



**Hochschule  
Albstadt-Sigmaringen**  
University of Applied Sciences

Fakultäten Informatik

Smart Textiles &  
IT-Sicherheit  
**GATEX**



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 & Digitale Forensik
  - Bachelorstudiengang IT Security
  - Institut für Wissenschaftliche Weiterbildung



## Praktikum Cybersecurity

IT Security (Bachelor) – 4. Semester  
Prof. Holger Morgenstern

## Seminar Cybersecurity

IT Security (Bachelor) – 4. Semester  
Prof. Holger Morgenstern

## Digitale Forensik

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

## Projektstudium

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

## Grundlagen Digitale Forensik

IT GRC Management – 4. Semester  
Prof. Dr. Stefan Ruf

## Workshops & Vorträge

Blog rund um meine Aktivitäten:  
<https://scheible.it>

Smart Textiles &  
IT-Sicherheit

# Hochschule Albstadt-Sigmaringen

- 1971 Gründung der Fachhochschule Sigmaringen

Fakultät  
Engineering



Fakultät  
Business Science  
and Management

- 1988/89 Campus Albstadt



- 2004 Fachhochschule wird in Hochschule umbenannt

Fakultät Life  
Sciences



Fakultät  
Informatik

- 24 Bachelor- und Masterstudiengänge

- Weiterbildung (berufsbegleitende Angebote)

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

Smart Textiles &  
IT-Sicherheit

# Zahlen & Fakten



## Smart Textiles & IT-Sicherheit

# Agenda

- Informatik & Textil
- Gestern
  - Geschichte der Schadsoftware
- Heute
  - Faktor Mensch
  - Cybercrime as a Service
- Morgen
  - IoT - Internet of Things
- Zukunft
  - Projekt SEKT

## Smart Textiles & IT-Sicherheit

Informatik & Textil

Gestern

Heute

Morgen

Zukunft

A night sky filled with fireworks. A large, bright firework is exploding in the center, creating a starburst pattern of light. Other smaller fireworks are visible in the background, and a blue horizontal banner is overlaid at the bottom of the image.

# Informatik & Textil

# ZEW Kurzexpertise im Auftrag des BMWi

## Smart Textiles & IT-Sicherheit

### Informatik & Textil

Gestern

Heute

Morgen

Zukunft

„Ein großes Marktpotenzial wird auch in der Herstellung der smarten Textilien selbst gesehen, da verschiedene Produkte verbunden werden müssen und damit auch Marktpotenziale entstehen werden. Der Schlüssel hierbei sind oftmals Kooperationen zwischen Unternehmen verschiedener Branchen.“

FashionTech – Smart Textiles, Dr. Jörg Ohnemus & Dr. Fabienne Rasel, 8. Januar 2018



WD Western Digital

S/N: WJNANR5CST105  
Product Warranty will be void if seal has been broken or tampered.  
U.S. Patent: 6778552, 5581818, 6058461, 6281615  
Product of Malaysia

5VDC --- 0.6A  
12VDC --- 1.8A

Drive Parameters:  
LBA 16525000  
80.0 GB

Canada ICES - 003 Class B1  
NMB - 003 Classe B

WJNANR5CST105  
WD Green® SE  
MFG. WORLDWIDE  
DATE: 03/2011  
DCA: 888818121

DSN NY - 01R54 - 1235 - 718 - 018

DPN 01R54  
CO NY

Ref A40

WD S/N: WJNANR5CST105

WARRANTY: SEE DRIVE DATA SHEET UNDER POWER SUPPLY  
DO NOT USE THIS DRIVE FOR ARCHIVAL STORAGE OR DATA RECOVERY

CE  
RoHS  
RECYCLED

DO NOT COVER  
DRIVE HOLES  
FRAGILE







Gestern

00000000



## Smart Textiles & IT-Sicherheit

### Informatik & Textil

#### Gestern

[Pin-Code Beispiel](#)

Schadsoftware

Ransomware

#### Heute

#### Morgen

#### Zukunft

00000000

# Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

Smart Textiles &  
IT-Sicherheit

Informatik & Textil

Gestern

[Pin-Code Beispiel](#)

Schadsoftware

Ransomware

Heute

Morgen

Zukunft

# Geschichte der Schadsoftware

## ■ Proof of Concept

- 80er Jahre Der Begriff Computervirus wird zum ersten Mal verwendet und erste Konzepte werden öffentlich vorgestellt und diskutiert
- 1985 Zum ersten Mal berichtet eine deutschsprachige Zeitung über Computerviren
- 1988 Zum ersten Mal werden Würmer (sich selbst replizierende Schadsoftware) eingesetzt

## ■ Ausnutzung von Schwachstellen

- 1997 Schadsoftware nutzt nun gezielt Schwachstellen in Programmen, Betriebssystemen oder in Hardware aus
- 2000 „I love you“ Virus findet auch in Deutschland große Verbreitung
- 2000 Erster Trojaner für mobile Endgeräte (PDAs)

## ■ Krimineller Hintergrund

- 2004 Schadsoftware wird immer mehr von organisierten Kriminellen eingesetzt
- 2005 Erster Wurm verbreitet sich automatisch auf Symbian Smartphones per MMS

# Ransomware - AIDS

- Bereits 1989 wurden die ersten Angriffe mit Ransomware durchgeführt
- Die Schadsoftware wurde per 5,25“ Diskette ca. 20.000 Mal mit der Post verschickt
- Nach 90 Starts wurden die Dateinamen auf dem Laufwerk C: verschlüsselt
  - Eine italienische AIDS Organisation verlor Forschungsergebnisse aus 10 Jahren
  - Ersteller der Ransomware wurde 1990 verhaftet

```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378. You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue
```

Quelle: [wikipedia.org](https://de.wikipedia.org/wiki/AIDS) (3)

## Smart Textiles & IT-Sicherheit

### Informatik & Textil

#### Gestern

Pin-Code Beispiel  
Schadsoftware  
[Ransomware](#)

#### Heute

#### Morgen

#### Zukunft

.....  
15.11.2018 | GATEX

Tobias Scheible, M.Eng.



Heute

# Was ist die häufigste Angriffsmethode?

Ausnutzung von Schwachstellen

A

Physische Attacken

B

Manipulation von Personen

C

Ausnutzung von Fehlern

D

Smart Textiles &  
IT-Sicherheit

Informatik & Textil

Gestern

Heute

[Angriffsmethoden](#)

Faktor Mensch

Social Engineering

Passwortsicherheit

Cybercrime as a Service

Ransomware

Morgen

Zukunft



# Faktor Mensch

I wonder what the code could be...



Quelle: [pics-for-fun.com](https://pics-for-fun.com) (4)



Quelle: [de.pinterest.com](https://de.pinterest.com) (5)

## Smart Textiles & IT-Sicherheit

### Informatik & Textil

#### Gestern

#### Heute

- Angriffsmethoden
- [Faktor Mensch](#)
- Social Engineering
- Passwortsicherheit
- Cybercrime as a Service
- Ransomware

#### Morgen

#### Zukunft

.....  
15.11.2018 | GATEX

Tobias Scheible, M.Eng.

# Faktor Mensch



- Passwort für Raketen-Warnsystem stand wohl monatelang im Internet
- Klassiker – Post-it Zettel auf Monitor
- Passwort: `warningpoint2`

## Smart Textiles & IT-Sicherheit

### Informatik & Textil

#### Gestern

#### Heute

Angriffsmethoden  
[Faktor Mensch](#)  
Social Engineering  
Passwortsicherheit  
Cybercrime as a Service  
Ransomware

#### Morgen

#### Zukunft

# Social Engineering



Quelle: youtube.com (7)

## Smart Textiles & IT-Sicherheit

### Informatik & Textil

#### Gestern

#### Heute

- Angriffsmethoden
- Faktor Mensch
- Social Engineering
- Passwortsicherheit
- Cybercrime as a Service
- Ransomware

#### Morgen

#### Zukunft

.....  
15.11.2018 | GATEX

Tobias Scheible, M.Eng.

# Social Engineering

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

**SPIEGEL ONLINE SCHULSPIEGEL**

Login | Registrierung

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.**

Quelle: [spiegel.de](https://www.spiegel.de) (8)

## Smart Textiles & IT-Sicherheit

### Informatik & Textil

#### Gestern

#### Heute

- Angriffsmethoden
- Faktor Mensch
- Social Engineering
- Passwortsicherheit
- Cybercrime as a Service
- Ransomware

#### Morgen

#### Zukunft

.....  
15.11.2018 | GATEX

Tobias Scheible, M.Eng.

# Social Engineering

Freitag, 12. Februar 2016 | Service | Abo | Shop | Newsletter | Login | Registrieren | Suchbegriff, WKN, ISIN

**WirtschaftsWoche** | UNTERNEHMEN | FINANZEN | POLITIK | **ERFOLG** | TECHNOLOGIE

Trends | **Management** | Gründer | Beruf | Jobsuche | Campus & MBA | Karriere | Jobturbo

DAX® 8.752,67 -2,93%	E-STOXX 50® 2.680,35 -3,90%	MDAX® 17.594,68 -2,83%	Dow Jones 15.660,18 -1,60%	Gold (USD) 1.242,83 -0,30%	EUR/USD 1,1315 -0,00%	■ Börsenkurse ■ cM Indikationen
-------------------------	--------------------------------	---------------------------	-------------------------------	-------------------------------	--------------------------	------------------------------------


Die WirtschaftsWoche > Erfolg > Management > Falsche Chefs zocken Firmen ab: Den Enkeltrick gibt's auch bei Unternehmen

## Falsche Chefs zocken Firmen ab

18. August 2015

★★★★☆  
0  
Kommentare

Versenden  
Drucken  
Merken  
Startseite



Nicht nur gutgläubige Senioren werden Opfer von Trickbetrü gern.

Bild: dpa

**Während sich manche Betrüger als vermisste Enkel ausgeben, um ans Ersparte von Senioren zu kommen, probieren es andere eine Nummer größer. Sie geben sich als Chef aus und erleichtern Unternehmen um Millionenbeträge.**

"Hallo, ich bin's, der Chef. Bitte überweisen Sie folgenden Betrag auf folgendes Konto..." So oder so ähnlich funktioniert die Betrugsmasche "CEO Fraud", die derzeit nach Deutschland schwappt. Dabei kontaktieren die mutmaßlichen Betrüger per Telefon und E-Mail Mitarbeiter von Unternehmen und geben sich als Vertreter der Geschäftsführung aus. Dann fordern sie bestimmte Beträge auf

Quelle: [wiwo.de](http://wiwo.de) (9)

## Smart Textiles & IT-Sicherheit

### Informatik & Textil

Gestern

Heute

Angriffsmethoden  
Faktor Mensch  
Social Engineering  
Passwortsicherheit  
Cybercrime as a Service  
Ransomware

Morgen

Zukunft

.....  
15.11.2018 | GATEX

Tobias Scheible, M.Eng.

# Passwortsicherheit



Quelle: youtube.com (10)

## Smart Textiles & IT-Sicherheit

### Informatik & Textil

#### Gestern

#### Heute

Angriffsmethoden  
Faktor Mensch  
Social Engineering  
Passwortsicherheit  
Cybercrime as a Service  
Ransomware

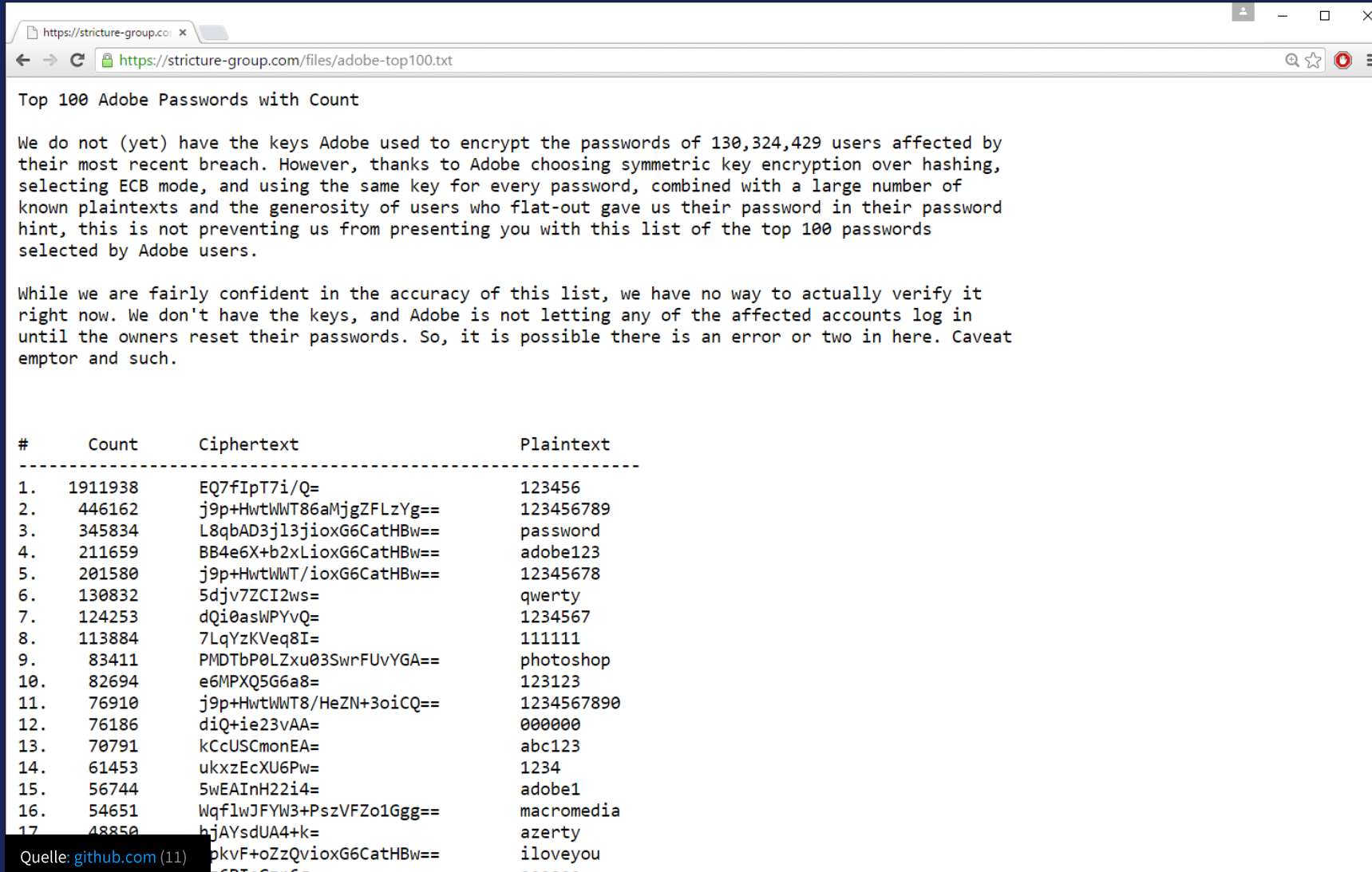
#### Morgen

#### Zukunft

.....  
15.11.2018 | GATEX

Tobias Scheible, M.Eng.

# Passwortsicherheit



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	L8qbAD3j13jioxG6CatHBw==	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	5wEAIhH22i4=	adobe1
16.	54651	WqflwJFYW3+PszVFZo1Ggg==	macromedia
17.	48850	hJAYsdUA4+k=	azerty

Quelle: [github.com](https://github.com) (11)

## Smart Textiles & IT-Sicherheit

### Informatik & Textil

#### Gestern

#### Heute

- Angriffsmethoden
- Faktor Mensch
- Social Engineering
- Passwortsicherheit
- Cybercrime as a Service
- Ransomware

#### Morgen

#### Zukunft

# Cybercrime as a Service



Koordinator

## Smart Textiles & IT-Sicherheit

### Informatik & Textil

#### Gestern

#### Heute

- Angriffsmethoden
- Faktor Mensch
- Social Engineering
- Passwortsicherheit
- Cybercrime as a Service
- Ransomware

#### Morgen

#### Zukunft



# Ransomware - Locky

- Effektive Methode, um Geld zu ergaunern
- Auf deutsche Benutzer ausgerichtete Varianten
- Verschlüsselt alle Benutzerdateien auch auf Netzwerklaufwerke
  
- Zeitlicher Ablauf:
  - 15.02.2016 Locky wird als Schläfer aktiviert (Makros)
  - 22.02.2016 Gefälschte Unternehmensrechnung (JScript)
  - 24.02.2016 Gefälschtes Sipgate Fax (JScript)
  - 26.02.2016 Neue Infektionstechnik mit Batch-Dateien
  - 02.03.2016 Gefälschte BKA E-Mail (EXE-Datei)

## Smart Textiles & IT-Sicherheit

### Informatik & Textil

#### Gestern

#### Heute

Angriffsmethoden  
Faktor Mensch  
Social Engineering  
Passwortsicherheit  
Cybercrime as a Service  
[Ransomware](#)

#### Morgen

#### Zukunft



Morgen



# IoT – Internet of Things

- Ein Bot-Netz, das sich aus IoT-Geräten zusammensetzt
- Es wurde genutzt, um DDOS-Angriffe auszuführen
- Konnte auch gemietet werden
- Seiteneffekte:
  - Es wurde versucht, Router über eine Schnittstelle zur Fernwartung zu übernehmen
  - Durch eine fehlerhafte Umsetzung „stürzten“ die Router ab
  - 900.000 Router der Deutschen Telekom waren nicht mehr erreichbar



## Smart Textiles & IT-Sicherheit

### Informatik & Textil

Gestern

Heute

Morgen

[IoT – Internet of Things](#)

Hardware Tools

Ransomware

Zukunft

# Hardware Tools



## Smart Textiles & IT-Sicherheit

### Informatik & Textil

Gestern

Heute

Morgen

IoT – Internet of Things

[Hardware Tools](#)

Ransomware

Zukunft

# IoT – Ransomware



## Smart Textiles & IT-Sicherheit

### Informatik & Textil

Gestern

Heute

Morgen

IoT – Internet of Things

Hardware Tools

Ransomware

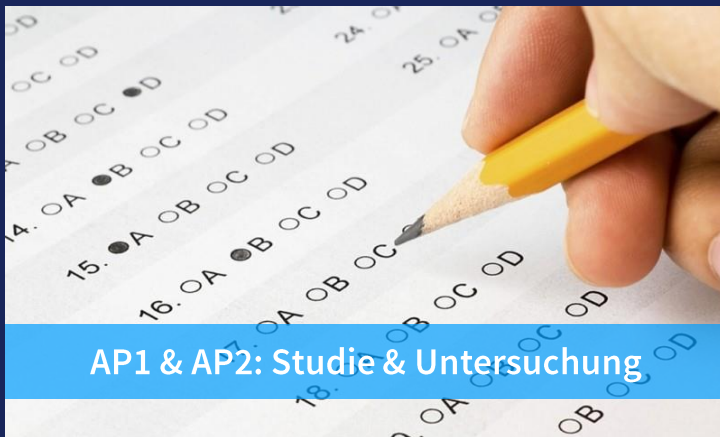
Zukunft



Zukunft

# Projektantrag SEKT

- SEKT - IT-Sicherheit von elektronischen Kommunikationssystemen in smarten textilen Produkten



## Smart Textiles & IT-Sicherheit

Textil & IT

Gestern

Heute

Morgen

Zukunft

[Projektantrag SEKT](#)  
Beispiel RFID

# Beispiel RFID

## Smart Textiles & IT-Sicherheit

Textil & IT

Gestern

Heute

Morgen

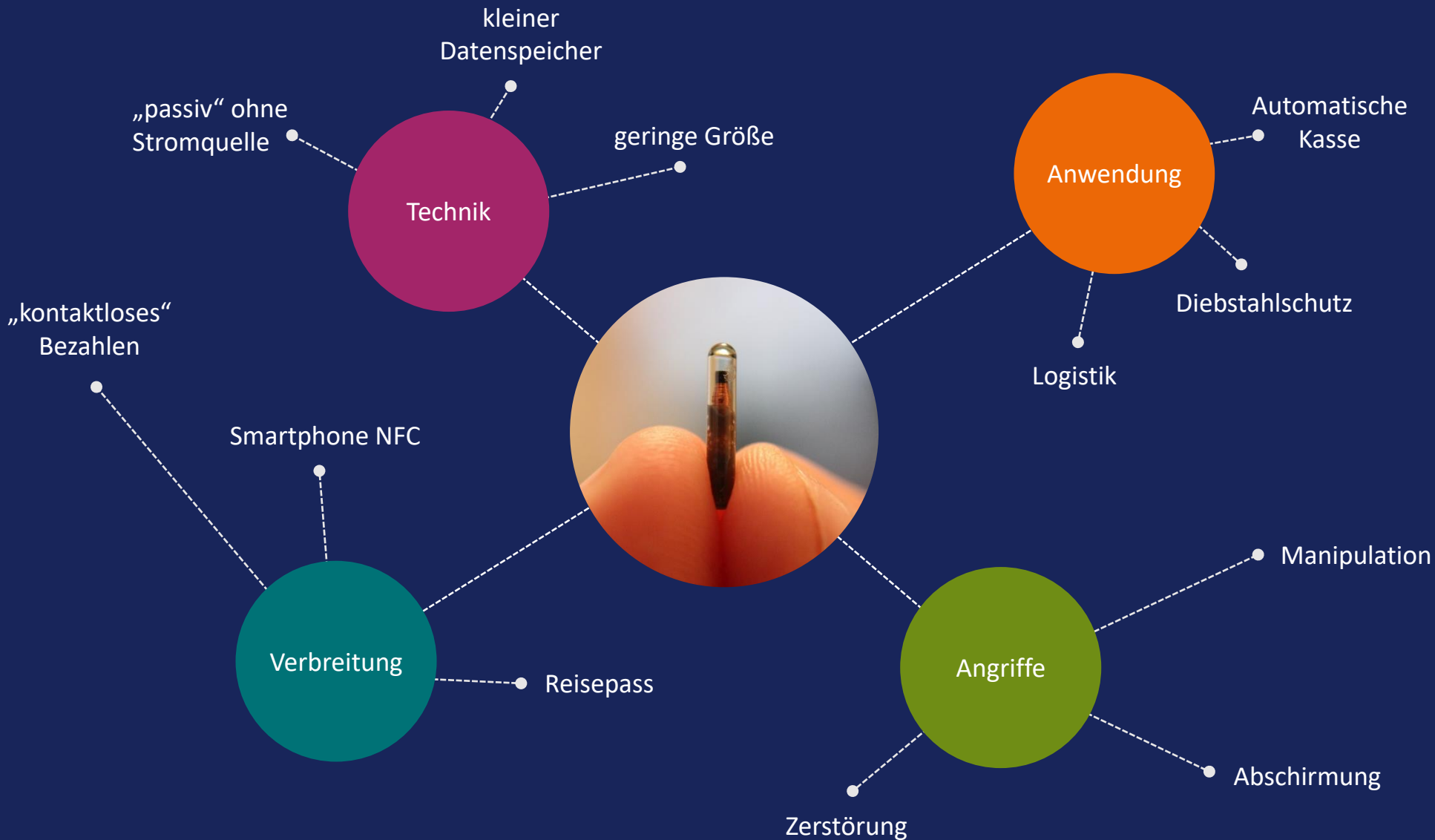
Zukunft

Projektantrag SEKT

[Beispiel RFID](#)

15.11.2018 | GATEX

Tobias Scheible, M.Eng.





# Vielen Dank für Ihre Aufmerksamkeit

Präsentation bald online unter: <https://scheible.it>

# Quellen

- (1) 00000000: Passwort für US-Atomraketen, <http://www.heise.de/security/meldung/00000000-Passwort-fuer-US-Atomraketen-2060077.html>, abgerufen am 14.11.2018
- (2) Was ist eigentlich die Geschichte der Malware?, <https://www.gdata.de/ratgeber/was-ist-eigentlich-die-geschichte-der-malware>, abgerufen am 14.11.2018
- (3) AIDS (Schadprogramm), [https://de.wikipedia.org/wiki/AIDS\\_\(Schadprogramm\)](https://de.wikipedia.org/wiki/AIDS_(Schadprogramm)), abgerufen am 14.11.2018
- (4) Code, <http://pics-for-fun.com/wonder-what-the-code-could-be/>, abgerufen am 14.11.2018
- (5) And the valuables are in the closet on the top shelf in a box marked, <https://de.pinterest.com/pin/3025924727584002/>, abgerufen am 14.11.2018
- (6) The Agency That Messed Up Hawaii's Nuclear Alert Keeps Passwords on Post-Its, [https://www.vice.com/en\\_us/article/qvwmx5/the-agency-that-messed-up-hawaiis-nuclear-alert-keeps-passwords-on-post-its-vgtrn](https://www.vice.com/en_us/article/qvwmx5/the-agency-that-messed-up-hawaiis-nuclear-alert-keeps-passwords-on-post-its-vgtrn), abgerufen am 14.11.2018
- (7) Legisdigit@ - Groupe Mutuel Versicherungen, <https://www.youtube.com/watch?v=WvRL5l1eU3E>, abgerufen am 14.11.2018
- (8) Gefälschte E-Mail Schulfrei ermöglicht, <http://www.spiegel.de/schulspiegel/schulfrei-in-niedersachsen-wegen-gefaelschter-e-mail-a-1071105.html>, abgerufen am 14.11.2018
- (9) Den Enkeltrick gibt's auch bei Unternehmen, <https://www.wiwo.de/erfolg/management/falsche-chefs-zocken-firmen-ab-den-enkeltrick-gibts-auch-bei-unternehmen/12201572.html>, abgerufen am 14.11.2018
- (10) What is Your Password?, <https://www.youtube.com/watch?v=opRMRfAlil>, abgerufen am 14.11.2018
- (11) Top 100 Adobe Passwords with Count, <https://github.com/morontt/symfobroute/blob/master/adobe-top100.txt>, abgerufen am 14.11.2018
- (12) Locky, <https://de.wikipedia.org/wiki/Locky>, abgerufen am 14.11.2018
- (13) UK police arrested the alleged mastermind of the MIRAI attack on Deutsche Telekom, <http://securityaffairs.co/wordpress/56604/cyber-crime/mirai-attack-deutsche-telekom.html>, abgerufen am 14.11.2018

# Quellen

- (14) The Original USB KeyLogger 8MB Black, <http://www.amazon.com/KeyGrabber-USB-KeyLogger-8MB-Black/dp/B004TUBOKW>, abgerufen am 07.07.2018
- (15) Pocket Jammer, <http://www.pki-electronic.com/products/jamming-systems/pocket-jammer/>, abgerufen am 07.07.2018
- (16) Mobile Mini GSM Alarmanlage Quadband mit Rückruffunktion, <https://www.amazon.de/Mobile-Alarmanlage-Quadband-Rückruffunktion-Geräuschaktivierungs-Lautstärke-Schwarz/dp/B00RC7SF8S>, abgerufen am 07.07.2018
- (17) USB Rubber Ducky, <https://hakshop.com/products/usb-rubber-ducky-deluxe>, abgerufen am 07.07.2018
- (18) How do USB killers work?, <https://www.quora.com/How-do-USB-killers-work>, abgerufen am 07.07.2018
- (19) Hackers demonstrated first ransomware for IoT thermostats at DEF CON, <https://www.computerworld.com/article/3105001/security/hackers-demonstrated-first-ransomware-for-iot-thermostats-at-def-con.html>, abgerufen am 14.11.2018