
Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Fakultät Informatik

# IT Security – realistisch und machbar?

## IHK Südlicher Oberrhein

Tobias Scheible, M.Eng.

# Tobias Scheible, M.Eng.

- Studium Kommunikations- und Softwaretechnik, Fachrichtung Kommunikationstechnik, Hochschule Albstadt-Sigmaringen
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter an der Hochschule Albstadt-Sigmaringen Im Bereich IT-Sicherheit & Forensik

**Praktikum IT Security 2**
IT Security (Bachelor) – 2. Semester
Prof. Holger Morgenstern

**Seminar IT Security 2**
IT Security (Bachelor) – 2. Semester
Prof. Holger Morgenstern

**Digitale Forensik**
IT Security (Bachelor) – 5. Semester
Prof. Holger Morgenstern

**Projektstudium**
IT Security (Bachelor) – 5. Semester
Prof. Holger Morgenstern

**Einführung in die Informatik**
Digitale Forensik (Master) – 1. Semester
Prof. Dr. Martin Rieger

**Internet Grundlagen**
Digitale Forensik (Master) – 1. Semester
Prof. Dr. Martin Rieger

**Betriebssystemforensik**
Digitale Forensik (Master) – 3. Semester
Prof. Dr. Martin Rieger

**Vorträge & Workshops**
zu aktuellen Themen der IT-Sicherheit, u. a. für den VDI und die IHK

**Blog scheible.it**
Blog rund um meine Aktivitäten
https://scheible.it

# Hochschule Albstadt-Sigmaringen

- 1971 Gründung der Fachhochschule Sigmaringen
- 1988/89 Campus Albstadt
- 2004 Fachhochschule wird in Hochschule umbenannt
- 24 Bachelor- und Masterstudiengänge


- Weiterbildung (berufsbegleitende Angebote)
  - Zertifikate, Data Science (Master), Digitale Forensik (Master) und IT GRC Management (Master)



**IT Security – realistisch und machbar?**

# Zahlen & Fakten


190
Lehrbe-
auftragte

184
Mitarbeiter

57 %
Campus
Albstadt

43 %
Campus
Sigmaringen

61
Verwaltung
und zentrale
Einrichtungen

123
Mitarbeiter
Studiengänge

3.477
Studierende

184
Studentische
Hilfskräfte

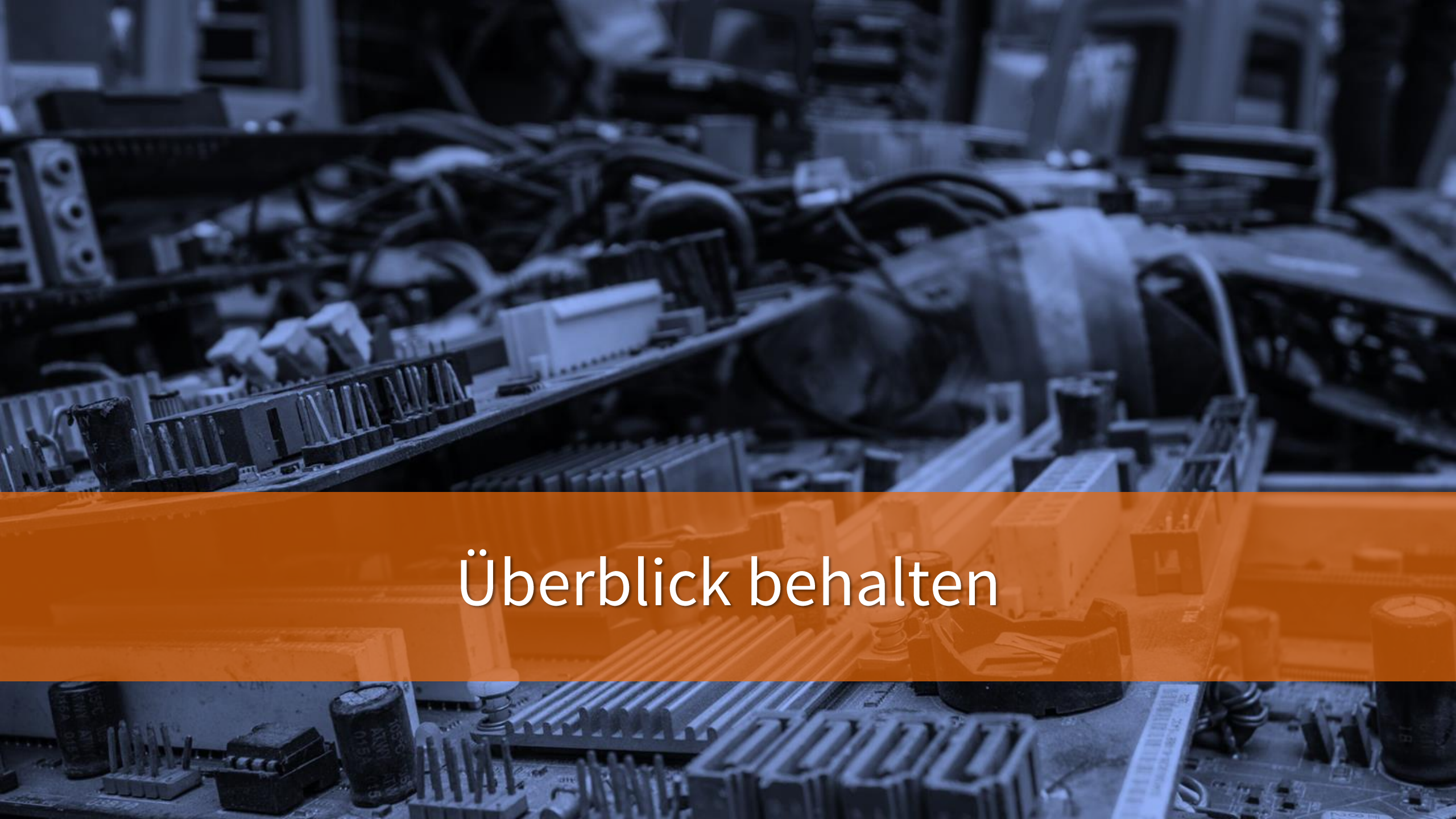
81
Professoren /
Professorinnen



**IT Security –
realistisch und machbar?**

# Handlungsempfehlungen

- Überblick behalten
- Regelmäßige Updates
- Sichere Passwörter
- Fallback-Strategien
- Sicherheitsbewusstsein



# Überblick behalten

# Cybercrime as a Service

- Viele Tools sind sehr ausgereift und können ohne tiefgreifende Fachkenntnisse bedient und eingesetzt werden
- Angriffe können in einschlägigen Foren oder in Online-Shops im Deep Web gebucht werden

- „Wir erleben derzeit eine starke Professionalisierung der Hacker.“
  Florian Seitner vom Bayerischen Landesamt für Verfassungsschutz
- Spaß-Hacks spielen so gut wie keine Rolle mehr
- Hackaktivisten und Cyberkriminelle sind die größten Gruppen

# Cybercrime as a Service

Quelle: youtube.com



**IT Security –
realistisch und machbar?**

Überblick behalten

Regelmäßige Updates

Sichere Passwörter

Fallback-Strategien

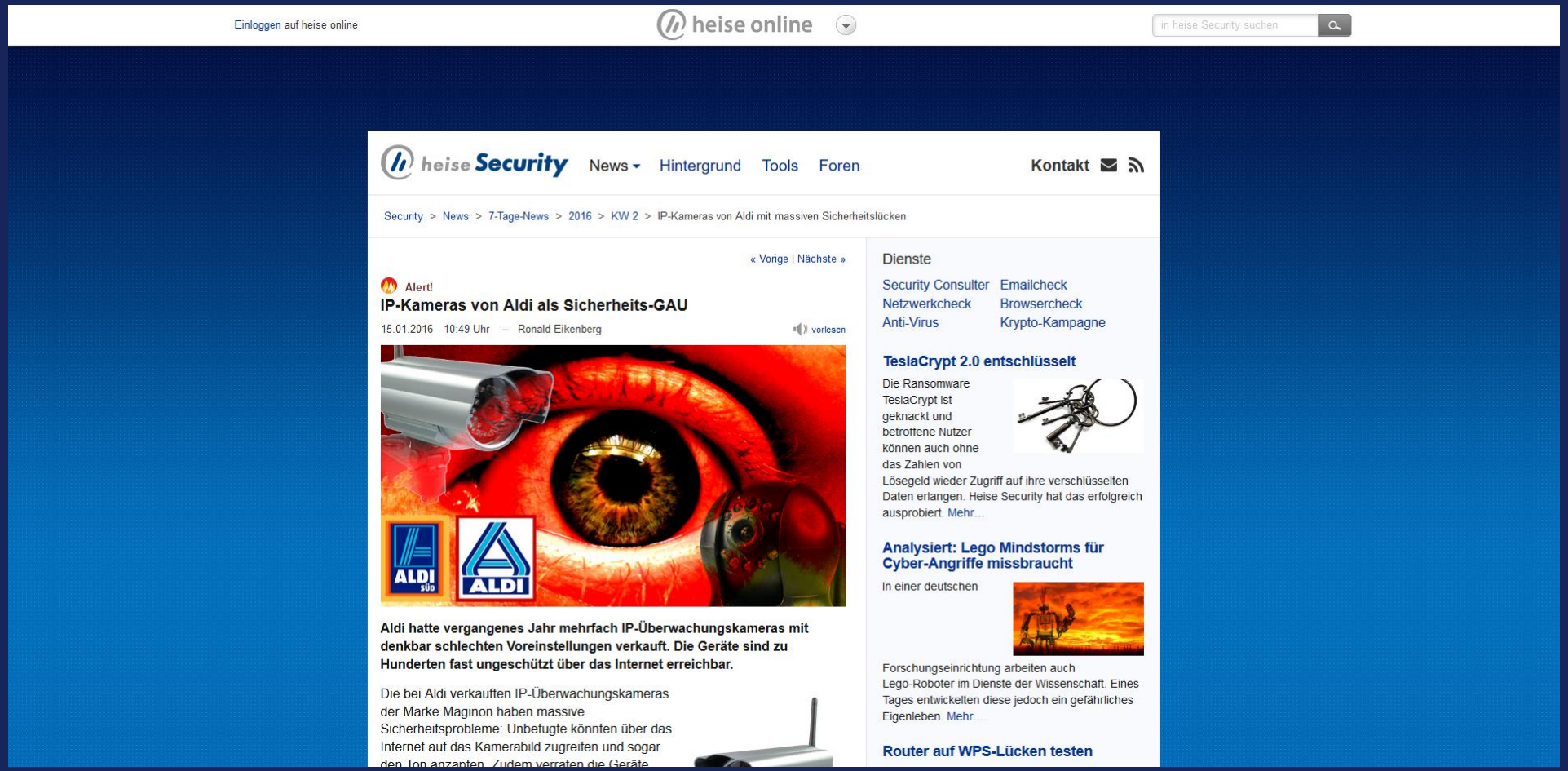
Sicherheitsbewusstsein

# Überblick behalten

- Häufig sind ältere Geräte Opfer von Cyber-Attacken
- Infrastruktur erfassen
  - Netzwerkkomponente (Router, Access Points, …)
  - Tragbare Geräte (Smartphones, Tablets, …)
  - Alle Rechner (Desktops, Server, …)
  - Vernetzte Geräte (Überwachungskameras, Industriemaschinen, …)
- Physische Sicherheit ebenfalls mit beachten

# Regelmäßige Updates

# Bug or Feature?




Quelle: heise.de

# Mirai Bot-Netz

- Ein Bot-Netz, das sich aus IoT-Geräten zusammensetzt
- Es wurde genutzt, um Anschlüsse zu überlasten
- Konnte auch gemietet werden

- Beispiel:
  - Es wurde versucht, Router über eine Schnittstelle zur Fernwartung zu übernehmen
  - Durch eine fehlerhafte Umsetzung „stürzten“ die Router ab
  - 900.000 Rechner der Deutschen Telekom waren nicht mehr erreichbar

# Regelmäßige Updates

- Viele Angriffe finden über bereits geschlossene Sicherheitslücken statt
- Halten Sie alle Systeme (Rechner, Router, Drucker, …) auf dem neuesten Stand
- Entfernen Sie nicht mehr genutzte Geräte und Anwendungen
- Ist dies nicht möglich – isolieren Sie diese Systeme
- Sicherheitssoftware muss ebenfalls aktuell sein

# Sichere Passwörter

# 00000000

?

Quelle: heise.de



**IT Security –
realistisch und machbar?**

Überblick behalten

Regelmäßige Updates

Sichere Passwörter

Fallback-Strategien

Sicherheitsbewusstsein

# 00000000

# Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

Quelle: heise.de



**IT Security –
realistisch und machbar?**

# Atomraketen: Steuerungstechnik aus den 70ern

Quelle: zeit.de

Quelle: chip.de



**IT Security –
realistisch und machbar?**

Überblick behalten

Regelmäßige Updates

**Sichere Passwörter**

Fallback-Strategien

Sicherheitsbewusstsein

# Häufige Passwörter

https://stricture-group.com/files/adobe-top100.txt

Top 100 Adobe Passwords with Count

We do not (yet) have the keys Adobe used to encrypt the passwords of 130,324,429 users affected by their most recent breach. However, thanks to Adobe choosing symmetric key encryption over hashing, selecting ECB mode, and using the same key for every password, combined with a large number of known plaintexts and the generosity of users who flat-out gave us their password in their password hint, this is not preventing us from presenting you with this list of the top 100 passwords selected by Adobe users.

While we are fairly confident in the accuracy of this list, we have no way to actually verify it right now. We don't have the keys, and Adobe is not letting any of the affected accounts log in until the owners reset their passwords. So, it is possible there is an error or two in here. Caveat emptor and such.

| # | Count | Ciphertext | Plaintext |
|---|---|---|---|
| 1. | 1911938 | EQ7fIpT7i/Q= | 123456 |
| 2. | 446162 | j9p+HwtWWT86aMjgZFLzYg== | 123456789 |
| 3. | 345834 | L8qbAD3jl3jioxG6CatHBw== | password |
| 4. | 211659 | BB4e6X+b2xLioxG6CatHBw== | adobe123 |
| 5. | 201580 | j9p+HwtWWT/ioxG6CatHBw== | 12345678 |
| 6. | 130832 | 5djv7ZCI2ws= | qwerty |
| 7. | 124253 | dQi0asWPYvQ= | 1234567 |
| 8. | 113884 | 7LqYzKVeq8I= | 111111 |
| 9. | 83411 | PMDTbP0LZxu03SwrFUvYGA== | photoshop |
| 10. | 82694 | e6MPXQ5G6a8= | 123123 |
| 11. | 76910 | j9p+HwtWWT8/HeZN+3oiCQ== | 1234567890 |
| 12. | 76186 | diQ+ie23vAA= | 000000 |
| 13. | 70791 | kCcUSCmonEA= | abc123 |
| 14. | 61453 | ukxzEcXU6Pw= | 1234 |
| 15. | 56744 | 5wEAInH22i4= | adobe1 |
| 16. | 54651 | WqflwJFYW3+PszVFZo1Ggg== | macromedia |
| 17. | 48850 | hjAYsdUA4+k= | azerty |
| 18. | 47142 | rpkvF+oZzQvioxG6CatHBw== | iloveyou |
| 19. | 44281 | xz6RIeGzn6g= | aaaaaa |

Quelle: stricture-group.com

# Passwortsicherheit

Quelle: youtube.com

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Fakultät Informatik

**IT Security –
realistisch und machbar?**

Überblick behalten

Regelmäßige Updates

Sichere Passwörter

Fallback-Strategien

Sicherheitsbewusstsein

# Sichere Passwörter

- Dringend abgeraten wird von…
  - gängige Wörtern, Namen, Geburtstagen, Zitaten etc. beziehungsweise
  - Zeichenmustern (12345, asdf, abcdef,…).
- Verschiedene Passwörter für verschiedene Bereiche verwenden
- Passwortmanager zum Speichern der Passwörter
- Zweifaktorauthentifizierung wenn möglich nutzen

# Fallback-Strategien

# Entsorgter Rechner




**IT Security –
realistisch und machbar?**

Überblick behalten

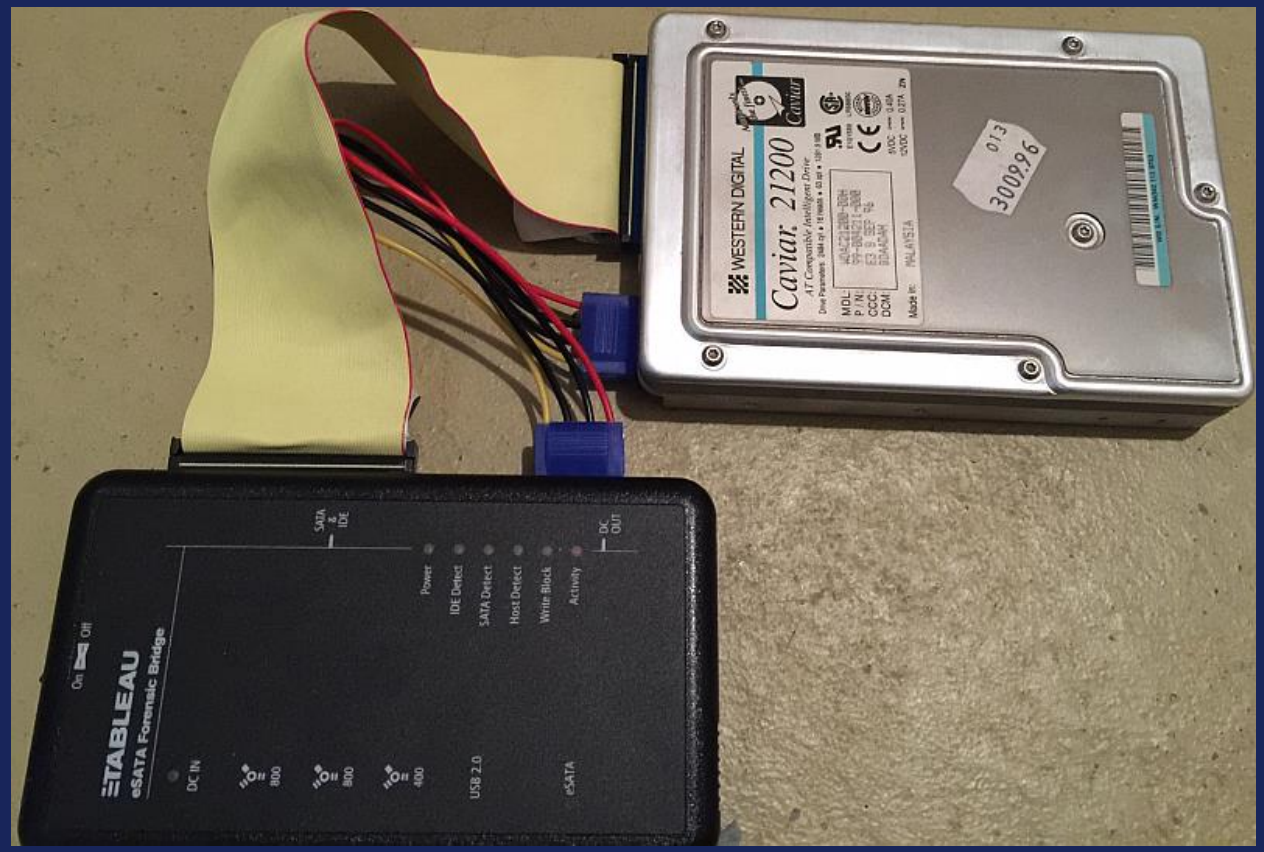
Regelmäßige Updates

Sichere Passwörter

**Fallback-Strategien**

Sicherheitsbewusstsein

# Entsorgter Rechner




Text | Hex | Doc | Transcript | Picture | Report | Console | Details | Out

| | |
|---|---|
| Name | PC found in Gammertingen |
| Actual Date | 23/11/15 01:37:55 |
| Target Date | 23/11/15 01:37:55 |
| File Path | E:\img\hdd1.E01 |
| Case Number | found-pc |
| Evidence Number | 1 |
| Examiner Name | Morgenstern |
| Model | WDC AC21200H |
| Serial Number | WD-WM3421150763 |
| Drive Type | Fixed |
| File Integrity | Completely Verified, 0 Errors |
| Acquisition MD5 | bb03b4ad6f80c971741bde92ab8e6326 |
| Verification MD5 | bb03b4ad6f80c971741bde92ab8e6326 |
| GUID | 8140b400917a11e59226f9786a146615 |
| EnCase Version | 6.01 |
| System Version | Linux |
| Is Physical | • |
| Raid Stripe Size | 0 |
| Error Granularity | 2 |
| Process ID | 0 |
| Index File | C:\Program Files\EnCase6\Index\PC found in Gammertingen-8140b400917a11e59226f9786a146615.Index |
| Read Errors | 0 |
| Missing Sectors | 0 |
| CRC Errors | 0 |
| Compression | Good |
| Total Size | 1.281.982.464 Bytes (1,2GB) |
| Total Sectors | 2.503.872 |
| Disk Signature | 00000000 |
| Partitions | Valid |

**Partitions**

| Name | Id | Type | Start Sector | Total Sectors | Size |
|---|---|---|---|---|---|
| | 0b | FAT32 | 0 | 2.499.840 | 1,2GB |



**IT Security – realistisch und machbar?**

Überblick behalten

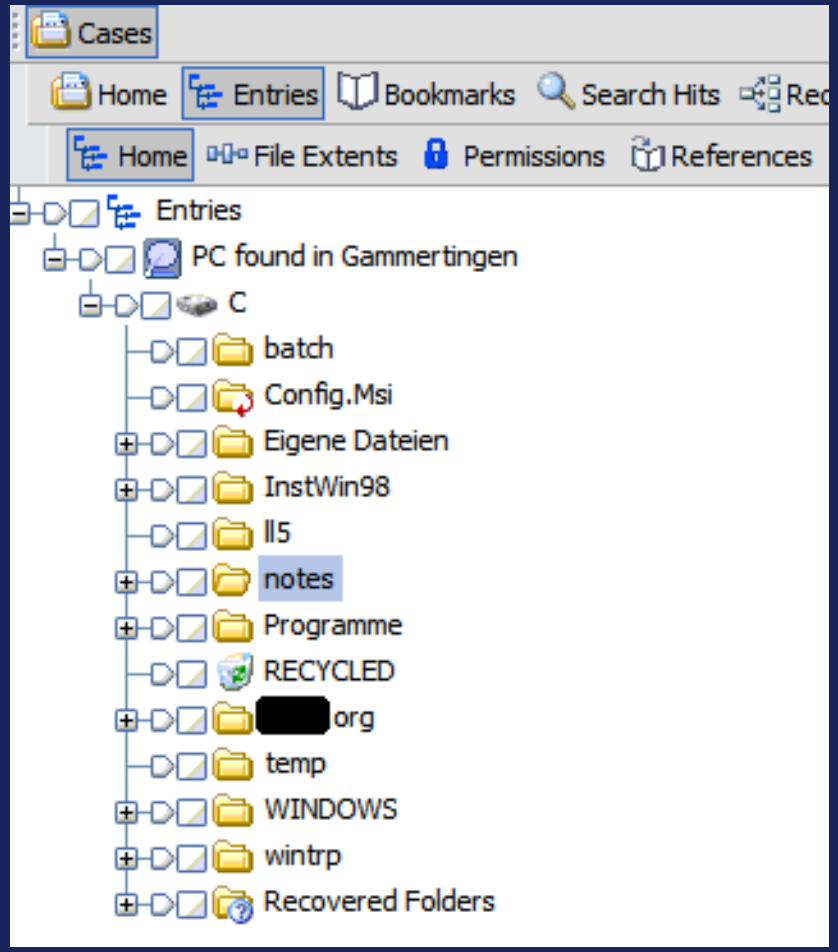
Regelmäßige Updates

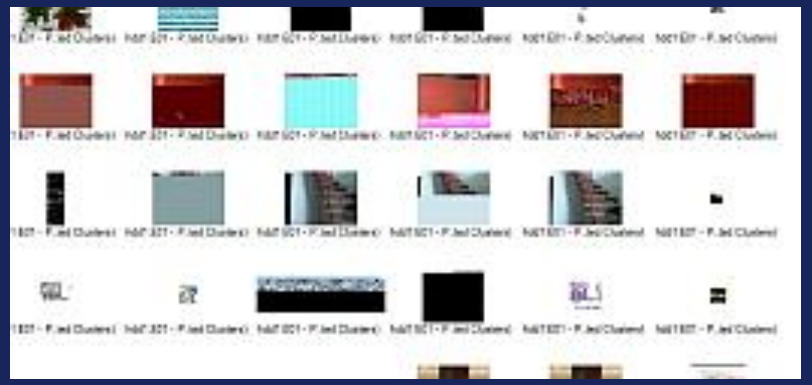
Sichere Passwörter

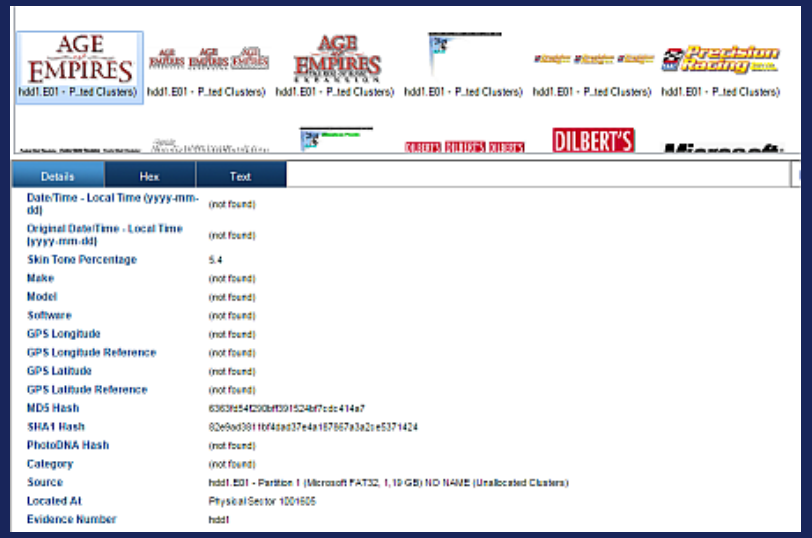
**Fallback-Strategien**

Sicherheitsbewusstsein

# Entsorgter Rechner








**IT Security –
realistisch und machbar?**

Überblick behalten

Regelmäßige Updates

Sichere Passwörter

Fallback-Strategien

Sicherheitsbewusstsein

# Fallback-Strategien

- Nicht nur eine äußere Verteidigung etablieren, sondern eine Defense in Deep Strategie konsequent anwenden

- Verschlüsselungs-Strategie
  - Festplatten- bzw. Geräteschutz aktivieren
  - Datenträgerverschlüsselung nutzen
  - Einfache Verschlüsselung durch Zip-Dateien

- Backup-Strategie
  - Automatisiertes Backup ohne Aufwand
  - Vor Veränderungen geschütztes Backup
  - Backupspeicher am besten an einem anderen Ort und mit getesteter Wiederherstellung


# Sicherheitsbewusstsein


Quelle: pics-for-fun.com



**IT Security –
realistisch und machbar?**

Überblick behalten

Regelmäßige Updates

Sichere Passwörter

Fallback-Strategien

Sicherheitsbewusstsein


Quelle: de.pinterest.com



## IT Security – realistisch und machbar?

Überblick behalten

Regelmäßige Updates

Sichere Passwörter

Fallback-Strategien

**Sicherheitsbewusstsein**

# Social Engineering - Gefälschte E-Mail

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL TV | Abo | Shop Schlagzeilen | Wetter | TV-Programm | mehr ▼

Login | Registrierung

SPIEGEL ONLINE SCHULSPIEGEL

Abi - und dann? | Querweltein | Leben U21 | Wissen

Nachrichten > SchulSPIEGEL > Wetter > Schulfrei in Niedersachsen wegen gefälschter E-Mail

**Gefälschte E-Mail: Schulfrei ermogelt**

DPA

Winterwetter in Niedersachsen: Freier Tag im Schnee wegen gefälschter E-Mail

**Eine gefälschte E-Mail hat Schülern in Niedersachsen einen freien Tag beschert. Der Unterricht falle wegen des Winterwetters aus, hieß es darin. Hunderte Schüler glaubten der Meldung - und blieben zu Hause.**

Hochschule Albstadt-Sigmaringen
University of Applied Sciences

Fakultät Informatik

**IT Security – realistisch und machbar?**

Überblick behalten

Regelmäßige Updates

Sichere Passwörter

Fallback-Strategien

Sicherheitsbewusstsein

Quelle: spiegel.de

# Gefängnisausbruch mittels E-Mail

- Moderner Ausbruch aus einem britischen Gefängnis (März 2015)
- SocialEngineering Angriff auf das Gefängnis
  - Smartphone eingeschmuggelt
  - Domain reserviert, die dem zuständigen Gericht ähnelt
  - E-Mail Adresse mit dieser Domain eingerichtet
  - Hat sich als leitender Beamter ausgegeben
  - Anweisungen zu seiner Entlassung gegeben

- Gefangener kam frei

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Fakultät Informatik



Quelle: heise.de

# Sicherheitsbewusstsein

- Social Engineering (engl. "angewandte Sozialwissenschaft" eher "soziale Manipulation"); unterschiedliche Formen:
  - Human Based Social Engineering
    - Angreifer gibt sich als Mitarbeiter, IT-Support o. ä. aus
  - Computer Based Social Engineering
    - Angreifer versucht über Malware, gefälschte E-Mails, Phishing an Zugangsdaten, persönliche Informationen o. ä. zu gelangen
  - Reverse Social Engineering
    - Angreifer verursacht ein Problem und hilft dann vermeintlich bei der Beseitigung

- Sensibilisieren der Mitarbeiter und Schulung der Mitarbeiter über Social Engineering-Strategien und -Methoden

# Vielen Dank für Ihre Aufmerksamkeit

Präsentation online unter: https://scheible.it

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Fakultät Informatik

**IT Security –
realistisch und machbar?**

Überblick behalten

Regelmäßige Updates

Sichere Passwörter

Fallback-Strategien

Sicherheitsbewusstsein