

Tárgytematika / Course Description

Információ-biztonság

GKLM_TATM046

Tárgyfelelős neve /

Teacher's name: Répás Sándor Rudolf

Félév / Semester: 2019/20/2

Beszámolási forma /

Assesment: Vizsga

Tárgy heti óraszám /

Teaching hours(week): 0/0/0

Tárgy féléves óraszám /

Teaching hours(sem.): 15/0/0

OKTATÁS CÉLJA / AIM OF THE COURSE

A tárgy célja, hogy a mérnökök megismerjék a TCP/IP alapú számítógéphálózatok nélkülözhetetlen biztonsági kérdéseit és problémáit. Alapismereteket adjon a különböző komplex információs hálózatok biztonságos kialakításához és védelméhez. Képessé tegye a mérnököket megérteni az információbiztonság összetett feladatrendszerét, valamint kockázattal arányos, proaktív védelem kialakítására.

TANTÁRGY TARTALMA / DESCRIPTION

Tantárgy tematikája, rövid tartalma

1.hét	Bevezetés: a tárgy témaköre, alapfogalmak, biztonság, védelem, támadások fajtái.
2.hét	Támadások fajtái, CVE és OWASP. Titkosítás, szimmetrikus kulcsú, blokk titkosítás.
3.hét	Lenyomat képzés. Nyilvános kulcsú titkosítás, digitális aláírás, titkosított levelezés.
4.hét	X.509 tanúsítványok, PKI felépítése és működése. PGP.
5.hét	Összetett támadások. APT. Komplex védelmi eszközök, IDM, DLP, MDM.
6.hét	Erős hitelesítés. Mobil eszközök biztonsága és VOIP alkalmazás.
7.hét	Dolgok internetének biztonsága és jellemző problémák. Felhő biztonság.
8.hét	Adat, információ, tudás, bölcsesség. Adat védendő tulajdonságai és értéke. B,S,R.
9.hét	Adatvagyon felmérés és Információbiztonsági kockázatelemzés.
10.hét	Szabályzatrendszer kialakítása. IBP, IBS, IBSz. ÜFT készítése.

11.hét	Biztonsági szabványok, ajánlások. Cobit, ISO27001, NIST, ITIL, CC, KIB.
12.hét	Jogszabályi környezet. Infotv, ibtv, GDPR.
13.hét	Kritikus infrastruktúrák védelme. Ágazatok, szabályozás, technológia, kialakítás.
14.hét	Incidens kezelés.

SZÁMONKÉRÉSI ÉS ÉRTÉKELÉSI RENDSZERE / ASSESSMENT'S METHOD

2 kisZH, ellenőrző mérés, vizsga

KÖTELEZŐ IRODALOM / OBLIGATORY MATERIAL

Kötelező irodalom	<p>Dr. Lencse Gábor: Hálózatok biztonsága Répás Sándor: Kritikus információs infrastruktúrák védelme nyílt forráskódú kiberbiztonsági szoftverek segítségével Valamint a tárgy honlapján elérhető anyagok. Répás Sándor: Aktív hálózati eszközök támadása és védekezési lehetőségek</p>
Ajánlott irodalom	<p>Virrasztó Tamás: Titkosítás és adatrejtés Berta István Zsolt: Nagy e-szignó könyv Szádeczky Tamás: Információbiztonsági szabványok Kovács László - Krasznay Csaba: Digitális Mohács, Egy kibertámadási forgatókönyv Magyarország ellen OWASP Top Ten</p>