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 2016/2017

Course information

Semester	5
ECTS credits to win	4
Course type	obligatory
Teaching language	polish
Author of syllabus	• 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 autentykacji 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 bezprzewodowych (MasterCard PayPass i Visa PayWave). Mechanizmy zabezpieczeń popularnych systemów operacyjnych urządzeń mobilnych (Android, IOS, Windows).

Podpis cyfrowy. Mechanizm składania i weryfikacji podpisu. Ustawa o podpisie elektronicznym. Usługi dodatkowe (znakowanie czasem, podpis wielokrotny itp). Podpis kwalifikowany. Posługiwanie się certyfikatami.

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 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 systemu funkcjonowania państwa: urzędy skarbowe, e-sąd, elektroniczne biura podawcze itp.

Przegląd rozwiązań komercyjnych zapewniających bezpieczeństwo elektroniczne urządzeń i procesów przetwarzania danych „w chmurze” (np. IBM Rational AppScan, IBM Tivoli, CISCO Secure Borderless Network).

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
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
Zna wybrane przepisy obowiązujących aktów prawnych związanych z bezpieczeństwem danych i systemów teleinformatycznych	• K_W03 • K_W22	• an evaluation test	• Lecture
Rozumie konieczność stosowania algorytmów i protokołów kryptograficznych w celu ochrony danych	• K_W16 • K_W20	• 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
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
Rozumie konieczność ciągłego uaktualniania wiedzy odnośnie bezpieczeństwa systemów teleinformatycznych, związanego z rozwojem wiedzy i technologii	• K_K01	• a discussion	• Lecture • Laboratory
Ma świadomość zagrożeń, jakie niesie ze sobą powszechne używanie środków komunikacji sieciowej	• K_K02	• a discussion	• Lecture • Laboratory
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 ciągłego uaktualniania wiedzy odnośnie bezpieczeństwa systemu związanego z rozwojem wiedzy i technologii	• K_K01	• a discussion	• Lecture • Laboratory

Assignment conditions

Wykład - sprawdzian w formie pisemnej i/lub ustnej, realizowany na koniec semestru.

Laboratorium – ocena końcowa stanowi sumę ważoną ocen uzyskanych za realizację poszczególnych ćwiczeń laboratoryjnych.

Ocena końcowa = 50 % oceny zaliczenia z formy zajęć wykład + 50 % oceny zaliczenia z formy zajęć laboratorium.

Recommended reading

1. Kępa, L., Tomasik, P., Dobrzyński, S., Bezpieczeństwo systemu e-commerce, czyli jak bez ryzyka prowadzić biznes w internecie, Gliwice, Helion, 2013.
2. Liderman, K., Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, 2009.
3. Cichoń, M., Biblia e-biznesu, Gliwice, Helion, 2013

Further reading

1. Lukatsky, A., Wykrywanie włamań i aktywna ochrona danych, Helion, 2004.
2. Stallings, W., Kryptografia i bezpieczeństwo sieci komputerowych, Tomy 1-2, Helion, 2012.
3. Lehtinen, R., i in., Podstawy ochrony komputerów, Helion (O’Reilly), 2007.
4. Russell, R., i in., Hakerzy atakują. Jak przejąć kontrolę nad siecią, Helion, 2004.

Notes

Modified by dr hab. inż. Marcin Mrugalski, prof. UZ (last modification: 29-09-2016 21:08)