Information systems security - course description

General information

Course name	Information systems security
Course ID	11.3-WE-BEP-BE
Faculty	Faculty of Computer Science, Electrical Engineering and Automatics
Field of study	E-business
Education profile	practical
Level of studies	First-cycle studies leading to Engineer's degree
Beginning semester	winter term 2021/2022

Course information

Semester	5
ECTS credits to win	4
Course type	obligatory
Teaching language	polish
Author of syllabus	• dr inż. Grzegorz Bazydło • dr hab. inż. Bartłomiej Sulikowski, prof. UZ

Classes forms

The class form	Hours per semester (full-time)	Hours per week (full-time)	Hours per semester (part-time)	Hours per week (part-time)	Form of assignment
Lecture	30	2	18	1,2	Credit with grade
Laboratory	15	1	9	0,6	Credit with grade

Aim of the course

Zapoznanie słuchaczy z zagadnieniami związanymi z bezpieczeństwem danych cyfrowych oraz wykorzystania Internetu w celu przeprowadzenia bezpiecznych transakcji. Prezentacja mechanizmów zabezpieczeń oraz zagrożeń w sieci Internet. Nauczenie i wykształcenie wymogu korzystania z tzw. dobrych praktyk bezpieczeństwa. Wykształcenie umiejętności rozpoznawania zagrożeń występujących Internecie. Prezentacja przykładów mechanizmów zabezpieczających transakcje zawierane za pośrednictwem sieci Internet.

Prerequisites

Znajomość technicznych aspektów funkcjonowania Internetu.

Scope

- Bezpieczeństwo komputerów osobistych. Typy złośliwego oprogramowania (malware), mechanizmy jego dystrybucji. Sposoby ochrony przed malware. Bezpieczeństwo systemów z rodziny MS Windows i Linux. Uaktualnienia systemowe. Oprogramowanie antywirusowe. Firewalle programowe. Kopie bezpieczeństwa.
- Podstawy kryptograficznej ochrony danych. Algorytmy symetryczne i asymetryczne. Funkcje skrótu. Zastosowania algorytmów kryptograficznych w praktyce biznesowej. Kryptoanaliza.
- Kontrolowanie dostępu do danych chronionych. Metody uwierzytelniania i autoryzacji użytkowników oraz stron transakcji. Mechanizmy ochrony przechowywania danych wrażliwych. Szacowanie siły haseł i mocy mechanizmów zabezpieczających dostęp do danych. Włamania do systemów – rozpoznawanie i zapobieganie. Potencjalne konsekwencje kradzieży danych cyfrowych.
- Kradzieże danych osobistych. *Phishing* i ochrona przed nim.
- Zagrożenia systemów teleinformatycznych. Ataki DoS i DDoS. Ochrona przesyłu danych. Sieci VPN. Ataki typu *„Man in the Middle”* i *„spoofing”* – rozpoznawanie i reagowanie. Inne typy ataków (SQL injection, XSS scripting). Zapewnianie bezpieczeństwa elektronicznego środkami sprzętowymi (role firewalli sprzętowych, mechanizmy IDS/IPS, koncentratory VPN, routery z zintegrowanymi usługami).
- Bezpieczeństwo urządzeń mobilnych. Zasady bezpiecznego korzystania ze smartphone'ów, tabletów, notebooków. Bezpieczeństwo transakcji z wykorzystaniem kart bankowych. Bezpieczeństwo kart zbliżeniowych (MasterCard PayPass i Visa PayWave). Mechanizmy zabezpieczeń popularnych systemów operacyjnych urządzeń mobilnych (Android, IOS).
- Podpis cyfrowy. Mechanizm składania i weryfikacji podpisu. Ustawa o podpisie elektronicznym. Usługi dodatkowe (znakowanie czasem, podpis wielokrotny itp). Podpis kwalifikowany. Posługiwanie się certyfikatami. Profil zaufany.
- Bezpieczne zawieranie transakcji. Protokół SSL. Autoryzacja kontrahenta na podstawie certyfikatów. Zagrożenia związane z korzystaniem z certyfikatów.
- Stan prawny. Wybrane przepisy ustaw (o ochronie informacji niejawnej; o cyberbezpieczeństwie; o prawie autorskim i prawach pokrewnych; o ochronie danych osobowych; o ochronie konkurencji i konsumentów) i ich zastosowanie w kontekście bezpieczeństwa systemów handlu elektronicznego. Porównanie regulacji polskich z zapisami prawodawstwa UE.
- Mechanizmy zabezpieczania transakcji internetowych na wybranych przykładach: bankowość elektroniczna - dostęp do rachunków bankowych, wykonywanie operacji bankowych; funkcjonowanie sklepów elektronicznych; elektroniczne systemy funkcjonowania państwa: urzędy skarbowe, e-sąd, elektroniczne biura podawcze, obywatel.gov.pl itp.
- Przegląd rozwiązań komercyjnych zapewniających bezpieczeństwo elektroniczne urządzeń i procesów przetwarzania danych „w chmurze”.

Teaching methods

Wykład - wykład konwencjonalny z wykorzystaniem wideoprojektora.

Laboratorium - zajęcia praktyczne w laboratorium komputerowym.

Learning outcomes and methods of theirs verification

Outcome description	Outcome symbols	Methods of verification	The class form
Rozumie konieczność ciągłego uaktualniania wiedzy odnośnie bezpieczeństwa systemu związanego z rozwojem wiedzy i technologii	• K_K01	• a discussion	• Lecture • Laboratory
Potrafi oszacować poziom zabezpieczeń oraz zaproponować i wdrożyć adekwatne rozwiązania gwarantujące bezpieczeństwo elementów składowych transakcji biznesowych	• K_U17	• a discussion • activity during the classes • an evaluation test	• Laboratory
Zna mechanizmy bezpiecznego przechowywania i przesyłu danych cyfrowych; rozumie zagrożenia wynikające z braku lub stosowanie zbyt słabych zabezpieczeń	• K_W04 • K_W05 • K_W08	• an evaluation test	• Lecture
Potrafi w sposób bezpieczny przeprowadzić transakcje elektroniczne	• K_U17	• activity during the classes • an evaluation test • an observation and evaluation of the student's practical skills	• Lecture • Laboratory
Zna wybrane przepisy obowiązujących aktów prawnych związanych z bezpieczeństwem danych i systemów teleinformatycznych	• K_W03 • K_W22	• an evaluation test	• Lecture
Ma świadomość roli społecznej absolwenta uczelni technicznej, a zwłaszcza rozumie potrzebę formułowania i przekazywania społeczeństwu informacji na temat aspektów działalności inżynierskiej i biznesowej w sposób powszechnie zrozumiały	• K_K11	• a discussion	• Lecture • Laboratory
Rozumie konieczność stosowania algorytmów i protokołów kryptograficznych w celu ochrony danych	• K_W16 • K_W20	• an evaluation test	• Lecture
Ma świadomość zagrożeń, jakie niesie ze sobą powszechne używanie środków komunikacji sieciowej	• K_K02	• a discussion	• Lecture • Laboratory
Rozumie konieczność ciągłego uaktualniania wiedzy odnośnie bezpieczeństwa systemów teleinformatycznych, związanego z rozwojem wiedzy i technologii	• K_K01	• a discussion	• Lecture • Laboratory

Assignment conditions

Wykład – warunkiem zaliczenia jest uzyskanie pozytywnych ocen z kolokwiów pisemnych przeprowadzonych co najmniej raz w semestrze.

Laboratorium – warunkiem zaliczenia jest uzyskanie pozytywnych ocen ze wszystkich ćwiczeń laboratoryjnych, przewidzianych do realizacji w ramach programu laboratorium.

Ocena końcowa = wykład: 50% + laboratorium: 50%.

Recommended reading

1. Dutko, M., Biblia e-biznesu 2. Nowy Testament, Gliwice, Helion, 2016.
2. Kępa, L., Tomasik, P., Dobrzyński, S., Bezpieczeństwo systemu e-commerce, czyli jak bez ryzyka prowadzić biznes w internecie, Gliwice, Helion, 2012.
3. Aumasson, J-P., Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania, Gliwice, Helion, 2018.
4. Karbowski, M., Podstawy kryptografii. Wydanie III, Gliwice, Helion, 2014.
5. Pieleszek, M., Bądź bezpieczny w cyfrowym świecie. Poradnik bezpieczeństwa IT dla każdego, Gliwice, Helion, 2018.

Further reading

1. Stallings, W., Brown, L., Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Wydanie IV. Tomy 1-2, Gliwice, Helion, 2019.
2. Forshaw, J., Atak na sieć okiem hakera. Wykrywanie i eksploatacja luk w zabezpieczeniach sieci, Gliwice, Helion, 2019.
3. Chojnowski, A., Informatyka sądowa w praktyce, Gliwice, Helion, 2019.
4. Schneier, B., Kliknij tutaj, aby zabić wszystkich. Bezpieczeństwo i przetrwanie w hiperpołączonym świecie, Gliwice, Helion, 2019.
5. Zalewski, M., Splątana sieć. Przewodnik po bezpieczeństwie nowoczesnych aplikacji WWW, Gliwice, Helion, 2019.
6. Nabywaniec, D., Anonimizacja i maskowanie danych wrażliwych w przedsiębiorstwach, Gliwice, Helion, 2019.

Notes

Modified by dr inż. Grzegorz Bazydło (last modification: 30-04-2021 14:35)