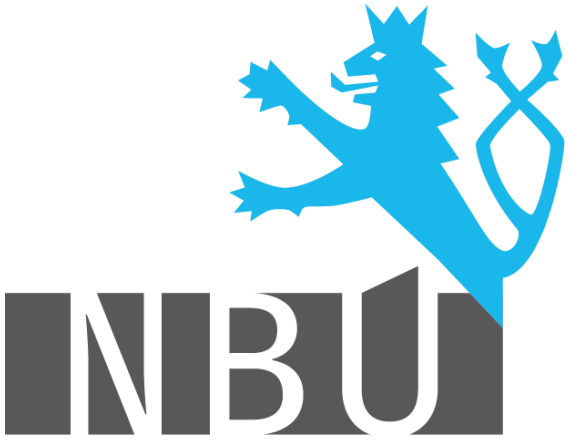
NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
Národní centrum kybernetické bezpečnosti



KYBERNETICKÉ (NE)BEZPEČÍ

Sylabus pro předmět
Kybernetické (ne)bezpečí
Univerzita Palackého v Olomouci

SYLABUS

Předmět Kybernetické (ne)bezpečí je jednosemestrální celouniverzitní kurz s alokací 4 hodin za měsíc. Kurz studentům poskytne úvodní seznámení s problematikou kybernetické bezpečnosti. Jednotlivé semináře se postupně věnují teoretickým, historickým, konceptuálním, legislativním a částečně také technickým aspektům kybernetické bezpečnosti. V rámci výuky budou studenti seznámeni se základní teorií kybernetické bezpečnosti, používanou odbornou terminologií, současným zajišťováním kybernetické bezpečnosti v České republice a ve světě či s historií kybernetických útoků, jejich taxonomií a typologií. Specifikem kurzu je rovněž poskytnutí praktických informací z oblasti zajišťování kybernetické bezpečnosti v České republice. To je dáno charakterem přednášejících, které představují zejména pracovníci Národního centra kybernetické bezpečnosti. Kurz se dále věnuje fenoménům jako je kybernetická válka, kybernetická špionáž či roli nestátních aktérů v kyberprostoru a významu médií a internetu v dnešním světě. Náplní kurzu budou rovněž diskuze o nebezpečích, která nejčastěji číhají na uživatele na internetu i to, jak těmto nástrahám předcházet či jak se jim bránit.

Literatura

- Bude doplněno
- Základ: koncepční dokumenty, zákon o KB, Tallinnský manuál 2.0, Cybersecurity and cyberware (Singer&Friedman), stránky www.GovCERT.cz, Výkladový slovník AFCEA a další

Hodnocení

- Závěrečný test

Program kurzu

1. týden (30.9.)

- Seznámení s obsahem a požadavky na zakončení předmětu
- Role NBÚ/NCKB při zajišťování kybernetické bezpečnosti v ČR
- Základní koncepční dokumenty
- Úvod do problematiky KB, konceptuální vymezení kybernetické bezpečnosti a obrany
- Seznámení se základní terminologií KB

2. týden (14.10.)

- Geneze kybernetických hrozeb
- Taxonomie kybernetických útoků, základní typologie a motivace útočníků
- Vybrané případové studie

3. týden (28.10.)

- Ochrana kritické informační infrastruktury
- Kybernetické útoky s dopadem na fyzickou infrastrukturu, ICS/SCADA útoky
- Případové studie
- Role CERT/CSIRT týmů
- ZKB ČR

4. týden (11.11.)

- Přiblížení fenoménu kyberkriminality – kyberstalking, kyberšikana, kybergrooming
- Statistiky a kazuistiky útoků
- Bezpečnostní desatero
- Prevence a osvěta v oblasti informační kriminality

5. týden (25.11.)

- Současné trendy a aktéři v kontextu KB
- Fenomén kybernetická válka, kyberšpionáž, hacktivismus, kyberterorismus, informační válka, role nestátních aktérů, hybridní válka
- Význam mezinárodní spolupráce

6. týden (9.12.)

- shrnutí učiva
- závěrečný test