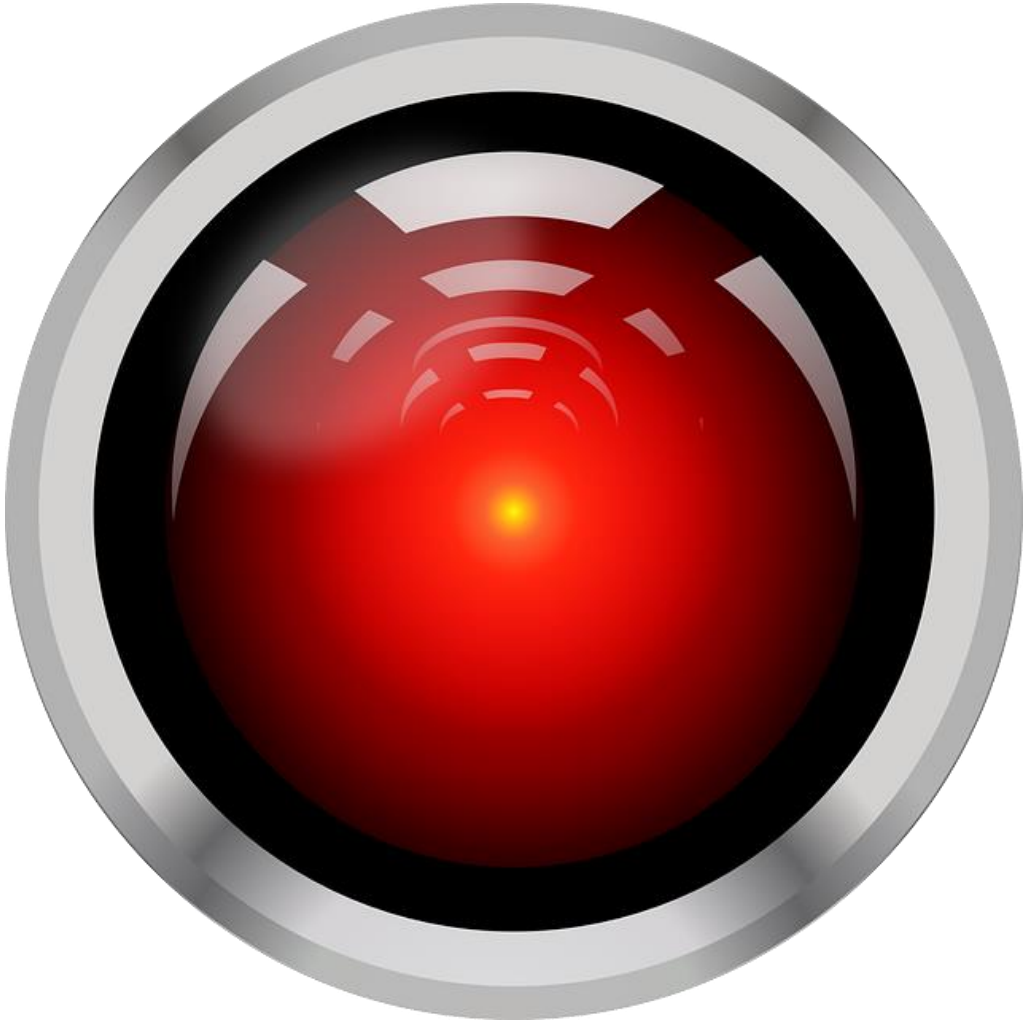
Informationssicherheit und IT-Forensik

1-01 – Einführung

Kurze Begrüßung und erste Schritte

- Mein Name: Martin Wundram
- Lehrbeauftragter der Universität zu Köln
- Erster 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?



Sicher?

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 Phase 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

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

Vorlesung Tag 1 (04.02.19 09:00 bis 17:00 Uhr – 106 Seminarraum S01)

1. Einführung (35 Folien)
2. Grundlagen (72 Folien)
3. Crypto (135 Folien) {bis 13:00 Uhr – Mittagspause}
4. *Gastbeitrag* RA Gerald Spyra zu juristischen Grundlagen (1,75 Stunden) {ab 14:00 Uhr – Nach Mittagspause}
5. Authentifikation und digitale Identitäten (40 Folien)
6. Sicherheitsmodelle und Zugriffskontrolle (33 Folien)
7. IPv4/IPv6 und Netzwerksicherheit (76 Folien)
8. Web-Security (66 Folien)
9. Firewalls und weitere Sicherheitstechniken (54 Folien)

Agenda

Vorlesung Tag 2 (05.02.19 09:00 bis 17:00 Uhr – 106 Seminarraum S01)

1. Awareness/Faktor Mensch (31 Folien)
2. Mobile Security/Internet of Things (31 Folien)
3. Techniken für Client-Security (34 Folien)
4. Grundlagen sicherer Softwareentwicklung (28 Folien) {bis 13:00 Uhr – Mittagspause}
5. *Gastbeitrag* Christian Schneider zu Aspekten (Un-)sicherer Softwareentwicklung (ca. 1,75 Stunden) {ab 14:00 Uhr – Nach Mittagspause}
6. Penetrationstests und Vertiefungseinheit Angriffstechniken (37 Folien)
7. Systematisches Security-Management (25 Folien)
8. Incident Response (33 Folien)

Agenda

Vorlesung Tag 3 (06.02.19 14:00 bis 18:00 Uhr – 411 PC-Pool 3.04)

1. IT-Forensik (66 Folien)
2. Grundlagen der IT-forensischen Gutachtertätigkeit (28 Folien)
3. *Gastbeitrag* Stefan Hirschmeier zu geeignetem Dokumentieren und zum „Stand der Technik“ (ca. 0,75 Stunden)
4. Offene Fragerunde zum Ende der Vorlesung

Agenda

Übung

- 2,5 Tage
  - 11.02.19 09:00 bis 18:00 Uhr
  - 12.02.19 09:00 bis 18:00 Uhr
  - 15.02.19 08:00 bis 12:00 Uhr
- Vertiefung der Inhalte aus der Vorlesung
- Praktische Arbeit am PC (z.B. Buffer Overflow, Web-Security)
- Möglichkeit, Fragen zu den Vorlesungsinhalten zu stellen + Diskussion

- WICHTIG:
  - wer wird an der Übung teilnehmen? Bitte verbindlich jetzt per Handzeichen melden.
  - Wer kann ein eigenes Laptop mitbringen und darauf VirtualBox installieren (mindestens 8 GB RAM, mindestens 30 GB freier RAM)?
  - Es ist auch möglich, dass sich zwei Personen ein Gerät teilen!

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: 8 Personen)
- Kunden von KMU bis DAX + 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
- 7 Jahre Vollzeit IT-Sicherheit, davon über 1 Jahr 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

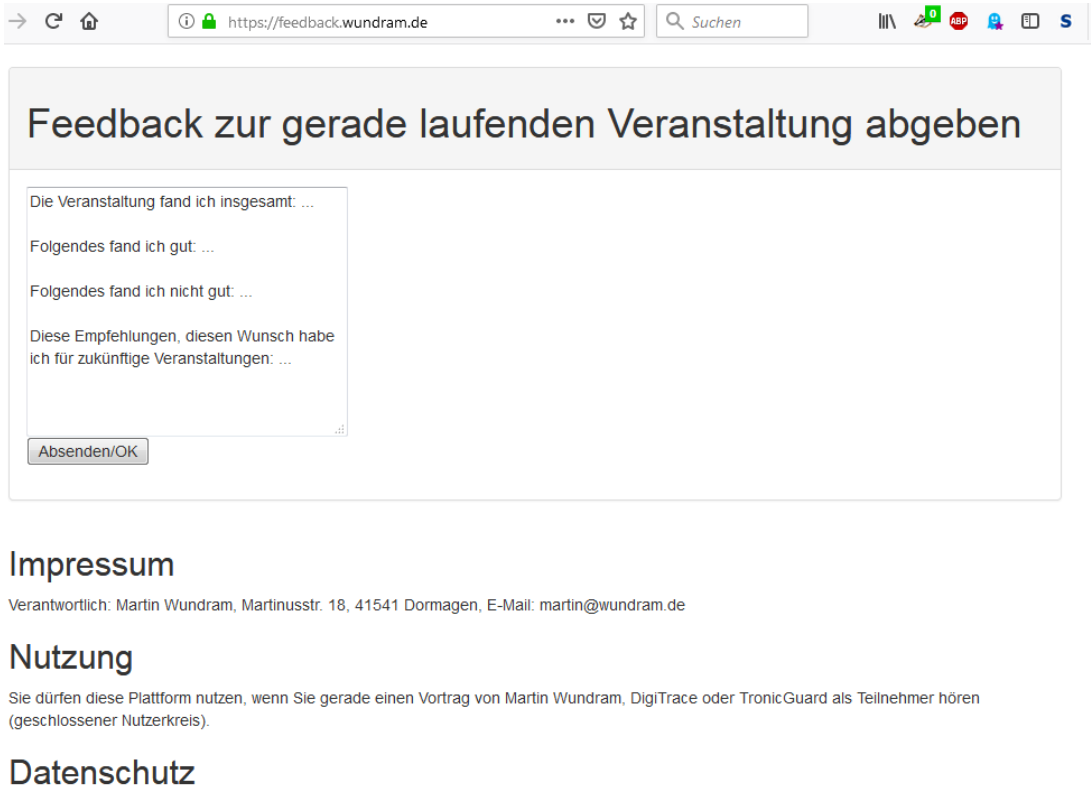
Erreichbarkeit für Fragen und Anmerkungen

Am besten per E-Mail

- martin@wundram.de
- phil.knuefer@rub.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
- Anonymes Feedback-System: https://feedback.wundram.de



Prüfungsmodalitäten

1 Prüfungstermin, schriftliche Prüfung

- 26.02.2019 17:30 Uhr bis 19:00 Uhr

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

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

- 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.
- Nehmen Sie sich dafür jetzt 10 Minuten Zeit
- Beantworten und begründen Sie unter eigenen Annahmen z.B. folgende 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 ja/nein?
  - Definieren Sie verschiedene Benutzerrollen
  - Skizzieren Sie mögliche Problemstellen. Wo könnten Probleme lauern?

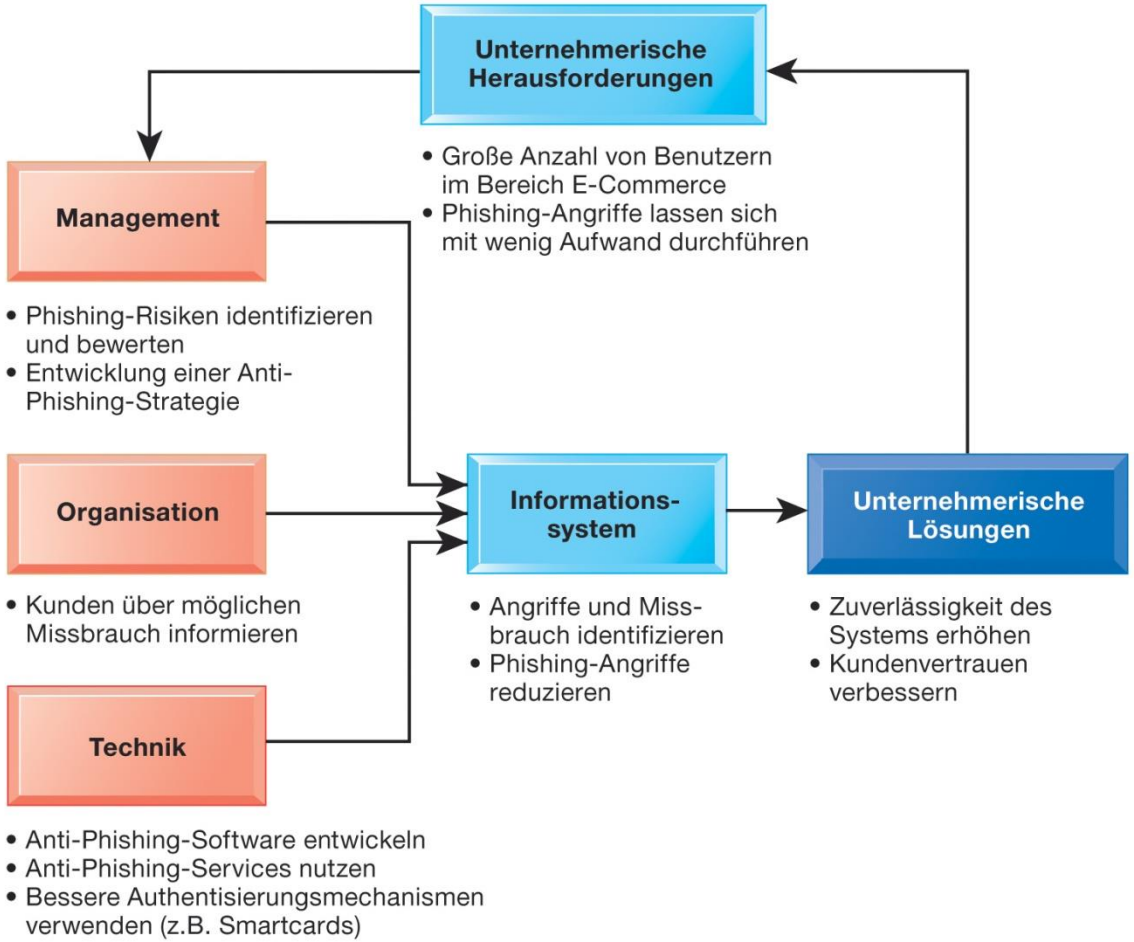
Informationssicherheit: typische Rollen

- Was ist die typische Rolle des Geschäftsführers?
- 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

(Auswahl)

- Wirtschaftsinformatik: Eine Einführung (Pearson Studium - Economic BWL), Laudon/Laudon/Schoder, gesamtes Kapitel zu IT-Sicherheit
- IT-Sicherheit: Konzepte - Verfahren - Protokolle (De Gruyter Studium), Eckert
- Angewandte Kryptographie (Hanser), Ertel
- Understanding Cryptography: A Textbook for Students and Practitioners, Paar/Pelzl
- Forensische Informatik, Dewald/Freiling
- Computer-Forensik (iX Edition): Computerstraftaten erkennen, ermitteln, aufklären, Geschonneck
- TeleTrusT-Handreichung "Stand der Technik" 2018 (PDF/Online)

- Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, Singh
- BLACKOUT - Morgen ist es zu spät, Elsberg

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