TECHNISCHE HOCHSCHULE DEGGENDORF

Modulhandbuch
Master Cyber Security

Fakultät Angewandte Informatik

Prüfungsordnung 15.03.2021

Stand: Donnerstag 02.03.2023 14:24

CY-01 CYBERSECURITY FUNDAMENTALS

Modul Nr.	CY-01
Modulverantwortliche/r	Prof. Dr. Peter Fröhlich
Kursnummer und Kursname	CY-01 Security Lifecycle Management
Lehrende	Prof. Dr. Peter Fröhlich
Semester	1
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/90
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Die Studierenden sollen das Security Lifecycle Management für Industrie und Automotive kennen lernen. Sie 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 Kennntisse 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 Studenten 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 Studenten können den Security-Lebenszyklus auf komplexe technische Systeme anwenden. Zumdem 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)
- Grundlagen vernetzter Steuerungssysteme (Prof. Dr.-Ing. Terezia Toth)
  - Grundlagen der Steuerungstechnik
    - Definitionen
    - Anwendungsbereiche
    - Geschichte
    - Stand der Technik
  - ISO/OSI 7-Schichten-Modell
  - Kommunikationssysteme im Automobil
    - Anforderungen und Architekturen
    - Beispiele
  - Kommunikationsprotokolle auf Ethernet-Basis
    - Ethernet im Überblick
    - Anforderungen und Architekturen
    - Beispiele

- Grundlagen des Hacking (M.Sc Michael Heigl)
  - Einblicke & Analyse Schadsoftware
  - Linux-Basics für Hacker
  - Penetration Testing Methodik
  - Information Gathering Techniken
  - Exploitation u.a. Schadcode Erstellung
- Programming Revisited (M.Sc 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)
- 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 dem Studenten zur Nacharbeit und zur Aneignung der

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

Im Workshops 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 Studenten ausgewählte Themen selbstständig vor und präsentieren die Ergebnisse an Hand einer Poster Session.

Besonderes

Vorträge von Gastdozenten

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**
- 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
- 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

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.

CY-02 SECURITY ENGINEERING I

Modul Nr.	CY-02
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	CY-02 Security Engineering I
Semester	1
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
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.

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 Studenten 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
- Betriebssysteme (M.Sc. Martin Aman)
  - Aufbau und Sicherheitsarchitektur
  - Security in Linux
  - Workshop
- Secure Software Engineering (Prof. Dr.-Ing. Jürgen Mottok)
  - Verlässliche Softwarearchitekturen / Codierregeln
  - Sicherheitsanforderungen für einen Anwendungsfall

- Bedrohungsanalyse für den Anwendungsfall
- Workshop

- Sicherheitsmodelle, -architekturen und -strategien (ISO 27000) (Dr. Thomas Störtkuhl)
  - Regulatorische Situation
  - Einführung i ISI/IEC 27001
  - Kontinuierlicher Verbesserungsprozess; Zertifizierungen

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

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 dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden Security Engineering vermittelt

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
- Bundesnetzargentur: 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)

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.

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.

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 Bedrohungen und 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.

CY-03 SECURITY ENGINEERING II

Modul Nr.	CY-03
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	CY-03 Security Engineering II
Semester	2
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
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 und können Open Innovation Methoden und Methoden des wiss. Arbeitens auf Security Probleme übertragen.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können das Security Engineering auf komplexe technische Systeme wie Industrieanlagen und Automobile anwenden. Die Studenten können wird mit Methoden von Open Innovation sowie Methoden des wiss. Arbeitens auf neue technische Problem 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
- Schwachstellenanalyse /Bewertung von Systemen (M.Sc. Martin Aman)
  - Kategorisierung von Schwachstellen, Schwachstellen-Datenbanken
  - Workshop
- Workshop: Open Innovation und Kreativitätstechniken (Kristian Wanieck)
  - Innovationsprozess
  - Bionik als Kreativitätstechnik
- Wissenschaftliches Arbeiten (Dr. Kristin Seffer)

- Definition einer wiss. Aufgabenstellung
- Literaturrecherche, Methoden, Daten, Schreiben, Präsentieren

- Secure Coding und Cyber Security Challenge (Dr. Santiago Suppan)
  - Methoden der sicheren Codierung
  - Workshop
- Offensive Web Application Security (Ralf Reinhardt)
  - OWASP als Organisation
  - OWASP Top 10
  - Offensive Security, Red Teaming, Ethical Hacking, Definitionen

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

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 dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden Security Engineering vermittelt

Im Workshops 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

IT-Grundschutz-Baustein für 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.

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.

Grundlagen Hacking

- Eckert, Claudia: IT-Sicherheit – Konzepte - Verfahren – Protokolle, 10. Auflage, Oldenbourg Verlag, 2018
- 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

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.296–304
- 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

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.

- Blüchel, Kurt (Hg.) (2006): Faszination Bionik. Die Intelligenz der Schöpfung. München: Bionik Media.
- 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).
- Lindemann, Udo (2009): Methodische entwicklung technischer produkte. Methoden flexibel und situationsgerecht anwenden. [Place of publication not identified]: Springer.
- Mattheck, Gerhard Claus (2010): Denkwerkzeuge nach der Natur. Karlsruhe: Karlsruher Institut für Technologie.
- Nachtigall, W. (2002): Bionik. Grundlagen und Beispiele für Ingenieure und Naturwissenschaftler. 2., vollständig neu bearb. Aufl. Berlin: Springer.
- Nachtigall, Werner (2005): Biologisches Design. Systematischer Katalog für Bionisches Gestalten. [Online-ausg.]. Berlin [u.a.]: Springer (SpringerLink: Springer e-Books).
- Nachtigall, Werner (2010): Bionik als Wissenschaft. Erkennen - Abstrahieren - Umsetzen. Dordrecht: Springer.
- Nachtigall, Werner; Blüchel, Kurt (2000): Das grosse Buch der Bionik. Neue Technologien nach dem Vorbild der Natur. Stuttgart: Deutsche Verlags-Anstalt.
- Wanieck, Kristina; Fayemi, Pierre-Emmanuel; Maranzana, Nicolas; Zollfrank, Cordt; Jacobs, Shoshanah (2017): Biomimetics and its tools. In: Bioinspired, Biomimetic and Nanobiomaterials 6 (2), S. 53–66. DOI: 10.1680/jbibn.16.00010.

CY-04 SECURE PRODUCT DEVELOPMENT FOR INDUSTRIAL AND AUTOMOTIVE APPLICATIONS

Modul Nr.	CY-04
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Schwerpunkt	Automotive IT Security
Kursnummer und Kursname	CY-A0401 Automotive Security Standards and Laws CY-A0402 Security Architectures for Automotive Embedded Systems
Semester	2
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Kern- / Wahlpflichtfach
Niveau	Postgraduate
SWS	5
ECTS	10
Workload	Präsenzzeit: 75 Stunden Selbststudium: 225 Stunden Gesamt: 300 Stunden
Prüfungsarten	PStA
Gewichtung der Note	10/90
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Automotive Security Standards and Laws

Fachkompetenz

Die Studierenden sollen für den Schutz von Automobilen und automotiver Infrastruktur die grundlegenden Standards und gesetzlichen Bestimmungen vermittelt werden.

Dazu erwerben die Studierenden die folgenden Kompetenzen in Car IT Security Standards and Laws:

Gemeinsames Begriffsverständnis über Bedrohungen, Schwachstellen, Gegenmaßnahmen und verwandte Konzepte, Wichtigste Gefährdungen/Bedrohungen für Industrial Control Systems kennen und einordnen können; Systematik wichtiger Publikationen (SAE J3061, NHTSA - Cybersecurity Best Practices for Modern Vehicles, Works of ISO/TC 22 (Road vehicles) ISO/SAE 21434 - Road Vehicles -- Cybersecurity engineering) verstehen und einordnen können; Maßnahmen für Car IT Security kennen und auf praktische Szenarien anwenden können, Anwendung der Standards auf die sichere Produkt- und Anlagenentwicklung.

Methodenkompetenz

Die Studenten verknüpfen die technischen Standards, Gesetze und Verordnungen mit dem Security-Lebenszyklus am Beispiel eines Automobils.

Persönlichen Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können technischen Standards, Gesetze und Verordnungen bewerten und auf komplexe technische Systeme wie ein Automobil anwenden.

Security Architectures for Automotive Embedded Systems

Fachkompetenz

Die Studierenden sollen das das bisher erworbene Wissen vertiefen und auf Automotive Anwendungen transferieren. Es werden Werkzeuge, Prozesse und Methoden für angepasste Security Mechanismen für Car IT Security vorgestellt.

Dazu erwerben die Studierenden die folgenden Kompetenzen:

Grundlagen Safety – Einfluss auf Security; Security Aspects von Car IT Systems, Sichere Implementierung kryptographischer Verfahren.

Methodenkompetenz

Die Studenten können Werkzeuge, Prozesse und Methoden für angepasste Security Mechanismen für Car IT bewerten.

Persönlichen Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können wird mit Methoden von Open Innovation das erlernte Wissen auf neue technische Problem 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

Industrial Security Standards and Laws

- Industielle Sicherheits-Standards,-Regularien, - Richtlinien und Gesetze (Dr. Thomas Störtkuhl)
  - Regulatorische Situation, IT-Sicherheitsgesetz
  - IEC62443
  - Kontinuierlicher Verbesserungsprozess/ Zertifizierungen
- Sichere Produktentwicklungsprozesse (M.Sc. Lautin Dörr)
  - Product Development Requirement
  - Technical Security Requirements
  - Design Priciples
- Grundlagen der CAR IT Security (Dr. Matthias Wachs)
  - 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.-Ing. Andreas Grzemba)
  - Präsentation und Disskussion von Themen aus aktuellen Forschungsprojekten

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

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 dem Studenten 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

Im Workshops wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt:

Security Standards and Laws: Grundbedrohung, Schutzziele für Industrieanalgen und Forschungslabors, Angreifermodelle, Konzeption eines sichern Produkts

Design of robust Industrial Contral Systems: Montgomery Arithmetik, Security Konzept für eine Industriesteuerung, Open Innovation für die Entwicklung neuer Ideen und der Transfer auf Security Aspekten von Industrieanlagen und Automotive E/E-Architekturen

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 Contral 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_IEC62443
- .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

- 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

CY-05 SECURE OPERATIONS AND MAINTENANCE

Modul Nr.	CY-05
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Kursnummer und Kursname	CY-05 Secure Operations and Maintenance
Semester	2
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
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 **w**ird 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 Studenten die Aufgaben und Kompetenen des Bundesamt für Informationssicherheit (BSI) kenne. 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. Sie 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)
- Risikoanalyse (M.Sc. Laurin Dörr)
  - Methoden und Vorgehensmodelle der Risikoanalyse,
  - Risikobewertung von technischen Systemen
- ICS Security-Bedrohungen, Gefahren und Gegenmaßnahmen (Dr. Thomas Nowey)
  - Gefährdungen und Bedrohungen
  - Maßnahmen für ICS Security
  - Definierte Schutzlevel erreichen
- Social Engineering (Prof. Dr. Johannes Edler)
- Aufgaben des BSI / Aktuelles Lagebild ICS-Security (M.Sc. Biss)
  - Formale Angreifermodelle
  - Geläufige Modelle
- Themenfindung (Prof. Dr. Wofgang Dorner)
  - Erkenntnistheorie
  - Forschungsansatz

- Gliederung wiss. Arbeiten
- Schreibstrategien

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

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 dem Studenten 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 Workshops 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.

CY-06 CYBERSECURITY PROJECT

Modul Nr.	CY-06
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Kursnummer und Kursname	CY-06 Cybersecurity Project
Semester	3
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	2
ECTS	20
Workload	Präsenzzeit: 30 Stunden Selbststudium: 570 Stunden Gesamt: 600 Stunden
Prüfungsarten	PStA, Präsentation 20 Min.
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 Studenten 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 Studenten können den betreuenden Professor ein Thema vorschlagen. In der Projektarbeit sollen immer praktische Untersuchungen mit theoretischen Anteilen verbunden werden. Mit den Betreuern bzw. Mitarbeitern 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.

CY-07 INDUSTRIAL AND AUTOMOTIVE COMMUNICATION AND NETWORK SECURITY

Modul Nr.	CY-07
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Schwerpunkt	Automotive IT Security
Kursnummer und Kursname	CY-A0701 Security Aspects of Automotive Protocols CY-A0702 Automotive Network Security Laboratory Excercise
Semester	4
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Kern- / Wahlpflichtfach
Niveau	Postgraduate
SWS	5
ECTS	10
Workload	Präsenzzeit: 75 Stunden Selbststudium: 225 Stunden Gesamt: 300 Stunden
Prüfungsarten	PStA
Gewichtung der Note	10/90
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Security Requirements

Fachkompetenz

Dazu erwerben die Studierenden die folgenden Kompetenzen:

Fortgeschrittene Themen der Automatisierungstechnik, Moderne industrielle Kommunikationsprotokolle, Car IT Security, Implementierung von Sicherheitsmaßnahmen und Zugriffskontrolle in industriellen Netzwerken, Industrial Network and Design Architecture. Moderne automotive Kommunikationsprotokolle

Methodenkompetenz

Die Studierenden sollen die wichtigen Methoden für die gesamten organisatorischen und technischen Prozesse für die Absicherung von Industrieanlagen kennenlernen. Es werden angepasste Methoden für eine Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in Industrieanlagen sowie in IOT und Car IT sowie hierzu vorbereitende Maßnahmen und Prozesse vorgestellt.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können komplexe technische Systeme analysieren und deren Schwachstellen erkennen.

Security Laboratory Excercises

Fachkompetenz

Die Studierenden sollen im Labor praktische Erfahrungen mit wichtigen Prozess Control Protocols und ihrer Absicherung kennenlernen

Dazu erwerben die Studierenden die folgenden Kompetenzen:

Security Monitoring von industriellen und in-Car Netzwerken, Software Defined Networks in der Securty, Cyber Security Evaluation industrieller Netzwerke, Zugangskontrolle und Schaffung von Resilienz in kritischen Infrastrukturen

Methodenkompetenz

Die Studierenden verstehen die Protokolle und können geeignete Absicherungsmaßnahmen auswählen.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können komplexe technische Protokolle analysieren und deren Schwachstellen erkennen sowie geeignete Absicherungsmaßnahmen ergreifen.

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

Security Requirements for Industrial Plants

- 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 industrieller Netzwerke und der digitalen Kommunikation
  - Security-Mechanismen im OSI-Modell
  - Architektur eines secure Car
- Cloud Security (Florian Hettenbach (Amazon))
  - Web Service und Security
- Business Continuity Management in der IT Sicherheit (Prof. Dr. Helena Liebelt)
  - Grundlagen BCM
  - BCM in der IT
  - Security Anforderungen

Security Laboratory Excercises

- Robuste Netzwerke durch Software-defined Networking und Network Function Virtualization (Prof. Dr.-Ing Andreas Fischer)
  - Grundlagen von SDN
  - SDN in der Securtiy
  - Workshop
- Implementierung von Sicherheitsmaßnahmen und Zugriffskontrolle in industriellen Netzwerken (Prof. Dr.-Ing. Nicolai Kunze)
  - Moderne Sicherheitsmethoden
  - Zero-Touch-Verfahren

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

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 dem Studenten 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 Industrieautomation vermittelt

Im Workshops wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt: Feldbussysteme, Zugangsverfahren, CPS, Resilienz-Maßnahmen.

Empfohlene Literaturliste

Security Requirements for Industrial Plants / ICS Security Laboratory Excercises

- IEC62443-Familie
- BSI Webseite: www.bsi.de
- Wolfgang Mahnke: OPC Unified Architecture; Springer-Verlag
- Gaston C. Hillar: MQTT Essentials - A Lightweight IoT Protocol; Packt Publishing; ISBN: 978-1-78728-781-5
- Pascal Ackerman; Industrial Cybersecurity; Packt Publishing; ISBN: 978-1-78728-781-5

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

CY-08 SECURITY INCIDENT MANAGEMENT

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

Qualifikationsziele des Moduls

Fachkompetenz

Die Studierenden erwerben die folgenden Fachkompetenzen:

Organisatorische Maßnahmen für ein SIEM, Incident Response Methoden und Technologien, Forensik in embedded Netzwerken sowie Mabil- und Aritfakte-Forensik, Erkennung und Auswertung von Security Events. Darüber hinaus beschäftigen sich die Studenten mit Protection Methoden und Forensik Tools

Methodenkompetenz

Die Studierenden sollen wichtige Methoden, den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT-Systemen und Industrieanlagen sowie in IOT und Automotive sowie hierzu vorbereitende Maßnahmen und Prozesse kennenlernen. Dies umfassen organisatorische, rechtliche sowie technische Aufgabenstellungen. Sie können auf Auf Basis der Organisatorischen Maßnahmen für ein SIEM sowie der Forensik-Methoden die richtigen Maßnahmen im Falle eines Sicherheitsvorfalls ergreifen. Dazu wird die Kaspersky Interactive Protection Simulation eingesetzt

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Insbesondere verstehen die Studierenden das Vorgehen von Angreifern. Sie erlangen eine persönliche Kompeten, um im Angriffsfall souverän agieren zu 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

Inhalt

- Organisatorische Maßnahmen für ein SIEM (Winkler; Zeiss)
  - Architekturen und Prozesse
  - Tools
- Social Engineering (Prof. Johannes Edler)
  - Historie und Grundmuster
  - Typische Formen
  - Abwehr
- Incident Response Methoden und Technologien (Kaspersky)
  - Kaspersky Interactive Protection Simulation (KIPS)
  - Workshop Ghidra
  - Workshop YARA
- Forensik in embedded Netzwerken (M.Sc. Michael Heigl)
  - Datenerfassung (flüchtige, fragile, temporär zugreifbare Daten)
  - Anti-Forensik, Steganographie, File-Slack

- Malware Forensics, Datenträgerforensik, Netzwerkforensik
- Forensik-Tools

- Forensik in der polizeilichen Arbeit (Stephan Zollner; Bay. Polizei)

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

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 dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden für die Security Incident Management in der Industrieautomation vermittelt

Im Workshops wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt: Incident Response Methoden, Forensik, BCM

Empfohlene Literaturliste

- 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
- Christopher Hadnagy; Die Kunst des Human Hacking; mitp Professional
- Alexander Geschonneck: Computer Forensik ? Computerstraftaten erkennen, ermitteln, aufklären; 5., aktualisierte und erweiterte Auflage, dpunkt.verlag
- Clint P. Garrison: Digital Forensics for Network, Internet and Cloud Computing, Syngress, 2010
- Michael Sikorski, Andrew Honig: Practical Malware Analysis ? The Hands-On Guide to Dissecting Malicious Software; no starch press, 2012
- Jason T. Luttgens, Matthew Pepe, Kevin Mandia: Incident Response & Computer Forensics, 3rd Edition, McGraw-Hill Education, 2014
- Felix C. Freiling, Bastian Schwittay: A Common Process Model for Incident Response and Computer Forensics, Proceedings of the IMF, 2007

- Cameron Malin, Eoghan Casey, James Aquilina: A Practitioners Guide to Forensic Collection and Examination of Volatile Data, Syngress Elsevier, 2013
- Leighton R. Johnson III: Computer Incident Response and Forensics Team Management ? Conducting a Successful Incident Response, Syngress Elsevier, 2014

CY-09 BEST PRACTISE IN INFORMATION SECURITY AUDITING

Modul Nr.	CY-09
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Kursnummer und Kursname	CY-09 Best Practise in Information Security Auditing
Semester	4
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 0 Stunden Selbststudium: 150 Stunden Gesamt: 150 Stunden
Prüfungsarten	PStA, mdl. P. 20 Min.
Gewichtung der Note	5/90
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Ziel ist das Erfassen potentieller 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 Dokumentation (Anfertigen eines Audit-

Reports). Die Studenten 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 potentiellen Angriffsmöglichkeiten.

Dies umfasst:

- Methodik und Tools zum Pentrationtesting (M.Sc. Michael Heigl)
- Schwachstellenanalyse industrieller Protokolle (z.B. Beispiel Modbus) (M.Sc. Karl Leidl)
- Exploitation- Ausnutzung von Schwachstellen um ICS-Netzwerk zu kompromittieren (M.Sc. Laurin Dörr)
- Incident Response in IT-Netzwerken (M.Sc. Andreas Popp)
- IEC 62443 Best Practices (M.Sc. Laurin Dörr)

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 dem Studenten 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

- Jon Erickson: Hacking - The Art of Exploitation, 2nd Edition, no starch press, 2008.
- Georgia Weidman: Penetration Testing: A Hands-On Introduction to Hacking, 1. Auflage, 2014, No Starch Press.
- Claudia Eckert: IT-Sicherheit ? Konzepte - Verfahren - Protokolle, 10. Auflage
- IEC 62443 Reihe

CY-10 THESIS

Modul Nr.	CY-10
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Kursnummer und Kursname	CY-1001 Master´s Thesis CY-1002 Master´s Thesis Defense
Semester	5
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	0
ECTS	20
Workload	Präsenzzeit: 0 Stunden Selbststudium: 600 Stunden Gesamt: 600 Stunden
Prüfungsarten	Kolloquium
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