TECHNISCHE HOCHSCHULE DEGGENDORF

Modulhandbuch
Master Cyber Security

Fakultät Angewandte Informatik
Prüfungsordnung 01.10.2024
Stand: 30.07.2026 10:28

Inhaltsverzeichnis

M-CY-01 Cybersecurity Fundamentals

Modul Nr.	M-CY-01
Modulverantwortliche/r	Prof. Dr. Peter Fröhlich
Kursnummer und Kursname	M-CY 1101 Cyber Security Fundamentals
Lehrende	Martin Aman Stefan Felixberger Martin Fischer Prof. Dr. Peter Fröhlich Prof. Dr. Michael Heigl Prof. Dr. Terezia Toth
Semester	1
Dauer des Moduls	1Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60Stunden Selbststudium: 90Stunden Gesamt: 150Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90Min.
Gewichtung der Note	5/90
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Die Studierenden sollen das Security Lifecycle Management für Cyber Security kennen lernen. Dabei werden Schwerpunkte in Industrial Control System Security und Car IT Security gesetzt. Die Studierenden sollen es als ein Konzept zur nahtlosen Integration

sämtlicher Informationen, die im Verlauf des Security-Lebenszyklus einer Anlage, eines Produktes oder eines Automobils anfallen, verstehen. Das Konzept beruht auf abgestimmten Methoden, Prozessen und Organisationsstrukturen und setzt grundlegende Kenntisse von technischen Systemen voraus.

Dazu erwerben die Studierenden die folgenden Kompetenzen: Kenntnisse des Cybersecurity Framework, Grundlagen vernetzter Steuerungssysteme, Grundlagen Risikoanalyse für Industrieanlagen und Grundlagen des Business Continuity Management.

Methodenkompetenz

Die Studierenden wenden den Security-Lebenszyklus am Beispiel einer Produktionsanlage oder eines Automobils an. Sie bewerten und überprüfen darauf abgestimmte Methoden, Prozessen und Organisationsstrukturen basierend auf technischen Standards, Gesetzen und Verordnungen.

Persönliche Kompetenzen/ Schlüsselkompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studierenden können den Security-Lebenszyklus auf komplexe technische Systeme anwenden. Zudem werden Kompetenzen zu Recht in der Informationstechnologie vermittelt.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

- Cyber Security Framework (Prof. Dr.-Ing. Peter Fröhlich)
  - Security Awareness für OT
  - Herausforderungen OT Security
  - Use Case
- Grundlagen vernetzter Steuerungssysteme (Prof. Dr.-Ing. Terezia Toth)
  - Grundlagen der Steuerungstechnik
  - Definitionen
  - Anwendungsbereiche
  - Geschichte

    - Stand der Technik
    - ISO/OSI 7-Schichten-Modell
    - Anforderungen und Architekturen
    - Beispiele
    - Kommunikationsprotokolle auf Ethernet-Basis
    - Ethernet im Überblick
    - Anforderungen und Architekturen
    - Beispiele
- Grundlagen des Hacking (Prof. Dr. Michael Heigl)
    - Einblicke & Analyse Schadsoftware
- - Linux-Basics für Hacker
    - Penetration Testing Methodik
    - Information Gathering Techniken
    - Exploitation u.a. Schadcode Erstellung
- Betriebssysteme (M.Sc. Martin Aman; TG Alpha)
    - Aufbau und Sicherheitsarchitektur
    - Security in Linux
    - Workshop
- Recht in der Informationsgesellschaft (Stefan Felixberger; Richter)
    - Grundlagen/Compliance
    - Strafrechtliche und zivilrechtliche Aspekte
    - Datenschutz
    - IT-Sicherheit aus rechtlicher Sicht
    - Grundprinzipien des Online-Rechts
    - Rechtskonforme Internetnutzung/Vorgaben für Websites und geschäftliche Mails
    - Outsourcing und Auftragsverarbeitung
    - Elektronische Steuerprüfung
    - Urheberrecht und Abmahnungen

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum, Infomarkt

Im Unterricht werden die Inhalte unter Einbeziehung der Studenten erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch

Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen den Studierenden zur Nacharbeit und zur Aneignung der Inhalte.

Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden Security Lifecycle Management

Im Workshop wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt: Risikoanalyse von Industrieanlagen, CAN und Ethernet-Netzwerke in Steuerungssystemen

Im Infomarkt bereiten die Studierenden ausgewählte Themen selbstständig vor und präsentieren die Ergebnisse.

Besonderes

Vorträge von Gastdozierenden

Empfohlene Literaturliste

Allgemein

- ISO 2700x
- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren ? Protokolle; Oldenburg Verlag; 10. Auflage
- Kersten, Heinrich, Klett, Gerhard: Business Continuity und IT-Notfallmanagement; Springer-Verlag; ISBN 978-3-658-19118-4

Hacking

Industrie

- IEC 62443
  - https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/industriellesicherheit_node.html
  - https://ics-cert.us-cert.gov/

Automotive

- SAE J3061
- EVITA Projekt
- NHTSA - Cybersecurity Best Practices for Modern Vehicles
- Works of ISO/TC 22 (Road vehicles)
- ISO/SAE 21434 - Road Vehicles -- Cybersecurity engineering

Cyber Security Framework

- Byres, Eric , Tofino Security and Cusimano, John, exida Consulting LLC: 7 Steps to ICS and SCADA Security ? White Paper; Feb. 16, 2012; www.tofinosecurity.com
- http://isa99.isa.org/ISA99%20Wiki/WP_Overview.aspx

Recht in der Informationsgesellschaft

Datenschutzrecht

- Rüpke, Giselher; Lewinski, Kai von; Eckhardt, Jens (2022): Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung. München: C.H. Beck (Studium und Praxis)
- Paal/Pauly (Hrsg.) (2021): Datenschutz-Grundverordnung, Kommentar.

Verlag C.H. Beck. 3. Auflage. München (2021)

- Gola, Peter; Jaspers, Andreas; Müthlein, Thomas; Schwartmann, Rolf: Datenschutz-Grundverordnung im Überblick. Erläuterungen, Schaubilder und Organisationshilfen für die Datenschutzpraxis. 3. Auflage. Frechen: DATAKONTEXT

Online

- https://www.stiftungdatenschutz.org/dsgvo-info/
- https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz/EU-DSGVO/Datenschutzkonforme-Datenverarbeitung.html
- https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo
- https :// vds.de/fileadmin/vds_publikationen/vds_10010_web.pdf
- http://rsw.beck.de/rsw/upload/ZD/ZD_01-2018_-_Beitrag_Veil_1.pdf
- https://fg-secmgt.gi.de/fileadmin/FG/SECMGT/2017/3_Sachs_gi_informatik_dsgvo_sec.pdf

Aktuelle Tätigkeitsberichte der Datenschutz-Aufsichtsbehörden BW/Bayern

- https://www.baden-wuerttemberg.datenschutz.de/tatigkeitsbericht /
- https://www.lda.bayern.de/media/baylda_report_08.pdf

Beschäftigtendatenschutz:

- https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/Ratgeber-ANDS-2.-Auflage.pdf

Vernetze Steuerungssysteme

- IEEE 802.x: http://standards.ieee.org/about/get/802/. Online verfügbar unter http://standards.ieee.org/about/get/802/.
- Bender, K. (1992): Profibus. Der Feldbus für die Automation. 2. Aufl.

München: Hanser.

- Bormann, Alexander; Hilgenkamp, Ingo (2006): Industrielle Netze. Ethernet-Kommunikation für Automatisierungsanwendungen. Heidelberg: Hüthig (Praxis). Online verfügbar unter http://deposit.dnb.de/cgi-bin/dokserv?id=2695541&prov=M&dok_var=1&dok_ext=htm.
- Büsing, Alexander; Meyer, Holger (2002): INTERBUS-Praxisbuch.

Projektierung, Programmierung, Anwendung, Diagnose. Heidelberg: Hüthig (Praxis).

- Etschberger, Konrad (2009): Controller-Area-Network. Grundlagen, Protokolle, Bausteine, Anwendungen. 4. Aufl. München: Hanser, Carl.
- Popp, Manfred (2005): Das PROFINET IO-Buch. Grundlagen und Tipps für Anwender. Heidelberg: Hüthig (Praxis).

- Reißenweber, Bernd (2011): Feldbussysteme zur industriellen Kommunikation. 3. Aufl. München: Deutscher Industrieverlag (Automatisierungstechnik 2016).
- Sauter, Martin (2015): Grundkurs mobile Kommunikationssysteme. LTE-Advanced, UMTS, HSPA, GSM, GPRS, Wireless LAN und Bluetooth. 6., überarb. und erw. Aufl. Wiesbaden: Springer Vieweg. Online verfügbar unter http://dx.doi.org/10.1007/978-3-658-08342-7.
- Schnell, Gerhard; Wiedemann, Bernhard (Hg.) (2012): Bussysteme in der Automatisierungs- und Prozesstechnik.
- Grundlagen, Systeme und Anwendungen der industriellen Kommunikation. 8., aktualisierte und erw. Aufl. Wiesbaden: Springer Vieweg (Praxis).
- Tanenbaum, Andrew S.; Wetherall, D. (2011): Computer networks. 5th ed. Boston, Momtreal: Pearson Prentice Hall.

Betriebssysteme

- Kofler, Michael; Zingsheim, André; Gebeshuber, Klaus; Widl, Markus; Aigner, Roland; Hackner, Thomas et al. (2018): Hacking & Security. Das umfassende Handbuch. 1. Auflage, 2. korrigierter Nachdruck. Bonn: Rheinwerk (Rheinwerk Computing).
- Stallings, William (2015): Operating systems. Internals and design principles. Eighth edition. Boston: Pearson.

Grundlagen Hacking

Auflage, Oldenbourg Verlag, 2018

- Eckert, Claudia: IT-Sicherheit Konzepte - Verfahren Protokolle, 10.
- Elisan, Christopher C.; Davis, Michael A.; Bodmer, Sean M.; LeMasters, Aaron; Lemastes, Aaron: Hacking Exposed - Malware & Rootkits, The McGraw-Hill Companies, 2016
- Hertzog, Raphael; O'Gorman, Jim; Aharoni, Mati Kali: Linux Revealed - Mastering the Penetration Testing Distribution, OFFSEC PRESS, 2017
- Kaspersky, Eugene: Malware - Von Viren, Würmern, Hackern und Trojanern und wie man sich vor ihnen schützt, Hanser, 2008
- Kim, Peter: The Hacker Playbook - Practical Guide to Penetration Testing, Secure Planet LLC, 2014
- Messner, Michael: Hacking mit Metasploit - Das umfassende Handbuch zu Penetration Testing und Metasploit, 3. Auflage, dpunkt.verlag, 2018
- Patel, Rahul Singh Kali: Linux Social Engineering, Packt Publishing, 2013
- Schrödel, Tobias: Ich glaube es hackt! - Ein Blick auf die irrwitzige Realität der IT-Sicherheit, 3. Auflage, Springer Spektrum, 2014
- Sikorski, Michael; Honig, Andrew: Pracitical Malware Analysis - The Hands-On Guide to Dissecting Malicious Software, no starch press, 2012
- Smith, Craig: The Car Hacker's Handbook, no starch press, 2016

- Weidman, Georgia: Penetration Testing - A Hands-On Introduction to Hacking, no starch press, 2014
- Weidman, Georgia: Penetration Testing - A Hands-On Introduction to Hacking, no starch press, 2014

M-CY-02 Security Engineering I

Modul Nr.	M-CY-02
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	M-CY 1102 Security Engineering I
Lehrende	Prof. Dr. Michael Heigl Prof. Dr. Helena Liebelt N.N. Prof. Dr. Martin Schramm Prof. Dr. Roland Zink
Semester	1
Dauer des Moduls	1Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60Stunden Selbststudium: 90Stunden Gesamt: 150Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90Min.
Gewichtung der Note	5/90
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Die Studierenden sollen das Security Engineering als ganzheitlichen Ansatz begreifen. Es werden Werkzeuge, Prozesse und Methoden für Entwurf, Implementierung und Test von verlässlichen IT-Systemen in Industrie, IOT und Automotive behandelt.

Dazu erwerben die Studierenden die folgenden Kompetenzen in Security Engineering:

Mathematische Grundlagen der modernen Kryptographie, Grundlegende kryptographische Algorithmen und Protokolle, Sicherheitsmodelle, -architekturen und -strategien (ISO 27000), Betriebssysteme, Sichere Programmiertechniken, Sichere Konfiguration von Netzwerken.

Weiterhin wird bei der Programmier-Kompetenz der Schwerpunkt auf verlässliche Architekturen und Code Styles gelegt.

Methodenkompetenz

Die Studierenden begreifen das Security Engineering als ganzheitlichen Ansatz.
Die vermittelten Werkzeuge, Prozesse und Methoden können auf den Entwurf, Implementierung und Test von verlässlichen IT-Systemen in Industrie, IOT und Automotive angewendet und bewertet werden.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studierenden können das Security Engineering auf komplexe technische Systeme anwenden.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

- Mathematische Grundlagen der modernen Kryptographie (Prof. Dr. Martin Schramm)
  - (Erweiterter) Euklidischer Algorithmus
  - Modulo Arithmetik, Restklassenmengen
  - Primzahlen
- Grundlegende kryptographische Algorithmen und Protokolle (Prof. Dr. Martin Schramm)
  - Symmetrische und asymmetrische Algorithmen
  - Integritätsalgorithmen
  - Digitale Signaturen und Public Key Infrastrukturen

- Programming Revisited (Prof. Dr. Michael Heigl)
  - C Revisited (u.a. Stack, Heap, CISC vs. RISC)
  - Schwachstellenanalyse von C-Code mittels GDB
  - Python Revisited
  - Exploits in C und Python
  - Schutzmaßnahmen - Secure Coding (Standards/Guidelines)
- Secure Coding und Cyber Security Challenge (Dr. Santiago Suppan / Dr. Tiago Gasiba (Siemens AG)
  - Verlässliche Softwarearchitekturen / Codierregeln
  - Sicherheitsanforderungen für einen Anwendungsfall
  - Bedrohungsanalyse für den Anwendungsfall
  - Workshop
- Sicherheitsmodelle, -architekturen und -strategien (ISO 27000) (Prof. Dr. Helena Liebelt)
  - Regulatorische Situation
  - Einführung ISO/IEC 27001
  - Kontinuierlicher Verbesserungsprozess; Zertifizierungen
- Wissenschaftliches Arbeiten (Prof. Dr. Javier Valdes)
  - Definition einer wiss. Aufgabenstellung
  - Literaturrecherche, Methoden, Daten, Schreiben, Präsentieren

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studierenden erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen den Studierenden zur Nacharbeit und zur Aneignung der Inhalte.

Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden Security Engineering vermittelt

Besonderes

Vorträge von Gastdozierenden

Empfohlene Literaturliste

- Buchmann, Johannes (2016): Einführung in die Kryptographie. 6., überarbeitete Aufl. Berlin, Heidelberg: Springer (Springer-Lehrbuch).

- Wätjen, Dietmar (2018): Kryptographie. Grundlagen, Algorithmen, Protokolle. 3., aktualisierte und erweiterte Auflage. Wiesbaden: Springer Vieweg (Lehrbuch).
- ISO 2700x
- Bundesnetzagentur: IT-Sicherheit im Energiesektor: https:// www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/ Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/ IT_Sicherheit.html
- IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/ Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/ IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf
- Claudia Eckert: IT-Sicherheit: Konzepte Verfahren, Protokolle; Oldenburg Verlag; 10. Auflage (2018)

Sichere Programmiertechniken

- Internet Security Glossary. Online verfügbar unter https://www.rfc-archive.org/getrfc.php?rfc=2828.
- Checklisten Handbuch IT-Grundschutz. Prüffragen zum IT-Grundschutz-Kompendium (2019). 3. aktualisierte Sonderausgabe, Stand: 1. Edition. Köln: Bundesanzeiger Verlag GmbH (Unternehmen und Wirtschaft).
- Bundesamt für Sicherheit in der Informationstechnik. Cyber-Sicherheits-Umfrage 2015- Cyber-Risiken, Meinungen und Maßnahmen, https:// www.bsi.bund.de. Bonn. Online verfügbar unter https://www.bsi.bund.de.
- Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz.

G 5.42 Social Engineering. Bonn. Online verfügbar unter https:// www.bsi.bund.de/DE/ Themen/ITGrundschutz/ITGrundschutzKataloge/ Inhalt/_content/g/g05/g05042.html.

- Bundesamt für Sicherheit in der Informationstechnik (2017): BSI: Die Lage der Informationssicherheit in Deutschland 2017. Bonn. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/

Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?

blob=publicationFile&v=4.

- Dilts, Robert B. (2010): Die Veränderung von Glaubenssystemen. NLP-Glaubensarbeit. 5. Aufl. Paderborn: Junfermann (Coaching fürs Leben).
- Eckert, Claudia: IT-Sicherheit. Konzepte - Verfahren - Protokolle: De Gruyter.
- Graves, Clare W. (2016): Levels of Existence. An Open System Theory of Values. In: Journal of Humanistic Psychology 10 (2), S. 131?155. DOI: 10.1177/002216787001000205.
- Hadnagy, Christopher (2011): Die Kunst des Human Hacking. Social engineering. 2. Auflage. Heidelberg: Mitp.

- Hadnagy, Christopher; Ekman, Paul; Dubau, Jürgen (2014): Social Engineering enttarnt. 1. Auflage. [Heidelberg]: Mitp.
- Hutchins, Eric M.; Cloppert, Michael J.; Rohan M. Amin, Rohan M.; Ph.D. (2011): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,. Online verfügbar unter https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.
- Mitnick, Kevin D.; Simon, William L. (2011): Die Kunst der Täuschung.

Risikofaktor Mensch. [Heidelberg]: Mitp.

- Mottok, Jürgen; Merk, Josef, Falter, Thomas (2016): Proceedings of 2016 IEEE Global Engineering Education Conference (EDUCON). Date and venue: 10-13 April 2016, Abu Dhabi, UAE. A multi dimensional view of the Graves value systems model on teaching and learning leading to a students-centered learning: Graves model revisited. [Piscataway, New Jersey]: IEEE.
- Paulus, Sachar (2011): Basiswissen Sichere Software. Aus- und Weiterbildung zum ISSECO Certified Professionell for Secure Software Engineering. 1. Auflage. Heidelberg: Dpunkt.verlag GmbH.
- Polizei Sachsen: Achtung: geänderte Bankverbindung!, Betrug bei Rechnungsstellung per E-Mail. Online verfügbar unter https://www.polizei.sachsen.de/de/44606.htm.
- Rost, Johann; Glass, Robert L. (2011): The dark side of software engineering. The ethics and realities of subversion, lying, espionage, and other nefarious activities. Los Alamitos, CA, Hoboken, New Jersey: IEEE Computer Society; John Wiley & Sons, Inc.
- Schulz von Thun, Friedemann (2006): Miteinander reden. Orig.-ausg., Sonderausg. Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag (Rororo Sachbuch, 62224).
- Steffens, Timo (2018): Auf der Spur der Hacker. Wie man die Täter hinter der Computer-Spionage enttarnt. Berlin, Germany, [Heidelberg]: Springer Vieweg.
- Watson, Gavin; Mason, Andrew; Ackroyd, Richard (2014): Social engineering penetration testing. Executing social engineering pen tests, assessments and defense. Waltham, MA: Syngress.

Industrielle Sicherheitsmodelle, -standards

- VDI/VDE 2182, Informationssicherheit in der industriellen Automatisierung, Allgemeines Vorgehensmodell, Blatt 1, (2011), Januar 2011. Online verfügbar unter https://www.vdi.eu/uploads/tx_vdirili/pdf/1728600.pdf.
- ISO/IEC 27005, Information technology ? Security techniques ? Information security risk management (2011).

- ISO/IEC 27002, Information technology ? Security techniques ? Code of practice for information security controls,. INTERNATIONAL STANDARD, ISO/IEC 27002 (Second edition, 2013).
- DIN ISO/IEC 27001, Information technology ? Security techniques ? **Information security management systems ? Requirements. (ISO/ IEC 27001:2013 + Cor. 1:2014). English translation of DIN ISO/IEC 27001:2015-03 (2015), März 2015.**
- Bundesamt für Sicherheit in der Informationstechnik (BSI-CS 005 Version 1.30 vom 2019): Industrial Control System Security, Top 10 Bedrohungenund Gegenmaßnahmen, BSI-CS 005 Version 1.30 vom 01.01.2019. Online verfügbar unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/ downloads/BSI-CS_005.pdf?blob=publicationFile&v=9.
- Schäffter, M., Störtkuhl T., Public Key Infrastruktur, Aufbau und Implementierung in Banken und Sparkassen, Banken&Sparkassen, 2, 2001
- Beck, Ulrich (2016): Risikogesellschaft. Auf dem Weg in eine andere Moderne. 23. Auflage. Frankfurt am Main: Suhrkamp (Edition Suhrkamp, 1365 = N.F., 365).
- Störtkuhl, T., Sicherheit für den Mittelstand, e-commerce Magazin 02/04
- Störtkuhl, T.IT-Sicherheit in Zeiten offener Netze, LANline Spezial V/2005
- Adlmanninger,U., Störtkuhl, T., Compliance in der Informationssicherheit, IT-Sicherheit, 6/2006
- Störtkuhl, T. et al., Ganzheitliches Management der Informationssicherheit, IT-Risiken in der Automatisierung, Wie man sie korrekt identifiziert, kontrolliert und minimiert,SecuMedia, 19. September 2008
- Störtkuhl, T., messtec drives Automation, 1-2/2018, http://www.md-automation.de/applikationen/standpunkte/it-risiken-der-automatisierung .

M-CY-03 Security Engineering II

Modul Nr.	M-CY-03
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	M-CY 2101 Security Engineering II
Semester	2
Dauer des Moduls	1Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60Stunden Selbststudium: 90Stunden Gesamt: 150Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90Min.
Gewichtung der Note	5/90
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Die Studierenden sollen das Security Engineering weiter vertiefen. Es werden Werkzeuge, Prozesse und Methoden für Entwurf, Implementierung und Test von verlässlichen IT-Systemen in Industrie, IOT und Automotive behandelt.

Die Studierenden erwerben die folgenden Kompetenzen in Security Engineering:

Weiterführende kryptographische Verfahren (Elliptische Kurven, Pairing-Based Cryptography, Identity-/Attribute-Based Cryptography, gitterbasierte Kryptographie, Post-Quantum Cryptography, Leichtgewichtige Kryptographie), Grundlegende Mechanismen für Manipulationsschutz und Zugriffsschutz, Grundlegende Vorgehensweisen für Schwachstellenanalyse, Bedrohungs- und Risikomodellierung.

Methodenkompetenz

Die Studierenden begreifen das Security Engineering als ganzheitlichen Ansatz.
Die vermittelten Werkzeuge, Prozesse und Methoden können auf den Entwurf, Implementierung und Test von verlässlichen IT-Systemen in Industrie, IOT und Automotive angewendet und bewertet werden. Sie verstehen grundlegende Vorgehensweisen für die Schwachstellenanalyse, Bedrohungs- und Risikomodellierung, Definition und Entwurf von Sicherheitsstrategie und Sicherheitsmodell sowie die Grundlagen der Hardware Security und können das Erlernte auf die Absicherung von Netzen und Webinterfaces übertragen. Zudem können sie die Risiken der Postquanten-Kryptographie einschätzen.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studierenden können das Security Engineering auf komplexe technische Systeme wie Industrieanlagen und Automobile anwenden. Die Studierenden können mit Methoden von Open Innovation sowie Methoden des wiss. Arbeitens auf neue technische Probleme applizieren.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

- Weiterführende kryptographische Algorithmen und Protokolle (Prof. Dr. Martin Schramm)
  - Elliptische Kurven Kryptographie (ECC)
  - Post-Quantum Cryptography (PQC)
  - Leichtgewichtige Kryptographie
- Hardware Security (Prof. Dr. Martin Schramm)
  - Was ist Hardware-Sicherheit?
  - Hardware-Security vs. Hardware-Trust
  - Angriffe, Schwachstellen und Gegenmaßnahmen
  - Konflikt zwischen Sicherheit und Test/Debug
  - Hardwareangriffe: Analyse, Beispiele und Bedrohungsmodelle
  - Hardware-Sicherheitsprimitive

- Einführung in High-Performance Computing und Kryptographische Verfahren (Prof. Dr. Helena Liebelt)
- Sichere Konfiguration von Netzwerken (Prof. Dr. Andreas Wölfl)
  - Fundamentals
  - Link-Layer Security
  - Network-Layer Security
  - Network Security Architecture
- Offensive Web Application Security (Ralf Reinhardt)
  - OWASP als Organisation
  - OWASP Top 10
  - Offensive Security, Red Teaming, Ethical Hacking, Definition

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studierenden erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen den Studierenden zur Nacharbeit und zur Aneignung der Inhalte.

Durch anwendungsorientierte Beispiele und Aufgaben wird der Nutzen der Begriffe und Methoden Security Engineering vermittelt

Im Workshop wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt: Schwachstellenanalysen, OWASP TOP 10, Defense in Depth Architekturen

Empfohlene Literaturliste

- Sanders , C.; Smith , J.: Applied NetworkSecurity Monitoring:Collection, Detection and Analysis . Elsevier Science &Technology Books,2013 (Syngress Media). ISBN 9780124172081
- IT-Grundschutz-Baustein für Webanwendungen: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Vorabversionen/Baustein_Webanwendungen.pdf

Security in Webanwendungen

- OWASP Top 10 (2013). Online verfügbar unter https://www.owasp.org/index.php/Top_10_2013-Table_of_Contents.
- Anderson, Ross (2008): Security engineering. A guide to building dependable distributed systems. - Cover title. 2nd ed. Indianapolis, Ind.: Wiley Pub.
- Bejtlich, Richard (2010, ©2005): The Tao of network security monitoring.

Beyond intrusion detection. Boston: Addison-Wesley.

- Bejtlich, Richard (2013): The practice of network security monitoring. Daly City, California: No Starch Press,US.
- Bernstein, Daniel J.; Buchmann, Johannes; Dahmen, Erik (2009): Post-quantum cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg.
- Buchmann, Johannes; Ding, Jintai (2008): Post-quantum cryptography. Second international workshop, PQCrypto 2008, Cincinnati, OH, USA, October 17-19, 2008 : proceedings. Berlin, New York: Springer (LNCS sublibrary: SL 4--Security and cryptology, 5299).
- Chatterjee, Sanjit; Sarkar, Palash (2011): Identity-Based Encryption.

Boston, MA: Springer US.

- Esslinger, Bernhard (2018): CrypTool Book. Learning and Experiencing Cryptography with CrypTool and SageMath, CrypTool Project, 2018. Online verfügbar unter https://www.cryptool.org/images/ctp/documents/CT-Book-en.pdf.
- Randall, Liam (2013): Applied network security monitoring - collection, detection, and analysis: Syngress Media,u.s.
- Rannenberg, Kai; Camenisch, Jan; Sabouri, Ahmad (2015): Attribute-based credentials for trust. Identity in the information society. Cham, Switzerland, New York, New York: Springer.
- Werner, Annette (2002): Elliptische Kurven in der Kryptographie. Berlin, Heidelberg: Springer Berlin Heidelberg.

Defense in Depth Architekturen

- Coletta A. , Armando A. ; Springer , Cham (Hrsg.): Security Monitoring for Industrial Control Systems . Bécue A., Cuppens-Boulahia N., Cuppens F., Katsikas S., Lambrinoudakis C.(eds) Security of Industrial Control Systems and Cyber Physical Systems, CyberICS 2015, WOS-CPS 2015.Lecture Notes in Computer Science, vol 9588., 2016
- Heberlein , L.T.; Dias , G.V.; Levitt , K.N.; Mukherjee , B.; Wood , J.; Wolber , D.: A network security monitor.In: Proceedings. 1990 IEEE Computer Society Symposium on Research in Security and Privacy ,1990, S.296304
- Hutchins , Eric M. ; Cloppert , Michael J. ; Amin , Rohan M.: Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In: Leading Issues in Information Warfare &Security Research 1 (2011), S.80

Sichere Konfiguration von Netzwerken

- Schreiner, Rüdiger (2012): Computernetzwerke. Von den Grundlagen zur Funktion und Anwendung. 4., überarb. und erw. Aufl. München: Hanser.
- Tanenbaum, Andrew S.; Wetherall, David (2014): Computernetzwerke. 5., aktualisierte Aufl., 2. Dr. München: Pearson (Pearson Studium - IT).

- Weidman, Georgia; van Eeckhoutte, Peter (2014): Penetration testing. A hands-on introduction to hacking. San Francisco, California: No Starch Press.

Hardware Security

- Anderson, Ross J. Security Engineering: A Guide to Building Dependable Distributed Systems (3rd Edition, 2020)
- Katzenbeisser, Stefan; Çetin Kaya Koç (Hrsg.) Trusted Computing (Springer, 2008)
- Wolf, Marilyn; Wolf, David Embedded System Security (Springer, 2019)
- Mark Tehranipoor & Cliff Wang (Hrsg.) Introduction to Hardware Security and Trust (Springer, 2011)
- Trusted Computing Group (TCG) TPM Library Specification 2.0 https://trustedcomputinggroup.org/resource/tpm-library-specification/
- Arthur, Will; Challener, David; Goldman, Kenneth A Practical Guide to TPM 2.0 (Apress, 2015)
- Maes, Roel Physically Unclonable Functions: Constructions, Properties and Applications (Springer, 2013)

M-CY-04 Secure Product Development for Industrial and Automotive Applications

Modul Nr.	M-CY-04
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Schwerpunkt	Automotive IT Security
Kursnummer und Kursname	M-CY 2102 Secure Product Development for Industrial and Automotive Applications
Semester	2
Dauer des Moduls	1Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	5
ECTS	10
Workload	Präsenzzeit: 75Stunden Selbststudium: 225Stunden Gesamt: 300Stunden
Prüfungsarten	PStA
Gewichtung der Note	10/90
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Die Studierenden sollen die grundlegenden Standards und gesetzlichen Bestimmungen für den Schutz von Automobilen und der Automobilinfrastruktur sowie für Operational Technology (OT) in der Industrie verstehen. Dazu gehört:

- Die Anwendung von OT Security-Prinzipien in Verbindung mit den grundlegenden Car IT Security Standards und gesetzlichen Vorgaben.
- Ein umfassendes Verständnis der Sicherheitsanforderungen für industrielle Kontrollsysteme (ICS), SCADA-Systeme und deren Integration in die Automobilindustrie.

- Die Fähigkeit, Bedrohungen, Schwachstellen und Schutzmaßnahmen speziell für die OT Security in der Automobilbranche sowie in der Industrie zu identifizieren und anzuwenden.

Zusätzlich werden die Studierenden mit den spezifischen Anforderungen für OT Security vertraut gemacht, die für den sicheren Betrieb von Automatisierungssystemen und kritischen Infrastrukturen notwendig sind.

Methodenkompetenz

Die Studierenden sollen die erlernten Sicherheitsstandards, -methoden und -prozesse auf komplexe Automobil- und Industriesteuerungssysteme anwenden können. Ein weiterer Fokus liegt auf der Bewertung von Sicherheitsanforderungen und der Optimierung von Sicherheitsmechanismen für moderne Fahrzeugarchitekturen und industrielle Steuerungssysteme, einschließlich der Anwendung von Open Innovation-Methoden.

Persönlichen Kompetenzen

Die Studierenden sollen die Fähigkeit entwickeln, sowohl technische als auch gesetzliche Anforderungen in der Automobilindustrie sowie in industriellen Automatisierungssystemen zu bewerten und praktische Lösungen zu erarbeiten. Dies umfasst die Entwicklung innovativer Sicherheitsarchitekturen und die Analyse komplexer technischer Systeme.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

Industrial Security Standards and Laws

- Industielle Sicherheits-Standards,-Regularien, - Richtlinien und Gesetze (Prof. Dr. Thomas Störtkuhl)
- Regulatorische Situation, IT-Sicherheitsgesetz
- IEC62443
- Kontinuierlicher Verbesserungsprozess/ Zertifizierungen
- Sichere Produktentwicklungsprozesse (M.Sc. Laurin Dörr, TG alpha)
    - Product Development Requirement
    - Technical Security Requirements
    - Design Priciples

- Grundlagen der Automobilen Kommunikationsarchitekturen (Prof. Dr.-Ing. Andreas Grzemba)
  - Entwicklungstrends bei den Automobilen Kommunkationsarchitekturen
  - Einführung in die Car IT Security
  - Security Methoden in automobilen Kommunikationssystemen
- Automotive Security (ISO21432) (Jean Jäger, TÜV Süd)
  - Regularien der UNECE R155 und R156
  - Einführung in die ISO21434
- Grundlagen Safety; Einfluss auf Security in Automotive und Industrie (Prof. Dr. Rolf Jung)
-
  - Industrial scenarios
  - Legal bases of Functional Safety
  - Risk and Functional analysis
  - Security and safety
- Industrial Control Systems (Prof. Dr. Terezia Toth)
  - Architekturen modern Steuerungssysteme
  - Security Parameter moderner Steuerungssysteme
  - Workshop Simantic S7
- Ausgewählte Themen aus der Wissenschaft (Prof. Dr. Michael Heigl)
  - Präsentation und Diskussion von Themen aus aktuellen Forschungsprojekten
- Workshop: Open Innovation und Kreativitätstechniken (Prof. Dr. Kristina Wanieck)
  - Innovationsprozess
  - Bionik als Kreativitätstechnik

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studierenden erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen dem Studierenden zur Nacharbeit und zur Aneignung der Inhalte.

Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden der Industrial und Automotive Security Standards and Laws vermittelt

In Workshops wird das in der Vorlesung Erlernte gefestigt.

Empfohlene Literaturliste

Industrial Security Standards and Laws

- IEC 62443 Teil1-4
  - IT-Sicherheitsgesetz
  - BSI Publikationen zu ICS Security: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/industriellesicherheit_node.html
  - Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren - Protokolle; Oldenburg Verlag; 10. Auflage (2018)
  - Cybersecurity Framework; https://www.nist.gov/cyberframework/framework
  - ISO 27000 Familie
    - DIN ISO/IEC 27001, Information technology ? Security techniques ? Information security management systems ? Requirements (ISO/ IEC 27001:2013 + Cor. 1:2014), English translation of DIN ISO/IEC 27001:2015-03, März 2015
    - ISO/IEC 27002, Information technology ? Security techniques ? Code of practice for information security controls, INTERNATIONAL STANDARD, ISO/IEC 27002, Second edition, 2013-10-01
    - ISO/IEC 27005, Information technology ? Security techniques ? Information security risk management, Second Edition, Juni 2011
    - SO/IEC 27002, Information technology ? Security techniques ? Code of practice for information security controls, INTERNATIONAL STANDARD, ISO/IEC 27002, Second edition, 2013-10-01
    - ISO/IEC 27005, Information technology ? Security techniques ? Information security risk management, Second Edition, Juni 2011

Industrial Control Systems

- Ausbildungsunterlagen der Fa. Siemens: Online verfügbar unter https://www.siemens.com/global/de/home/unternehmen/nachhaltigkeit/ausbildung/sce.html.
- IEC 62443.
  - Tiegelkamp, Michael; John, Karl Heinz (2009): SPS-Programmierung mit IEC 61131-3. Berlin, Heidelberg: Springer Berlin Heidelberg.
  - Wellenreuther, Günter; Zastrow, Dieter (2008): Automatisieren mit SPS ? Theorie und Praxis. Wiesbaden: Vieweg+Teubner.

Design of robust Industrial Contral Systems

- Josef Börcsök: Funktionale Sicherheit: Grundzüge sicherheitstechnischer Systeme
- Hans-Leo Ross: Funktionale Sicherheit im Automobil: ISO 26262, Systemengineering auf Basis eines Sicherheitslebenszyklus und bewährten Managementsystemen
- Lindemann, Udo: Methodische Entwicklung technischer Produkte; Springer Verlag; ISBN 978-3-642-01423-9

Industrial Security - Bedrohungen, Gefahren und Gegenmaßnahmen

- BSI: Die Lage der IT-Sicherheit in Deutschland 2018 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf
- BSI: IT-Grundschutz-Kompendium https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/FD_BS_Kompendium.pdf
- BSI: Industrial Control Systems Security ? Top 10 Bedrohungen und Gegenmaßnahmen 2016 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf
- BSI: BSI Standard 200-2 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf
- BSI: ICS-Security Kompendium
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.pdf
- Hisolutions / VDMA: Leitfaden Security für den Maschinen- und Anlagenbau
- https://industrialsecurity.vdma.org/documents/16227999/16499033/1492086887896_INS_NAM_2016_Industrial_Security_IEC
- .pdf/c2e80bdb-c820-42cb-b3cc-fedd68571e1e
- BSI: Register aktueller Cyber-Gefährdungen und -Angriffsformen v2.0 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_026.html
- Tremmel Moritz:: Per Weblogin ins Klärwerk https://www.golem.de/news/schwachstellen-aufgedeckt-per-weblogin-ins-klaerwerk-1812-138363.htmlBSI: ICS-Fallbeispiel: Servicetechniker ? Der Virus kommt zu Fuß! https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_095c.pdf

Grundlagen Safety - Einfluss auf Security

- Norm DIN EN ISO 26262, ?Road vehicles?Functionalsafety?, Teile 1 bis 10, Beuth Verlag
- Norm DIN EN IEC 61508, ?Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme?, Teile 1 bis 7, Beuth Verlag
- Norm DIN EN ISO 13849, ?Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen?, Teile 1 bis 2 , Beuth Verlag
- Josef Börcsök: Funktionale Sicherheit, VDE Verlag GmbH 2015/5/ Löw, Pabst, Petry: Funktionale Sicherheit in der Praxis, dpunkt.Verlag 2010

Automotive Security Standards and Laws

- NHTSA - Cybersecurity Best Practices for Modern Vehicles,
- ISO/SAE 21434 - Road Vehicles -- Cybersecurity engineering
- ISO 27000 Familie
- IT-Sicherheitsgesetz

- BSI Publikationen zu ICS Security: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/industriellesicherheit_node.html
- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren ? Protokolle; Oldenburg Verlag; ISBN 978-3-486-72138-6
- Cybersecurity Framework; https://www.nist.gov/cyberframework/framework

Security Architectures for Automotive Embedded Systems

- Koscher et al., Experimental Security Analysis of a Modern Automobile (2010): https://www.researchgate.net/publication/220713691_Experimental_Security_Analysis_of_a_Modern_Automobile
- Miller & Valasek, Remote Exploitation / Jeep Hack (2015): https://illmatics.com/Remote%20Car%20Hacking.pdf
- ISO/SAE 21434:2021 Road vehicles Cybersecurity engineering (Engineering-Anforderungen für Automotive-Cybersecurity, Lebenszyklus).
- UNECE WP.29 / R155 (Cybersecurity Management System) und R156 (Software-Updates) regulatorische Anforderungen für Typgenehmigung / CSMS in vielen Märkten.
- SAE J3061 Cybersecurity Guidebook / Prozessrahmen
- Josef Börcsök: Funktionale Sicherheit: Grundzüge sicherheitstechnischer Systeme
- Hans-Leo Ross: Funktionale Sicherheit im Automobil: ISO 26262, Systemengineering auf Basis eines Sicherheitslebenszyklus und bewährten Managementsystemen
- Lindemann, Udo: Methodische Entwicklung technischer Produkte; Springer Verlag; ISBN 978-3-642-01423-9

Bionik

- Biologically Inspired Design (2014). [Erscheinungsort nicht ermittelbar]: Springer.
- Barzel, Bärbel (2012): 50 Jahre - 50 Augenblicke. 1962-2012; [Festschrift Pädagogische Hochschule Freiburg]. Bionik Faszinierende Lösungen der Natur für die Technik der Zukunft. 1. Aufl. Freiburg im Breisgau: Pädag. Hochsch. Freiburg (Schriftenreihe der Pädagogischen Hochschule Freiburg, 22).
- Benyus, Janine M. (2009): Biomimicry. Innovation inspired by nature. [Nachdr.]. New York, NY: Perennial.
- Cerman, Zdenek; Barthlott, Wilhelm; Nieder, Jürgen (2011): Erfindungen der Natur. Bionik - was wir von Pflanzen und Tieren lernen können. 3. Aufl. Reinbek bei Hamburg: Rowohlt (Rororo science, 62024).
- Chirazi, Jacques; Wanieck, Kristina; Fayemi, Pierre-Emmanuel; Zollfrank, Cordt; Jacobs, Shoshanah (2019): What Do We Learn from Good Practices of Biologically Inspired Design in Innovation? In: Applied Sciences 9 (4), S. 650. DOI: 10.3390/app9040650.

- Fayemi, P. E.; Wanieck, K.; Zollfrank, C.; Maranzana, N.; Aoussat, A. (2017): Biomimetics: process, tools and practice. In: Bioinspiration & biomimetics 12 (1), S. 11002. DOI: 10.1088/1748-3190/12/1/011002.
- Gruber, P. (Hg.) (2013): Biomimetics - materials, structures and processes. Examples, ideas and case studies. Berlin: Springer (Biological and medical physics, biomedical engineering).

M-CY-05 Secure Operations and Maintenance

Modul Nr.	M-CY-05
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Kursnummer und Kursname	M-CY 2103 Secure Operations and Maintenance
Semester	2
Dauer des Moduls	1Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60Stunden Selbststudium: 90Stunden Gesamt: 150Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90Min.
Gewichtung der Note	5/90
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Die Studierenden sollen die wichtigen Methoden zum Betrieb und Wartung von Automationsanlagen und IOT kennen lernen. Es werden Werkzeuge, Prozesse und Methoden für angepasste Security Mechanismen für die Industrieautomation vorgestellt. Insbesondere wird auf den Faktor Mensch und die Zugangskontrolle eingegangen.

Zudem werden neue Entwicklungen aus der Forschung diskutiert. Dazu erwerben die Studierenden die folgenden Kompetenzen:

Identitäts- und Zugangsmanagement; Sichere Fernwartung, Netzwerkdiagnose und Problembehandlung, Methoden und theoretische Grundlagen der Eignungsdiagnostik, Cyber Security Awareness, Ethik und der Faktor Mensch

Methodenkompetenz

Die Studierenden verstehen die wichtigen Methoden zum Betrieb und Wartung von Automationsanlagen und IOT und setzen sie zielgerichtet ein. Darüber hinaus lernen die Studierenden die Aufgaben und Kompetenzen des Bundesamt für Informationssicherheit (BSI) kennen. Zudem erlernen die Studierenden Methoden für das wiss. Arbeiten wie Literaturrecherche und Themenfindung

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Insbesondere erwerben sie die Kompetenz, den Faktor Mensch im Kontext der Cyber Security zu bewerten. Die Studierenden wissen, wie sie die Kompetenzen des BSI nutzen können.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

- Identitäts- und Zugangsmanagement Systeme (Prof. Dr. Nicolai Kunze)
- Authentication
- Public Key Infrastructure (PKI)
- Certificates
    - X.509 Certificate
    - Online Certificate Status Protocol (OCSP)
    - Certificate Revocation Lists (CRLs)
- Pretty Good Privacy (PGP)
    - Confidentiality and Authentication
    - Key Management
- Access Control
    - Authentication Protocols
    - Transport Layer Security (TLS)
    - Kerberos
    - Network Authentication
    - Single Sign-On (SSO)
    - OpenID

    - OAuth
- Identity and Access Management (IAM)
- Risikoanalyse (M.Sc. Laurin Dörr)
    - Methoden und Vorgehensmodelle der Risikoanalyse,
    - Risikobewertung von technischen Systemen
- ICS Security-Bedrohungen, Gefahren und Gegenmaßnahmen (Dr. Thomas Nowey, KRONES AG)
    - Gefährdungen und Bedrohungen
    - Maßnahmen für ICS Security
    - Definierte Schutzlevel erreichen
- Social Engineering (Florian Hettenbach, AWS)
    - Was ist Social Engineering?
    - Psychologische Hintergründe
    - Abwehrmaßnahmen
    - Use Cases
- Aufgaben des BSI / Lagebild ICS (Dr. Klaus Biss)
    - Formale Angreifermodelle
    - Geläufige Modelle
- KI Security (Markus Hupfbauer, KPMG)
    - Adversarial Machine Learning
    - Sicherheitslücken durch Trainingsdaten
    - KI-basierte Sicherheitslücken
    - Angriffe auf die Infrastruktur von KI-Systemen
    - Schutz von Modellen gegen Fehlverhalten
    - Erklärbarkeit und Nachvollziehbarkeit von KI-Entscheidungen
    - Ethik und Verantwortlichkeit in der KI
    - Regulierung und Gesetzgebung der KI-Sicherheit
    -
- Themenfindung für die Projekte (Prof. Dr. Martin Schramm)
    - Erkenntnistheorie
    - Forschungsansatz
    - Gliederung wiss. Arbeiten

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studierenden erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen den Studierenden zur Nacharbeit und zur Aneignung der Inhalte.

Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden für die Industrieautomation vermittelt. An einem Fallbeispiel wir der Aufbau einer wiss. Arbeit erarbeitet.

Im Workshop wird das in der Vorlesung Erlernte gefestigt.

Empfohlene Literaturliste

- ISO 2700x
- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren? Protokolle; Oldenburg Verlag; 10. Aufl. (2018)

Sichere Fernwartung

- Crist, Eric F.; Keijser, Jan Just (2015): Mastering OpenVPN: Packt Publishing.
- Du, Wenliang (2017): Computer security. A hands-on approach. [Lieu de publication non identifié]: CreateSpace.
- Knapp, Eric D.; Langill, Joel Thomas (2015): Industrial network security. Securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems. Second edition. Amsterdam: Elsevier.
- Stallings, William (2017): Cryptography and network security. Principles and practice. Seventh edition, global edition. Boston: Pearson Education Limited.

Betriebssysteme:

- Stallings, William (2015): Operating systems. Internals and design principles. Eighth edition. Boston: Pearson.
- Tanenbaum, Andrew S. (2015): Modern operating systems. Fourth edition. Boston: Pearson.
- Schwachstellenanalyse:
- Forshaw, James (2018): Netzwerke hacken. Sicherheitslücken verstehen, analysieren und schützen. 1. Auflage. Heidelberg: dpunkt.
- Tanenbaum, Andrew S. (2015): Modern operating systems. Fourth edition. Boston: Pearson.

Netzwerkdiagnose und -problembehandlung

- Eckert, Claudia (2009): IT-Sicherheit. Konzepte - Verfahren - Protokolle. 6., überarb. und erw. Aufl. München: Oldenbourg.
- Schreiner, Rüdiger (2012): Computernetzwerke. Von den Grundlagen zur Funktion und Anwendung. 4., überarb. und erw. Aufl. München: Hanser.
- Tanenbaum, Andrew S.; Wetherall, David (2014): Computernetzwerke. 5., aktualisierte Aufl., 2. Dr. München: Pearson (Pearson Studium - IT).
- Weidman, Georgia; van Eeckhoutte, Peter (2014): Penetration testing. A hands-on introduction to hacking. San Francisco, California: No Starch Press.

Social Engineering

- Christopher Hadnagy; Die Kunst des Human Hacking; mit Professional

M-CY-06 Cybersecurity Project

Modul Nr.	M-CY-06
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Kursnummer und Kursname	M-CY 3101 Cybersecurity Project
Lehrende	Prof. Dr. Michael Heigl Prof. Dr. Martin Schramm
Semester	3
Dauer des Moduls	1Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	2
ECTS	20
Workload	Präsenzzeit: 30Stunden Selbststudium: 570Stunden Gesamt: 600Stunden
Prüfungsarten	Portfolio
Gewichtung der Note	20/90
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Die Erstellung der Projektarbeit soll den Studierenden die Fähigkeit vermitteln, komplexe wissenschaftlich-technische Probleme aus dem Bereich Cyber Security weitgehend selbstständig oder in kleinen Gruppen unter Anleitung eines kompetenten Hochschulwissenschaftlers zu bearbeiten. Dazu müssen die Studierenden ihr Vorgehen zeitlich und inhaltlich planen und strukturieren und die Ergebnisse in entsprechender Form dokumentieren.

Methodenkompetenz

Die Studierenden können für ein konkretes Projekt die geeigneten Methoden der Cyber Security auswählen und anwenden.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Insbesondere prüfen sie in Form einer Selbstreflexion den Erfolg der ausgewählten Methoden.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

- Das Thema des Projekts muss sich nicht direkt auf ein Modul aus dem Kurs beziehen, muss aber ein Thema aus dem Fachgebiet Cyber Security sein. Die Studierenden können den betreuenden Professoren ein Thema vorschlagen. In der Projektarbeit sollen immer praktische Untersuchungen mit theoretischen Anteilen verbunden werden. Mit den Betreuern bzw. Mitarbeitenden der betreuenden Institute soll ein ständiger und intensiver Kontakt bestehen, um fachliche Inhalte zu vermitteln.
- Die schriftliche Projektarbeit wird zum Ende des Semesters dem Betreuer vorgelegt. Sie soll neben dem methodischen Vorgehen und den fachlichen Ergebnissen auch Bestandteile enthalten, wie sie in Berichten großer Projekte üblich sind (z.B. Einschätzungen der Marktsituation, Vergleich mit dem internationalen Stand von Wissenschaft und Technik). Die konkreten Vorgaben sind vom Thema abhängig und werden vom jeweiligen Betreuer gestellt.

M-CY-07 Industrial and Automotive Communication and Network Security

Modul Nr.	M-CY-07
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Schwerpunkt	Automotive IT Security
Kursnummer und Kursname	M-CY 4101 Industrial and Automotive Communication and Network Security
Semester	4
Dauer des Moduls	1Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	5
ECTS	10
Workload	Präsenzzeit: 75Stunden Selbststudium: 225Stunden Gesamt: 300Stunden
Prüfungsarten	Portfolio
Gewichtung der Note	10/90
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Die Studierenden verfügen über vertiefte Kenntnisse industrieller und automobilnaher Kommunikations- und Netzwerksysteme sowie moderner Protokolle (z. B. CAN, Automotive Ethernet, SDN/NFV). Sie verstehen Konzepte der Automatisierungstechnik, Industrie 4.0, Car-IT-Security sowie wesentliche Sicherheitsmechanismen entlang des OSI-Modells. Darüber hinaus besitzen sie grundlegende fachliche Kompetenz in Digitaler Forensik und den zentralen Bedrohungen im Bereich Cybercrime, einschließlich Malware, Phishing, Botnetzen und Darknet-Strukturen.

Methodenkompetenz

Die Studierenden wenden strukturierte Methoden zur Analyse, Bewertung und Absicherung industrieller, IoT-basierter und automobilnaher Systeme an. Dazu zählen Verfahren zur Schwachstellen- und Risikoanalyse, zur Auswahl geeigneter Schutzmaßnahmen sowie zur Untersuchung und Behandlung von Sicherheitsvorfällen.

Sie beherrschen grundlegende forensische Methoden (Spurensicherung, Datenträgeranalyse, Dokumentation) und können typische Cybercrime-Angriffe methodisch einordnen und analysieren.

Zusätzlich nutzen sie Verfahren zur Anomalieerkennung, Resilienzanalyse sowie Methoden zur Modellierung und Bewertung von SDN- und NFV-basierten Netzwerkarchitekturen.

Persönliche Kompetenzen

Die Studierenden können komplexe technische Systeme strukturiert beurteilen, sicherheitsrelevante Schwachstellen erkennen und fundierte Entscheidungen über geeignete Maßnahmen treffen auch im Kontext forensischer Analysen und Cybercrime-Szenarien.

Sie arbeiten verantwortungsbewusst, sorgfältig und sowohl eigenständig als auch im Team. Durch den hohen Praxisanteil entwickeln sie ausgeprägte Problemlöse- und Analysefähigkeiten sowie die Fähigkeit, technische Zusammenhänge und Untersuchungsergebnisse adressatengerecht zu kommunizieren.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

- Fortgeschrittene Themen der Automatisierungstechnik (Prof. Dr.-Ing. Ludwig Gansauge)
  - Konzepte von Industrie 4.0
  - Cyber Physical Systems
- Einführung Automotive Netzwerke und Car IT Security (Prof. Dr.-Ing. Andreas Grzemba)
  - Grundlagen automobiler Netzwerke und der digitalen Kommunikation

    - Security-Mechanismen im OSI-Modell
    - Architektur eines secure Car
    - Workshop
- Robuste und widerstandsfähige Netzwerke (Prof. Dr.-Ing. Andreas Fischer)
    - Komplexe Systeme
    - Network Function Virtualization
    - Virtualisierungstechnologien
    - Network Function Virtualization
    - Wie unterscheidet sich NFV von herkömmlicher Netzwerk Virtualisierung?
    - Welche Probleme ergeben sich bei der Vernetzung von Netzwerkfunktionen?
    - Überblick über NFV MANO
    - Resiliente Systeme
    - Fault-Error-Failure Kette
    - Fehlertoleranz
    - Security und Safety
    - Anomalieerkennung
    - Grundlagen von SDN
    - Konzept, Komponenten, Schnittstellen
    - SDN Protokolle: OpenFlow, P4
    -
- Digitale Forensik (Prof. Dr. Michael Heigl)
    - Einführung
    - Prozess der Digitalen Forensik
    - Forensic Readiness und Incident Response
    - Anforderungen an eine forensische Untersuchung
    - Digitale Spuren
    - Forensische Dokumentation (Gutachten)
    - Vorgehen am Tatort
    - Datenträger-/Dateiforensik
    - Speichertypen
    - Dateisysteme
    - Sichern, Analyse von Datenträgern
    - Tools
    - Betriebssystemforensik
    - Linux, Windows
    - Post-Mortem Forensik
    - Arbeitsspeicher-/Anwendungsforensik
    - Akquise und Analyse,
    - Workshop

- Cybercrime (Stephan Zollner; Geschäftsstelle Bayerischer Landesbeauftragter für den Datenschutz, Referent Cybersecurity)
  - Cybercrime, Cybercrime-Landschaft, große Bedrohungen
  - Bulletproof-Hosting
  - Surface Web, Deep Web, Darknet: TOR-Netzwerk, Hidden Services
  - Malware
  - Phishing-Methoden
  - Identitätsdiebstahl
  - Botnetze

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studierenden erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen den Studierenden zur Nacharbeit und zur Aneignung der Inhalte.

Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden für die Security Requirements in der IOT und Car IT Security sowie der digitalen Forensik vermittelt

In Workshops wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt: Bussysteme, NFV, Digitale Forensik, Resilienz- Maßnahmen.

Empfohlene Literaturliste

Car IT Security

- Dennis Kengo Oka: Building Secure Cars: Assuring the Software Development Lifecycle; John Wiley & Sons, Ltd.; 2021; Print ISBN:9781119710745; Online ISBN:9781119710783
- Lars Schnieder; Leitfaden Automotive Cybersecurity Engineering; Springer Vieweg; 2023; ISBN 978-3-662-67332-4 ISBN 978-3-662-67333-1 (eBook)
- Ahmad Nasser; Automotive Cybersecurity Engineering Handbook; packt; 2023
- (Fernández de Arroyabe et al; Cybersecurity in the Automotive Industry: A Systematic Literature Review; 2023 - Systematische Literaturübersicht mit 537 Papieren, zeigt Forschungslücken im Bereich. https://www.tandfonline.com/doi/full/10.1080/08874417.2022.2103853

Security Aspects of Automotive Protocols

- ISO/SAE 21434 - Road Vehicles -- Cybersecurity engineering
- BSI Webseite: www.bsi.de

- Siegmund, Gerd: SDN - Software-defined Networking; VDE-Verlag; ISBN 978-3-8007-4511-1
- Gaston C. Hillar: MQTT Essentials - A Lightweight IoT Protocol; Packt Publishing; ISBN: 978-1-78728-781-5
- Kirsten Matheus, Thomas Königseder: Automotive Ethernet; Cambridge Press, 2017
- Wolfhard Lawrenz, Nils Obermöller, CAN: Controller Area Network: Grundlagen, Design, Anwendungen, Testtechnik; VDE-Verlag

Resiliente Systeme

- H. Kopetz, Real-Time Systems, 2nd ed., Springer, 2011.
- K. Shortridge und A. Rinehart, Security Chaos Engineering. Sebastopol, UNITED STATES: OReilly Media, Incorporated, 2023.
- Sterbenz et al. Resilience and survivability in communication networks: Strategies,principles, and survey of disciplines, Elsevier Com. Net., 54, pp. 12451265, 2010.
- Smith et al. Network resilience: a systematic approach, IEEE Com. Mag., 49, 7, pp. 8897, 2011.
- Chandola et al., Anomaly detection: A survey, ACM Comput. Surv., Bd. 41, Nr. 3, S. 15:1-15:58, 20

SDN

- Kurose & Ross, Computer NetworkingA Top-Down Approach, 7th ed., Ch. 5
- Kreutz et al., Software-defined Networking: A Comprehensive Survey, Proc. of the IEEE, 103, 1, pp. 1416, 2015.
- Open Networking Foundation, SDN Architecture Overview, v1.0, 2013.
- Open Networking Foundation, OpenFlow Switch Specification, v1.5.1, 2015.

Digitale Forensik

- Alexander Geschonneck: Computer Forensik ? Computerstraftaten erkennen, ermitteln, aufklären; 5., aktualisierte und erweiterte Auflage, dpunkt.verlag
- André Årnes. Digital Forensics. Vereinigtes Königreich, Wiley, 2017.
- Cameron Malin, Eoghan Casey, James Aquilina: A Practitioners Guide to Forensic Collection and Examination of Volatile Data, Syngress Elsevier, 2013
- Carrier, Brian. File system forensic analysis. Deutschland: Addison-Wesley, 2005.
- Casey, Eoghan. Handbook of Digital Forensics and Investigation. Niederlande, Elsevier Science, 2009.
- Clint P. Garrison: Digital Forensics for Network, Internet and Cloud Computing, Syngress, 2010
- Felix C. Freiling, Bastian Schwittay: A Common Process Model for Incident Response and Computer Forensics, Proceedings of the IMF, 2007

- Geschonneck, Alexander. Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären. Deutschland, dpunkt-Verlag, 2014.
- Hassan, Nihad A.. Digital Forensics Basics: A Practical Guide Using Windows OS. Deutschland, Apress, 2019.
- Jason T. Luttgens, Matthew Pepe, Kevin Mandia: Incident Response & Computer Forensics, 3rd Edition, McGraw-Hill Education, 2014
- Leighton R. Johnson III: Computer Incident Response and Forensics Team Management ? Conducting a Successful Incident Response, Syngress Elsevier, 2014
- Michael Sikorski, Andrew Honig: Practical Malware Analysis ? The Hands-On Guide to Dissecting Malicious Software; no starch press, 2012

M-CY-08 Security Incident Management

Modul Nr.	M-CY-08
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Kursnummer und Kursname	M-CY 4102 Security Incident Management
Semester	4
Dauer des Moduls	1Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60Stunden Selbststudium: 90Stunden Gesamt: 150Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90Min.
Gewichtung der Note	5/90
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Die Studierenden verfügen über fundierte Kenntnisse der organisatorischen und technischen Grundlagen des Security Incident Management. Sie verstehen Aufbau und Betrieb von SIEM- und SOC-Strukturen, zentrale Incident-Response-Verfahren, Grundlagen der Cloud Security, Web Services Security sowie IDS- und Anomalieerkennung, einschließlich ML- und DL-Methoden.

Sie kennen die Prinzipien des Business Continuity Managements, der Network Security sowie der Implementierung von Sicherheitsmaßnahmen und Zugriffskontrolle in industriellen Netzwerken. Zudem verfügen sie über Grundwissen in Fuzzing, digitaler Forensik und typischen Cybercrime-Bedrohungen. Inhalte der Personalführung ergänzen

die fachlichen Kompetenzen um organisatorische Aspekte in sicherheitsrelevanten Bereichen.

Methodenkompetenz

Die Studierenden wenden strukturierte Methoden zur Erkennung, Analyse und Behandlung von Sicherheitsvorfällen an. Dazu gehören SIEM-gestützte Monitoring- und Korrelationsverfahren, Incident-Response-Methoden sowie grundlegende forensische Techniken und Verfahren der Cloud-Sicherheitsanalyse.

Sie nutzen Methoden der Anomalie- und IDS-Auswertung, der Zugriffskontrolle und Absicherung industrieller Netzwerke, des Network Traffic Monitoring, der Application-based Protection sowie Fuzzing-Techniken zur Schwachstellenidentifikation.

Im BCM-Bereich führen sie Risikoanalysen und Business-Impact-Methoden durch. Grundlagen der Personalführung unterstützen sie bei Kommunikations- und Entscheidungsprozessen im Incident Management.

Persönliche Kompetenzen

Die Studierenden können sicherheitskritische Situationen verantwortungsbewusst und strukturiert bewältigen. Sie interpretieren sicherheitsrelevante Ereignisse aus SIEM-, IDS-, Cloud- und Netzwerkumgebungen und treffen fundierte Entscheidungen auch unter Zeitdruck.

Sie wirken effektiv in Incident-Management-Teams, kommunizieren klar und setzen Prioritäten in komplexen technischen Umgebungen. Durch die Inhalte der Personalführung stärken sie ihre Fähigkeiten in Teamkoordination, situativem Führungsverhalten und adressatengerechter Darstellung von Ergebnissen.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

- Organisatorische Maßnahmen für ein SIEM (Thomas Bullinger, Oliver Ortlieb; Zeiss)
  - Design eines Security Operations Center
  - Aufbau eines SIEM
  - Betrieb eines SOC

    - Incident Response
- Cloud Security (Florian Hettenbach; AWS)
    - Web Service und Security
- IDS/Anomalieerkennung (Prof. Dr. Michael Heigl; Martin Aman, TG alpha)
    - Signatur-basierte IDS
    - Maschinelles Lernen
    - Deep Learning
    - Workshop: Signatur-basierte IDS
- Business Continuity Management in der IT-Sicherheit (Prof. Dr. Helena Liebelt)
    - Grundlagen BCM
    - BCM in der IT
    - Security Anforderungen
- Implementierung von Sicherheitsmaßnahmen und Zugriffskontrolle in industriellen Netzwerken (Prof. Dr.-Ing. Nicolai Kunze)
    - Network Security
    - Industrial Networks
    - Basic Concept of Attack Detection
    - IDS-Systeme
    - Network Traffic Monitoring
    - Application-based Protection
    - Tool: Tarpit
- Workshop: Fuzzing (Nicolais Tiefing)
    - Fuzzing Introduction
    - Basics of Fuzzing
    - Blackbox, Greybox, Whitebox
- Personalführung (Prof. Bernt Mayer)
    - Führungsstile
    - Persönlichkeitsprofile verstehen und entwickeln
    - Situational Leadership
    - Transformational Leadership

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studierenden erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen den Studierenden zur Nacharbeit und zur Aneignung der Inhalte.

Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden für SIEMs vermittelt

Im Workshop wird das in der Vorlesung Erlernte gefestigt. Es werden die Themen behandelt: Betrieb SOC, IDS, BCM, Fuzzing

Empfohlene Literaturliste

SIEM

- Arslan, M.: IT-Sicherheit mit einem SIEM-System. GRIN Verlag, 2018.
- Miller, D.; Harris, S.; Harper, A.; Security Information and Event Management (SIEM) Implementation. McGraw-Hill, 2010. ISBN: 978-3-668-63183-4
- Schmidt, K.: IT Security managen. Hanser Fachbuchverlag, 2. Auflage 2024. ISBN 978-3-446-47759-9.
- González-Granadillo, G.; González-Zarzosa, S.; Díaz, R.: Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors 21(14), 2021. DOI:10.3390/s21144759.
- Hase, L.: The Path to Choosing a SIEM System A Systematic Literature Review. FH Wedel Seminararbeit, 2024: https://www.fh-wedel.de/fileadmin/Mitarbeiter/Records/Hase_2024_-_The_Path_to_Choosing_a_SIEM_System_-_A_Systematic_Literature_Review.pdf
- Vielberth, M.:Security Information and Event Management (SIEM). In: Encyclopedia of Cryptography, Security and Privacy. Springer, 2021.
- Fakiha, B.: Business Organization Security Strategies to Cyber Security Threats. International Journal of Safety and Security Engineering 11(1), 2021.

BCM

- ISO 2700x
- BSI Webseite: www.bsi.de
- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren ? Protokolle; Oldenburg Verlag; 10. Aufl. (2018)
- Kersten, Heinrich, Klett, Gerhard: Business Continuity und IT-Notfallmanagement; Springer-Verlag; ISBN 978-3-658-19118-4
- ISO 22301:2019 Security and resilience Business continuity management systems Requirements
- HBR Tools: SWOT Analysis: Harvard Business Review ; 2015; https://store.hbr.org/product/hbr-tools-swot-analysis/TLSWOT?sku=TLSWOT-ZIP-ENG
- Dr. Patchin Curtis | Mark Carey: Risk assessment in practice; Deloitte & Touche LLP; https://www.deloitte.com/global/en/services/consulting-risk/perspectives/risk-assessment-in-practice.html

- NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy; 2018; https://csrc.nist.gov/pubs/sp/800/37/r2/final
- ISO/TS 22317:2021; Security and resilience Business continuity management systems Guidelines for business impact analysis
- BSI: Vorschläge zu Business-Continuity-Strategien (BC-Strategien); Hilfsmittel zum BSI-Standard 200-4; 2023; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_Vorschlaege_zu_BC_Strategien.pdf?__blob=publicationFile&v=3

Implementierung von Sicherheitsmaßnahmen und Zugriffskontrolle in industriellen Netzwerken

- Ariel Segal: Introduction To Trusted Computing; https://opensecuritytraining.info/IntroToTrustedComputing.html
- Will Arthur , David Challener , Kenneth Goldman: A Practical Guide to TPM 2.0; springer link; open access book; 2015; https://link.springer.com/book/10.1007/978-1-4302-6584-9
- Felix Bohling u.a.: Subverting Linux Integrity Measurement Architecture; Uni Hamburg; 2020; https://svs.informatik.uni-hamburg.de/publications/2020/2020-08-27-Bohling-IMA.pdf
- Remote Attestation With Tpm2 Tools; 2020; https://tpm2-software.github.io/2020/06/12/Remote-Attestation-With-tpm2-tools.html#what-is-a-pcr-and-how-are-pcr-values-generated
- strongSwan Documentation: Integrity Measurement Architecture; https://wiki.strongswan.org/projects/strongswan/wiki/IMA

Personalführung

- v. Rosenstiel / Regnet / Domsch (Hrsg.): Führung von Mitarbeitern, Handbuch für erfolgreiches Personalmanagement. 8. Auflage. 2020
- Gröbel, R., Dransfeld-Haase, I. (Hrsg.): Strategische Personalarbeit in der Transformation Partizipation und Mitbestimmung für ein erfolgreiches HRM. Frankfurt a. M. 2022
- Bartscher, T., Nissen, R.: Personalmanagement. Hallbergmoos. 2017
- Seiwert, L., Gay, F.: Das 1x1 der Persönlichkeit (2016). Gräfe & Unzer

Fuzzing

- Michael Sutton, Adam Greene, Pedram Amini: Fuzzing: Brute Force Vulnerability Discovery.; http://www.fuzzing.org/
- Mingyuan Wu, Ling Jiang, Jiahong Xiang, et al. One Fuzzing Strategy to Rule Them All. In: Proceedings of the 44th International Conference on Software Engineering. ICSE 22. Pittsburgh, Pennsylvania: Association for Computing Machinery, 2022, pp. 16341645. isbn: 9781450392211. doi: 10.1145/3510003.3510174.; https://doi.org/10.1145/3510003.3510174 .

- Andreas Zeller, Rahul Gopinath, Marcel Böhme, et al. The Fuzzing Book. Retrieved. CISPA Helmholtz Center for Information Security, 2021

IDS

- Liu, H., & Lang, B. (2019): Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey, Applied Sciences, 9(20), 4396; DOI: 10.3390/app9204396
- Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2017); DOI: 10.48550/arXiv.1701.02145
- Maseer, Z., Othman, M. F., Shakir, M. Z., & Zainuddin, N. M. M. (2023)
- Meta-Analysis and Systematic Review for Anomaly Network Intrusion Detection Systems: Detection Methods, Dataset, Validation Methodology, and Challenges; DOI: 10.48550/arXiv.2308.02805
- Xu, J., Chen, K., & Zhang, L. (2025): Deep Learning-Based Intrusion Detection Systems: A Survey; DOI: 10.48550/arXiv.2504.07839
- Chua, F. B., & Salam, A. (2022): Evaluation of Machine Learning Algorithms in Network-Based Intrusion Detection System; DOI: 10.48550/arXiv.2203.05232
- Vaishalini, C., Ramachandran, R., & Karthik, S. (2022): Comprehensive Survey of Deep Learning-Based Intrusion Detection and Prevention Systems for Secure Communication in the Internet of Things; International Journal of Intelligent Systems and Applications in Engineering (IJISAE), 10(4), 56475656; DOI: 10.18201/ijisae.2022.5647
- Aldweesh, A., Derhab, A., & Emam, A. Z. (2020)
- Deep Learning Approaches for Anomaly-Based Intrusion Detection Systems: A Survey, Taxonomy, and Open Issues. Information, 11(2), 78. DOI: 10.3390/info11020078
- Khan, M. A., & Gumaei, A. (2021): Machine Learning and Deep Learning for Network Intrusion Detection: An Overview; In: Artificial Intelligence and Security, Lecture Notes in Computer Science, vol. 12706, Springer.ISBN: 978-3-030-78618-7

M-CY-09 Best Practise in Information Security Auditing

Modul Nr.	M-CY-09
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Kursnummer und Kursname	M-CY 4103 Best Practise in Information Security Auditing
Semester	4
Dauer des Moduls	1Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60Stunden Selbststudium: 90Stunden Gesamt: 150Stunden
Prüfungsarten	Portfolio
Gewichtung der Note	5/90
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Ziel ist das Erfassen potenzieller Sicherheitslücken unterschiedlicher Systeme. Dazu gehört die Evaluierung von Systemen in Bezug auf IT-Sicherheit, z.B. das Erkennen von Schwachstellen in Applikationen und Betriebssystemen oder das Durchführen einer entsprechenden Sicherheitsbewertung nach aktuellen Normen.

Methodenkompetenz

Die Studierenden sollen für mögliche Gefahren in der IT-Welt sensibilisiert werden, um das erlangte Wissen gezielt für geeignete Präventionsmaßnahmen einsetzen zu können. Dazu erwerben die Studierenden die folgenden Kompetenzen in Security Auditing.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studierenden können Möglichkeiten zur Informationsbeschaffung, Schwachstellenanalyse, Exploitation- Ausnutzung von Schwachstellen, Post Exploitation in der Praxis testen und geeignet dokumentieren (Anfertigen eines Audit-Reports). Die Studierenden bearbeiten selbstständig online die gestellten Aufgaben. Sie müssen in einem definierten Zeitrahmen praktikable Lösungen erarbeiten.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

Vermitteln von fortgeschrittenen Kenntnissen über IT-Sicherheit und potenziellen Angriffsmöglichkeiten.

Dies umfasst:

- Methodik und Tools zum Penetrationtesting (Prof. Dr. Michael Heigl, Matthias Hoffmann)
    - Konzept, Definition
    - Penetration Testing Prozess
    - Rechtliche Rahmenbedingungen
    - Pentesting vs. Hacking
    - Zertifizierung
    - Passive & Aktive Informationsbeschaffung
    - Pentesting Examples
- Schwachstellenanalyse industrieller Protokolle (z.B. Beispiel Modbus) (M.Sc. Stefanie Merz)
- Exploitation- Ausnutzung von Schwachstellen, um ICS-Netzwerk zu kompromittieren (Andreas Popp)
- Incident Response in IT-Netzwerken (M.Sc. Andreas Popp)
- IEC 62443 Best Practices (M.Sc. Andreas Popp)
    - Security Program Maturity
    - Risikobewertung Nach PDCA-Zyklus
    - Risikoabschätzung

- System Design

Lehr- und Lernmethoden

Online Modul, Praktikum

Im Online-Kurs können die Studierenden in einer Testumgebung durch praktische Übungen eigenständig Übungsaufgaben bearbeiten. Kontrollfragen, Hinweise und Musterlösungen dienen den Studierenden zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden Security Auditing vermittelt.

In den einzelnen Lernmodulen werden die individuellen Themen behandelt, die für die Durchführung eines Audits notwendig sind. In einem abschließenden vollständigen System-Audit wird das in der Vorlesung Erlernte gefestigt.

Empfohlene Literaturliste

V. Costa-Gazcón, Practical Threat Intelligence and DataDriven Threat Hunting. Packt Publishing Ltd, 2021.

P. Yosifovich, M. E. Russinovich, D. A. Solomon, and A. Ionescu, Windows Internals, Part 1, 7th ed., Microsoft Press, 2021.

J. Forshaw, Attacking Network Protocols: A Hacker's Guide to Capture, Analysis, and Exploitation. No Starch Press, 2018

Eric D. Knapp; Joel T. Langill, Industrial Network Security 3rd Edition, 2024

Mohammad Ashiqur Rahman u.a., Securing Industrial Control Systems, 2026

Lakshmi Parvathie Vedantam; Phani Kumar Hotha, The Complete SOC Handbook: From Fundamentals to Advanced Threat Hunting and Incident Response, 2025

Mark Murphy, Security Information Event Management (SIEM) Engineering: Maximizing Cyber Threat Visibility and Response, 2023

Diana Kelley; Ed Moyle, Practical Cybersecurity Architecture 2nd Edition, 2023

Megan Roddie; Jason Deyalsingh; Gary J. Katz, Practical Threat Detection Engineering: A hands-on guide to planning, developing, and validating detection capabilities, 2023

Gerardus Blokdyk, The Operational Excellence Library; Mastering IEC 62443, 2024

Pascal Ackerman, Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment, 2021

Raghu Boddu; Sami Lamppu; Rod Trent, Microsoft Unified XDR and SIEM Solution Handbook, 2024

Hands-On Online Ressourcen:
TryHackMe
Available: https://tryhackme.com/ (Last Access: 22.01.2026)

HackTheBox
Available: https://www.hackthebox.com/ (Last Access: 22.01.2026)

M-CY-10 Thesis

Modul Nr.	M-CY-10
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Kursnummer und Kursname	M-CY 5101 Master´s Thesis M-CY 5102 Master´s Thesis Defense
Semester	5
Dauer des Moduls	1Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	0
ECTS	20
Workload	Präsenzzeit: 0Stunden Selbststudium: 600Stunden Gesamt: 600Stunden
Prüfungsarten	Kolloquium, Masterarbeit
Gewichtung der Note	20/90
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Übergeordnetes Lernziel: Fähigkeit, ein umfangreiches Problem aus der Cyber Security selbstständig auf wissenschaftlicher Grundlage zu bearbeiten und zu lösen. Der Schwerpunkt soll auf der kreativen Entwicklung neuer Verfahren und Methoden liegen, wobei der umfassende Systemgedanke einen wesentlichen Anteil zu spielen hat.

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

- Das Thema der Masterarbeit wird von einem Professor der beteiligten Hochschulen gestellt, betreut und inhaltlich begleitet.
- Die Masterarbeit muss enthalten:
    - Darstellung des Standes der Wissenschaft und Technik des bearbeiteten Themas
    - Beschreibung der Methodik und des Ablaufs des eigenen theoretischen und experimentellen Vorgehens
    - Die Einbindung der eigenen Arbeiten in die Arbeit der betreuenden Institute/Fakultäten und eventueller Industriepartner
    - Bericht über eigene Veröffentlichungen
    - Die erreichten fachlichen Ergebnisse und deren Bewertung