



Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

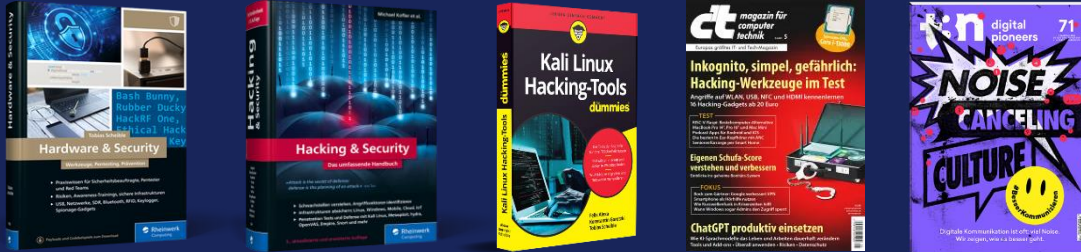
Institut für Wissenschaftliche Weiterbildung (IWW)

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle IT-SAD



Tobias Scheible, M.Eng.

- 1999 GeoCities, 2000 Domain, 2001 Kundenprojekte & ab 2010 eigener Blog
- 2009 bis 2012: Softwareingenieur im Bereich Web Development (Gute Aussicht)
- Seit 2012: Akademischer Mitarbeiter an der Hochschule Albstadt-Sigmaringen
- Autor, Blogger, Referent & Dozent



Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Agenda

- Hacking Hardware

- Pentest- & Hacking-Tools
- Angriffsszenarien
- Bezugsquellen

- Keylogger

- USB-Keylogger
- WLAN-Keylogger
- Keylogger-Kabel
- Exkurs: Screenlogger

- BadUSB

- Rubber Ducky
- DSTIKE WIFI Duck
- USBNinja
- BashBunny
- EXKURS USB-Killer

- Gegenmaßnahmen

- Software
- Hardware

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hinweis

Die komplette Präsentation wird im Anschluss unter tu-braunschweig.de/ciso/it-sad/ und scheible.it bereitgestellt.



Hacking Hardware

Pentest- & Hacking-Tools

Hacking Hardware (Hacking Gadgets, Pentest Hardware/Tools, IT Security Hardware/Tools): Geräte, mit denen Rechnersysteme oder Kommunikationsverbindungen angegriffen werden können. Dabei handelt es sich um kompakte Geräte mit einem Mikrocontroller, die vorab programmierte Befehle ausführen. Zum Teil können sie über Funk-Chips ferngesteuert werden.

- Sie wurden für White Hat Hacker, Penetration-Tester, Security-Forscher und Sicherheitsbeauftragte entwickelt, um Schwachstellen aufzuspüren und anschließend schließen zu können.
- Sie werden auch immer wieder von kriminellen Angreifern eingesetzt.
 - Es handelt sich dabei um sehr gezielte Angriffe
 - Meist werden diese Geräte von Innentätern eingesetzt
 - Hacking Hardware ist i.d.R. einfach zu bedienen

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware
[Pentest- & Hacking-Tools](#)
Angriffsszenarien
Bezugsquellen

Keylogger

BadUSB

Gegenmaßnahmen

Angriffsszenario



Spionage-Gadgets



USB-Keylogger



Opfer



Screenlogger



ehemaliges oder frustriertes Personal



Personal von Drittfirmen



Praktikanten/-innen



falsche Kunden/Interessenten

Angreifer
Innentäter

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Pentest- & Hacking-Tools

[Angriffsszenarien](#)

Bezugsquellen

Keylogger

BadUSB

Gegenmaßnahmen

Bezugsquellen

- IT Security Hardware muss nicht über zwielichtige Kanäle oder gar über das Darknet beschafft werden, sondern kann teilweise z.B. über die Onlineshops von Amazon und eBay einfach bestellt werden.
- Neben großen Shoppingplattformen gibt es mehrere Onlineshops, die sich auf den Vertrieb dieser Art von Hardware spezialisiert haben.
- In Deutschland werden diese Geräte auch häufig über Online-Shops angeboten, die im Bereich der Detektivausrüstung aktiv sind.
- Einige Geräte sind in Deutschland nicht erlaubt, können jedoch sehr einfach im Ausland bestellt werden – teilweise auch in EU-Nachbarstaaten.

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware
Pentest- & Hacking-Tools
Angriffsszenarien
Bezugsquellen

Keylogger

BadUSB

Gegenmaßnahmen

A blurred background image of a person with dark hair, wearing a red shirt, sitting at a desk and looking at a computer monitor. The office has a modern design with a ceiling made of horizontal wooden slats and several long, horizontal light fixtures. A semi-transparent blue banner is overlaid across the middle of the image.

Keylogger

USB-Keylogger



Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

USB-Keylogger

WLAN-Keylogger

Keylogger-Kabel

Realer Vorfall

Exkurs: Screenlogger

BadUSB

Gegenmaßnahmen

WLAN-Keylogger



Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

USB-Keylogger

[WLAN-Keylogger](#)

Keylogger-Kabel

Realer Vorfall

Exkurs: Screenlogger

BadUSB

Gegenmaßnahmen

Keylogger-Kabel



Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

USB-Keylogger

WLAN-Keylogger

Keylogger-Kabel

Realer Vorfall

Exkurs: Screenlogger

BadUSB

Gegenmaßnahmen

Realer Vorfall - Keylogger

Keylogger-Affäre in der taz

Dateiname LOG.TXT

Anfang 2015 kam heraus, dass Computer in der taz mehr als ein Jahr lang ausgespäht wurden. Die Recherche zum Fall führt bis nach Asien.



Der Keylogger wurde inzwischen an die Polizei übergeben

Foto: taz

Ein Editorial der taz zu dieser Recherche [findet sich hier](#).

Es ist wohl reiner Zufall, dass der Keylogger am Ende entdeckt wird. Mindestens ein Jahr lang ist er zuvor im Einsatz. Er wandert von Computer zu Computer, im ersten, dritten und vierten Stock der Rudi-Dutschke-Str. 23 und schneidet dort die Tastaturanschlüsse mit, Passwörter, Mails, Kontodaten. Das geht so lange, bis am Nachmittag des 17. Februar 2015, ein Dienstag, die Computertastatur einer Praktikantin nicht mehr funktioniert.

Quelle: [taz.de](https://www.taz.de) (1)

SCHWERPUNKT ÜBERWACHUNG



Gesellschaft / Medien

4. 6. 2016



MARTIN KAUL

Reporter



SEBASTIAN ERB

Reporter



THEMEN

[#Keylogger](#)

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

- USB-Keylogger
- WLAN-Keylogger
- Keylogger-Kabel
- Realer Vorfall
- Exkurs: Screenlogger

BadUSB

Gegenmaßnahmen

.....
10.15.2023 | IT-SAD

Tobias Scheible, M.Eng.

EXKURS Screenlogger - VideoGhost

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

- USB-Keylogger
- WLAN-Keylogger
- Keylogger-Kabel
- Realer Vorfall
- Exkurs: Screenlogger

BadUSB

Gegenmaßnahmen



EXKURS Screenlogger - Screen Grab



Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

- USB-Keylogger
- WLAN-Keylogger
- Keylogger-Kabel
- Realer Vorfall
- Exkurs: Screenlogger

BadUSB

Gegenmaßnahmen



BadUSB

Rubber Ducky



Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

BadUSB

[Rubber Ducky](#)

DSTIKE WIFI Duck

USBNinja

BashBunny

Realer Vorfall

EXKURS USB-Killer

Realer Vorfall

Gegenmaßnahmen

DSTIKE WIFI Duck

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

BadUSB

Rubber Ducky

[DSTIKE WIFI Duck](#)

USBNinja

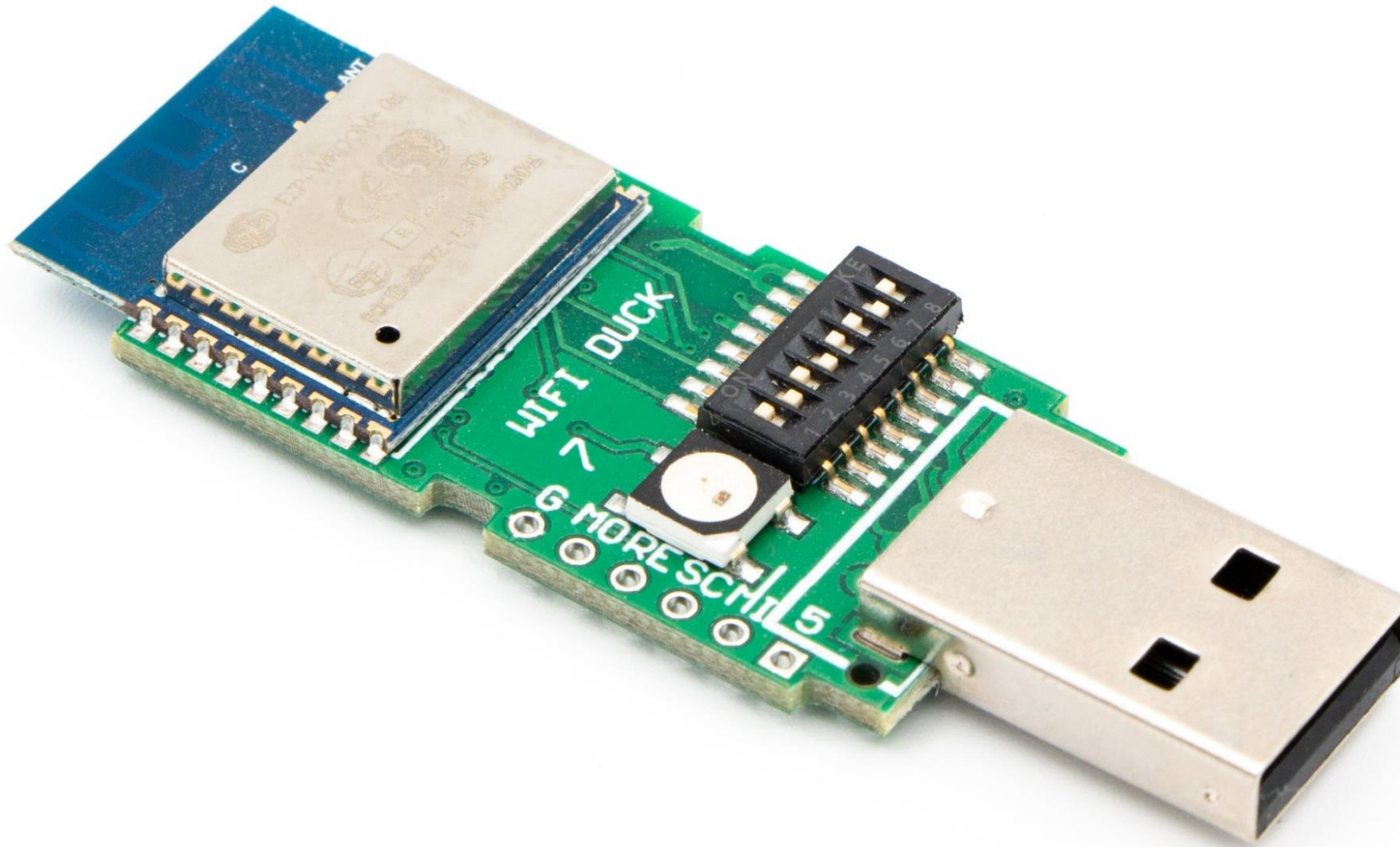
BashBunny

Realer Vorfall

EXKURS USB-Killer

Realer Vorfall

Gegenmaßnahmen





Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

BadUSB

- Rubber Ducky
- DSTIKE WIFI Duck
- [USBNinja](#)
- BashBunny
- Realer Vorfall
- EXKURS USB-Killer
- Realer Vorfall

Gegenmaßnahmen

BashBunny



Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

BadUSB

- Rubber Ducky
- DSTIKE WIFI Duck
- USBNinja
- BashBunny
- Realer Vorfall
- EXKURS USB-Killer
- Realer Vorfall

Gegenmaßnahmen

Realer Vorfall - BadUSB

The Record

BY RECORDED FUTURE

About

Contact

Podcast

Q

Leadership

Cybercrime

Nation-state

Government

People

Technology

Subscribe




IMAGE: THE RECORD, ALIEXPRESS

Catalin Cimpanu

January 7, 2022

Cybercrime

Government

Malware

News

FBI: FIN7 hackers target US companies with BadUSB devices to install ransomware

The US Federal Bureau of Investigation says that FIN7, an infamous cybercrime group that is behind the Darkside and BlackMatter ransomware operations, has sent malicious USB devices to US companies over the past few months in the hopes of infecting their systems with malware and carrying out future attacks.

“Since August 2021, the FBI has received reports of several packages containing these USB devices, sent to US businesses in the transportation, insurance, and defense industries,” the Bureau said in a security alert sent yesterday to US organizations.

“The packages were sent using the United States Postal Service and United Parcel Service,” the agency added.

“There are two variations of packages—those imitating HHS [US Department of Health and Human Services] are often accompanied by letters referencing COVID-19 guidelines enclosed with a USB; and those imitating Amazon arrived in a decorative gift box containing a fraudulent thank you letter, counterfeit gift card, and a USB.”

In both cases, the packages contained LilyGO-branded USB devices.

Some BadUSB attacks lead to ransomware

But the FBI says that if recipients plugged the USB thumb drives into their computers, the devices would execute a **BadUSB attack**, where the USB drive would register itself as a keyboard instead and send a series of preconfigured automated keystrokes to the user’s PC.

BRIEFS

F5 investigating reports of NGINX zero day

April 11, 2022

BlackCat ransomware group claims attack on Florida International University

April 11, 2022

WonderHero game disabled after hackers steal \$320,000 in cryptocurrency

April 7, 2022

Researcher finds cryptomining malware targeting AWS Lambda

April 6, 2022

Block says former Cash App employee accessed data from US customer accounts

April 6, 2022

Ukrainian CERT details Russia-linked phishing attacks targeting government officials

April 5, 2022

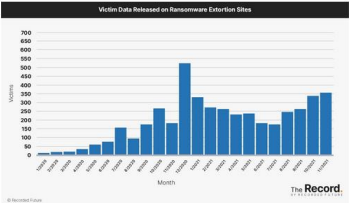
German wind turbine maker shut down after cyberattack

April 4, 2022

Hacker accessed 319 crypto- and finance-related Mailchimp accounts, company said

April 4, 2022

RANSOMWARE TRACKER: THE LATEST FIGURES [MARCH 2022]



RANSOMWARE TRACKER: THE LATEST FIGURES [MARCH 2022]

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

BadUSB

- Rubber Ducky
- DSTIKE WIFI Duck
- USBNinja
- BashBunny
- Realer Vorfall
- EXKURS USB-Killer
- Realer Vorfall

Gegenmaßnahmen

Quelle: therecord.media (2)

10.15.2023 | IT-SAD

Tobias Scheible, M.Eng.

23

EXKURS USB-Killer - USBKill



Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

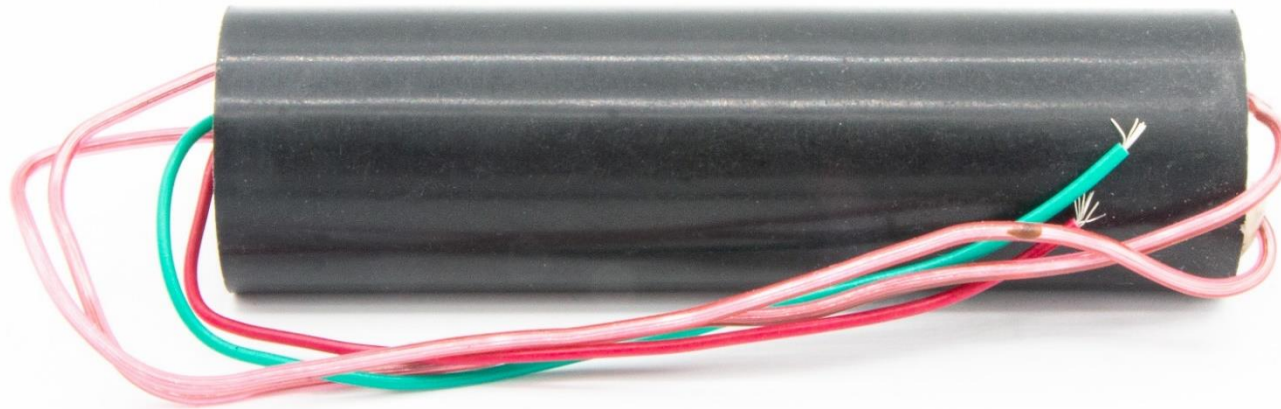
Keylogger

BadUSB

- Rubber Ducky
- DSTIKE WIFI Duck
- USBNinja
- BashBunny
- Realer Vorfall
- EXKURS USB-Killer
- Realer Vorfall

Gegenmaßnahmen

EXKURS USB-Killer - Stromschock



Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

BadUSB

- Rubber Ducky
- DSTIKE WIFI Duck
- USBNinja
- BashBunny
- Realer Vorfall
- EXKURS USB-Killer
- Realer Vorfall

Gegenmaßnahmen

Realer Vorfall – USB-Killer

THE VERGE

TECH ▾ REVIEWS ▾ SCIENCE ▾ CREATORS ▾ ENTERTAINMENT ▾ VIDEO FEATURES MORE ▾



POLICY US & WORLD TECH

Student used 'USB Killer' device to destroy \$58,000 worth of college computers 46

The former College of Saint Rose student faces up to 10 years in prison

By Chris Welch | @chriswelch | Apr 17, 2019, 3:07pm EDT



Quelle: theverge.com (3)

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

BadUSB

- Rubber Ducky
- DSTIKE WIFI Duck
- USBNinja
- BashBunny
- Realer Vorfall
- EXKURS USB-Killer
- Realer Vorfall

Gegenmaßnahmen

.....
10.15.2023 | IT-SAD

Tobias Scheible, M.Eng.

A blurred background image of an office interior. Several people are visible working at desks with computer monitors. Large windows in the background let in bright light. A solid blue horizontal band is overlaid across the middle of the image, containing the text 'Gegenmaßnahmen' in white.

Gegenmaßnahmen

- Generelle Maßnahmen
 - Zugangsbeschränkung, damit nur autorisierte Personen Zutritt haben
 - Übersichtliche und aufgeräumte Arbeitsplätze und Büros
 - Schulungen, damit Hacking Hardware erkannt wird
- Sicherung von Rechnersystemen durch bauliche Maßnahmen
- Erkennen und Melden von Unterbrechungen, wenn die Verbindung zu einzelnen Geräten verloren gegangen ist
- Key- & Screenlogger
 - Mobile Rechner sind unterwegs nicht betroffen, aber evtl. mit Docking Station
 - Tastaturen, die mit Bluetooth (integriertes Modul) angebunden sind, sind nicht betroffen
- BadUSB
 - Rechner sperren, damit während der Abwesenheit kein BadUSB-Gerät angeschlossen wird

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

BadUSB

Gegenmaßnahmen

Allgemein

Software

Hardware

Software

- Verwendung von Sicherheitssoftware (z.B. USB Keyboard Guard), die den Typ von USB-Geräten erkennt
- Windows: Konfiguration per Gruppenrichtlinien möglich, damit keine neue Tastaturen hinzugefügt werden können
- Linux: Ähnliche Konfiguration per *udev* Regeln möglich
- BIOS/UEFI Konfiguration
 - Deaktivierung von ungenutzten Schnittstellen

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

BadUSB

Gegenmaßnahmen

Allgemein

Software

Hardware

Hardware

- USB-Netzteil



- USB-Protector



- USB-Schlösser



Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

Keylogger

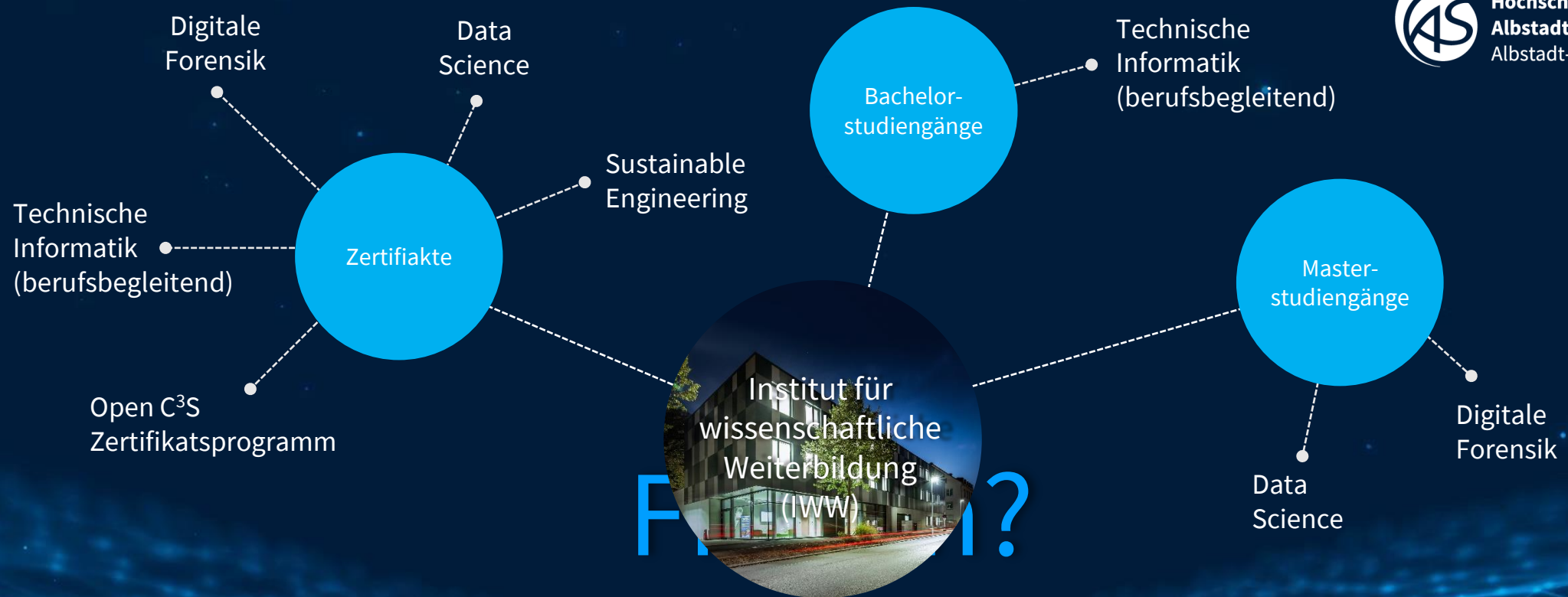
BadUSB

Gegenmaßnahmen

Allgemein

Software

Hardware



Vielen Dank für Ihre Aufmerksamkeit

Weitere IT-SAD Vorträge: <https://www.tu-braunschweig.de/ciso/it-sad/>

Quellen

- 1) Keylogger-Affäre in der taz - Dateiname LOG.TXT, <https://taz.de/Keylogger-Affaere-in-der-taz/!5307828/>, abgerufen am 09.05.2023
- 2) FBI: FIN7 hackers target US companies with BadUSB devices to install ransomware, <https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install-ransomware/>, abgerufen am 09.05.2023
- 3) Student used 'USB Killer' device to destroy \$58,000 worth of college computers, <https://www.theverge.com/2019/4/17/18412427/college-saint-rose-student-guilty-usb-killer-destroyed-computers>, abgerufen am 09.05.2023

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle