Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für Wissenschaftliche Weiterbildung (IWW)

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

IT-SAD

Tobias Scheible, M.Eng.

Tobias Scheible, M.Eng.

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

- 1999 GeoCities Website, 2000 eigene Domain, 2001 Kundenprojekte
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter
  - Aktuelle & ehemalige Lehrmodule (Auswahl):
    - Netzsicherheit I: IT-Sicherheit von Netzwerken Hochschulzertifikatsprogramm
    - Grundlagen der digitalen Forensik Masterstudiengang IT GRC Management
    - Internettechnologien Hochschulzertifikatsprogramm
    - Cloud Technologies and Cloud Security Architectures Masterstudiengang IT GRC Management
    - Digitale Forensik Bachelorstudiengang IT Security
    - Internet Grundlagen Masterstudiengang Digitale Forensik
    - Informationssicherheit Bachelorstudiengang Wirtschaftsinformatik
- Buch- & Zeitschriftenautor, Blogger, Referent, …

**Keylogger & BadUSB –
Angriffe über die USB-Schnittstelle**

Hochschule Albstadt-Sigmaringen

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

Fakultät Engineering

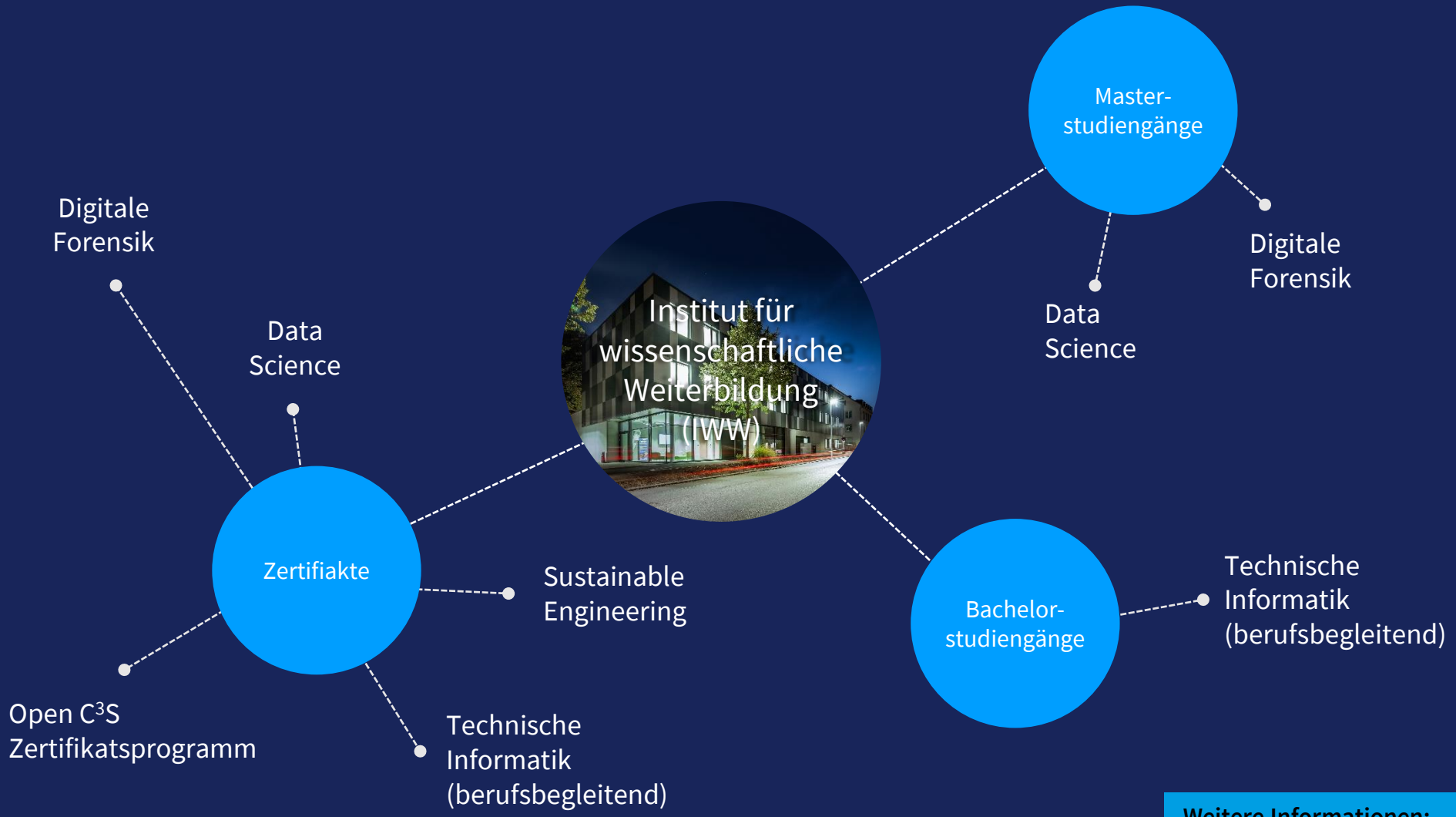
Fakultät Business Science and Management

Fakultät Life Sciences

Fakultät Informatik

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Institut für wissenschaftliche Weiterbildung



Weitere Informationen:
www.hs-albsig.de/iww

**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

Hinweis
Die komplette Präsentation wird im Anschluss unter *blogs.tu-braunschweig.de/it/* und *www.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

Angriffsszenario

Spionage-Gadgets

USB-Keylogger

Opfer

Screenlogger

ehemaliges oder frustriertes Personal

Personal von Drittfirmen

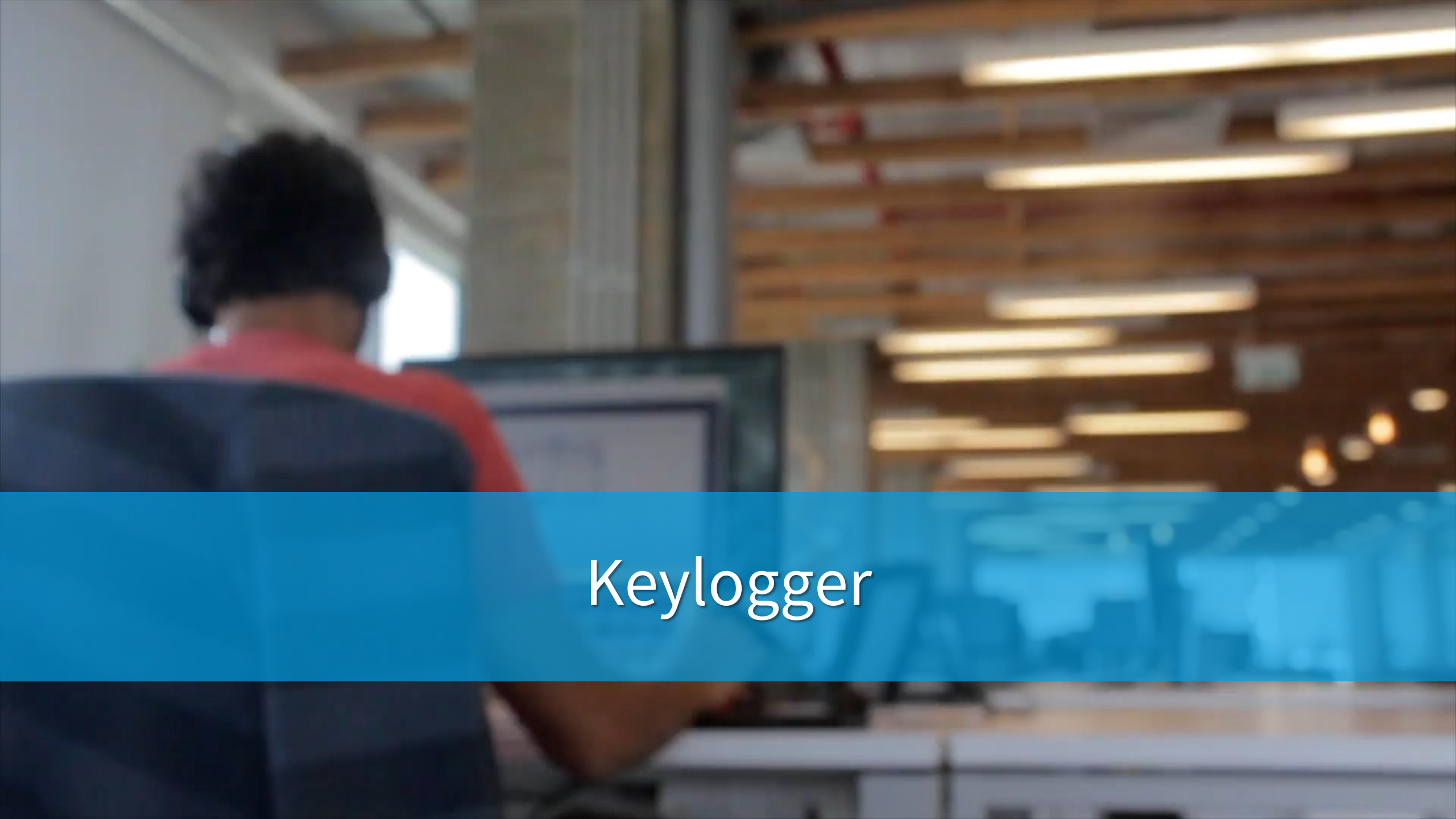
Praktikanten/-innen

falsche Kunden/Interessenten

Angreifer
Innentäter

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

USB-Keylogger

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für Wissenschaftliche Weiterbildung (IWW)

WLAN-Keylogger

Keylogger-Kabel

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für Wissenschaftliche Weiterbildung (IWW)

**Keylogger & BadUSB –
Angriffe über die USB-Schnittstelle**

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 Tastaturanschläge mit, Passwörter, Mails, Kontodaten. Das geht so lange, bis am Nachmittag des 17. Februar 2015, ein Dienstag, die Computertastatur einer Praktikantin nicht mehr funktioniert.

SCHWERPUNKT ÜBERWACHUNG

Gesellschaft / Medien 4. 6. 2016

MARTIN KAUL
Reporter

SEBASTIAN ERB
Reporter

THEMEN
#Keylogger

Quelle: taz.de (1)

EXKURS Screenlogger - VideoGhost

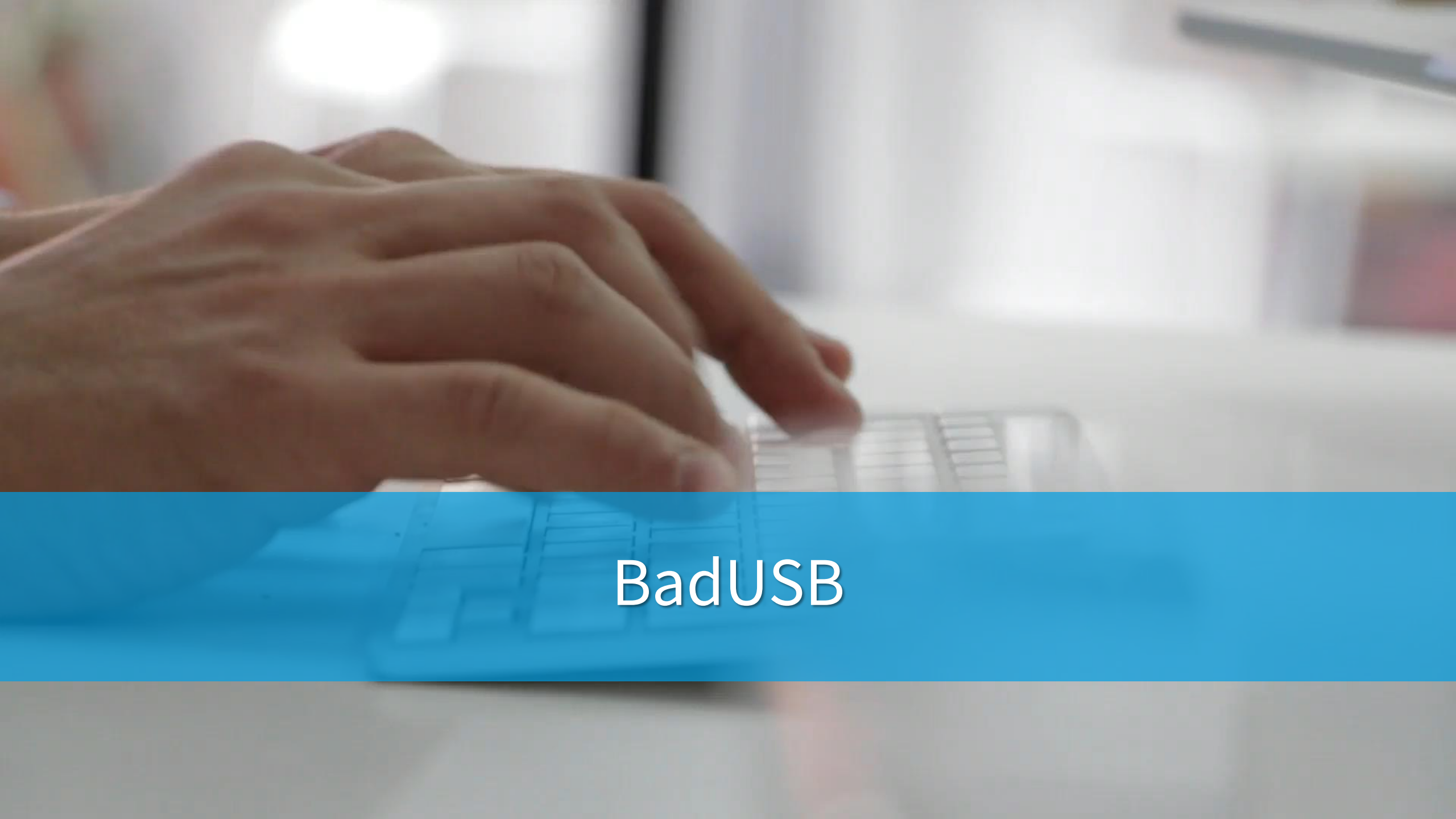
Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für Wissenschaftliche Weiterbildung (IWW)

EXKURS Screenlogger - Screen Grab

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

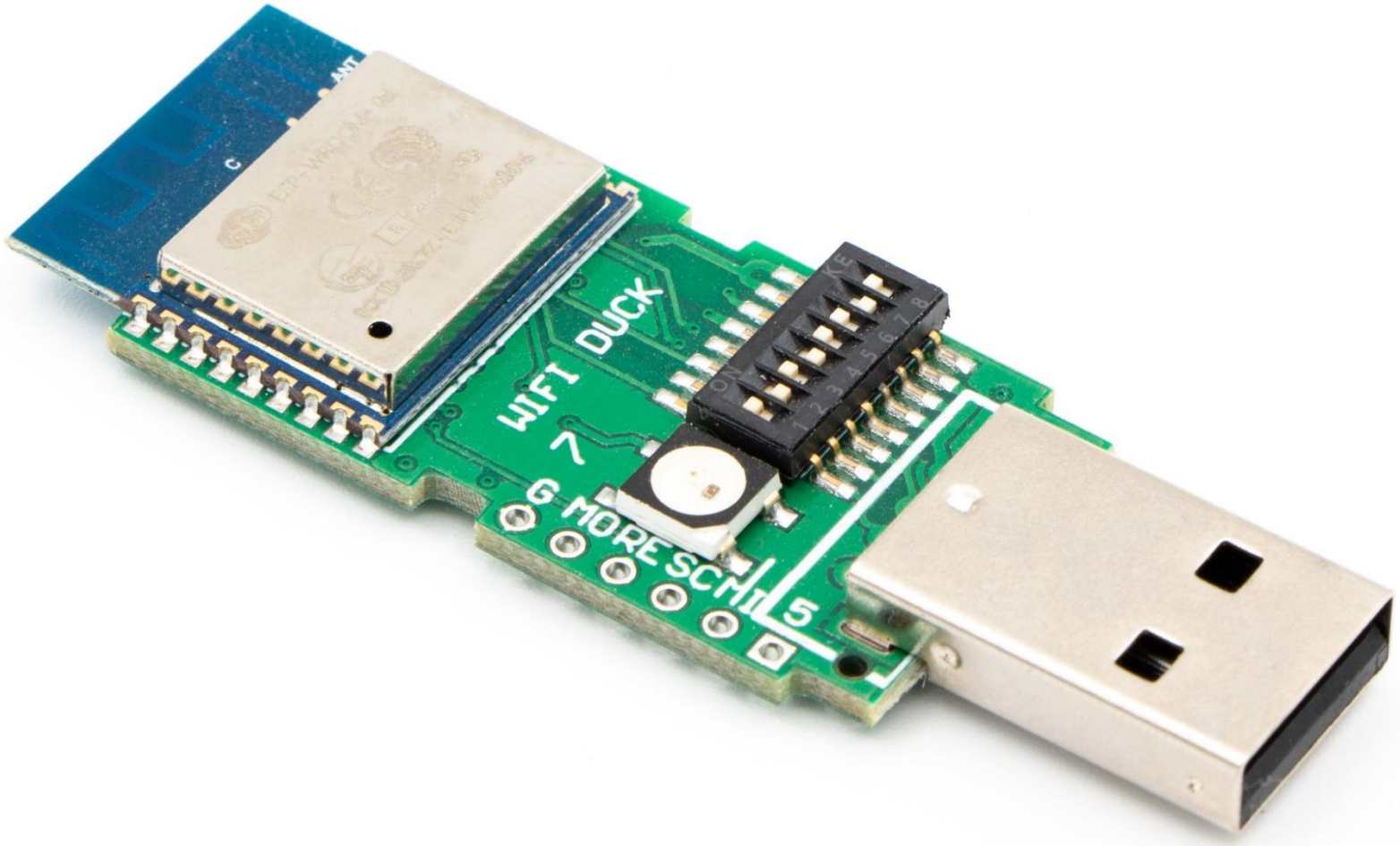
Institut für Wissenschaftliche Weiterbildung (IWW)



BadUSB

Rubber Ducky

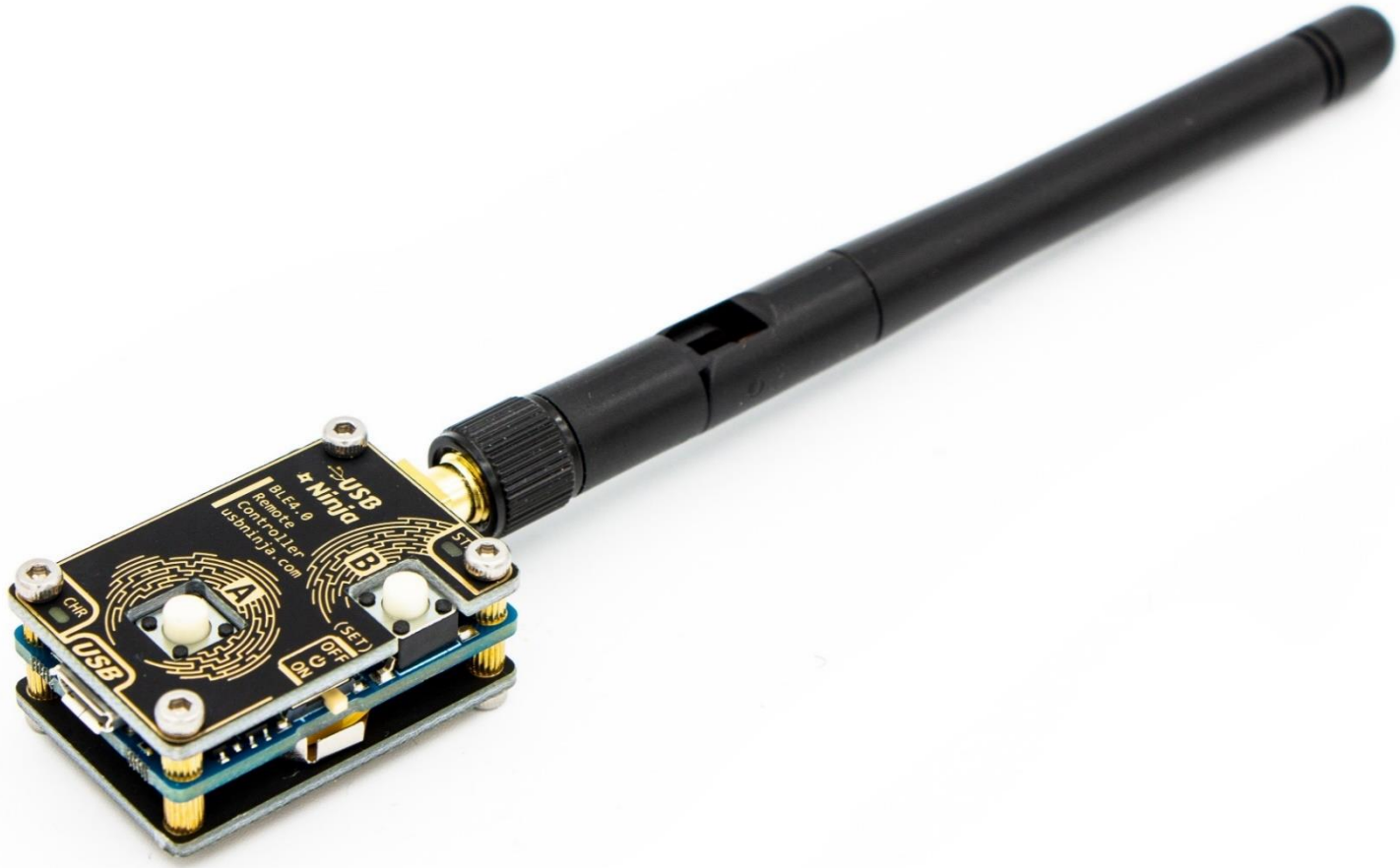
DSTIKE WIFI Duck



USBNinja

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für Wissenschaftliche Weiterbildung (IWW)



Keylogger & BadUSB –
Angriffe über die USB-Schnittstelle

Hacking Hardware

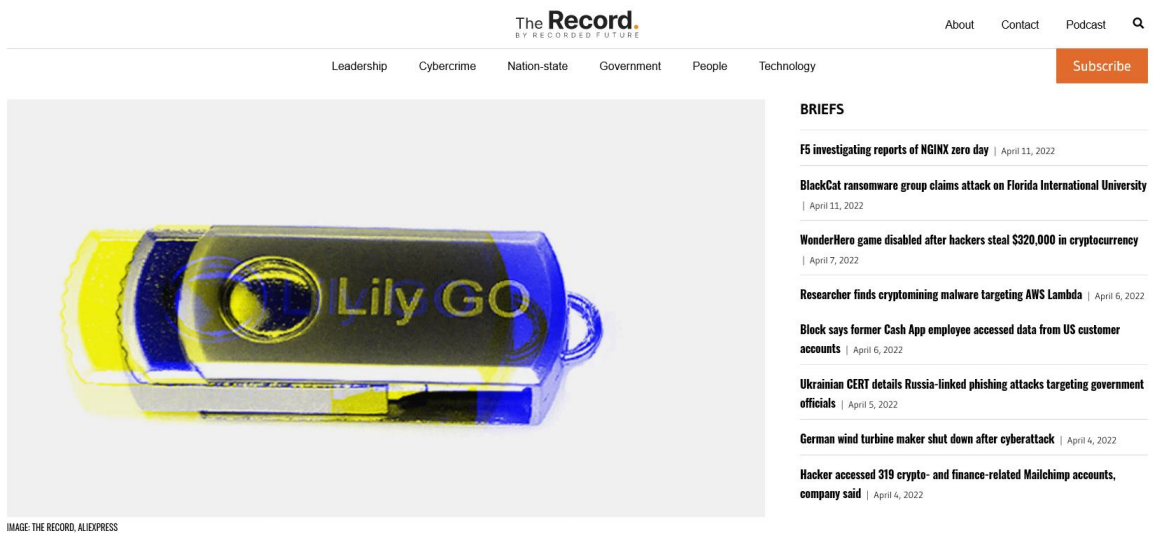
Keylogger

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

Gegenmaßnahmen

BashBunny

Realer Vorfall - BadUSB



The Record. BY RECORDED FUTURE

About Contact Podcast

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

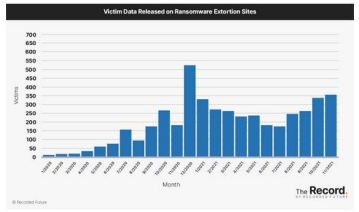
Block says former Cash App employee accessed data from US customer accounts | April 6, 2022

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]

Quelle: therecord.media (2)

Keylogger & BadUSB – Angriffe über die USB-Schnittstelle

Hacking Hardware

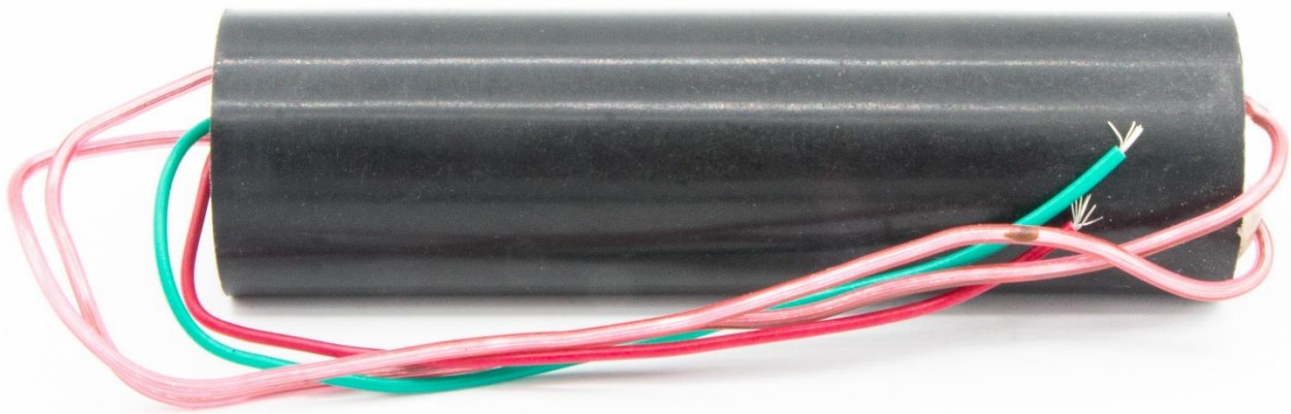
Keylogger

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

Gegenmaßnahmen

EXKURS USB-Killer - USBKill

EXKURS USB-Killer - Stromschock



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**

Gegenmaßnahmen

Allgemein

- 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

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

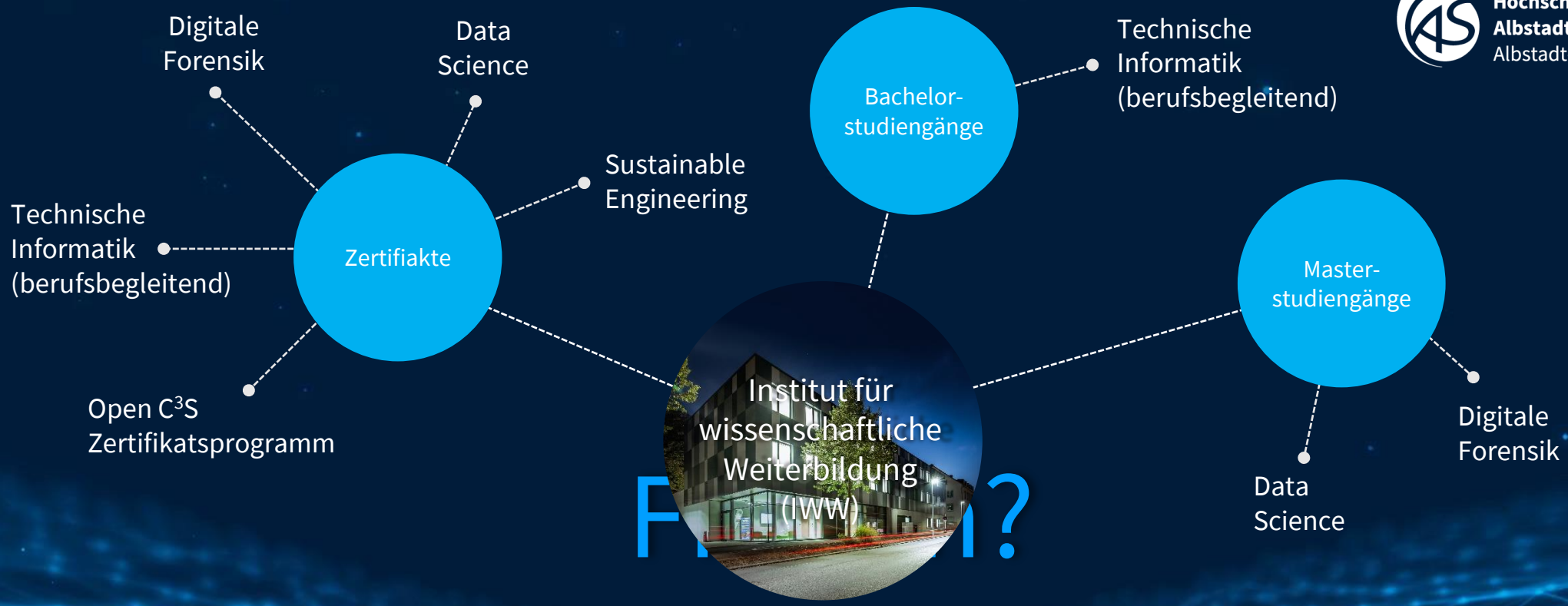
Hardware

- USB-Netzteil

- USB-Schlösser

- USB-Protector

**Keylogger & BadUSB –
Angriffe über die USB-Schnittstelle**



Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Vielen Dank für Ihre Aufmerksamkeit

19.10. - 10:00 Uhr: Public Key Infrastrukturen - Eine Frage des Vertrauens

Weitere IT-SAD Vorträge: https://blogs.tu-braunschweig.de/it/

Quellen

1) Keylogger-Affäre in der taz - Dateiname LOG.TXT, https://taz.de/Keylogger-Affaere-in-der-taz/!5307828/, abgerufen am 17.10.2022

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 17.10.2022

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 17.10.2022