, biztonsági audit, incidenskezelés
- A biztonság technikai vonatkozásai az együttműködés során – bizalmasság, sértetlenség, hitelesség biztosítása
- Milyen szempontok szerint készítsek kockázatelemzést? Mennyire célszerűek a szúrópróbaszerű ellenőrzéseket?
- Az együttműködés lezárása – szellemi tulajdon; adatok átadása/megsemmisítése?

Előadó: Pávlicz György, Chief Information Security Officer, Raiffeisen Bank Zrt., a Magyar Bankszövetség Információbiztonsági Munkacsoportjának vezetője

14[40] SCADA veszélyek – a Stuxnet esetről dióhéjban

- A SCADA rendszerekről,
- Atomháború bitszinten - a Stuxnet story,
- Tanulságok

Előadó: Pávlicz György, Chief Information Security Officer, Raiffeisen Bank Zrt., a Magyar Bankszövetség Információbiztonsági Munkacsoportjának vezetője

SZPONZORÁCIÓ ÉS KIÁLLÍTÁS: Hemeder Adrienn, Sales Manager
+36 1 459 7325 +36 70 703 5274 +36 1 459 7301
adrienn.hemeder@iir-hungary.hu

Együttműködő partnerünk

BalaBit IT Security

Médiapartnerünk

itB

ESETTANULMÁNY

14[55] A távmunka információbiztonsági aspektusai?

- A távmunka beágyazódása egy nem tisztán informatikai projektbe.
- A távmunkával kapcsolatban felmerülő információbiztonsági kihívások és lehetséges kezelésük.
- A távmunka biztonságának megközelítése informatikai, üzleti és HR szempontból.
- A távmunkát támogató informatikai rendszerek.

Előadó: Bus László, IT manager, belső projektek felügyelete, Ricoh Hungary Kft.

15[35] Kávészünet

16[00] Data Loss Prevention

- Mi az adatszivárgás motivációs háttere?
- Milyen szempontok alapján mérjük fel, hogy mely az szükséges adatkör/adatvagyon, amelyet védenünk kell?
- Mik azok a kontrollehetőségek (olcsóbbtól a drágább eszközök felé) amik csökkenthetik a kockázatokat?
- Hogyan lehet védekezni, milyen DLP technológiai megoldások léteznek erre? Mit jelent az adatszivárgás/adat vesztés esetén a kockázatarányos védelem?
- Hol a határ a valós kontroll és az elrettentésen alapuló kontrollok között?
- Milyen aspektusai fontosak az adatszivárgás megelőző rendszer bevezetésének: jogi háttér, céges policy, HR oldal, szakszervezeti háttér, üzemi tanács, stb.
- Milyen projektfolyamat mentén kell egy ilyet implementálni?
- Hogyan jutunk el addig, hogy konkrét szabályrendszerek kialakulnak?
- Milyen módon kommunikálunk? Mi a normál sztenderd, mit küldhetek emailben, mi a kezelési módja, adok-e technikai megoldást, van-e szabályzat erre?
- Hogy néz ki egy incidenskezelés? Hogyan határozom meg az érintettek körét és hány szintű az eljárás? Mely eseményeket érdemes megvizsgálni egy csalásfelderítés során?
- Kinek milyen jogosultságai vannak, ki mihez fér hozzá? Miért fontos ezt meghatározni?
- Esettanulmány: Milyen incidensekre derült fény a bevezetés után?

Előadó: Niklai Norbert, Information Security Officer, E.ON Hungária Zrt.

16[40] Adathalászat – a naivitás és tudatlanság vámszedői

Az előadásban bemutatásra kerül az adathalászat, mint támadási módszer fejlődése az utóbbi tíz év távlatában napjainkig. Számos hazai példán keresztül megismerhetjük az adathalászat veszélyeit és az ilyen támadások ellen való védekezés módjait. Az előadás foglalkozik a saját és céges adatok védelmére koncentráló egyik legolcsóbb és leghatékonyabb védelmi intézkedéssel, a biztonságtudatossági oktatás és tudatosítás módszereivel.

Az előadás főbb témái

- Adathalászat fejlődése 2005-től napjainkig
- Hazai adathalászat példák és tanulságok
- Legfőbb védekezés a tudatosítás
- A biztonságtudatosság előnyei az egyén és cégünk szempontjából
- Hogyan építsünk fel és tegyünk hatékonnyá egy tudatossági kampányt?
- Miért kell a biztonságtudatossággal foglalkozni gyermekkortól?

Előadó: Solymos Ákos, CISM, CRISC, információbiztonsági szakértő

17[20] A konferencia vége

Az IIR Magyarország felnőttképzési intézmény.
Intézményakkreditációs lajstromszám: AL-2748

1. RÉSZTVEVŐ

Vezetéknév _____ Keresztnév _____
Beosztás _____
Osztály _____
Végzettség _____
Telefon _____
Fax[1] _____
Mobiltelefon[1] _____
E-mail[1] _____
Aláírás[2] _____

A RÉSZVÉTELT ENGEDÉLYEZŐ/ELRENDELŐ SZEMÉLY

Vezetéknév _____ Keresztnév _____
Beosztás _____
Osztály _____

ADMINISZTRATÍV KAPCSOLATTARTÓ

Vezetéknév _____ Keresztnév _____
Beosztás _____
Osztály _____

HELYETTESÍTŐ SZEMÉLY[3]

Vezetéknév _____ Keresztnév _____
Beosztás _____
Osztály _____
Aláírás[2] _____

2. RÉSZTVEVŐ

Vezetéknév _____ Keresztnév _____
Beosztás _____
Osztály _____
Végzettség _____
Telefon _____
Fax[1] _____
Mobiltelefon[1] _____
E-mail[1] _____
Aláírás[2] _____

10%

3. RÉSZTVEVŐ

Vezetéknév _____ Keresztnév _____
Beosztás _____
Osztály _____
Végzettség _____
Telefon _____
Fax[1] _____
Mobiltelefon[1] _____
E-mail[1] _____
Aláírás[2] _____

20%

SZÁMLÁZÁSI CÍM

Cégnév _____
Irányítószám _____ Helység _____
Utca/Postafiók _____

1 E-mail címének, fax- és mobilszámának megadásával hozzájárul ahhoz, hogy az IIR további rendezvényeiről e csatornákon is kapjon tájékoztatást. 2 A képzésre/rendezvényre regisztráló személy alírásával igazolja, hogy a képzésen/rendezvényen személyesen vesz részt. 3 Az Ön helyettese, amennyiben Ön nem tud részt venni a rendezvényen.

RÉSZVÉTELI DÍJ	NAPOK	ÁR
IT security 2015 2015. június 9.	IT security megoldásokat **felhasználó**, gyakorló vállalatok munkatársai számára	**79.000,-**
	IT security megoldásokat **szolgáltató**, tanácsadó vállalatok munkatársai számára	**149.000,-**

Áraink nem tartalmazzák az áfát. | A feltüntetett megtakarítások a több napos rendezvények határidös kedvezményét, valamint a regisztrált napok számától függö kedvezmény nettó összegét tartalmazzák. | A részvételi díj tartalmazza az étkezés költségét, mely a számlán külön tételként feltüntetésre kerül. | A rendezvényen kép- és hangfelvétel készülhet.

CSOPORTOS KEDVEZMÉNY

Két fő jelentkezése esetén a 2. személy **10%** kedvezményt kap. Amennyiben három fö regisztrál, a 2. személy 10%, a 3. személy pedig **20%** kedvezményt kap. **4 főtől kérje egyedi ajánlatunkat!** +36 1 459 7334

JELENTKEZÉSI LAP

IT security 2015
június 9., Budapest
CT5004

VAN MÉG KÉRDÉSE?

Ügyfélszolgálat: Takács Tünde ☎+36 1 459 7300 | Koncepció: Papp Martina ☎+36 1 459 7326 +36 70 419 8623 | Marketing: Mile Mónika ☎+36 1 459 7334 | Szponzoráció: Hemeder Adrienn ☎+36 1 459 7325 +36 70 703 5274

FIZETÉS, VISSZALÉPÉS

Jelentkezésével elfogadja a jelentkezési és visszalépési feltételeket. Jelentkezésének beérkezése után visszaigazolást és a költségviselő számlázási címére kiállított előlegbekérőt küldünk. Kérjük az ott feltüntetett összeget szíveskedjen a rendezvény előtt átutalni. A rendezvényre való bejutás csak akkor garantált, ha befizetése cégünkhöz 3 munkanappal a rendezvény előtt beérkezik. Ha az utalás a rendezvény kezdete előtt 2 munkanapon belül történik meg, kérjük, hogy azt a bankkivonat másolatával igazolni szíveskedjen a rendezvény helyszínén a regisztráláskor. Fizetési késedelem esetén a költségviselő késedelmi pótlék fizetésére kötelezett. Esetleges program-és helyszínváltoztatás jogát fenntartjuk. Visszalépés csak írásban lehetséges. A részvétel visszamondása esetén 20.000 Ft+ÁFA/fő, a rendezvényt megelőző 2 héten belüli lemondás esetén 40.000 Ft+ÁFA/fő adminisztrációs költséget számolunk fel. A rendezvényt megelőző 2 munkanapon belüli lemondás esetén a költségviselő a teljes részvételi díjat köteles megtéríteni. A bejelentett résztvevő részvételének módosítása meghatározott feltételek mellett lehetséges. Amennyiben további információra lenne szüksége ügyfélszolgálatunk (+36 1 459 7300) készséggel áll rendelkezésére illetve a www.iir-hungary.hu honlapunkon tovább tájékozódhat.

IIR