Nachhaltige Sicherheitslösungen und Datenschutz

Allgemeine Angaben

Kürzel	M_NSD
Modulverantwortliche	Prof. Dr. Koch
Dozenten	Prof. Dr. Koch, Prof. Dr. Stehr, Dr. Loeser, Dr. Speth
Lehrsprache	Deutsch
Semester	4
ECTS-Punkte	5
Kontaktstunden	40
Selbststudium	85
Dauer	1 Semester
Art	Pflicht im Rahmen der Spezialisierung
Häufigkeit	jedes Studienjahr
Gewichtung	5/120
Prüfungsleistung	R**S**

Stichwörter

- Sicherheitslösungen (SIEM, SOAR und SOC)
- Business Continuity Management
- Datenschutz

Zugangsvoraussetzungen

- Grundlagen im Bereich IT-Sicherheit und Riskmanagement sind vorhanden, Sicherheitsanalytik, Identitäts- und Zugriffsmanagement sowie industrielle und anwendungsbezogen Sicherheit

Verwendbarkeit

- Masterthesis und ggf. weiterführende Arbeiten für Forschungsprojekte und möglicherweise eine Promotion/DBA; verwendbar in weiteren Spezialisierungsmodulen Cyber Security.

Qualifikations- und Kompetenzziele

Die Studierenden können Sicherheitsinformationen und -events in Unternehmen interpretieren und verstehen es, entsprechende konkrete Maßnahmen abzuleiten und umzusetzen. Sie kennen die Prinzipien und Arbeitsweisen von Security Information and Event Management Systemen (SIEM) und sind vertraut mit den Aufgaben von Security Operation Centern (SOC). Sie kennen die Funktionen von Security Orchestration, Automation and Response (SOAR) Systemen und verstehen diese anzuwenden.
Sie haben ein gutes Verständnis von Business Continuity Management und wissen dies in Unternehmen umzusetzen. Sie können die Auswirkungen von Krisen und Katastrophen für Unternehmen einordnen und entsprechende Maßnahmen zum Erhalt und zur Business Continuity definieren und umsetzen (z.B. Notfallpläne).
Sie verstehen die historische und zukünftige Bedeutung des Datenschutzes und wissen nationale, europäischen und internationale Datenschutzregeln zu bewerten. Sie kennen technische Maßnahmen, um Datenschutzkonzepte so weit wie möglich zu etablieren und umzusetzen.

Lehr- und Lernmethoden

Die Analyse und Bewertung vorgegebener Themen sowie Einordnung und Abgrenzung der Inhalte wird an Fallbeispielen geübt.

Inhalte

- Ganzheitliche Sicherheitslösungen
    - Security Information and Event Management (SIEM)

    - Security Orchestration, Automation and Response (SOAR)
    - Security Operation Center (SOC)
    - Managed PKI
- Business Continuity Management
    - Lebenszyklus-Modell und Betrachtung von Risiken
    - Unterbrechung durch Katastrophen- und Krisenbedingungen
    - IT-Notfallmanagement und Sicherstellung der ökonomischen Nachhaltigkeit
- Datenschutz
    - Historische Einordnung, Prinzipien und zukünftige Bedeutung
    - EU-DSGVO, Internationale Abkommen
    - Technische Möglichkeiten
    - Beispielanwendungen, wie Cloud-Services

.

Grundlegende Literaturhinweise

Murdoch, D.: Blue Team Handbook: SOC, SIEM and Threat Hunting, Independently published,2019
Emmer,M.: Praktisches Business Continuity Management: So stellen Sie Ihr Unternehmen resilient und zukunftssicher auf, Space Net, 2021
Kersten, H. und Klett, G.: Business Continuity und IT-Notfallmanagement: Grundlagen, Methoden und Konzepte, Springer Vieweg, 2017
Eckert, C.: IT-Sicherheit: Konzepte - Verfahren - Protokolle, De Gruyter Studium, 2018
Petrlic, R. et. al.: Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, Springer Vieweg, 2nd Edition, 2023