

Angriffsszenarien und Vorfallreaktion

Modulcode: DLMIMWCK1

Modultyp s. Curriculum	Zugangsvoraussetzungen keine	Niveau MA	ECTS n/a	Zeitaufwand Studierende 150 h
----------------------------------	--	---------------------	--------------------	---

Semester s. Curriculum	Dauer Minimaldauer: 1 Semester	Regulär angeboten im WiSe/SoSe	Unterrichtssprache Deutsch
----------------------------------	---	--	--------------------------------------

Modulverantwortliche(r)

Prof. Dr. Alexander Lawall (Angriffsszenarien und Vorfallreaktion)

Kurse im Modul

- Angriffsszenarien und Vorfallreaktion (DLMIMWCK01)

Art der Prüfung(en)

Modulprüfung

Studienformat: Fernstudium
Klausur, 90 Minuten

Teilmodulprüfung

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Bedrohungsszenarien
- Angriffsvektoren
- Präventive Maßnahmen
- Reaktive Maßnahmen
- Aktuelle Lage der IT-Sicherheit

Qualifikationsziele des Moduls**Angriffsszenarien und Vorfallreaktion**

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Bedrohungsszenarien und deren Auswirkungen zu bewerten.
- Angriffsvektoren zu benennen und adäquate Gegenmaßnahmen auszuwählen.
- Verfahren der elektronischen Beweisführung auf gewählte Angriffsszenarien anzuwenden.
- präventive Maßnahmen zu erarbeiten.
- reaktive Maßnahmen zu benennen und deren Wirksamkeit zu bewerten.
- Information zur aktuellen Bedrohungssituation zu sammeln und auszuwerten.

Bezüge zu anderen Modulen im Studiengang

Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung

Bezüge zu anderen Studiengängen der IUBH

Alle Bachelor-Programme im Bereich IT & Technik

Angriffsszenarien und Vorfallreaktion

Kurscode: DLMIMWCK01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		n/a	keine

Beschreibung des Kurses

Der Kurs vermittelt Studierenden Kenntnisse zur Identifizierung und Maßnahmenplanung im Umgang mit kriminellen Angriffen im digitalen Umfeld. Er beschreibt, wie Schwachstellen in Hardware und Software sowie in deren Anwendung für kriminelle Aktivitäten ausgenutzt werden können. Dazu werden typische Bedrohungsszenarien vorgestellt und die Wege, auf denen angreifende Systeme in ein Computersystem eindringen können. Der Kurs führt zudem in Methoden der elektronischen Beweisführung ein und zeigt, wie im Angriffsfall rechtlich verwertbare Informationen gewonnen werden können. Im Anschluss werden die Entwicklung präventiver Maßnahmen und die Reaktionsmöglichkeiten im konkreten Bedrohungsfall erörtert. Der Kurs behandelt abschließend, wie aus Berichten der Sicherheitsbehörden (wie etwa BSI, Europol, NCA, FBI) Informationen zur aktuellen Sicherheitslage gewonnen werden können.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Bedrohungsszenarien und deren Auswirkungen zu bewerten.
- Angriffsvektoren zu benennen und adäquate Gegenmaßnahmen auszuwählen.
- Verfahren der elektronischen Beweisführung auf gewählte Angriffsszenarien anzuwenden.
- präventive Maßnahmen zu erarbeiten.
- reaktive Maßnahmen zu benennen und deren Wirksamkeit zu bewerten.
- Information zur aktuellen Bedrohungssituation zu sammeln und auszuwerten.

Kursinhalt

1. Einführung
 - 1.1 Computerkriminalität in Abgrenzung zu anderen Angriffen
 - 1.2 Schwachstellen in Computer und Mobilgeräten
 - 1.3 Eine Übersicht über Schadsoftware
 - 1.4 Social Engineering und der menschliche Faktor
2. Strafrechtliche Basis
 - 2.1 Identitätsmissbrauch
 - 2.2 Diebstahl von geistigem Eigentum
 - 2.3 Fälschung beweiserheblicher Daten
 - 2.4 Computerbetrug

3. Spezifische Delikte
 - 3.1 Datendiebstahl
 - 3.2 Digitale Erpressung
 - 3.3 Computersabotage
 - 3.4 Industriespionage
4. Angriffsvektoren
 - 4.1 Angriffe auf Chip- und Firmware-Ebene
 - 4.2 Angriffe auf Betriebssystemebene
 - 4.3 Angriffe auf Netzwerk- und Serverebene
 - 4.4 Angriffe auf Anwendungsebene
 - 4.5 Angriffe auf Organisationsebene
5. IT-Forensik und elektronische Beweisführung
 - 5.1 Identifizierung, Lokalisierung und der Umgang mit Polymorphismen
 - 5.2 Mechanismen zur Angriffserkennung
 - 5.3 Auffinden elektronischer Beweise
 - 5.4 Wiederherstellung von Daten und Beweiserückgewinnung
 - 5.5 Rechtliche Grenzen und prädiktive Methoden
6. Präventive Maßnahmen
 - 6.1 Maßnahmen auf Hardware-Ebene
 - 6.2 Zugangsberechtigung, Autorisierung und Authentifizierung
 - 6.3 Sensibilisierung & Schulung
 - 6.4 Vorfalldaktionsplanung
7. Reaktive Maßnahmen
 - 7.1 Erstbeurteilung und Schadensausmaß
 - 7.2 Unterbindung anhaltender Schäden
 - 7.3 Sammlung, Austausch und Verteilung von Information
 - 7.4 Zusammenarbeit mit Sicherheitsbehörden und Kooperationspartnern
 - 7.5 Handlungsempfehlungen für Unternehmen
8. Die aktuelle Sicherheitslage
 - 8.1 Aktuelle Berichte der Sicherheitsbehörden
 - 8.2 Bewertung der Empfehlungen der Sicherheitsbehörden
 - 8.3 Aktuelle Themen der Europol Awareness Campaign

Literatur**Pflichtliteratur****Weiterführende Literatur**

- Fleischer, D. (2016): Wirtschaftsspionage. Springer Fachmedien, Wiesbaden.
- Klipper, S. (2015): Cyber Security. Ein Einblick für Wirtschaftswissenschaftler. Springer, Berlin.
- Kraft, P./Weyert, A. (2017): Network Hacking. Professionelle Angriffs- und Verteidigungstechniken gegen Hacker und Datendiebe. Franzis Verlag, München.
- Labudde, D./Spranger, M. (Hrsg.) (2017): Forensik in der digitalen Welt. Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt. Springer, Berlin.
- Lenhard, T. H. (2017): Datensicherheit. Technische und organisatorische Schutzmassnahmen gegen Datenverlust und Computerkriminalität. Springer, Berlin.
- Lewis, J./Baker, S. (2013): The economic impact of cybercrime and cyber espionage. McAfee, Santa Clara, CA.
- Müller, K. R. (2018): IT-Sicherheit mit System. Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement–Sichere Anwendungen–Standards und Practices. Springer, München.
- Yar, M./Steinmetz, K. F. (2019): Cybercrime and society. SAGE Publications, Thousand Oaks, CA.
- Hyperlinks zu aktuellen Berichten und Empfehlungen von Sicherheitsbehörden und Institutionen (z.B. BSI, Europol, FBI) werden im Kurs zur Verfügung gestellt.

Studienformat Fernstudium

Studienform Fernstudium	Kursart Online-Vorlesung
-----------------------------------	------------------------------------

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	BOLK: Ja Evaluation: Nein
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	Präsenzstudium	Tutorium	Selbstüberprüfung	Praxisanteil	Gesamt
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden	
<input type="checkbox"/> Learning Sprints® <input checked="" type="checkbox"/> Skript <input type="checkbox"/> Vodcast <input checked="" type="checkbox"/> Shortcast <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Musterklausur	<input type="checkbox"/> Repetitorium <input type="checkbox"/> Creative Lab <input type="checkbox"/> Prüfungsleitfaden <input type="checkbox"/> Live Tutorium/Course Feed