Department	07 Computer Science and Mathematics
Course title	**Cloud Infrastructure Security**
Hours per week (SWS)	4
Number of ECTS credits	5
Course objective	• Students can specify the shared responsibilities for securing cloud systems • Students explain the terms, systems, and concepts relevant to securing cloud infrastructures in their own words • Students analyze the security properties of a given infrastructure • Students configure the access control and security systems of the cloud system under study and operate them • Students react sensibly to successful attacks on cloud infrastructures.
Prerequisites	Basic knowledge of IT security. Helpful: Cloud Computing
Recommended reading	• Up to date online sources and documentation • Chris Dodson: Practical cloud security : a guide for secure design and deployment (2019) • Evan Gilman, Doug Barth: Zero Trust Networks : Building Secure Systems in Untrusted Networks (2017) • Adam Shostack: Threat Modeling : Designing for Security (2014)
Teaching methods	Whiteboard, projector, digital sources, LMS as well as practical exercises using one or more public cloud providers.
Assessment methods	Term paper, practical exam or oral exam
Language of instruction	English
Name of lecturer	Prof. Dr. Johannes Ebke
Email	johannes.ebke@hm.edu
Link	https://www.cs.hm.edu/die_fakultaet/ansprechpartner/professoren/ebke/index.de.html
Course content	More and more companies are using public cloud providers. Their security concept is based on shared responsibility between cloud provider and customer – the cloud provider is solely responsible for the security of the services offered per se, while the responsibility for secure operation of these services falls to the customer. This means that the customer not only has to manage the regular secure development and protection of the operated services and applications, but also the correct configuration and secure operation of their cloud infrastructure. In this module, the principles of cloud infrastructure security are introduced and exercised. The access control and security systems of large public cloud providers as well as selected private cloud systems are presented and illustrated by concrete examples. Complex security requirements are analyzed, corresponding security security concepts are designed and implemented in practice. Approaches to organizing cloud use in large companies are illustrated using concrete examples. In addition, practical exercises for detecting and responding to attacks will also be carried out.
Remarks	