Module:	***Continuity Planning and Organisational Aspects of Cyber Defense***
Lecturer:	Dr.-Ing. Thomas Mundt
Language:	English
Teaching Method:	Lecture and practical exercise
Credit Points:	1 ECTS
Attendance requirements:	Basics in computer science Basics in Management would be a plus
Goals / Skill:	This lecture gives an introduction on organisational aspects of computer security. Planning for accidents and maintaining awareness is a key factor for companies. The course introduces possible threats and risks, such as earthquakes, sabotage, terrorism, cyber attacks, thefts etc. It mainly focuses on companies with a large IT infrastructure that is vital for their business processes.
Detailed Content:	1. Introduction – Threats, risk, Attacks, Methods, responsibilities. 2. Planning for the Expected – Recovery plans, Data Security, Work site security, Secondary work sites, Disaster tolerant telecom and IT infrastructures, Planning readiness of employees. 3. Planning for the Unexpected – Emergency command structures, Tests and certification programs, Implementing a process of "learning lessons" from incidents, Disaster communication and public relations. 4. Best Practise.
Media Used:	Electronic Presentation, Discussion, Blackboard Illustrations, Practical Demonstrations, Lab Exercises performed by the students.
Literature:	Andrew Hiles: The Definitive Handbook of Business Continuity Management, John Wiley & Sons, 2010 The Cabinet Office: Business Continuity For Dummies, John Wiley & Sons, 2012 Robert J. Fischer, Edward P. Halibozek, David C. Walters: Introduction to Security, Butterworth Heinemann, 2012
Assigned Tutorial:	Developing a security plan.
Suggested Reading before the start of the summer school:	Preparedness Planning for Your Business - http://www.ready.gov/business Lene Hansen, Helen Nissenbaum: Digital Disaster, Cyber Security, and the Copenhagen School, Wiley and Sons, 2009 - http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2478.2009.00572.x/full