Popis předmětu

Pracoviště / Zkratka	KIT / NNBOD			**Akademický rok**	2023/2024
Název	Bezpečnost a ochrana osobních dat v ICT			**Způsob zakončení**	Zkouška
Název dlouhý	Bezpečnost a ochrana osobních dat v mobilních ICT				
Akreditováno/Kredity	Ano, 5 Kred.			**Forma zakončení**	Kombinovaná
Rozsah hodin	Přednáška 2 [HOD/TYD] Cvičení 2 [HOD/TYD]				
Obs/max	Statut A	Statut B	Statut C	**Zápočet před zkouškou**	ANO
Letní semestr	0 / -	1 / -	0 / 0	**Počítán do průměru**	ANO
Zimní semestr	0 / -	0 / -	0 / -	**Min. (B+C) studentů**	nestanoveno
Rozvrh	Ano			**Opakovaný zápis**	NE
Vyučovací jazyk	Čeština			**Vyučovaný semestr**	Letní semestr
Volně zapisovatelný předmět	Ano			**Počet dnů praxe**	0
Hodnotící stupnice	A|B|C|D|E|F			**Hodn. stup. zp. před zk.**	S|N
Počet hodin kontaktní	0				
Automat. uzn. záp. před zk.	Ne				
Periodicita	K				
Nahrazovaný předmět	KIT/INBOD				
Vyloučené předměty	Nejsou definovány				
Podmiňující předměty	Nejsou definovány				
Předměty informativně doporučené	Nejsou definovány				
Předměty,které předmět podmiňuje	Nejsou definovány				

Cíle předmětu (anotace):

Cílem předmětu je seznámit studenty s pravidly a postupy v oblasti kybernetické bezpečnosti a ochrany osobních dat, zaměřené na mobilní ICT. Znalosti z předmětu studentům umožní uplatňovat bezpečnostní zásady při navrhování a implementaci aplikací ve shodě s nařízeními EU jako jsou GDPR či ePrivacy, vyžadovanými v praxi.

Požadavky na studenta

V praktické práci student navrhne a vyvine webovou aplikaci (PHP, JavaScript, HTML, SQL) ve které uplatní vyučované techniky zabezpečení aplikace proti nejčastějším zranitelnostem.

Obsah

1. Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation, zkr. GDPR) a jeho důsledky pro informační společnost.
2. Nová práva subjektů, které GDPR deklaruje a z toho vyplývající povinnosti správce osobních dat. Povinnosti správce dat při narušení bezpečnosti osobních dat, potenciální sankce pro instituci.
3. Nařízení ePrivacy doplňující GDPR a ochranu metadat odvozených od mobilní elektronické komunikace (geolokační údaje, atd.)
4. Identifikace osobních údajů a zvláštních osobních údajů, kvazi-identifikátory.
5. Osobní údaje uživatelů získávané aplikacemi díky současným senzorům v mobilních zařízeních (geolokační, biometrické, atd.).
6. Digitální časoprostorové otisky mobilního uživatele a jejich minimalizace.
7. Současné metody využívané k lokaci uživatele, jejich přesnost, výhody a nevýhody.
8. Identifikace podvodných technik a software (sociální inženýrství, phishing, malware).
9. Hrozby úniku osobních údajů a eroze soukromí uživatelů mobilních ICT.
10. Korektní manipulace s hesly a dalšími citlivými informacemi ve webových aplikacích a databázích.
11. Zabezpečení a ochrana spravovaných dat pomocí šifrování, anonymizace a pseudonimizace osobních údajů uživatelů.
12. Funkce pověřence pro ochranu osobních údajů (Data Protection Officer, zkr. DPO).
13. Zabezpečení webových aplikací (v PHP, SQL a JavaScriptu) proti nejčastějším zranitelnostem Cross-Site Scripting

(XSS), CSRF (Cross-Site Request Forgery), SQL Injection, Session hijacking, atd.

Předpoklady - další informace k podmíněnosti studia předmětu

Prerekvizitou tohoto předmětu je základní orientace v problematice mobilních ICT.

Získané způsobilosti

Absolvováním předmětu jsou získány informace o kybernetické bezpečnosti, což podporuje návrh a vývoj webových aplikací odolným proti zranitelnostem.

Studijní opory

V případě mimořádných opatření bude výuka probíhat vzdáleně s využitím programu MS Teams v době dle rozvrhu. Účast na schůzkách skupiny v MS Teams je ekvivalentní účasti na přednáškách a cvičeních.

Garanti a vyučující

- **Garanti:** Ing. Jiří Kysela, Ph.D.
- **Přednášející:** Ing. Jiří Kysela, Ph.D. (100%)
- **Cvičící:** Ing. Jiří Kysela, Ph.D. (100%)

Literatura

- **Základní:** Analysis of Privacy Erosion of Geosocial Networks (KYSELA, Jiří) - http://ieeexplore.ieee.org/document/7382922/ >
- **Základní:** KOLOUCH, Jan. *CyberCrime*. Praha, 2016. ISBN 978-80-88168-15-7.
- **Základní:** HARWOOD, Mike. *Internet Security: how to defend against attackers on the web*. Burlington, MA: Jones & Barlett Learning, 2016. ISBN 978-1-284-09055-0.
- **Doporučená:** Top 10 - 2017 : The Ten Most Critical Web Application Security Risks (OWASP) - https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf >

Časová náročnost

Prezenční forma studia

Aktivity	Časová náročnost aktivity [h]
Kontaktní výuka	52
Celkem:	**52**

Vyučovací metody

Hodnotící metody

Ústní zkouška
Písemná zkouška
Posouzení zadané práce

Předmět je zařazen do studijních programů:

Studijní program	Typ stud.	Forma stud.	Obor	Etapa V.st.pl.	Rok	Blok	Statut	D.roč.	D.sem.
Informační technologie	Navazující	Prezenční	Informační technologie	1 2022	2023	Povinně volitelné 1. ročník - typ A	B	1	LS

Studijní program	Typ stud.	Forma stud.	Obor	Etapa V.st.pl.	Rok	Blok	Statut	D.roč.	D.sem.
Informační technologie	Navazující	Prezenční	Informační technologie	1 2023	2023	Povinně volitelné 1. ročník - typ A	B	1	LS
Informační technologie	Navazující	Prezenční	Informační technologie	1 2021	2023	Povinně volitelné 1. ročník - typ A	B	1	LS