Information systems security - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Information systems security
Kod przedmiotu	11.3-WE-BizElP-BezpElektron-Er
Wydział	Wydział Informatyki, Elektrotechniki i Automatyki
Kierunek	Biznes elektroniczny
Profil	praktyczny
Rodzaj studiów	Program Erasmus pierwszego stopnia
Semestr rozpoczęcia	semestr zimowy 2022/2023

Informacje o przedmiocie

Semestr	5
Liczba punktów ECTS do zdobycia	4
Typ przedmiotu	obowiązkowy
Język nauczania	angielski
Sylabus opracował	• dr inż. Grzegorz Bazydło • dr hab. inż. Bartłomiej Sulikowski, prof. UZ

Formy zajęć

Forma zajęć	Liczba godzin w semestrze (stacjonarne)	Liczba godzin w tygodniu (stacjonarne)	Liczba godzin w semestrze (niestacjonarne)	Liczba godzin w tygodniu (niestacjonarne)	Forma zaliczenia
Wykład	30	2	-	-	Zaliczenie na ocenę
Laboratorium	15	1	-	-	Zaliczenie na ocenę

Cel przedmiotu

To familiarize students with issues related to the security of digital data and the use of the Internet to conduct secure transactions. Presentation of security mechanisms and threats on the Internet. Teaching and practice using so-called good security practices. Developing skills in recognizing Internet threats. Presentation of examples of so-called good security practices.

Wymagania wstępne

Knowledge of technical aspects of the Internet.

Zakres tematyczny

- Personal computer security. Malware types, its distribution mechanisms, and ways to protect against it. Security of MS Windows. System updates. Anti-virus software. Software firewalls. Backups.
- Basics of cryptographic data protection. Symmetrical and asymmetrical algorithms. Hash functions. Applications of cryptographic algorithms in business practice. Cryptanalysis.
- Controlling access to protected data. Authentication and authorization methods. Protection mechanisms for sensitive data storage. Estimating password strength and power of mechanisms securing access to data. Intrusion into systems - recognition and prevention. Potential consequences of theft of digital data.
- Theft of personal data. *Phishing* and protection against it.
- Threats to ICT systems. DoS and DDoS attacks. Data transmission protection. VPN networks. “Man in the Middle” and *spoofing* attacks - recognition and defense. Other types of attacks (e.g., SQL injection, XSS scripting). Ensuring electronic security with hardware solutions (role of hardware firewalls, IDS/IPS mechanisms, VPN hubs, routers with integrated services).
- Security of mobile devices. Best practices for the safe use of smartphones, tablets, and notebooks. The security of transactions using pay cards like MasterCard, Visa (incl. wireless cards e.g., PayPass, Visa PayWave). Security mechanisms of popular systems for mobile devices (Android, iOS).
- Digital signature. Signature submission and verification. Law basics regarding electronic signature. Additional services (time stamping, multiple signatures, etc.). Qualified signature. Handling certificates.
- Secure transactions. SSL protocol. Authorization based on certificates. Threats related to the use of certificates.
- Law basics regarding the security of data (incl. personal data). The application of law in the context of the security of e-commerce systems. Comparison of Polish regulations with the EU legislation.
- Mechanisms for securing internet transactions on selected examples: electronic banking - access to bank accounts, performing banking operations; electronic stores; Polish government systems: tax offices, e-court, electronic offices, etc.
- Review of commercial solutions ensuring electronic security of devices and cloud data processing.

Metody kształcenia

Lecture - conventional lecture (with the use of video projector).

Laboratory - practical laboratory exercises.

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Understands the need to constantly update his knowledge regarding the ICT systems security.		• dyskusja	• Wykład • Laboratorium
Knows the selected regulations in the field of data security and ICT systems.		• kolokwium	• Wykład
Is able to estimate the level of security and to propose and implement adequate solutions guaranteeing the security of business transaction components		• aktywność w trakcie zajęć • dyskusja • kolokwium	• Laboratorium
Understands the need of using cryptographic algorithms and protocols to protect data.		• kolokwium	• Wykład
Is aware of the social role of a university graduate, and in particular understands the need to share his engineering and business knowledge with the public.		• dyskusja	• Wykład • Laboratorium
Knows the mechanisms for secure storage and transmission of digital data; understands the risks arising from the lack of security or using of weak security methods		• kolokwium	• Wykład
Can safely conduct electronic transactions.		• aktywność w trakcie zajęć • kolokwium • obserwacje i ocena umiejętności praktycznych studenta	• Wykład • Laboratorium
Is aware of the risks associated with the widespread use of network communication.		• dyskusja	• Wykład • Laboratorium

Warunki zaliczenia

Lecture – the passing condition is to obtain a positive mark from the final test (written or oral).

Laboratory – the passing condition is to obtain positive marks from all laboratory exercises being planned during the semester.

Calculation of the final grade: lecture 50% + laboratory 50%

Literatura podstawowa

1. Stallings, W., Brown, L., Computer Security: Principles and Practice (4th Edition), Pearson, 2017.
2. Forshaw, J., Attacking Network Protocols: A Hacker's Guide to Capture, Analysis, and Exploitation (1st Edition), No Starch Press, 2017.
3. Aumasson, J. P., Serious Cryptography: A Practical Introduction to Modern Encryption, Random House LCC US, 2017.
4. Lehtinen, R., i in., Computer Security Basics, Helion (O'Reilly), 2006.

Literatura uzupełniająca

1. Schneier, B., Click Here to Kill Everybody: Security and Survival in a Hyper-connected World, W. W. Norton & Company, 2018.
2. Mercer, D., Building Online Stores With Oscommerce: Professional Edition, Helion 2007.
3. Garfinkel, S., Spafford, G., Web Security, Privacy & Commerce. 2nd Edition, Helion, 2001.

Uwagi

Zmodyfikowane przez dr inż. Grzegorz Bazydło (ostatnia modyfikacja: 19-04-2022 18:50)