WEB SECURITY

LEVEL OF COURSE UNIT

Master

LEARNING OUTCOMES OF COURSE UNIT

The following learning outcomes are developed in the course:

- Students have detailed knowledge of security concepts on the client side, server side and on the transport level within web applications.

- Students know the most important cryptographic procedures in theory and practice and can use them specifically in the web environment.

- Students have detailed knowledge of current attack methods and suitable protection mecha-nisms in different web application areas.

- Students know options for testing web applications for security risks.

- Students know organizational structures and processes for supporting corporate strategy and goals, through IT.

- Students know procedures and standards for IT governance.

COURSE CONTENTS

The course teaches basic topics in the field of web security. This includes cryptographic pro-cedures, security in transport protocols (HTTPS, SSL and TLS), threats (e.g. code injection, cross site scripting, cross site request forgery) and appropriate countermeasures. Using ready-made, prepared web applications (e.g. JuiceShop), students attempt to exploit threats and security holes to gain a better understanding of the security of web applications. Based on these examples, countermeasures for selected threats are discussed (e.g. input validation, prepared statements). Students are also introduced to security problems at network level (e.g. ARP spoofing, denial-of-service attacks, etc.).

In the subject area of IT Governance, students are taught the basics of IT governance. To this end, important processes and organizational structures are discussed so that business and IT can be aligned with each other. Basic terms are discussed, as well as the classification of IT governance into corporate governance. Furthermore, frameworks and standards (e.g. Cobit, ITIL) are discussed.

LANGUAGE OF INSTRUCTION

English

NUMBER OF ECTS CREDITS ALLOCATED

3