Informationssicherheit und IT-Forensik

1-01 – Einführung, korrigiert: 13.02.2023

Kurze Begrüßung und erste Schritte

- Mein Name: Martin Wundram
- Lehrbeauftragter der Universität zu Köln
- Fünfter Vorlesungsdurchlauf
- Bitte notieren Sie kurz Ihre Einschätzung zu folgenden Fragen (5 Minuten):
  - Haben wir noch die volle Kontrolle über unsere Daten?
  - Haben Sie etwas (Daten?) zu verbergen?
  - Was ist Sicherheit?

Kurze Begrüßung und erste Schritte

- Keine Aufzeichnung dieser Vorlesung/Übung
- Aufzeichnung für Studierende untersagt!
- Vorteil: wir können „frei“ miteinander diskutieren
- Wir stellen eine komplette Aufzeichnung aus 2020 in Ilias online (inhaltlich im Wesentlichen 1:1 zu aktueller Version)

Kurze Begrüßung und erste Schritte

Rückblick 2019, 2020, 2021, 2022

- 2019: 22 Zuhörer und genau so viele Klausurteilnehmer
- Der Notendurchschnitt des ersten Klausurtermins liegt bei 2,5 und der des zweiten Termins bei 1,8
- Evaluation durch Teilnehmer
  - 15 ausgefüllte Fragebögen
  - Didaktische Qualität der Vorlesung:1,3
  - Wissenschaftliche Qualität:1,6
  - Atmosphärische Qualität: 1,1
  - Gesamtbeurteilung des Moduls:1,1
  - Dafür auch vielen Dank!

- 2020: Knapp 40 Zuhörer, 31 Prüfungsteilnehmer
- Notendurchschnitt erster Termin: 2,38 (Median 2,15)
- Evaluation durch Teilnehmer
  - Gesamtbeurteilung des Moduls: 1,1
  - Dafür auch vielen Dank!

- 2021
  - ~80 Zuhörer, 69 „vollständige“ Prüfungsteilnehmer
  - Durchschnitt 2,69 (Median 2,3)
- 2022
  - Knapp 100 Zuhörer, 69 „vollständige“ Prüfungsteilnehmer
  - Durchschnitt 2,02 (Median 1,7)

Kurze Begrüßung und erste Schritte

2022/2023

- Weiterhin „Corona-Modus“
  - Zu Beginn: Online-Vorlesung und Online-Übung
  - 2023: Voraussichtlich im Hörsaal vor Ort
  - Klausur vermutlich auch vor Ort, aber Portfolio-Projekt von Zuhause
- Alt: Kooperation mit der Verwaltungs u. Wirtschafts-Akademie Köln (VWA Köln)
  - Das war (erfolgreich) in 2021/2022
  - Mangels Studierenden dieses Mal wieder „nur“ Uni Köln
  - Macht für Uni-Köln-Studierende aber auch keinen Unterschied

Braingym: sicher?

Braingym: wirklich sicher?

Scheinbar sicher!

Das mehrfach unsichere Vorhängeschloss

- Es gibt einzelne Techniken (Schloss, Bügel, Tür, …) die für sich genommen sicher oder unsicher sein können (gemessen am Schutzbedarf)
- Diese müssen jedoch implementiert werden (Auswahl, Planung, Montage, Test).
- Bei jeder dieser Phasen kann etwas schief gehen, so dass im Ergebnis trotz sicherer Technik ein unsicheres Gesamtsystem entsteht

- Erkannte Probleme:
  - Beschlag lässt sich abschrauben
    - falsche Auswahl
  - Schloss lässt sich horizontal drehen, so kann der Riegel ohne Schlossöffnung so weit geöffnet werden, dass er nicht mehr sperrt
    - Fehlplanung und/oder Fehlmontage
  - Gesamtsystem ist damit nicht wirksam gegen die (mutmaßlich zu verhindernden) Bedrohungen
    - nicht ausreichend getestet

Sicherheit „damals“

- Wirtschaftsinformatik I, Hansen, 5. Auflage, 1987 (1. Auflage 1978), 767 Seiten
- *„Maßnahmen zur Datensicherheit […] sollen die jederzeitige Vollständigkeit und Korrektheit der Daten in der EDVA gewährleisten“* (5 Seiten, inkl. „Transaktionen“)
- *„Der Datenschutz […] soll den unbefugten Gebrauch von Daten verhindern. Zu schützen sind dabei die davon Betroffenen“* (5 Seiten, inkl. 2 Seiten zu technischen Maßnahmen und Krypto)

Murphys Gesetz

Und was wir daraus für die Informationssicherheit lernen können

- *„Alles, was schiefgehen kann, wird auch schiefgehen.“,* John W. Campbell Jr.
- *„Zweijähriger fällt in mehr als hundert Meter tiefes Bohrloch - In Spanien ist ein Kleinkind in ein nur 25 Zentimeter breites, 110 Meter tiefes Bohrloch gefallen. In dem Erdloch ist es feucht und kalt, die Retter kämpfen gegen die Zeit.“,* Quelle: spiegel.de (15.01.19)
- Nichts einfach so auf die leichte Schulter nehmen, nicht den Kopf in den Sand stecken, aber auch keine Angst haben
- Risikomanagement ist die Grundmaxime

Murphys Gesetz

Kontrolle behalten sollte ein Grundziel sein

https://www.heise.de/news/Terraria-Stadia-Version-nach-Bann-von-Google-Account-vor-dem-Aus-5049562.html

heise online heise+ An

IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft

TOPTHEMEN: SIGNAL, WHATSAPP & CO. REDDIT AMAZON CORONAVIRUS WINDOWS 10 E-AUTO

heise online ⟩ News ⟩ 02/2021 ⟩ "Terraria": Stadia-Version nach Bann von Google-Account vor dem Aus

"Terraria": Stadia-Version nach Bann von Google-Account vor dem Aus

Die Entwickler des Spiels "Terraria" erheben schwere Vorwürfe gegen Google: Ihr Google-Account sei ohne Begründung gesperrt worden. Nun gibt es Konsequenzen.

Lesezeit: 2 Min. In Pocket speichern 167

- Heise-Meldung vom 09.02.21

und dem Tech-Giganten: Ende Januar hatte Google den Youtube-Account des Indie-Studios gesperrt. Seitdem hat das Studio eigenen Angaben zufolge auch Zugriff auf alle anderen Google-Dienste verloren, darunter Gmail und Google Drive.

Andrew Spinks
@Demilogic

@Google my account has now been disabled for over 3 weeks. I still have no idea why, and after using every resource I have to get this resolved you have done nothing but given me the runaround.

8.2.2021, 06:20:00 via Twitter

powered by

IT-Sicherheit mit Fokus der WI

- Der Fokus für Wirtschaftsinformatiker liegt in Bezug auf IT-Sicherheit typischerweise in erster Linie mehr auf dem WAS (welche Technik im Gesamtsystem verwenden?)
- als auf dem WIE (wie soll eine einzelne Technik neu konstruiert werden?)
- und der Argumentation WARUM (warum diese und nicht andere Technik, warum diese mit den Parametern X, Y, Z).
- Um dies tun zu können, muss ein Wirtschaftsinformatiker in angemessenem Maße auch das WIE verstehen

Leitgedanke

- Sicherheit erfordert von Anfang an und konstant Arbeit und Einsatz
- Sicherheit kann man nicht einfach „einkaufen“
- Das schwächste Glied der Kette bricht
- Noch wichtiger als Modelle, Rahmenwerke, Theorie und Schlagworte ist, angstfrei die Thematik ernst zu nehmen und in den eigenen Alltag angemessen zu integrieren

Fundament dieser Vorlesung

- Wir sind „Architekten“, Verteidiger und Anwender von IT-Systemen
- Wir sind NICHT (illegitime) Angreifer/Täter
- Wir greifen insbesondere nicht die IT-Systeme Anderer an
- Die Beschäftigung mit Angriffstechniken dient dem besseren Verständnis des Themas Sicherheit auf allen Ebenen, damit wir uns besser verteidigen können
- Denn Täter beschäftigen sich ohnehin mit Angriffstechniken und wenden diese auch an
- Dieses Fundament ist keine Worthülse! Jeder Teilnehmer dieser Vorlesung muss sich dazu bekennen, das gewonnene Wissen rechtlich und ethisch einwandfrei anzuwenden

Agenda

„Corona-Flavor“ mit „Voraussichtlich“ ☺

1. 24.10.22 (Mo) 18:00-19:30
   - Vorlesung (Einführung)
   - Remote/Zoom
2. 07.11.22 (Mo) 18:00-19:30
   - Vorlesung (Grundüberlegungen)
   - Remote/Zoom
3. 23.02.23 (Do) 09:00-18:00
   - Vorlesung (Crypto)
   - Gastvorlesung „Datenschutz/Jura“
   - Übung (Crypto)
   - Vor Ort/Hörsaal

Agenda

„Corona-Flavor“ mit „Voraussichtlich“ ☺

4. 24.02.23 (Fr) 14:00-18:00
   - Tutorium (Crypto)
   - Vorlesung (IPv4/IPv6)
   - Vor Ort/Hörsaal
5. 25.02.23 (Sa) 09:00-18:00 (*Tausch mit Web-Security*)
   - Vorlesung (IT-Forensik)
   - Gastvorlesung „Gut Begutachten“
   - Übung
   - Vor Ort/Hörsaal
6. 02.03.23 (Do) 09:00-18:00 (*Tausch mit IT-Forensik*)
   - Vorlesung (Web-Security)
   - Gastvorlesung „7 Security Sins“
   - Übung
   - Vor Ort/Hörsaal

Agenda

„Corona-Flavor“ mit „Voraussichtlich“ ☺

7. 03.03.23 (Fr) 14:00-18:00:
   - Tutorium „Web-Security“
   - Vorlesung (Incident Response)
   - „Themenpuffer“
   - Vor Ort/Hörsaal
8. 04.03.23 (Sa) 09:00-18:00
   - Vorlesung (Authentifikation, Sicherheitsmodelle, Grundlagen Sicherer Softwareentwicklung)
   - Übung (World-Cafe, Probeklausur, Wiederholungsfragen)
   - Vor Ort/Hörsaal

Agenda

Wichtige Hinweise zur Übung

- Vertiefung der Inhalte aus der Vorlesung
- Praktische Arbeit am PC (z.B. Buffer Overflow, Web-Security)
- Möglichkeit, vertiefende oder wiederholende Fragen zu den Vorlesungsinhalten zu stellen + Diskussion
- Voraussetzung:
  - Kali-Linux (von uns bereitgestellte virtuelle Maschine {bevorzugt!}, oder selbst auf Festplatte/USB-Stick installiert, oder live von USB/DVD gestartet)
    - Benötigt: 64-Bit-i386-CPU, 4 GB RAM
    - Achtung mit ARM-Macs: hier rechtzeitig vorab prüfen, ob Virtual Box mittlerweile gut funktioniert (bei Fragen: fragen)
  - Internet-Uplink ;-)

Kurzvorstellung der Dozenten

Dipl.-Wirt.-Inf. Martin Wundram

- Von der IHK zu Köln öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung, insbesondere IT-Sicherheit und IT-Forensik
- Lehrbeauftragter der Universität zu Köln
- Geschäftsführer der DigiTrace GmbH (Standort Köln: 12 Personen, 11 IT‘ler)
- Kunden von KMU bis börsennotierte Konzerne + Behörden
  - Präventive Projekte: Audits, Penetrationstests, IT-Sicherheitskonzepte, strategische Beratung zu IT-Sicherheit, …
  - Reaktive Projekte: IT-Forensik, Incident Response, eDiscovery, …
  - Sachverständigentätigkeit / Gutachten zu allen Themen der IT
- Natürlich selbst an der Uni Köln Wirtschaftsinformatik studiert ;-)

Kurzvorstellung der Dozenten

M.Sc. Phil Knüfer

- Consultant für IT-Sicherheit und IT-Forensik bei DigiTrace
- Tätigkeitsschwerpunkte: präventive IT-Sicherheit (Penetrationstests, Sicherheitskonzepte), Aufklärung von IT-Sicherheitsvorfällen (Incident Response), IT-Forensik
- 11 Jahre Vollzeit IT-Sicherheit, davon über 5 Jahre berufstätig
  - 11/2016 – heute: DigiTrace GmbH, Köln
  - 2014-2016: Master-Studium IT-Sicherheit, Ruhr-Uni Bochum
  - Seit 2013: Freiberufliche Arbeit im Bereich IT-Sicherheit
  - 2010-2013: Bachelor-Studium IT-Sicherheit, Ruhr-Uni Bochum

Kurzvorstellung der Dozenten

Alexander Neff

- 7. Semester Wirtschaftsinformatik
- 23 Jahre aus Köln
- 2nd Time Tutor
- Hobby Saxophonist

- Merkhilfe: Der Tutor „tutoriert“, ist aber nicht der offizielle Ansprechpartner für alle Anliegen ;-)
- Verbindliche Aussagen insb. Zur Klausur: Martin Wundram

Erreichbarkeit für Fragen und Anmerkungen

Am besten per E-Mail

- martin@wundram.de
- phil.knuefer@rub.de
- aneff1@smail.uni-koeln.de

WICHTIG: Feedback geben

- Bitte geben Sie konstruktives Feedback!
- Nur so können wir Ihre Erwartungen bestmöglich erfüllen
- Z.B. nach einer Einheit oder nach einem Vorlesungs-/Übungstag

NOCH WICHTIGER: Fragen & „Aber“ sagen

Bitte stellen Sie sich kurz vor

- Gern alle die Kamera einschalten (aber kein muss)
- Bitte im Chat kurz die eigene Erwartung an die Vorlesung schreiben
- Gern auch per kurzer Sprachmeldung

Prüfungsmodalitäten

1. Prüfungstermin, Portfolio-Prüfung

- Studierende der Uni Köln:
  - Aktueller Planungsstand: zwei oder drei Teile
    - Klausur
    - Einzelpräsentation eines Fachbegriffes
    - Programmieraufgabe („Lückentext“)
  - Für uns ist das das dritte Mal online (Corona) und das dritte Mal Portfolio
  - Klausurtermin: 21.03.2023 10.00 Uhr bis 11.00 Uhr
  - Portfolioaufgabe
    - Beginn: 24.03.2023
    - Ende/Abgabe: 31.03.2023

Lernziele der Vorlesung

- Nichts ist sicher, question everything
- Sicherheit kostet Geld / Komfort / Freiheit / …
- „Unsere“ Daten haben mittlerweile aus vielen Gründen hohen Wert für Andere
- Das schwächste Glied der Kette bricht. Ein System muss insgesamt sicher sein. Manchmal reicht „ein falsches Bit“, und das ganze System ist unsicher
- Problembewusstsein ist die erste und vielleicht sogar wichtigste Maßnahme der Informationssicherheit
- Sicherheit des Entwurfs / Architektur / „Bauplans“ vs. Sicherheit des konkreten Produktes
- Safety vs. Security
- Kontrolle behalten

Scope und „Flughöhe“ dieser Vorlesung

Motivation aus der Perspektive der WI

- Das Themenfeld Informationssicherheit + IT-Forensik und insbesondere technische Aspekte (IT-Security) werden aus der Sicht der Wirtschaftsinformatik betrachtet
- Viele Themen und Herausforderungen werden lediglich „angerissen“. Das Ziel ist:
  - diese Themen, Problemfelder und Lösungen kurz vorzustellen,
  - damit man als WI‘ler diese später „auf dem Schirm“ hat, erkennen kann, wo man in die Tiefe gehen muss und dies dann fundiert tun kann.
  - Aufbau eines guten Grundverständnisses der Informationssicherheit und Entwicklung von Problemlösungskompetenz
- Viele Themen könnten je in einer eigenen Vorlesung betrachtet werden…

Scope und „Flughöhe“ dieser Vorlesung

Motivation aus der Perspektive der WI

- Warum Security?
- Wie war es früher?
- Wie wird es in Zukunft sein?
- Warum ist Sicherheit Chefsache?

Scope und „Flughöhe“ dieser Vorlesung

Motivation aus der Perspektive der WI

- Was ist zu tun, wenn es mal zu einem IT-Vorfall kommt?
- In welchem Umfang darf ich als Entscheider untersuchen?
- Was ist die typische Rolle eines Wirtschaftsinformatikers in Bezug auf Informationssicherheit?
- Welchen Wissens- und Fähigkeitsbedarf hat ein typischer Wirtschaftsinformatiker in diesem Themenfeld?

Folien zur Vorlesung

Download (alte Versionen + aktuelle Versionen)

- Neue Versionen (2022/2023):
  - Laden wir jeweils kurz vorher in Ilias hoch
- Alte Versionen (2020/2019)
  - Können Sie jeweils pro Tag von https://wundram.de -> „Lehrauftrag“ herunterladen
  - Das Passwort lautet:

Ein Auftrag an Sie: unser Musterfall

Wiederkehrende, vorlesungs- und übungsbegleitende Übungsaufgabe

- **Sie erhalten die Aufgabe, eine „smarte“ Einbruchmeldeanlage 2.0 für das Handwerksunternehmen Ihrer Eltern zu planen und zu errichten. Dies soll aus Sicht der WI erfolgen, also im Schwerpunkt Anforderungen und Systemeigenschaften definieren.**
- Hausaufgabe
- Beantworten und begründen Sie unter eigenen Annahmen die folgenden Fragen:
  - Make or buy?
  - Welche Anforderungen stellen Sie in Bezug auf ein von Ihnen festzulegendes Schutzniveau an Ihr Unternehmen sowie die Einbruchmeldeanlage?
  - Funk oder Kabel?
  - Cloud-Anbindung und Steuerung per Handy-App: ja/nein?
  - Definieren Sie verschiedene Benutzerrollen
  - Skizzieren Sie mögliche Problemstellen. Wo könnten Probleme lauern?

Ein Auftrag an Sie: unser Musterfall

Wiederkehrende, vorlesungs- und übungsbegleitende Übungsaufgabe

- **Achtung**:
  - Diese Aufgabe setzt sich in jeder Einheit mit neuen Teilaufgaben fort, jeweils zum Inhalt der bearbeiten Einheit (z.B. Zugriffskonzepte oder Crypto)
  - Wir werden voraussichtlich in der Klausur eine Aufgabe zu diesem „Entwicklungsprojekt“ stellen
  - Sie werden diese Aufgabe dann inhaltlich gut und schnell genug beantworten können, wenn Sie sich kontinuierlich als Hausaufgabe damit beschäftigt haben
    - Tipp: Teamarbeit, Gruppendiskussion, gemeinsame Abstimmung während der Nachbereitungsphase

Unser Angebot an Sie: Fragen zur Lernkontrolle

Wiederkehrende, vorlesungs- und übungsbegleitende Fragen

- Voraussichtlich alle 14 Tage per Ilias/E-Mail
- 3-5 Fragen vom Tutor, basieren auf der Pflichtlektüre und den bis dahin besprochenen Foliensätzen
- Sollen Ihnen helfen, „am Ball zu bleiben“
- Die Fragen dienen dem Selbststudium, Antworten sollen NICHT an uns übermittelt werden, aber Rückfragen (z.B. zum Verständnis, zur Thematik) sind jederzeit sehr willkommen! ☺

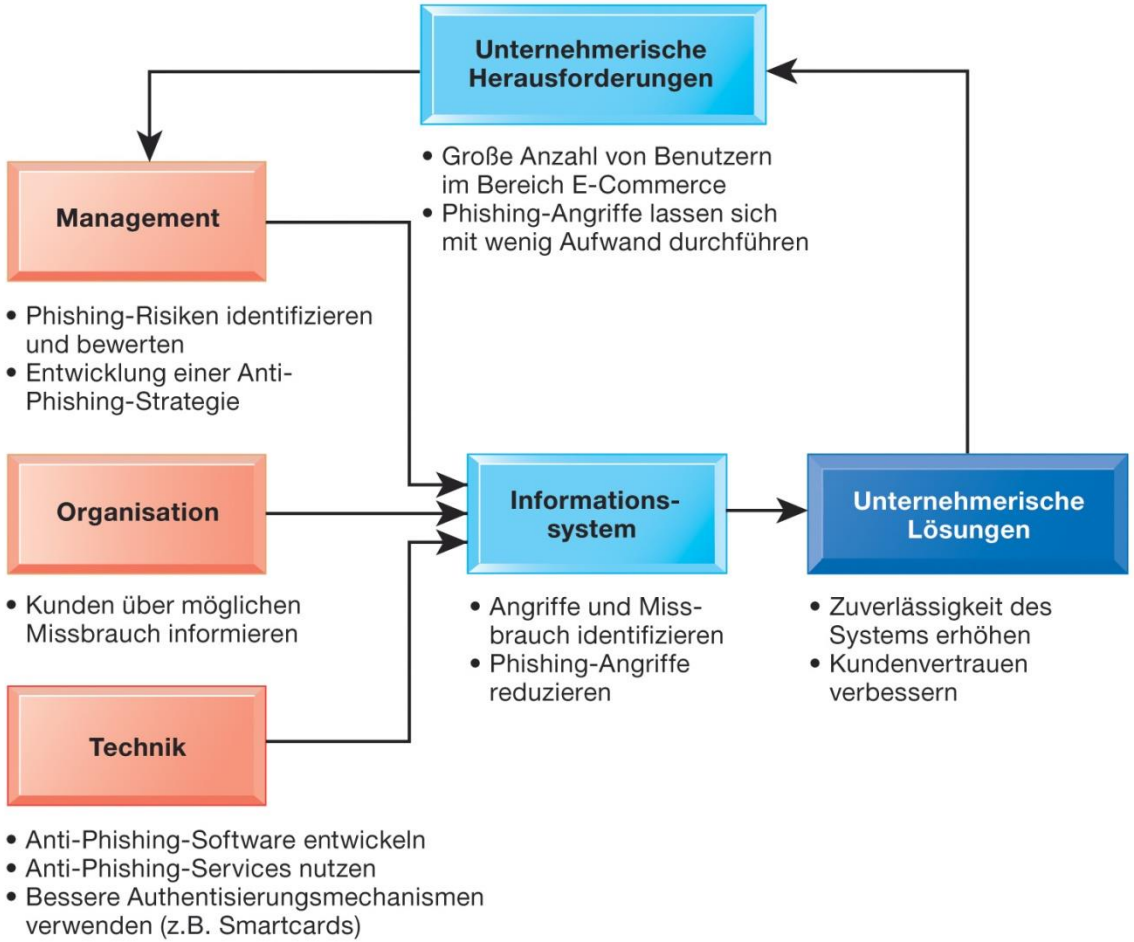
Informationssicherheit: typische Rollen

- Was ist die typische Rolle des Geschäftsführers/CEO?
- Des CIO?
- Des IT-Administrators?
- Des Programmierers?
- Des IT-Projektleiters?
- Des Anwenders?

- In welchen Situationen werden Sie als WI‘ler wahrscheinlich für IT-Sicherheit verantwortlich werden? Mit welchem Detailgrad?
- Wie können Sie Verantwortlichkeiten managen, vielleicht sogar delegieren?

Informationssicherheit: typische Rollen

Beispiel „Kontrolle von Phishing-Risiken“



Quelle: Laudon/Laudon/Schoder (2015)

Geeignete grundlegende Literatur

Lektüre: Disclaimer

- Pflicht- und optionale Lektüre
- Nicht wenig Text…
- Die gute Nachricht: Im Kern wenig Neues zur Vorlesung, Wiederholung, „anders formuliert“, z.T. vertieft oder ausführlicher vorgestellt

Geeignete grundlegende Literatur

Pflichtlektüre

- In den nächsten Wochen/Monaten bis Beginn Blockseminar lesen ☺
- Wirtschaftsinformatik: Eine Einführung (Pearson Studium), Kapitel 15: IT-Sicherheit (ca. 80 Seiten)
- Security Engineering, Ross Anderson, Kapitel 1: What is Security Engineering (14 Seiten) + Kapitel 4: Access Control (36 Seiten). Die (alte) zweite Auflage kann online frei heruntergeladen werden:
  - https://www.cl.cam.ac.uk/~rja14/book.html

Geeignete grundlegende Literatur

Optional, Lesevorschläge Fachliteratur

- Security Engineering, Ross Anderson, Kapitel 2: Usability and Psychology
- Der IT-Sicherheitsleitfaden, Pohlmann, Einleitung + Kapitel 1 + Kapitel 4.4.9 + Kapitel 4.4.10 + Kapitel 5.6 + Kapitel 7 | Kann frei heruntergeladen werden:
  - https://norbert-pohlmann.com/wp-content/uploads/2019/08/IT-Sicherheitsleitfaden-Prof.-Norbert-Pohlmann.pdf
- TeleTrusT-Handreichung Stand der Technik | Online frei verfügbar:
  - https://www.teletrust.de/publikationen/broschueren/stand-der-technik/
- Für technische Details (z.B. Einstieg in Linux, Vertiefung in Linux) mehrere Bücher online verfügbar:
  - https://www.rheinwerk-verlag.de/openbook/
  - Etwa "IT-Handbuch für Fachinformatiker", Kapitel 4 (Netzwerkgrundlagen), Kapitel 7 (Linux), Kapitel 13 (Server für Webanwendungen), Kapitel 17-19 (HTML, PHP, Javascript und co.), Kapitel 20 (Computer- und Netzwerksicherheit)
  - http://openbook.rheinwerk-verlag.de/linux/ -> Wissen zur Bedienung eines Systems ab Kapitel 6 (z.B. Bediendung der Shell, reguläre Ausdrücke, Texteditoren, ...)
- Bundesamt für Sicherheit in der Informationstechnik, Leitfaden „IT-Forensik“,
  - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2

Geeignete grundlegende Literatur

Optional, Lesevorschläge Romane

- Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, Singh
- BLACKOUT - Morgen ist es zu spät, Elsberg
- Snow Crash, Neal Stephenson
- Trilogie: Das Objekt, 00:01, Systemabsturz, Constantin Gillies

Geeignete grundlegende Literatur

Optional, aber sehr hilfreich: https://www.tryhackme.com

Tutorial/HowTo: weiterführende Infos folgen noch

Live-Hack

Katastrophen finden wie am Fließband für Jedermann mit SHODAN

- Shodan ist eine Suchmaschine (vergleichbar mit Google, bing, duckduckgo, …)
- Schwerpunkt liegt hier jedoch auf der systematischen Suche nach abgreifbaren Informationen von (möglichst) allen mit dem Internet verbundenen Geräten
- Beispiel: Frei abrufbare Webcams
- Kostenfreie „Basisfunktionalität“, kostenpflichtige „Profifunktionen“
- http://shodan.io

Live-Hack

Katastrophen finden wie am Fließband für Jedermann mit SHODAN

- Einige geeignete, vorformulierte Suchanfragen für Shodan (Achtung: Ausspähen von Daten / Manipulation von Systemen / etc. kann illegal sein!)
  - Set-Cookie: iomega=
    - Liefert NAS-Speicher ohne Passwort
  - AKCP Embedded Web Server country:de
    - Liefert Embedded-Systeme am Standort Deutschland
  - Jetty 3.1.8 (Windows 2000 5.0 x86) country:de
    - Liefert ebenfalls Embedded-Systeme in Deutschland
  - port:554 has_screenshot:true country:de
    - Liefert Video-Streaming-Server in Deutschland, für die direkter Abgriff möglich ist (mit Streamingclient, etwa vlc)
  - polycom command shell country:de
    - Liefert Polycom-Telefonkonferenzsysteme, die per Telnet ohne Passwort erreichbar sind
  - RFB 003.008 authentication disabled country:ch
    - Liefert VNC-Remotesysteme in der Schweiz, die kein VNC-Passwort erfordern
  - has_screenshot:true country:de
    - Liefert alle Geräte/Systeme in Deutschland, für die Shodan einen Screenshot abgreifen konnte (Webcams, VNC, Streaming, …)

Live-Hack

Katastrophen finden wie am Fließband für Jedermann mit SHODAN

Live-Hack

Katastrophen finden wie am Fließband für Jedermann mit SHODAN

Live-Hack

Katastrophen finden wie am Fließband für Jedermann mit SHODAN

Live-Hack

Katastrophen finden wie am Fließband für Jedermann mit SHODAN

FANGFRISCHE WEBCAMS & NAS-FRONTENDS

Live-Hack

Katastrophen finden wie am Fließband für Jedermann mit SHODAN

- Dazu im Laufe der Jahre auch zig Fernsehbeiträge und andere Berichterstattung
- Das Traurige: das Alles ist nicht neu, sondern uralt
- Schon 2011 haben wir unter der Erwartung, dass das bereits damals langjährig bekannte „Google-Hacking“ (Erfinder: Johnny Long) ein „alter Hut“ war mehrere Fachartikel veröffentlicht und dabei erschreckende Funde gehabt