



**Hochschule
Albstadt-Sigmaringen**
Albstadt-Sigmaringen University

Fakultät Informatik

Cyber Security – IT-Angriffe
und Risikofaktor Mensch
InnoCamp Sigmaringen



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
 - Open C³S - Open Competence Center for Cyber Security
 - Tätigkeit in verschiedenen Studiengängen



Cyber Security – IT-Angriffe
und Risikofaktor Mensch

Studium Initiale
(Hochschulzugangsberechtigung)

Zertifikatsprogramm
(Einzelzertifikate)

IT Security
(Bachelor)

Wirtschaftsinformatik
(Bachelor)

IT GRC Management
(Master)

Digitale Forensik
(Master)

- Seit 2019 im Forschungsprojekt SEKT www.projekt-sekt.de

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)

Cyber Security – IT-Angriffe
und Risikofaktor Mensch

Agenda

- Cyber Security
 - PIN Beispiel
 - Schadsoftware
 - Bug or Feature?
 - Suchmaschinen
 - Cybercrime as a Service
 - Internet of Things
- Faktor Mensch
 - Öffentliche Passwörter
 - Social Engineering
 - Versteckte Informationen
 - CEO Fraud
- Hardware Hacks
 - Hardware Tools

Cyber Security – IT-Angriffe
und Risikofaktor Mensch

Cyber Security

Faktor Mensch

Hardware Hacks



Cyber Security

00000000



Cyber Security – IT-Angriffe und Risikofaktor Mensch

Cyber Security

[PIN Beispiel](#)

Schadsoftware

Bug or Feature?

Suchmaschinen

Cybercrime as a Service

Internet of Things

Faktor Maschen

Hardware Hacks

Cyber Security – IT-Angriffe und Risikofaktor Mensch

Cyber Security

[PIN Beispiel](#)

Schadsoftware

Bug or Feature?

Suchmaschinen

Cybercrime as a Service

Internet of Things

Faktor Maschen

Hardware Hacks

00000000

Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

Atomraketen: Steuerungstechnik aus den 70ern



Cyber Security – IT-Angriffe
und Risikofaktor Mensch

Cyber Security

[PIN Beispiel](#)

Schadsoftware

Bug or Feature?

Suchmaschinen

Cybercrime as a Service

Internet of Things

Faktor Maschen

Hardware Hacks

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 (4)

Cyber Security – IT-Angriffe
und Risikofaktor Mensch

Cyber Security
PIN Beispiel
[Schadsoftware](#)
Bug or Feature?
Suchmaschinen
Cybercrime as a Service
Internet of Things

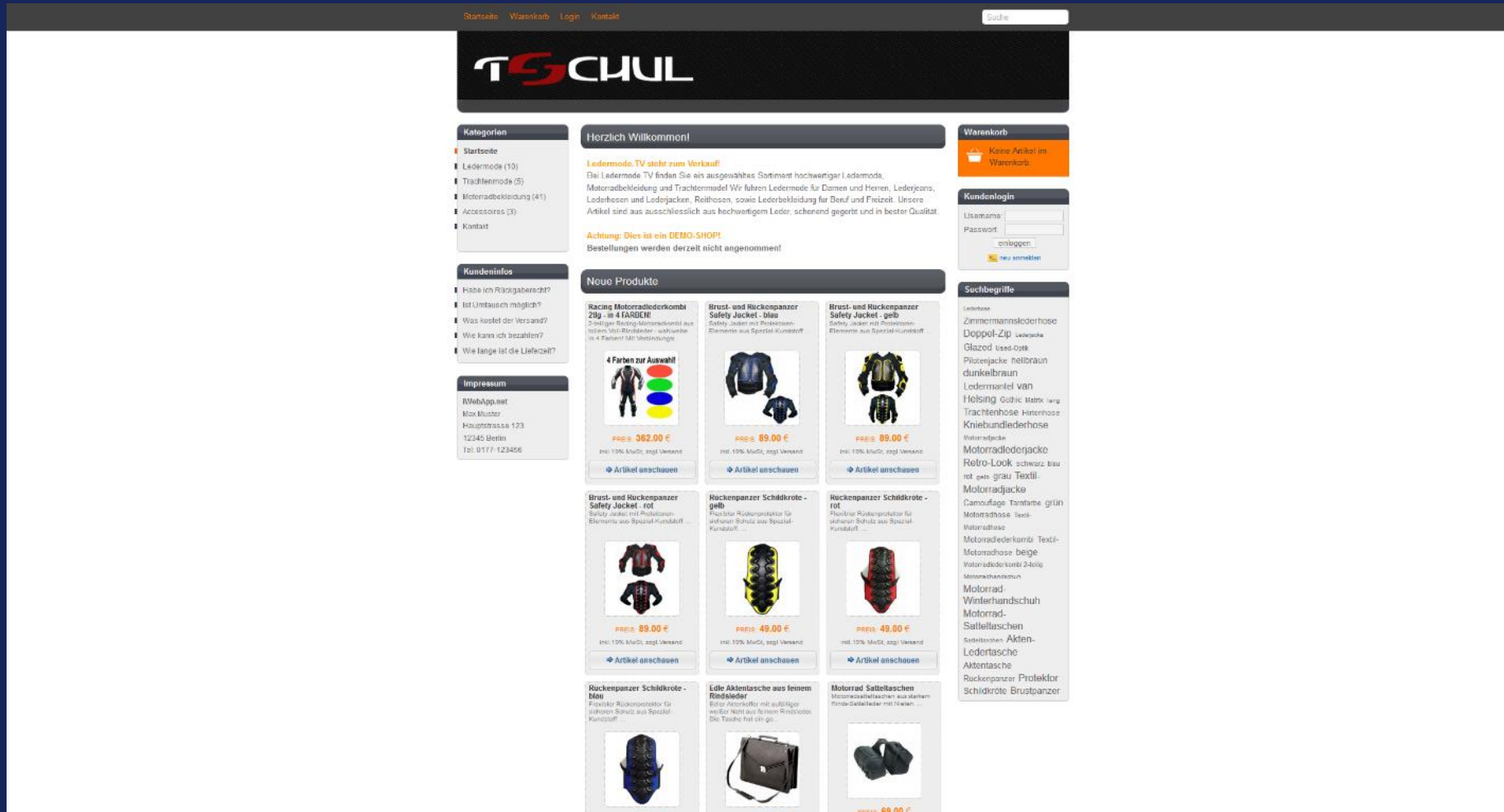
Faktor Maschen

Hardware Hacks

.....
10.04.2019 | InnoCamp Sigmaringen

Tobias Scheible, M.Eng.

DEMO Bug or Feature?



The screenshot shows the website 'ledermode.tv' with a navigation bar at the top containing 'Startseite', 'Warenkorb', 'Login', and 'Kontakt'. A search bar is also present. The main content area is titled 'Herzlich Willkommen' and features a 'Neue Produkte' section with a grid of items. Each item includes a product image, a title, a price, and a button to view the item. The items are:

- Racing Motorradlederkombi 2tlg. - in 4 FARBEN**: Preis: 362,00 €
- Brust- und Rückenpanzer Safety Jacket - blau**: Preis: 89,00 €
- Brust- und Rückenpanzer Safety Jacket - gelb**: Preis: 89,00 €
- 4 Farben zur Auswahl**: Preis: 362,00 €
- Brust- und Rückenpanzer Safety Jacket - rot**: Preis: 89,00 €
- Rückenpanzer Schildekrote - gelb**: Preis: 49,00 €
- Rückenpanzer Schildekrote - rot**: Preis: 49,00 €
- Rückenpanzer Schildekrote - blau**: Preis: 89,00 €
- Edle Aktentasche aus feinem Rindleder**: Preis: 69,00 €
- Motorrad Satteltaschen**: Preis: 69,00 €

Cyber Security – IT-Angriffe und Risikofaktor Mensch

Cyber Security
PIN Beispiel
Schadsoftware
Bug or Feature?

Suchmaschinen
Cybercrime as a Service
Internet of Things

Faktor Maschen

Hardware Hacks

Bug or Feature?

 Alert! 15.01.2016 10:49 Uhr | Security

IP-Kameras von Aldi als Sicherheits-GAU

Aldi hatte vergangenes Jahr mehrfach IP-Überwachungskameras mit denkbar schlechten Voreinstellungen verkauft. Die Geräte sind zu Hunderten fast ungeschützt über das Internet erreichbar.

Von Ronald Eikenberg

   411



Die bei Aldi verkauften IP-Überwachungskameras der Marke Maginon haben massive Sicherheitsprobleme: Unbefugte könnten über das Internet auf das Kamerabild zugreifen und sogar den Ton anzapfen. Zudem verraten die Geräte unter anderem die Passwörter für WLAN, E-Mail und FTP-Zugang ihres Besitzers. Hunderte Aldi-Kameras sind nahezu ungeschützt über das Internet erreichbar. Darauf hat uns der Zusammenschluss Digitale Gesellschaft aufmerksam gemacht.



Betroffen ist unter anderem die Außenkamera IPC-20 C. (Bild: Hersteller)

Drei Modelle sind betroffen

Die Kameras IPC-10 AC, IPC-100 AC und IPC-20 C hat Aldi mit einer Firmware

Cyber Security – IT-Angriffe und Risikofaktor Mensch

Cyber Security

[PIN Beispiel](#)

[Schadsoftware](#)

[Bug or Feature?](#)

[Suchmaschinen](#)

[Cybercrime as a Service](#)

[Internet of Things](#)

Faktor Maschen

Hardware Hacks

Suchmaschine für das Internet der Dinge



The screenshot shows the Shodan website homepage. At the top, there is a navigation bar with the Shodan logo, a search bar, and links for 'Explore', 'Developer Pricing', and 'Enterprise Access'. Below the navigation bar, a large banner features the text 'The search engine for Security' and 'Shodan is the world's first search engine for internet-connected devices.' There are two buttons: 'Create a Free Account' and 'Getting Started'. The main content area is divided into four sections, each with an icon and a title: 'Explore the Internet of Things' (cloud icon), 'See the Big Picture' (globe icon), 'Monitor Network Security' (eye icon), and 'Get a Competitive Advantage' (document icon). Below this, a blue banner highlights '56% of Fortune 100' and '1,000+ Universities'. The next section is titled 'Analyze the Internet in Seconds' and includes a world map and a 'Sample Report on Heartbleed' button. The final section is 'Beyond the Web', which mentions a public API and lists integrations like Nmap, Metasploit, Maltego, FOCA, Chrome, and Firefox.

Cyber Security – IT-Angriffe
und Risikofaktor Mensch

Cyber Security

PIN Beispiel

Schadsoftware

Bug or Feature?

[Suchmaschinen](#)

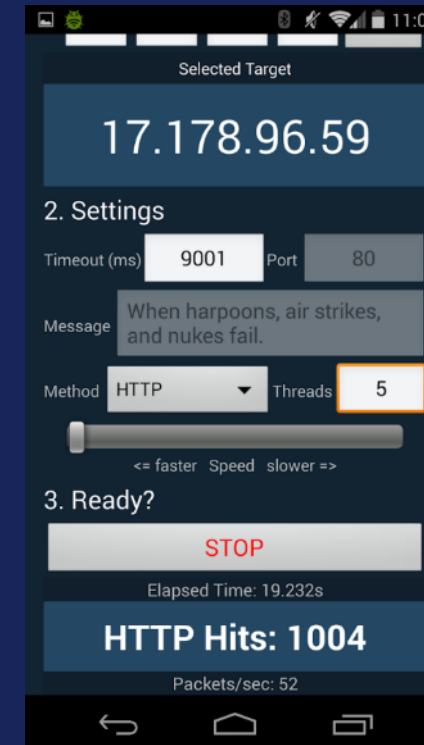
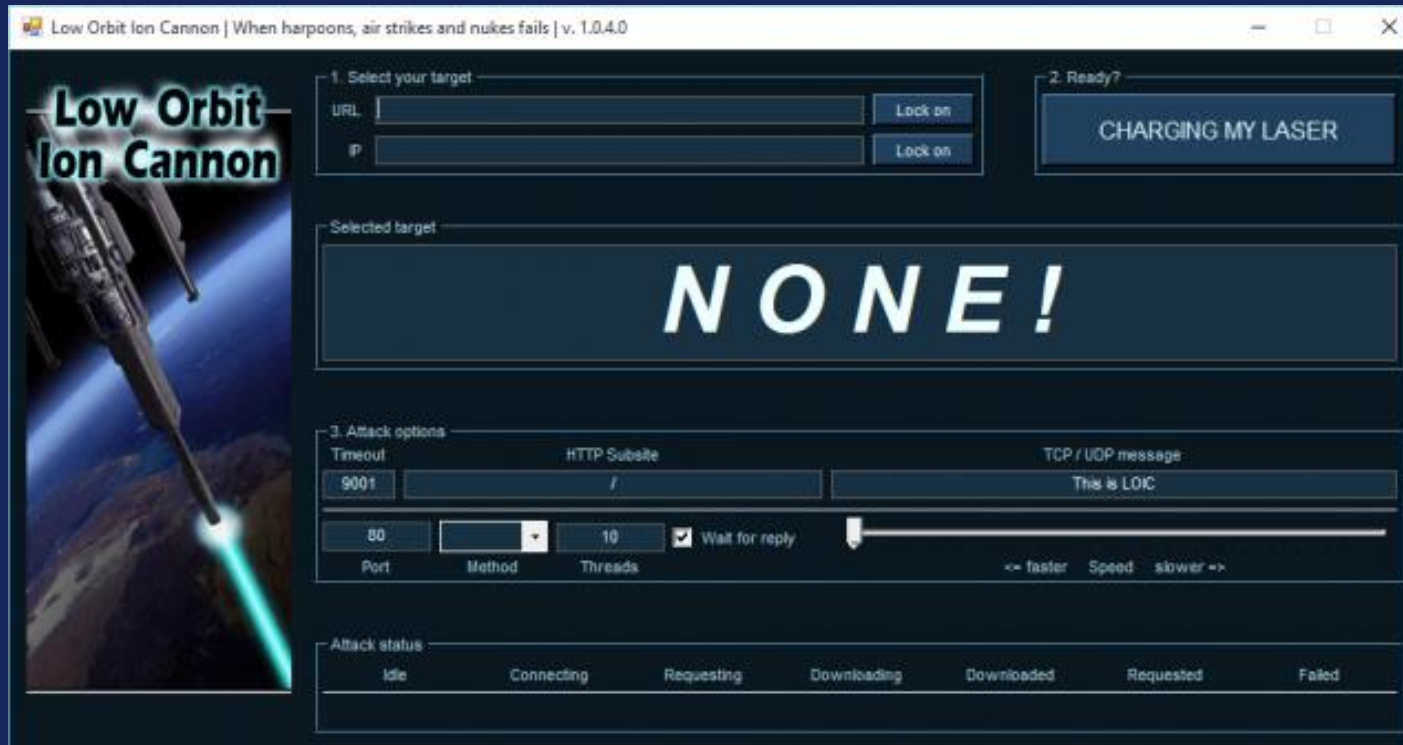
Cybercrime as a Service

Internet of Things

Faktor Maschen

Hardware Hacks

Cybercrime as a Service - Hackaktivisten



Cyber Security – IT-Angriffe
und Risikofaktor Mensch

Cyber Security
PIN Beispiel
Schadsoftware
Bug or Feature?
Suchmaschinen
[Cybercrime as a Service](#)
Internet of Things

Faktor Maschen

Hardware Hacks

Cybercrime as a Service



Quelle: [youtube.com](https://www.youtube.com/watch?v=10) (10)

Cyber Security – IT-Angriffe und Risikofaktor Mensch

Cyber Security

PIN Beispiel

Schadsoftware

Bug or Feature?

Suchmaschinen

[Cybercrime as a Service](#)

Internet of Things

Faktor Maschen

Hardware Hacks

Cybercrime as a Service



Koordinator

Cyber Security – IT-Angriffe und Risikofaktor Mensch

Cyber Security

PIN Beispiel

Schadsoftware

Bug or Feature?

Suchmaschinen

[Cybercrime as a Service](#)

Internet of Things

Faktor Maschen

Hardware Hacks

Cybercrime as a Service - Ransomware Locky

- Effektive Methode, um Geld zu ergaunern
- Auf deutsche Benutzer ausgerichtete Varianten
- Verschlüsselt alle Benutzerdateien, auch auf Netzwerklaufwerken
- 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)

Cyber Security – IT-Angriffe und Risikofaktor Mensch

Cyber Security

- PIN Beispiel
- Schadsoftware
- Bug or Feature?
- Suchmaschinen
- [Cybercrime as a Service](#)
- Internet of Things

Faktor Maschen

Hardware Hacks

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



Cyber Security – IT-Angriffe und Risikofaktor Mensch

Cyber Security

- PIN Beispiel
- Schadsoftware
- Bug or Feature?
- Suchmaschinen
- Cybercrime as a Service
- [Internet of Things](#)

Faktor Maschen

Hardware Hacks

IoT – Ransomware



Cyber Security – IT-Angriffe und Risikofaktor Mensch

Cyber Security

- PIN Beispiel
- Schadsoftware
- Bug or Feature?
- Suchmaschinen
- Cybercrime as a Service
- [Internet of Things](#)

Faktor Maschen

Hardware Hacks

A person is wearing a glowing blue neon mask. The mask has a grid pattern of lines forming a face. The background is dark, and the person's hair is visible. A blue horizontal bar is overlaid on the bottom half of the image.

Faktor Mensch

Was ist die häufigste Angriffsmethode?

Ausnutzung von Schwachstellen

A

Physische Attacken

B

Manipulation von Personen

C

Ausnutzung von Fehlern

D

Cyber Security – IT-Angriffe
und Risikofaktor Mensch

Öffentliche Passwörter



Cyber Security – IT-Angriffe
und Risikofaktor Mensch

Cyber Security

Faktor Maschen

[Öffentliche Passwörter](#)

[Social Engineering](#)

[Versteckte Informationen](#)

[CEO Fraud](#)

Hardware Hacks

Öffentliche Passwörter - Interview



Quelle: youtube.com (16)

Cyber Security – IT-Angriffe
und Risikofaktor Mensch

Cyber Security

Faktor Maschen

Öffentliche Passwörter

Social Engineering

Versteckte Informationen

CEO Fraud

Hardware Hacks

.....
10.04.2019 | InnoCamp Sigmaringen

Tobias Scheible, M.Eng.

Öffentliche Passwörter - Klassiker



Quelle: vice.com (17)

Cyber Security – IT-Angriffe
und Risikofaktor Mensch

Cyber Security

Faktor Maschen

Öffentliche Passwörter

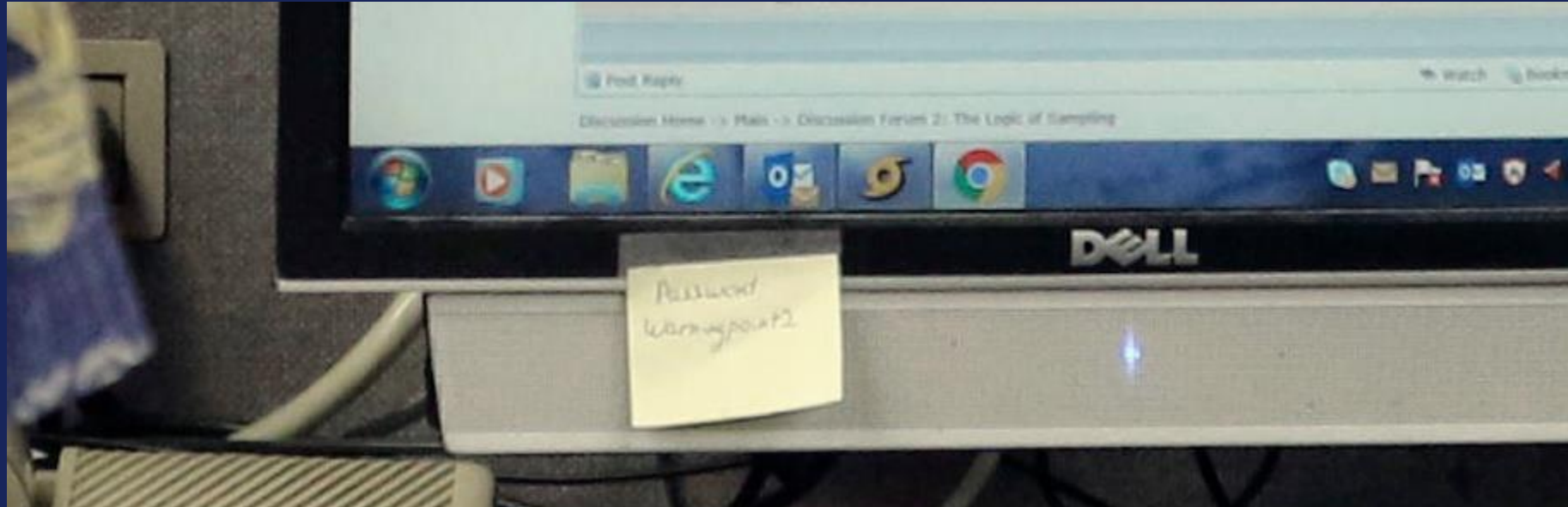
Social Engineering

Versteckte Informationen

CEO Fraud

Hardware Hacks

Öffentliche Passwörter - Klassiker



Klassiker – Post-it Zettel auf Monitor
Passwort: warningpoint2

Cyber Security – IT-Angriffe
und Risikofaktor Mensch

Cyber Security

Faktor Maschen

[Öffentliche Passwörter](#)

[Social Engineering](#)

[Versteckte Informationen](#)

[CEO Fraud](#)

Hardware Hacks

Social Engineering - Gefälschte E-Mail

Cyber Security – IT-Angriffe
und Risikofaktor Mensch

Cyber Security

Faktor Maschen

[Öffentliche Passwörter](#)

[Social Engineering](#)

[Versteckte Informationen](#)

[CEO Fraud](#)

Hardware Hacks

[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 ermöglicht



DPA

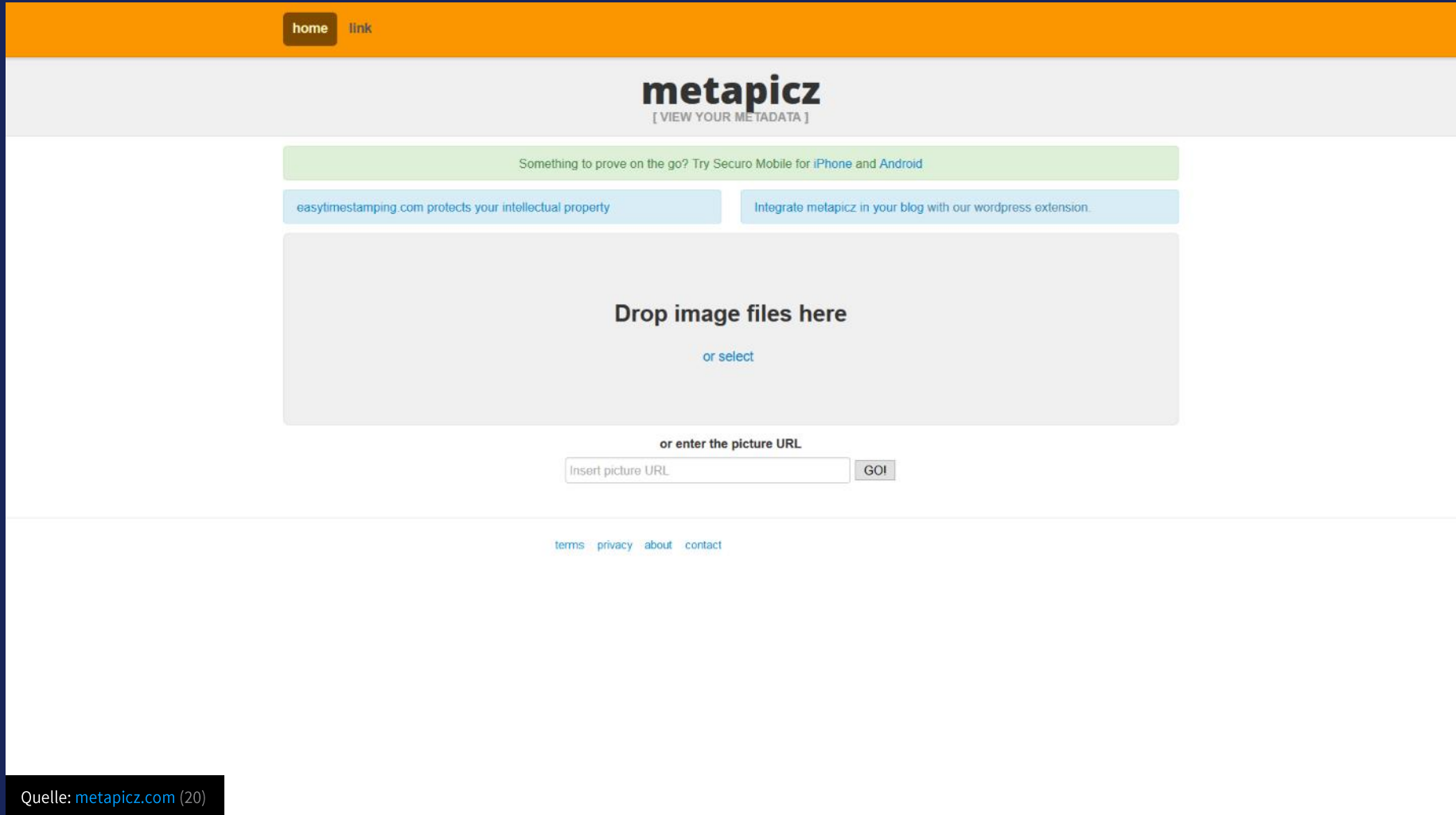
Winterwetter in Niedersachsen: Freier Tag im Schnee wegen gefälschter E-Mail

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.

Social Engineering - Gefängnisausbruch

- Moderner Ausbruch aus einem britischen Gefängnis (März 2015)
- Social Engineering 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

DEMO Versteckte Informationen auslesen



home link

metapicz
[VIEW YOUR METADATA]

Something to prove on the go? Try Securo Mobile for iPhone and Android

easytimestamping.com protects your intellectual property

Integrate metapicz in your blog with our wordpress extension.

Drop image files here
or select

or enter the picture URL

Insert picture URL GO!

terms privacy about contact

Quelle: metapicz.com (20)

Cyber Security – IT-Angriffe
und Risikofaktor Mensch

Cyber Security

Faktor Maschen

[Öffentliche Passwörter](#)

Social Engineering

Versteckte Informationen

CEO Fraud

Hardware Hacks

.....
10.04.2019 | InnoCamp Sigmaringen

Tobias Scheible, M.Eng.

CEO Fraud

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

Den Enkeltrick gibt's auch bei Unternehmen

18. August 2015

★★★★☆
0
Kommentare

Versenden
Drucken
Merken
Startseite



Nicht nur gutgläubige Senioren werden Opfer von Trickbetrügern.

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

Cyber Security – IT-Angriffe und Risikofaktor Mensch

Cyber Security

Faktor Maschen

[Öffentliche Passwörter](#)

[Social Engineering](#)

[Versteckte Informationen](#)

[CEO Fraud](#)

Hardware Hacks

A person wearing a dark hoodie stands in the center of a futuristic hallway. The hallway is illuminated with a grid of glowing blue and purple neon lights that recede into the distance, creating a strong sense of perspective. The person's silhouette is dark against the bright, glowing environment. A semi-transparent blue horizontal bar is overlaid across the middle of the image, containing the text "Hardware Hacks" in white.

Hardware Hacks

Hardware Tools



Cyber Security – IT-Angriffe
und Risikofaktor Mensch

Cyber Security

Faktor Mensch

Hardware Hacks
[Hardware Tools](#)

Vielen Dank für Ihre Aufmerksamkeit



Noch Fragen?

Präsentation 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 23.01.2019
- (2) Mit Floppy Disks Atombomben überwachen, <http://www.zeit.de/politik/ausland/2016-05/us-militaer-pcs-technologie-veraltet-rechnungshof>, abgerufen am 23.01.2019
- (3) Was ist eigentlich die Geschichte der Malware?, <https://www.gdata.de/ratgeber/was-ist-eigentlich-die-geschichte-der-malware>, abgerufen am 23.01.2019
- (4) AIDS (Schadprogramm), [https://de.wikipedia.org/wiki/AIDS_\(Schadprogramm\)](https://de.wikipedia.org/wiki/AIDS_(Schadprogramm)), abgerufen am 23.01.2019
- (5) iWebapp, <http://www.shop.ledermode.tv>, abgerufen am 23.01.2019
- (6) IP-Kameras von Aldi als Sicherheits-GAU, <http://www.heise.de/security/meldung/IP-Kameras-von-Aldi-als-Sicherheits-GAU-3069735.html>, abgerufen am 23.01.2019
- (7) Shodan, <https://www.shodan.io>, abgerufen am 23.01.2019
- (8) Low Orbit Ion Cannon (LOIC), https://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon#/media/File:LOIC-0.png, abgerufen am 23.01.2019
- (9) LOIC - Low Orbit Ion Cannon, <http://m.1mobile.com/genius.mohammad.loic.html>, abgerufen am 23.01.2019
- (10) Anuncio - gwapo's, <https://www.youtube.com/watch?v=5M9k7wfiWil>, abgerufen am 23.01.2019
- (11) Locky, <https://de.wikipedia.org/wiki/Locky>, abgerufen am 23.01.2019
- (12) 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 23.01.2019
- (13) 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 23.01.2019

Quellen

- (14) Code, <http://pics-for-fun.com/wonder-what-the-code-could-be/>, abgerufen am 23.01.2019
- (15) And the valuables are in the closet on the top shelf in a box marked, <https://de.pinterest.com/pin/3025924727584002/>, abgerufen am 23.01.2019
- (16) What is Your Password?, <https://www.youtube.com/watch?v=opRMrEfAlil>, abgerufen am 23.01.2019
- (17) 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-hawaiiis-nuclear-alert-keeps-passwords-on-post-its-vgtrn, abgerufen am 23.01.2019
- (18) Gefälschte E-Mail - Schulfrei ermogelt, <http://www.spiegel.de/schulspiegel/schulfrei-in-niedersachsen-wegen-gefaelschter-e-mail-a-1071105.html>, abgerufen am 23.01.2019
- (19) Gefängnisausbruch mittels E-Mail-Betrug, <http://www.heise.de/newsticker/meldung/Gefaengnisausbruch-mittels-E-Mail-Betrug-2587303.html>, abgerufen am 23.01.2019
- (20) Metapicz, abgerufen am 09.04.2019
- (21) 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 23.01.2019
- (27) The Original USB KeyLogger 8MB Black, <http://www.amazon.com/KeyGrabber-USB-KeyLogger-8MB-Black/dp/B004TUBOKW>, abgerufen am 23.01.2019
- (28) Pocket Jammer, <http://www.pki-electronic.com/products/jamming-systems/pocket-jammer/>, abgerufen am 23.01.2019
- (29) Mobile Mini GSM Alarmanlage Quadband mit Rückruffunktion, <https://www.amazon.de/Mobile-Alarmanlage-Quadband-Rückruffunktion-Geräuschaktivierungs-Lautstärke-Schwarz/dp/B00RC7SF8S>, abgerufen am 23.01.2019
- (30) USB Rubber Ducky, <https://hakshop.com/products/usb-rubber-ducky-deluxe>, abgerufen am 23.01.2019
- (31) How do USB killers work?, <https://www.quora.com/How-do-USB-killers-work>, abgerufen am 23.01.2019