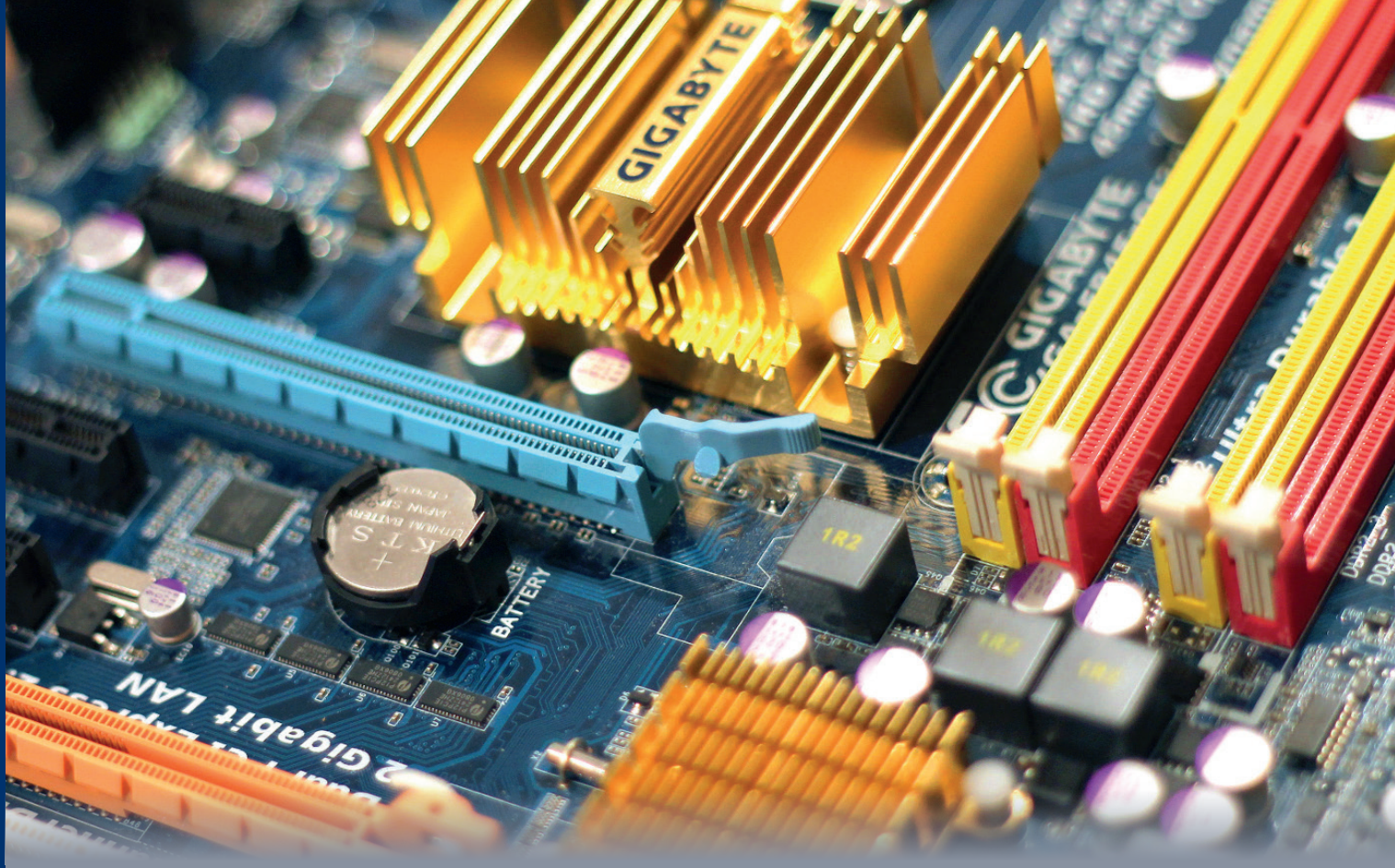

Zertifikatsprogramm - Z201

Applied Computer Systems

- Informationsverarbeitung im Computer
- Rechnersysteme
- Rechnernetzwerke
- Einführung in die Programmierung
- IT-Sicherheit

Prof. Dr. Martin Rieger
Patrick Eisoldt, M.Eng.
David Schlichtenberger, M.Sc.
Tobias Scheible, M.Eng.

Open C³S
Open Competence Center for Cyber Security

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Applied Computer Systems

Studienbrief 1: Informationsverarbeitung im Computer

Studienbrief 2: Rechnersysteme

Studienbrief 3: Rechnernetzwerke

Studienbrief 4: Einführung in die Programmierung

Studienbrief 5: ITSicherheit

Autoren:

Prof. Dr. Martin Rieger

Patrick Eisoldt, M.Eng.

David Schlichtenberger, M.Sc.

Dipl.-Ing. (FH) Tobias Scheible

7. Auflage

Hochschule Albstadt-Sigmaringen

Bundesministerium
für Bildung
und Forschung

AUFSTIEG DURCH BILDUNG >>
OFFENE HOCHSCHULEN

Institut für wissenschaftliche Weiterbildung
Open C^{3}S | Zertifikatsprogramm
Steinachstraße 11
72336 Balingen

7. Auflage (22. November 2017)

Didaktische und redaktionelle Bearbeitung:
Der Studienbrief wurde redaktionell bearbeitet.

Um die Lesbarkeit zu vereinfachen, wird auf die zusätzliche Formulierung der weiblichen Form bei Personenbezeichnungen verzichtet. Wir weisen deshalb darauf hin, dass die Verwendung der männlichen Form explizit als geschlechtsunabhängig verstanden werden soll.

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung, und Forschung unter dem Förderkennzeichen 16OH12024 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Inhaltsverzeichnis

Einleitung zu den Studienbriefen

I. Abkürzungen der Randsymbole und Farbkodierungen

Beispiel	B
Definition	D
Exkurs	E
Kontrollaufgabe	K
Quelltext	Q
Übung	Ü

II. Zu den Autoren

Prof. Dr. Martin Rieger studierte Elektro- und Informationstechnik an der Technischen Universität München und schloss an derselben Hochschule die Promotion mit Auszeichnung ab. Ein Schwerpunkt seiner Forschungsarbeit lag in der Erstellung von Methoden und Werkzeugen zur Modellierung sowie Analyse und Optimierung elektrischer Schaltungen. Er war fünf Jahre Leiter des Labors für schnelle Analog-ICs in der IC-Entwicklungsabteilung des Forschungs- und Entwicklungszentrums der Firma Thomson Multimedia in Villingen. In der Zeit bei Thomson Multimedia war er Erfinder bzw. Miterfinder an 15 deutschen, 12 europäischen und acht weltweiten Patenten.

Seit 1993 ist er als Professor an der Fakultät Engineering der Hochschule Albstadt-Sigmaringen auf den Gebieten Informatik und Informationstechnik tätig. Im Labor für Eingebettete Systeme und IT-Sicherheit betreibt er anwendungsnahe Forschung auf den Gebieten Embedded Systems und IT-Sicherheit. Er hatte über viele Jahre an der Hochschule Albstadt-Sigmaringen Positionen als Studiendekan, Prodekan, Prorektor und Rechenzentrumsleiter inne.

Prof. Dr. Rieger ist Initiator und Gründungs-Studiendekan des Master-Studiengangs Digitale Forensik, der in Kooperation mit der Friedrich-Alexander Universität Erlangen-Nürnberg und der Johann Wolfgang Goethe-Universität Frankfurt betrieben wird.

Er leitet das vom BMBF geförderte Zertifikatsprogramm Open-C^3S, das 35 Hochschul-Zertifikatsmodule auf dem Gebiet Cybersicherheit anbietet und das kooperativ von der Hochschule Albstadt-Sigmaringen, der Friedrich-Alexander-Universität Erlangen-Nürnberg, der Freien Universität Berlin und der Johann Wolfgang Goethe-Universität Frankfurt getragen wird.

Patrick Eisoldt, M. Eng. hat an der Hochschule Albstadt-Sigmaringen und der Glyndŵr University in Wales studiert. 2012 schloss er erfolgreich sein Masterstudium Systems Engineering ab. Im Rahmen seiner Master-Thesis konzipierte und realisierte er einen prototypischen Editor zur Projektierung von Prozessleitsystemen der Firma Siemens nach dem Ursache-Wirkung-Prinzip. Von November 2010 bis August 2011 unterstützte er das Institut für Wissenschaftliche Weiterbildung bei der Erstellung von Studienbriefen für den Studiengang Digitale Forensik.

Seit 2012 ist er für das Open Competence Center for Cyber Security als Modulentwickler tätig.

David Schlichtenberger studierte Medien- und Kommunikationsinformatik an der Hochschule Reutlingen. Nach seinem Masterstudium arbeitete er einige Jahre als Webentwickler und Kundenberater für Internetservices. Seit November 2014 ist er als akademischer Mitarbeiter an der Hochschule Albstadt-Sigmaringen am Institut für Wissenschaftliche Weiterbildung beschäftigt.

Tobias Scheible, Dipl.-Ing. (FH), studierte Kommunikations- und Softwaretechnik an der Hochschule Albstadt-Sigmaringen und schloss sein Studium 2009 in der Fachrichtung Kommunikationstechnik ab. In seiner Diplomarbeit beschäftigte er sich mit der Erhebung von spezifischen Anforderungen an asynchrone Web Applications.

Tobias Scheible begann seine berufliche Laufbahn in der Werbebranche, wobei er für die Konzeption und Entwicklung von Web Applications und Websites zuständig war. Des Weiteren veröffentlichte er Artikel zu den Themen Cloud Computing, IPv6 und HTML5 in den Fachzeitschriften Screenguide, Hakin9 und im Webstandards-Magazin. Außerdem bloggt er unter scheible.it über Web Development und Cybersecurity-Themen.

Seit 2012 ist er als wissenschaftlicher Mitarbeiter an der Hochschule Albstadt-Sigmaringen tätig. Dort arbeitet er als Autor und e-Tutor im Masterstudiengang Digitale Forensik und leitet im Bachelorstudiengang IT Security Praktika rund um das Thema Informationssicherheit. Darüber hinaus ist er Mitinitiator des Kompetenzzentrums Cyber Security Lab, welches Forschungsprojekte auf dem Gebiet der IT-Sicherheit koordiniert. Außerdem organisiert er im Rahmen des VDI Programms Workshops zu aktuellen Themen und Trends der IT-Sicherheit.

III. Modullehrziele

Das Modul „Applied Computer Systems“ bietet entsprechendes Basiswissen, um weiterführende Thematiken der Informatik besser verstehen zu können. Ihnen als Lernenden werden im ersten Studienbrief „Informationsverarbeitung im Computer“ Grundlagen des Bereiches Informationsverarbeitung vermittelt. Sie werden insbesondere mit computerinternen Zahlen- und Stellenwertsystemen sowie der Zeichencodierung (ASCII, Unicode) und logischen Operatoren vertraut gemacht.

Im zweiten Studienbrief „Rechnersysteme“ des Moduls erhalten Sie einen Einblick in den Aufbau von Computersystemen und deren Bestandteile. Sie sollen Kenntnisse über grundlegende Prinzipien der Daten- und Informationsverarbeitung als abstraktes Schema eines Rechners sowie die elementare Struktur und das Zusammenwirken verschiedener Bestandteile von Computern erwerben.

Im dritten Studienbrief „Rechnernetzwerke“ des Moduls werden Grundverständnisse für Netzwerke und die elektronische Kommunikation vermittelt. Zunächst erfassen Sie Begriffe der Netzwerktechnik und im weiteren Verlauf erlangen Sie insbesondere Kenntnisse über das Internet, Adressierung und Kommunikationsabläufe.

Im vierten Studienbrief „Einführung in die Programmierung“ wird in die Grundlagen der Programmierung eingeführt. Anhand von abstrakten allgemeingültigen Aussagen werden verschiedene Konzepte vermittelt.

Der letzte Studienbrief „ITSicherheit“ vermittelt einen allgemeinen Überblick über die grundlegenden Begriffe der IT-Sicherheit und stellt exemplarisch einige Sicherheitsvorfälle vor. Dadurch können Schwachstellen eingeschätzt werden und welche Bereiche eines Systems verletzt worden sind.

Nach Durcharbeiten des Moduls sind Sie mit Fachtermini vertraut und besitzen grundlegende Kenntnisse in den Bereichen Informationsverarbeitung, Computerhardware, Programmierung und IT-Sicherheit.

Studienbrief 1 Informationsverarbeitung im Computer

1.1 Lernergebnisse

Mit diesem Studienbrief sollen Sie sich grundlegende Begriffe der Informatik und Kenntnisse über die Verarbeitung von Informationen auf Binärebene aneignen. Sie sollen in die Lage versetzt werden, die grundlegenden Begriffe wie Bits, Bytes, Big/Little Endian sowie Unicode einordnen zu können. Zudem sollen Sie mit dem Umgang von Dual-, Oktal- und Hexadezimalzahlen vertraut gemacht werden und einfache Rechenoperationen mit den genannten Zahlensystemen durchführen können.

1.2 Advance Organizer

Um die nachfolgenden Module des Studiengangs besser verstehen zu können, soll ein Grundverständnis über die Zahlensysteme, die Anordnung von Bytes innerhalb eines Computers, das Arbeiten mit logischen Operatoren und das Darstellen von Zeichen über entsprechende Kodierungen vermittelt werden.

1.3 Einführung

```
There are 10 types of people in the world:
those who understand binary and those who do not.
```

Computer speichern Informationen in binärer Kodierung als Folgen von Einsen und Nullen ab. Um Zahlen, Texte oder Bilder zu speichern, müssen diese in eine binäre Kodierung umgesetzt werden, die dann im Arbeitsspeicher oder einem Speichermedium, wie z. B. einer Festplatte, gespeichert wird (siehe Abb. 1.1). Im folgenden Abschnitt erfahren Sie, wie und in welcher Form Daten in Computersystemen gespeichert und verarbeitet werden.

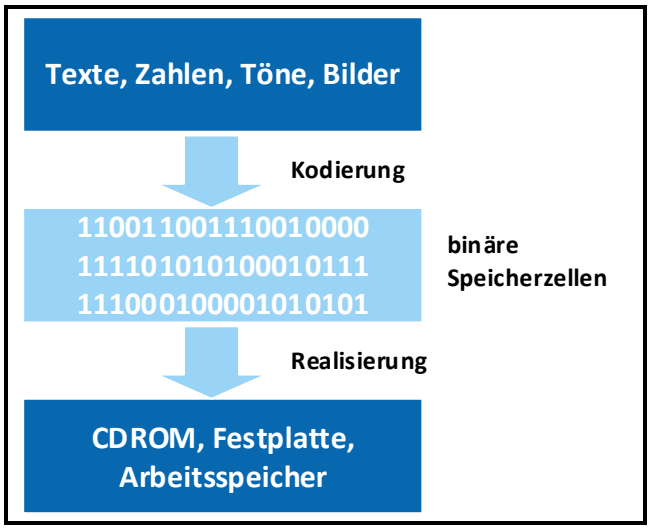

Abb. 1.1: Binäre Kodierung

1.3.0.0.1 Von Bits und Bytes

Die kleinste Einheit, die ein Rechner speichern kann, ist ein Bit. Die Abkürzung steht für **BI**nary digi**T** (d. h. Binärziffer). Ein Bit enthält die Informationsmenge einer Antwort auf eine Frage mit zwei Antwortmöglichkeiten (z. B. ja/nein,

Studienbrief 2 Rechnersysteme

2.1 Lernergebnisse

Im Studienbrief 1 haben Sie die Informationsverarbeitung im Rechner kennen gelernt. Im Folgenden stellen wir den Aufbau von Rechnersystemen und ihre Bestandteile vor. Damit erhalten Sie einen Einblick in grundlegende Prinzipien der Daten- und Informationsverarbeitung. Sie sollen zunächst die elementare Struktur und das Zusammenwirken der verschiedenen Bestandteile innerhalb von Rechnern erfassen. Hierbei erlangen Sie insbesondere Kenntnisse über die Hauptplatine mit ihren notwendigen Komponenten wie Hauptprozessor, Arbeitsspeicher und Bussystemen sowie die wichtigsten Peripheriegeräte bzw. deren Schnittstellen.

2.2 Advance Organizer

Ein moderner Rechner setzt sich aus verschiedenen Komponenten zusammen, die auf unterschiedliche Weise miteinander kommunizieren. Externe Schnittstellen stellen dabei ein nicht zu vernachlässigendes Sicherheitsrisiko dar. Ein bekanntes Beispiel aus dem Jahr 2010 ist der Computerwurm Stuxnet, der sich über USB-Speichermedien verbreiten konnte.

2.3 Grundlagen und Übersicht

Ein Rechner besteht im Prinzip aus Zentraleinheit und Peripherie. Die Bestandteile stellen wir im Einzelnen kurz vor:

- Die Zentraleinheit besteht aus dem Hauptprozessor und dem Hauptspeicher. Der Hauptprozessor (engl. Central Processing Unit, CPU) führt Operationen auf Daten aus. Da er selbst nur wenige Daten speichern kann, verwendet er den Haupt- bzw. Arbeitsspeicher (engl. main memory), um von dort Eingabedaten für seine Operation zu holen und Ergebnisse dorthin zurück zu speichern.
- Die Peripherie ergänzt die Zentraleinheit. Dazu gehören Geräte für die längerfristige Speicherung von Daten, wie z. B. Plattenspeicher (Festplatte, engl. hard disk), sowie Ein- und Ausgabegeräte wie Tastatur oder Bildschirm.

Verbindung über Busse

Alle Komponenten werden durch einen oder mehrere Busse miteinander verbunden, die für die Übertragung von Daten und Signalen genutzt werden.

2.3.1 EVA-Prinzip

Eingabe, Verarbeitung, Ausgabe

Abstrakt betrachtet arbeiten alle Rechner nach einem Schema, das als EVA-Prinzip bekannt ist. Das EVA-Prinzip beschreibt die **E**ingabe, die **V**erarbeitung und die **A**usgabe von Daten bzw. Informationen. Über periphere Eingabegeräte, wie Tastatur, Maus oder einen Datenträger, gelangen Daten in die zentrale Recheneinheit eines Rechners, werden durch diese verarbeitet und über Schnittstellen wie Monitor oder Drucker wieder ausgegeben (siehe Abb. 2.1).

Studienbrief 3 Rechnernetzwerke

3.1 Lehrergebnisse

Ziel dieses Studienbriefs ist es, ein Grundverständnis für Netzwerke und elektronische Kommunikation zu vermitteln, um die Grundlagen zur Bearbeitung der restlichen Module des Semesters zu schaffen. Zunächst erfassen Sie Begriffe der Netzwerktechnik. Im weiteren Verlauf erlangen Sie insbesondere Kenntnisse über das Internet, Adressierung und Kommunikationsabläufen.

3.2 Advance Organizer

In Betrieben ist eine Vernetzung von Rechnern und Arbeitsmitteln wie beispielsweise Druckern und Telefonanlagen unabdingbar, um ein produktives Arbeiten zu ermöglichen. Die nachfolgenden Themen veranschaulichen die Werkzeuge und Mechanismen, welche die Kommunikation der Geräte ermöglichen. Im Modul „Rechnernetze und Netzwerkforensik“ wird der Einstieg in die Rechnernetzwerke vertieft und auf Aspekte der Forensik ausgeweitet.

3.3 Netzwerke

Ein Netzwerk ist eine Gruppe miteinander verbundener Systeme, die untereinander kommunizieren können. Das kleinste Rechnernetzwerk besteht aus zwei Rechnern, die verbunden sind (per Kabel oder Funk) und Daten austauschen können. Außer dem Datenaustausch können in einem Netzwerk z. B. Ressourcen gemeinsam genutzt, zentrale Drucker geteilt, Speicher bereitgestellt oder Rechenleistung gebündelt werden. Das größte existierende Netzwerk ist das Internet, um das es im Folgenden hauptsächlich gehen wird.

Kontrollaufgabe 3.1: Vernetzung von Rechnern

Warum ist eine Vernetzung von Rechnern wichtig und sinnvoll?

K

3.3.1 Topologien

Die Art, wie Rechnersysteme miteinander verbunden sind, beschreibt die Topologie eines Netzwerkes. Entscheidende Faktoren wie Ausfallsicherheit, Performance und verwendete Hardware eines Netzwerkes werden durch dessen Topologie definiert. Bei Netzwerken wird zwischen physikalischer und logischer Topologie unterschieden. Erstere befasst sich mit der physikalischen Verkabelung der einzelnen Rechnersysteme. Die logische Topologie beschäftigt sich mit dem Datenfluss zwischen den Systemen. Die vier häufigsten Netzwerk-Topologien sind Ring-, Stern-, Bus- und Punkt-zu-Punkt-Topologie.

Ring

Jeder Teilnehmer ist mit zwei anderen Teilnehmern des Netzwerkes verbunden, sodass sich insgesamt ein geschlossener Kreis ergibt. Dabei verläuft der Informationsaustausch in eine Richtung des Kreises (im oder gegen den Uhrzeigersinn). Die Information gelangt so zum Zielrechner. Die Rechner im Netzwerk müssen die Ziel- und Quelladresse erhalten, damit sich der Ziel- bzw. Quellrechner einer Nachricht ermitteln lässt.

Studienbrief 4 Einführung in die Programmierung

4.1 Lernergebnisse

Der Studienbrief 4 verschafft einen Einblick in die Welt der Programmiersprachen und Programmierung: angefangen mit der Spezifikation eines Problems durch einen Algorithmus über die Klassifizierung der Programmiersprachen sowie deren Bestandteile und den Aufbau von Programmen bis zur Programmierumgebung. Sie lernen die elementaren Blöcke kennen, aus denen jedes Programm besteht, darunter auch solche, die Sie zur Steuerung eines Programmablaufs verwenden können.

4.2 Advance Organizer

Programme sind in der einfachsten Form Zusammenstellungen mehrerer Befehle die nacheinander (sequenziell) ausgeführt werden. Sie setzen dabei einen Algorithmus um, also eine formale Beschreibung für eine Problemlösung oder Vorgehensweise.

Werte, mit denen Sie in einem Programm arbeiten möchten, speichern Sie in Variablen; die Programmiersprachen merken sich für jede Variable nicht nur den Wert, sondern auch ihren Typ. So ist z. B. der Text „12“ nicht identisch mit der Zahl 12.

Um von einer starren, d. h. immer gleichen Reihenfolge bei der Programmausführung abweichen zu können, bieten alle Programmiersprachen die Möglichkeit, über Fallunterscheidungen situationsabhängig verschiedene Dinge zu tun oder bestimmte Befehle in Schleifen mehrfach auszuführen. Fallunterscheidungen und Schleifen werten Bedingungen aus: Das sind logische Ausdrücke, die entweder wahr oder falsch sind. Die Schleifen kommen in verschiedenen Varianten vor.

Die hier vorgestellten Elemente sind ausreichend, um die meisten Programmieraufgaben bewältigen zu können.

4.3 Einleitung

Um einen Rechner sinnvoll nutzen zu können, verwenden Sie für diese Maschine erstellte Programme. Diese bestehen aus Anweisungen, die der Rechner abarbeitet und so z. B. ein Berechnungsergebnis liefert. Programme lösen Probleme, die ohne die Hilfe des Rechners nur schwierig oder in nicht absehbarer Zeit zu bewältigen sind. Ein Programm wird in einer Programmiersprache geschrieben, die das Mittel der Kommunikation zwischen Programmierer (Mensch) und Rechner (Maschine) ist. Es gibt eine Vielzahl von Programmiersprachen die spezielle Eigenschaften und Funktionalitäten besitzen. Die Wichtigsten stellen wir im Verlauf von Modul M104 - Programmieren im Forensik-Umfeld vor.

4.4 Algorithmen

Nicht jedes Problem oder jede Aufgabe kann mit einem Rechner bzw. Programm gelöst werden. Es wird zuerst ein Konzept – eine sogenannte Spezifikation – entworfen, das auf seine Realisierbarkeit ausgewertet und anschließend als Programm umgesetzt (implementiert) wird. Der entstandene Entwurf wird als Algorithmus bezeichnet.

Studienbrief 5 ITSicherheit

5.1 Lernergebnisse

Im Studienbrief 5 „ITSicherheit“ lernen Sie grundlegende Begriffe der IT-Sicherheit kennen und können Bedrohungen erklären und einordnen. Dadurch können Sie Schwachstellen einschätzen und erkennen, welche Sicherheitsmaßnahmen in welchen Situationen relevant sind.

5.2 Advance Organizer

Im folgenden Studienbrief werden Ihnen die verschiedenen Themengebiete der IT-Sicherheit erklärt und welche Motivationen hinter den Angriffen stecken. Mit unterschiedlichen Beispielen werden einige Szenarien erläutert, um Bedrohungen und Sicherheitsmaßnahmen besser einschätzen zu können.

5.3 Einführung

IT-Lösungen

Das Leben im 21. Jahrhundert ist ohne Informations- und Kommunikationstechnik kaum mehr vorstellbar. Der schnelle Austausch digital gespeicherter Informationen in großen Netzwerken und eine wachsende Zahl von Übertragungswegen, das sind die zentralen Merkmale unserer Informationsgesellschaft, die in den nächsten Jahren mit Wireless LAN, LTE und anderen Breitbandkanälen auch zunehmend mobiler und in immer mehr Geräten integriert werden wird. Arbeits- und Geschäftsprozesse basieren immer stärker auf IT-Lösungen, daher sind Informationen ein wesentlicher Wert für Unternehmen und Behörden und müssen angemessen geschützt werden. bit bsi [b]

Sicherheit ist ein Grundbedürfnis des Menschen – und damit unserer Gesellschaft. Gerade in Zeiten von Globalisierung, steigender Mobilität und wachsender Abhängigkeit der Industrienationen von Informations- und Kommunikationstechnik nimmt das Sicherheitsbedürfnis immer mehr zu. Die Sicherheit und Zuverlässigkeit der Informations- und Kommunikationstechnik wird deshalb ebenso wie der vertrauenswürdige Umgang mit Informationen immer wichtiger. Unzureichend geschützte Informationen stellen einen häufig unterschätzten Risikofaktor dar, der für manche Institutionen existenzbedrohend sein kann. bit bsi [b]

Die Frage der Sicherheit von Informations- und Kommunikationsbeziehungen entwickelt sich daher immer mehr zu einer Schlüsselkategorie für die Entwicklung von neuen Systemen. Vor allem der wirtschaftliche Erfolg von Unternehmen hängt davon ab, inwieweit es gelingt, die internen Datenbestände oder die externe Kommunikation gegen Datenverlust oder Datenmissbrauch zu schützen. Umgekehrt können sich echte oder vermeintliche Sicherheitsprobleme zu einer zentralen Barriere für die wirtschaftliche Nutzung des Internets entwickeln. bit bsi [b]

Wachsende Verwundbarkeit und die Gefahr massiver wirtschaftlicher Schäden in Folge von Risiken bei der Informationsverarbeitung erhöhen den Handlungsdruck, durch aktives Informationssicherheitsmanagement Schäden zu verhindern und das Restrisiko zu minimieren. In der Praxis ist es aber meistens schwierig, ein angemessenes Sicherheitsniveau zu erreichen und aufrecht zu erhalten. Die Gründe dafür sind vielfältig: fehlende Ressourcen, zu knappe Budgets und nicht zuletzt die steigende Komplexität der IT-Systeme. Die Verantwortung beschränkt sich keineswegs auf die jeweiligen IT-Fachabteilungen, vielmehr muss die IT-Sicherheit im kompletten Unternehmen verankert sein. bit bsi [b]

5.6 Übungen

Bei dem Angriffsszenario BadUSB werden USB-Geräte so manipuliert, dass sie eine andere Funktion als vorgesehen ausführen. Damit kann zum Beispiel ein USB-Stick als Tastatur fungieren und so beliebige Befehle einschleusen. Um diesen Angriff nachzustellen, verwenden wir das Arduino Entwicklungsboard Teensy 3.2. Mit diesem Board kann eine automatische Tastatur simuliert werden.

Installation der Software
Laden Sie zuerst die kostenlose Anwendung „Arduino Software (IDE)“ von der offiziellen Website[3] herunter und installieren Sie diese auf Ihrem Rechner. Laden Sie anschließend die Erweiterung Teensyduino[4] herunter und installieren Sie diese ebenfalls.

Konfiguration
Die folgenden Konfigurationen müssen noch vorgenommen werden: + Arduino Software öffnen und unter „Werkzeug“ -> Platine „Teensy 3.1“ auswählen + Ebenso unter „Werkzeug“ -> USB Type „Keyboard“ und Keyboard Layout „Deutsch“ wählen

Einstieg
Auf der offiziellen Seite[5] finden Sie viele Tutorials und Beispiele die sie verwenden können. Die Programmierung selbst ist durch die IDE sehr abstrahiert, wobei technische Details weitgehend verborgen werden und weiter Bibliotheken automatisch eingebunden werden. Unter dem Menüpunkt „Datei“ > „Beispiele“ > „Teensy“ finden Sie zudem viele Beispiele die Sie für die Aufgaben adaptieren können.

Hilfe zum Einstieg
Da es gerade Anfangs schnell vorkommt, dass die Ausführung eines Skriptes zu unerwünschten Effekten führt (oder einfach zu schnell endet), ist es hilfreich dessen Start (bzw. einzelne Schritte) manuell auszulösen. Dafür kann z.B. die Taste NUM-LOCK verwendet werden. Ihr Status kann von einer Tastatur ausgelesen werden. Somit können Sie die Ausfürhung Ihres Skriptes anhalten und so die Auswirkung einzelner Schritte überprüfen. Dazu können Sie nachfolgenden Quelltext als Grundlage nutzen.

Ausgeführt werden diese Schritte:

1. Warten, bis Treiber geladen sind (Funktion: waitForDetection())
2. Warten auf Betätigung von NUM-LOCK (Funktion: waitForNumLock())
3. Öffnen eines Editors (Notepad.exe)
4. Warten auf Betätigung von NUM-LOCK
5. Eingabe von "Hallo "
6. Warten auf Betätigung von NUM-LOCK
7. Eingabe von "Welt"

Quelltext 5.1: Warten auf NUM-LOCK

```
1 #include "Keyboard.h"
2 #include <stdio.h>
```

Q

[3] hhttps://www.arduino.cc/en/Main/Software
[4] https://www.pjrc.com/teensy/td_download.html
[5] https://www.pjrc.com/teensy/teensyduino.html

```
3 #define caps 1
4 #define num 0
5
6 void setup() {
7   Keyboard.begin();
8   waitForDetection();
9   waitForNumLock();
10  pressCombination(KEY_R, MODIFIERKEY_GUI);
11  delay(100);
12  Keyboard.println("notepad.exe");
13  waitForNumLock();
14  Keyboard.print("Hello ");
15  waitForNumLock();
16  Keyboard.println("World");
17 }
18
19 void loop() {
20  delay(5000);
21 }
22
23 void waitForNumLock(){
24  boolean numLockState = false;
25  do{
26    numLockState = readNumLock();
27    delay(50);
28  }while(numLockState == readNumLock());
29 }
30
31 boolean readNumLock(){
32  return (keyboard_leds & (1<<num));
33 }
34
35 void waitForDetection(){
36  boolean numState = false;
37  do{
38    numState = readNumLock();
39    pressCombination(KEY_NUM_LOCK, 0);
40    delay(100);
41  }while(numState == readNumLock());
42  delay(100);
43 }
44
45
46 void pressCombination(int key, int modifier) {
47  Keyboard.set_modifier(modifier);
48  Keyboard.send_now();
49  Keyboard.set_key1(key);
50  Keyboard.send_now();
51  delay(20);
52  Keyboard.set_modifier(0);
53  Keyboard.set_key1(0);
54  Keyboard.send_now();
55 }
```

Die Funktion waitForDetection() bedient sich einer ähnlichen Vorgehensweise.

Dabei wird die Taste NUM-LOCK betätigt und kurz darauf deren Status ausgelesen. Hat sich der Wert geändert, wurde das Teensy vom Rechner erkannt. Falls es noch nicht erkannt wurde, konnte der Status nicht geändert/ausgelesen werden. Danach wird der Vorgang solange wiederholt, bis eine Änderung möglich ist.

Lösen Sie nun die folgenden Aufgaben:
Hinweis Bei der Bearbeitung der Übung haben Sie folgende Möglichkeiten:

- Die Aufgaben 1-10
- Aufgabe 11 und 3 selbstgewählte aus den Aufgaben 1-10

Übung 5.1: Teensy - Blinkende LED

Steuern Sie die integrierte LED des Teensy Boards an und lassen sie diese in unterschiedlichen Frequenzen blinken.

Ü

Übung 5.2: Teensy - Maus (positionieren)

Positionieren Sie den Mauszeiger in der Mitte des Bildschirms.

Ü

Übung 5.3: Teensy - Maus (bewegen)

Erstellen Sie ein Script welches den Mauszeiger kontinuierlich verschiebt – z.B. im Kreis.

Ü

Übung 5.4: Teensy - Maus (scrollen)

Schreiben Sie ein Script welches alle 500ms einen Scroll-Vorgang ausführt.

Ü

Übung 5.5: Teensy - Tastaturausgabe

Geben Sie mit dem Teensy automatisch „Hello World“ aus.

Ü

Übung 5.6: Teensy - Ausführen-Dialog aufrufen

Rufen Sie den Ausführen-Dialog mit der dazugehörigen Tastenkombination auf.

Ü

Übung 5.7: Teensy - Internet Explorer starten

Starten Sie den Internet Explorer über den „Ausführen“ Dialog von Windows.

Ü

Ü

Übung 5.8: Teensy - Website aufrufen

Starten Sie wieder den Internet Explorer und rufen Sie dabei eine bestimmte Website auf.

Ü

Übung 5.9: Teensy - Datei erstellen

Öffnen Sie den Text-Editor, schreiben Sie einen beliebigen Inhalt hinein und speichern Sie diese Datei ab.

Ü

Übung 5.10: Teensy - Datei herunterladen und ausführen

Laden Sie eine ausführbare Datei herunter und führen sie diese nach dem Download aus.

Ü

Übung 5.11: Teensy - Langes Skript in Powershell ausführen

Diese Aufgabe ist Optional.
Finden Sie eine Lösung, die folgendes abdeckt:

1. Öffnen einer Powershell
2. Erkennen, wann die Powershell bereit ist (manchmal dauert der Startvorgang einige Sekunden)
3. Sicherstellen, dass die Powershell im Vordergrund ist, wenn das Teensy beginnt, ein Skript einzugeben
4. Das Skript auf dem Rechner speichert und anzeigt (Ein Ausführen wird nicht gefordert, d.h. das Skript selbst muss keinen Sinn ergeben und kann aus mehrern Füllzeilen bestehen)

Hierzu empfielt es sich, beim Aufruf von Powershell bereits einige Befehle mitzugeben.
Beispielweise so:
powershell -noexit -command "Befehl1";"Befehl2"
Die Option noexit kann zusätzlich angegeben werden. Sie führt dazu, dass sich das Fenster nach Beendigung der Befehle nicht schließt.

Verzeichnisse

I. Abbildungen

II. Beispiele

III. Definitionen

IV. Exkurse

V. Kontrollaufgaben

VI. Tabellen

VII. Literatur

Runtime-Basic - Beschreibung-Kurz: CPU. http://runtimebasic.net/Assembler:Funktionen:Beschreibung-Kurz-CPU. (Stand: 10.07.2015).

Sicherheit für Systeme und Netze in Unternehmen. https://www.bitkom.org/Publikationen/2003/Leitfaden/Leitfaden-Sicherheit-fuer-Systeme-und-Netze-in-Unternehmen/ACF897.pdf. (Stand: 29.06.2016).

Die Lage der IT-Sicherheit. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile, a. (Stand: 04.07.2016).

Leitfaden Informationssicherheit. http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile, b. (Stand: 29.06.2016).

Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf?__blob=publicationFile&v=2, c. (Stand: 30.06.2016).

i8086/88 Referenz. http://www.i8086.de/. (Stand: 10.07.2015).

Zwei Tage ganz ohne Computerverbindung. http://newsv1.orf.at/090208-34794/. (Stand: 11.07.2016).

Locky Ransomware Is Becoming More Sophisticated - Cybercriminals Continue Email Campaign Innovation. https://www.proofpoint.com/tw/threat-insight/post/Locky-Ransomware-Cybercriminals-Introduce-New-RockLoader-Malware. (Stand: 12.07.2016).

Conficker-Wurm: Bundeswehr kämpft gegen Viren-Befall. http://www.spiegel.de/netzwelt/web/conficker-wurm-bundeswehr-kaempft-gegen-viren-befall-a-607567.html. (Stand: 11.07.2016).

Reverse Engineering. http://www.informatik.uni-bremen.de/gdpa/part3_d/p3re.htm. (Stand: 11.07.2016).

Sicherheit von Webanwendungen - Maßnahmenkatalog und Best Practices, August 2006. URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/WebSec/WebSec_pdf.pdf?__blob=publicationFile.

Passwortklau für Dummies, August 2007a. URL http://heise.de/-270910.

Viele Banken-Seiten weiter unzureichend gegen Missbrauch gesichert [Update], Juni 2007b. URL http://heise.de/-143847.

CSS / XSS – Angriff (Cross Site Scripting) - eine Analyse, August 2008. URL http://www.erich-kachel.de/?p=181.

Daniel Bachfeld. F-Secure: Jetzt neun Millionen Windows-PCs mit Conficker-Wurm befallen. http://www.heise.de/security/meldung/F-Secure-Jetzt-neun-Millionen-Windows-PCs-mit-Conficker-Wurm-befallen-199425.html. (Stand: 11.07.2016).

M. Becker, R. Haberfellner, G. Liebetrau, and S.P.D. Vössner. *EDV-Wissen für Anwender: Das Informatik-Handbuch für die Praxis*. io Verlag, 2004. ISBN 9783857437175.

Hanno Böck. Pseudowissenschaftliche Zahlenspiele. http://www.golem.de/news/karsten-nohl-usb-geraete-aller-typen-lassen-sich-fuer-badusb-nutzen-1411-110520.html. (Stand: 14.07.2016).

Claudia Eckert. *IT-Sicherheit - Konzepte - Verfahren - Protokolle*. Oldenbourg, Deutschland, überarbeitete und erweiterte auflage edition, 2013. ISBN 978-3486721386.

Ronald Eikenberg. Virenverseuchte Dia-Scanner bei Tchibo verkauft. http://www.heise.de/security/meldung/Virenverseuchte-Dia-Scanner-bei-Tchibo-verkauft-1776500.html. (Stand: 11.07.2016).

Bundesamt für Verfassungsschutz für die Verfassungsschutzbehörden in Bund und Ländern. Wirtschaftsspionage - Risiko für Ihr Unternehmen. http://www.uni-stuttgart.de/soz/oi/publikationen/soi_2013_2_Dolata_Schrape_Zwischen_Individuum_und_Organisation.pdf, 06 2008. (Stand: 04.07.2016).

Dr. Sandro Gaycken. Einführung Cyberwar. https://www.inf.fu-berlin.de/groups/ag-si/pub/Cyberwar_SB1-5_V160114.pdf, 11 2015. (Stand: 04.07.2016).

Hauke Gierow. Millionen Kundendaten gehackt. http://www.golem.de/news/t-mobile-usa-millionen-kundendaten-gehackt-1510-116647.html. (Stand: 12.07.2016).

Heinz-Peter Gumm and Manfred Sommer. *Einführung in die Informatik*. Oldenbourg Verlag, München, vollständig überarbeitete auflage edition, 2012. ISBN 978-3-486-70641-3.

Helmut Herold, Bruno Lurz, and Jürgen Wohlrab. *Grundlagen der Informatik - praktisch, technisch, theoretisch*. Pearson Studium, München, 1. aufl. edition, 2006. ISBN 978-3-827-37216-1.

Christian Horn, Immo O. Kerner, and Peter Forbig. *Lehr- und Übungsbuch Informatik 1*. Hanser Fachbuchverlag, 2003. ISBN 3446225439.

Thomas Jüngling. Computerviren stecken schon in ganz neuer Hardware. http://www.welt.de/wirtschaft/webwelt/article140195369/Computerviren-stecken-schon-in-ganz-neuer-Hardware.html. (Stand: 11.07.2016).

S. Kersken. *Handbuch für Fachinformatiker*. Galileo Computing. Galileo Press, 2005. ISBN 9783898426688.

Jürgen Kuri. Milliardenschäden für Firmen durch Wirtschaftsspione im Netz. http://www.heise.de/security/meldung/Milliardenschaeden-fuer-Firmen-durch-Wirtschaftsspione-im-Netz-2482756.html, 12 2014. (Stand: 04.07.2016).

Hans-Peter Königs. *IT-Risikomanagement mit System - Praxisorientiertes Management von Informationssicherheits- und IT-Risiken*. Springer-Verlag, Berlin Heidelberg New York, 4. aufl. edition, 2013. ISBN 978-3-834-82165-2.

Isabel Münch. Deutscher Verband für Post, Informationstechnologie und Telekommunikation e.V. http://www.dvpt.de/uploads_extern/dvpt/2014/mmf_2014_bsi.pdf. (Stand: 30.06.2016).

Karsten Nohl. USB-Geräte aller Typen lassen sich für BadUSB nutzen. http://www.golem.de/news/sicherheitsluecken-pseudowissenschaftliche-zahlenspiele-1503-113058.html. (Stand: 13.07.2016).

Zeit Online. Das Ausmaß des TV-Hacks macht ihn besonders. http://www.zeit.de/digital/datenschutz/2015-04/hacker-tv5monde-cyber-kalifat, a. (Stand: 08.07.2016).

Zeit Online. Sender zeigte unfreiwillig Redaktionspasswörter. http://www.zeit.de/digital/datenschutz/2015-04/tv5-hack-youtube-account, b. (Stand: 08.07.2016).

Patricia. Browser And Email: Top Attack Channels For Malware Delivery. https://labsblog.f-secure.com/2016/04/28/browser-and-email-top-attack-channels-for-malware-delivery/. (Stand: 12.07.2016).

Klaus Pommerening. Kryptologie - Zeichenhäufigkeiten in Deutsch. http://www.staff.uni-mainz.de/pommeren/Kryptologie/Klassisch/1_Monoalph/deutsch.html. (Stand: 12.07.2016).

Santiago Pontiroli. Social Engineering: Das Hacken des menschlichen Betriebssystems. https://blog.kaspersky.de/social-engineering-das-hacken-des-menschlichen-betriebssystems/2186/. (Stand: 07.07.2016).

Dipl.-Ing. Florian Bache Prof. Dr.-Ing. Tim Güneysu. BadUSB - Angriffsvektor USB-Anschluss. https://www.informatik.uni-bremen.de/cms/media.php/75/badusb.pdf. (Stand: 12.07.2016).

Andreas Koke Ramon Mörl. BadUSB, aktuelle USB Exploits und Schutzmechanismen. https://itwatch.de/content/download/1475/8588/file/BadUSB_aktuelle%20USB%20Exploits%20und%20Schutzmechanismen.pdf. (Stand: 12.07.2016).

M. Roming and J. Rohde. *Assembler: Grundlagen der Programmierung*. mitp, 2006. ISBN 9783826614699.

Wolfram Schiffmann, Helmut Bähring, and Udo Hönig. *Technische Informatik 3 - Grundlagen Der Pc-Technologie*. Springer DE, Berlin, 2011. aufl. edition, 2011. ISBN 978-3-642-16812-3.

Dennis Schirrmacher. Erpressungs-Trojaner - Geschäftsmodell: Ihre Daten als Geisel. http://www.heise.de/ct/ausgabe/2016-7-Geschaeftsmodell-Ihre-Daten-als-Geisel-3134538.html. (Stand: 12.07.2016).

Oliver Schonschek. Die Motivation der Hacker. https://www.datenschutz-praxis.de/fachartikel/die-motivation-der-hacker/. (Stand: 30.06.2016).

SCO. The Universal Application Server. Technical report, The Santa Cruz Operation Technical White Paper, Tarantella, Juli 1997.

Claude Elwood Shannon. A Mathematical Theory of Communication. Technical report, Bell System, Juli, Oktober 1948.

Daniel AJ Sokolov. Islamisten hacken TV5. http://www.heise.de/newsticker/meldung/Islamisten-hacken-TV5-2597578.html. (Stand: 08.07.2016).

Dipl. Oec. Michael Phan und Dipl. Inform (FH) Thomas Stasch. So arbeiten Hacker und Cyber-Kriminelle. http://www.tecchannel.de/sicherheit/management/3195799/bedrohungen_erkennen_und_abwehren_so_arbeiten_hacker_und_cyber_kriminelle/index2.html. (Stand: 01.07.2016).

Andrew S. Tanenbaum. *Computerarchitektur*. Pearson Studium, 2005. ISBN 3827371511.

Andrew S. Tanenbaum. *Moderne Betriebssysteme*. Pearson Deutschland GmbH, München, 3. aktualisierte auflage edition, 2009. ISBN 978-3-827-37342-7.

Jan Ulrich Dolata. Zwischen Individuum und Organisation - Neue kollektive Akteure und Handlungskonstellationen im Internet. http://www.uni-stuttgart.de/soz/oi/publikationen/soi_2013_2_Dolata_Schrape_Zwischen_Individuum_und_Organisation.pdf. (Stand: 04.07.2016).

Max Goncharov und Robert McArdle Vincenzo Ciancaglini, Marco Balduzzi. Deep Web und Cybercrime. http://www.trendmicro.de/media/wp/deep-web-and-cybercrime-whitepaper-de.pdf. (Stand: 08.07.2016).

Holger Vogelsang and Peter A. Henning. *Taschenbuch Programmiersprachen*. Hanser Fachbuchverlag, 2007. ISBN 3446407448.

VIII. ASCII-Tabelle

Dez	Hex	Okt	Zeichen	Dez	Hex	Okt	Zeichen
0	0x00	000	NUL	32	0x20	040	SP
1	0x01	001	SOH	33	0x21	041	!
2	0x02	002	STX	34	0x22	042	“
3	0x03	003	ETX	35	0x23	043	#
4	0x04	004	EOT	36	0x24	044	$
5	0x05	005	ENQ	37	0x25	045	%
6	0x06	006	ACK	38	0x26	046	&
7	0x07	007	BEL	39	0x27	047	’
8	0x08	010	BS	40	0x28	050	(
9	0x09	011	TAB	41	0x29	051	)
10	0x0A	012	LF	42	0x2A	052	*
11	0x0B	013	VT	43	0x2B	053	+
12	0x0C	014	FF	44	0x2C	054	,
13	0x0D	015	CR	45	0x2D	055	-
14	0x0E	016	SO	46	0x2E	056	.
15	0x0F	017	SI	47	0x2F	057	/
16	0x10	020	DLE	48	0x30	060	0
17	0x11	021	DC1	49	0x31	061	1
18	0x12	022	DC2	50	0x32	062	2
19	0x13	023	DC3	51	0x33	063	3
20	0x14	024	DC4	52	0x34	064	4
21	0x15	025	NAK	53	0x35	065	5
22	0x16	026	SYN	54	0x36	066	6
23	0x17	027	ETB	55	0x37	067	7
24	0x18	030	CAN	56	0x38	070	8
25	0x19	031	EM	57	0x39	071	9
26	0x1A	032	SUB	58	0x3A	072	:
27	0x1B	033	ESC	59	0x3B	073	;
28	0x1C	034	FS	60	0x3C	074	«
29	0x1D	035	GS	61	0x3D	075	=
30	0x1E	036	RS	62	0x3E	076	»
31	0x1F	037	US	63	0x3F	077	?

Dez	Hex	Okt	Zeichen	Dez	Hex	Okt	Zeichen
64	0x40	100	@	96	0x60	140	‘
65	0x41	101	A	97	0x61	141	a
66	0x42	102	B	98	0x62	142	b
67	0x43	103	C	99	0x63	143	c
68	0x44	104	D	100	0x64	144	d
69	0x45	105	E	101	0x65	145	e
70	0x46	106	F	102	0x66	146	f
71	0x47	107	G	103	0x67	147	g
72	0x48	110	H	104	0x68	150	h
73	0x49	111	I	105	0x69	151	i
74	0x4A	112	J	106	0x6A	152	j
75	0x4B	113	K	107	0x6B	153	k
76	0x4C	114	L	108	0x6C	154	l
77	0x4D	115	M	109	0x6D	155	m
78	0x4E	116	N	110	0x6E	156	n
79	0x4F	117	O	111	0x6F	157	o
80	0x50	120	P	112	0x70	160	p
81	0x51	121	Q	113	0x71	161	q
82	0x52	122	R	114	0x72	162	r
83	0x53	123	S	115	0x73	163	s
84	0x54	124	T	116	0x74	164	t
85	0x55	125	U	117	0x75	165	u
86	0x56	126	V	118	0x76	166	v
87	0x57	127	W	119	0x77	167	w
88	0x58	130	X	120	0x78	170	x
89	0x59	131	Y	121	0x79	171	y
90	0x5A	132	Z	122	0x7A	172	z
91	0x5B	133	[	123	0x7B	173	{
92	0x5C	134	\	124	0x7C	174	|
93	0x5D	135	]	125	0x7D	175	}
94	0x5E	136	ˆ	126	0x7E	176	-
95	0x5F	137	_	127	0x7F	177	DEL

Stichwörter

Open C³S
Open Competence Center for Cyber Security

Fort- und Weiterbildung

Neue Bedrohungszenarien stellen Sicherheitsexperten und IT-Verantwortliche in Unternehmen und einschlägigen Behörden vor immer größere Herausforderungen. Neue Technologien und Anwendungen erfordern zusätzliches Know-how und personelle Ressourcen.

Zur Erhöhung des Fachkräftepools und um neues Forschungswissen schnell in die Praxis zu integrieren, haben sich die im Bereich lehrenden und forschenden Verbundpartner zum Ziel gesetzt, ein hochschuloffenes transdisziplinäres Weiterbildungsprogramm im Sektor Cyber Security zu entwickeln. Auf der Grundlage kooperativer Strukturen werden wissenschaftliche Weiterbildungsmodule im Verbund zu hochschulübergreifenden Modulpaketen und abschlussorientierten Ausbildungslinien konzipiert und im laufenden Studienbetrieb empirisch getestet.

Die Initiative soll High Potentials mit und ohne formale Hochschulzugangsberechtigung über innovative Weiterbildungsangebote (vom Zertifikat bis zum Masterprogramm) zu Sicherheitsexperten aus- und fortbilden. Hierzu werden innovative sektorale Lösungen zur Optimierung der Durchlässigkeit von berulicher und hoch- schulischer Bildung entwickelt und für eine erfolgreiche Implementierung vorbereitet. Unter prominenter Beteiligung einschlägiger Verbände, der Industrie sowie Sicherheits und Ermittlungsbehörden verfolgt die Initiative das Ziel, im deutschsprachigen Raum eine Generation von Fachkräften wissenschaftlich aus- und weiterzubilden, die unser Internet schützen kann.

Open Competence Center for Cyber Security

Open C³S ist aus dem Verbundvorhabens Open Competence Center for Cyber Security entstanden. Das Gesamtziel des Programms war die Entwicklung eines hochschuloffenen transdisziplinären Programms wissenschaftlicher Weiterbildung im Sektor Cyber Security. Das Bundesministerium für Bildung und Forschung (BMBF) fördert das Großprojekt im Rahmen des Wettbewerbs „Aufstieg durch Bildung: offene Hochschulen“, der aus BMBF-Mitteln und dem Europäischen Sozialfonds finanziert wird.

Neun in Forschung und Lehre renommierte Hochschulen und Universitäten aus dem gesamten Bundesgebiet haben sich zum Ziel gesetzt, Online-Studiengänge auf dem Gebiet der Cybersicherheit zu entwickeln. Dieses Konzept soll den Studierenden ermöglichen, sich berufsbegleitend auf hohem Niveau wissenschaftliche Qualifikationen anzueignen und akademische Abschlüsse zu erlangen. Beruflich erworbene Kompetenzen können eingebracht werden. Die Bezeichnung „Open“ steht auch für die Öffnung des Zugangs zu akademischer Bildung ohne klassischen Hochschulzugang.

Mission der Initiative ist es, dringend benötigte Sicherheitsexperten aus- und fortzubilden, um mit einer sicheren IT-Infrastruktur die Informationsgesellschaft in Deutschland und darüber hinaus zu stärken.

Umsetzungsnahes Wissen ist ein wesentlicher Schlüssel um der wachsenden digitalen Bedrohung zu begegnen. Solange wir nicht in der Lage sind, Systeme hinreichend zu härten, Netzwerke sicher zu designen und Software sicher zu entwickeln, bleiben wir anfällig für kriminelle Aktivitäten. Unser Ziel ist es, die Mitarbeiter von heute zu Sicherheitsexperten und Führungskräften von morgen auszubilden und dafür zu sorgen, dass sich die Zahl und die Fertigkeiten dieser Experten nachhaltig erhöht.

Weitere Informationen zu Open C³S: https://open-c3s.de

Z201 Applied Computer Systems

Das Modul „Applied Computer Systems“ bietet entsprechendes Basiswissen, umweiterführende Thematiken der Informatik besser verstehen zu können. Ihnen als Lernenden werden im ersten Studienbrief „Informationsverarbeitung im Computer“ Grundlagen des Bereiches Informationsverarbeitung vermittelt. Sie werden insbesondere mit computerinternen Zahlen- und Stellenwertsystemen sowie der Zeichencodierung (ASCII, Unicode) und logischen Operatoren vertraut gemacht.

Im zweiten Studienbrief „Rechnersysteme“ des Moduls erhalten Sie einen Einblick in den Aufbau von Computersystemen und deren Bestandteile. Sie sollen Kenntnisse über grundlegende Prinzipien der Datenund Informationsverarbeitung als abstraktes Schema eines Rechners sowie die elementare Struktur und das Zusammenwirken verschiedener Bestandteile von Computern erwerben.

Im dritten Studienbrief „Rechnernetzwerke“ des Moduls werden Grundverständnisse für Netzwerke und die elektronische Kommunikation vermittelt. Zunächst erfassen Sie Begriffe der Netzwerktechnik und im weiteren Verlauf erlangen Sie insbesondere Kenntnisse über das Internet, Adressierung und Kommunikationsabläufe.

Im vierten Studienbrief „Einführung in die Programmierung“ wird in die Grundlagen der Programmierung eingeführt. Anhand von abstrakten allgemeingültigen Aussagen werden verschiedene Konzepte vermittelt.

Der letzte Studienbrief „ITSicherheit“ vermittelt einen allgemeinen Überblick über die grundlegenden Begriffe der IT-Sicherheit und stellt exemplarisch einige Sicherheitsvorfälle vor. Dadurch können Schwachstellen eingeschätzt werden und welche Bereiche eines Systems verletzt worden sind.

Nach Durcharbeiten des Moduls sind Sie mit Fachtermini vertraut und besitzen grundlegende Kenntnisse inden Bereichen Informationsverarbeitung, Computerhardware, Programmierung und IT-Sicherheit.

Zertifikatsprogramm

Die Zertifikatsmodule auf wissenschaftlichem Niveau und mit hohem Praxisbezug bilden ein passgenaues Angebot an Qualifikation und Spezialisierung in der nebenberuflichen Weiterbildung. Damit können einzelne Module nebenberuflich studiert werden. Durch die Vergabe von ECTS-Punkten können sie auf ein Studium angerechnet werden.

https://zertifikatsprogramm.de