ELTE Informatikai Kar

IT Biztonság Speciálkollégium I.

Tematika 2017 ősz

A tantárgy célja: A tárgy keretében a hallgatók megismerkednek a vállalati IT biztonsági rendszerek feladataival, elemeivel, felépítésével. A téma tárgyalása során kiemelten kezeljük a *módszertani, irányítási szempontokat*. Bemutatjuk a biztonsági rendszerelemek működési elvét, valamint az egyes védelmi intézkedések bevezetésének és üzemeltetésének lépéseit.

Helyszín: Lóczy L. terem, 0-804

Szeptember 13. 16:15 – 17:45	**Bevezetés: Sérülékenység elemzés és kezelés** Mit jelent a sérülékenység és miért veszélyes (vulnerability, exploits, patches, stb.). Sérülékenység kezelés folyamata (információgyűjtés, kockázat értékelés, patch management, review). Sérülékenységi információforrások. Sérülékenység elemzési módszerek (Ethical hacking, Penetration test, Vulnerability test, Code analysis). Esettanulmány. *Spala Ferenc, Euronet*
Szeptember 27. 16:15-17:45	**Bevezetés: IT biztonság általában** Az IT biztonság értelmezése. Az IT biztonság, mint üzleti követelmény, CIA elv. Fenyegetések, védelmi intézkedések. Az IT biztonsági menedzsment feladata és módszerei: kockázatelemzés, tervezés, megvalósítás, üzemeltetés. *Kovács Attila, ELTE*
Október 4. 17:00 – 18:00	**Fizikai biztonság** Támadási célpontok, veszélyforrások. Életvédelem, vagyonvédelem, információvédelmi környezetek. Bűnmegelőzés. Biztonsági technológiák és eszközök. Héjszerkezetes védelem. Területhatár és területvédelem. Megfigyelő eszközök, beléptetés. Tűzvédelem. *Kiss Szilárd, H1 Systems*
Október 11. 16:15 – 17:45	**Határvédelmi technológiák** Határvédelmi technológiák, működési elveik: Csomagszűrők és típusaik. Bastion host, Socks, Proxyk, transzparens proxy-k és moduláris proxy-k. Kapcsolódó technológiák: VPN, hitelesítés, tartalomszűrés. *Kovács Bálint, Balabit*
Október 18. 16:15 – 17:45	**Behatolásvédelem** Hálózatbiztonsági események és érzékelésük. Intrusion Detection és Intrusion Prevention rendszerek (IDS, IPS, nIDS, stb.). Egyéb érzékelési lehetőségek (honeypot/honeynet, Darknet, stb.). Esettanulmány. *Horváth Tamás, Brightdea*
Október 25. 16:15 – 17:45	**Naplófeldolgozás és elemzés, incidens menedzsment** A naplózás célja. Naplózási protokollok. Szabványos naplóformátum. A naplózási formátum hiányosságai. Naplóelemzés (on-the-fly/periodikus, korrelációelemzés). Hálózatbiztonsági incidensek meghatározása, típusai, kockázatai. Az incidenskezelés folyamata (információgyűjtéstől, a blokkoláson át, a rendszerek helyreállításáig). Esettanulmány. *Berkes Gábor, Kancellár*

November 8. 17:00 – 18:00	**Biztonsági kockázatok elemzése** A kockázatelemzés célja. A kvantitatív és kvalitatív kockázatelemzés alapjai. A folyamat alapú és a rendszer alapú megközelítések. Üzleti folyamatok azonosítása, feltérképezése. Információrendszer vagyonelemek azonosítása. Fenyegetéskatalógus. Kockázatérték számítási módszerek. *Botos Zsolt, Security.hu*
November 22. 16:15 – 17:45	**Hozzáférés-ellenőrzés és digitális aláírás I.** Elektronikus aláírás és aláírás ellenőrzés. Nyilvános kulcsú infrastruktúra alapjai, fő komponensek (CA, RA, címtár). PKI hierarchia kialakítása, regisztrációs módszerek, eljárások. Tanúsítvány tartalma, főbb mezők, egy konkrét tanúsítvány elemzése. Visszavonás ellenőrzés: OCSP, CRL. Időbélyeg. Kulcstároló eszközök, kulcsok menedzselése (HSM illetve CMS rendszerek, gyakorlati példaként a Margaréta kártyamenedzsment bemutatása) PKI-hoz kapcsolódó szabályzatok (CPS, CP, EASZ). Néhány gyakorlati példa, alkalmazás (levelezéstitkosítás, e-cégeljárás, e-számla). *Kovács Tamás, Noreg*
November 29. 17:00 – 18:00	**Szabályozások, módszertanok** Technikai szabályozás (Common Criteria, BS7799). Folyamat szabályozás (BS7799-1, COBIT4). Menedzsment (BS7799-2, COBIT4). ITIL, SOX és BASELII. *Dr. Krasznay Csaba, Balabit, NKE*
December 6. 16:15 – 17:45	**Hozzáférés-ellenőrzés és digitális aláírás II** SSL/TLS handshake step-by-step bemutatása alacsony szinten, Wireshark-kal, RFC alapján. Apache web server beállítása SSL használatára (csak szerver- és kétoldali (kliens+szerver) tanúsítvány alapú hitelesítés). Alapműveletek (digitális aláírás, rejtjelezés, SSL handshake) OpenSSL segítségével. Kriptográfia és ethical hacking: a 2004-es MD5 collision-től kezdődően napjainkig. *Szabó Áron, e-group*
December 13. 16:15 – 17:45	**Vírusvédelem** A számítógép vírusok készítésének, terjesztésének okai, terjedési módjaik. Mi ellen védekezzünk? Vírusok, trójaiak, férgek és társaik. Hogyan védekezzünk? A védelmi rendszerek felépítése, védelmi pontok, a vírusvédelmi rendszerek felépítése. *Szappanos Gábor, Sophos*

IT Biztonság Speciálkollégium II.

Tematika

2018 tavasz

A tantárgy célja: A tárgy keretében a hallgatók megismerkednek a vállalati IT biztonsági rendszerek üzemeltetésének elemeivel, a védekezési lehetőségekkel. A téma tárgyalása során kiemelten kezeljük a *technológiai szempontokat*. Bemutatjuk a kritikus rendszerelemek működési elvét, valamint az egyes védelmi intézkedések bevezetésének és üzemeltetésének lépéseit.	
Február	**Adatgyűjtés, adathalászat** Goolge hacking, Social networking, Netcraft, ServerSniff Whois, Ripe.net, DNS (nslookup, dig, host, forward/reverse lookup) Protokollok (OSI és TCP/IP), SNMP, NetBios (Null Session, samrdamp) Port scanning, ARP, Nmap, Stealth scanning
Február	**Web App security** XSS, SQL injection, CSRF, adatbázisok biztonsági kérdései Command injection, session hijacking, cookie mérgezés HTTP parameter mérgezés
Március	**Biztonságos programozás I.** Buffer overflow, heap overflow, format string támadás
Március	**Biztonságos programozás II.** Metasploit, rootkit-ek
Március	**Mobil biztonság**
Március	**Mobil biztonság**
Március	**Cryptography, Kleptography, jelszó elleni támadások** Online / offline, Hydra, Profiling, szivárványtáblák
Április	**Smart Card Security**
Április	**Single Sign-On security**
Május	**RSA problems**
Május	**PRNG problems**

Ajánlott irodalom

- Bruce Schneier: Secrets & Lies. Digital Security in a Networked World. John Wiley & Sons, 2000. ISBN 0-471-25311-1
- Harold F. Tipton (szerk.): Official (ISC)2 Guide to the CISSP CBK, Second Edition. Auerbach Publications, 2009. ISBN 1439809593
- Thomas Wilhelm: Professional Penetration Testing: Creating and Operating a Formal Hacking Lab. Syngress, 2009. ISBN 1597494259
- Stuart McClure, Joel Scambray, George Kurtz: Hacking Exposed: Network Security Secrets and Solutions, Sixth Edition. McGraw-Hill Osborne Media, 2009. ISBN 0071613749
- Michael E. Whitman, Herbert J. Mattord: Management of Information Security. Course Technology, 2010. ISBN 1435488849
- L. McCarthy: IT Security. Risking the Corporation Prentice Hall PTR, NJ, USA, 2002.
- http://www.isc2.org
- http://www.sans.org