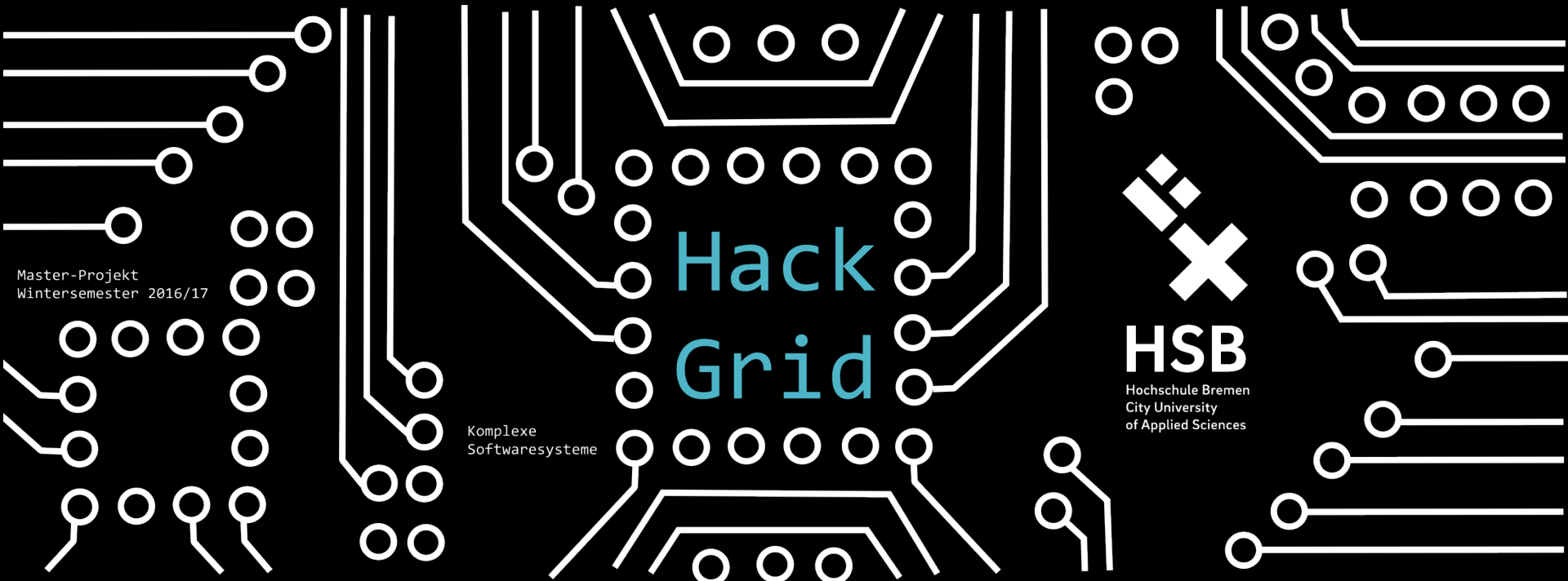
HID Angriffe

mit Rubber Ducky und BADUSB



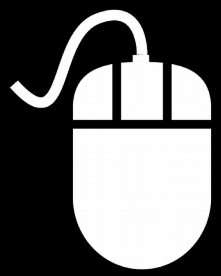
Agenda

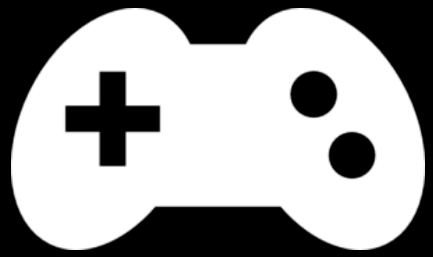
- HID
- HID Angriffe
- Rubber Ducky
- Arduino Rubber Ducky
- BADUSB
- PoisonTap
- Sonstiges
- Gegenmaßnahmen

USB-HID

USB-HID

- Geräteklasse des USB Standards
- Treiber meistens im OS integriert
- USB Geräteklasse kann zur Laufzeit wechseln
- Keine Prüfung der Geräteklasse
- Plattformunabhängig

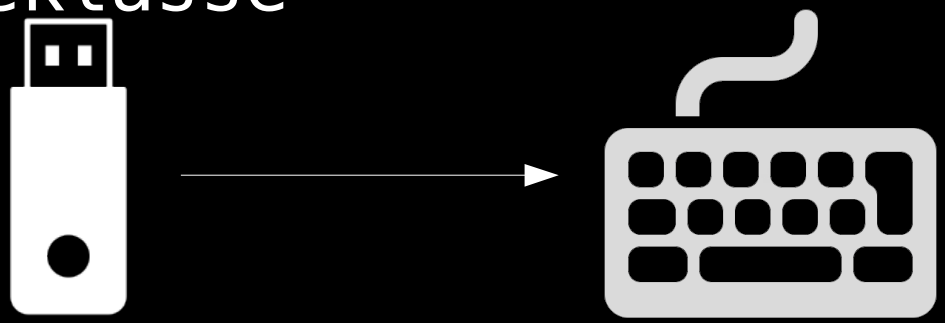




HID Angriffe

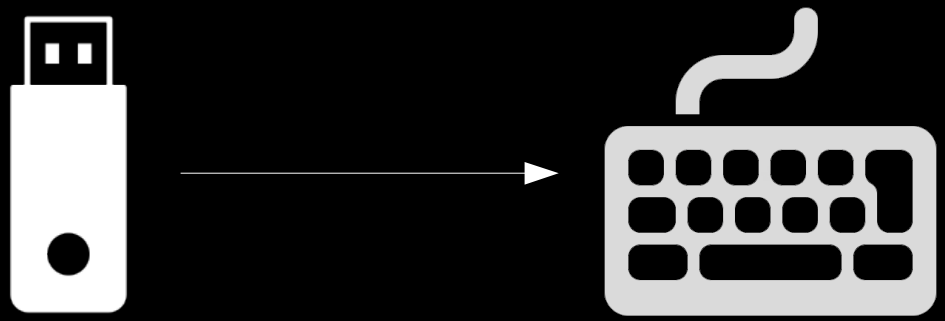
HID Angriffe

- Ausgangspunkt:
  - Opfer verwendet USB Gerät
  - Tastatur & Maus wird grundsätzlich vertraut
- Ziel:
  - Wechsel in mächtigere USB Geräteklasse



HID Angriffe

- Wechsel zur Tastatur
  - Eingabe einer vorher definierten Tastenfolge („Payload“)
- Wechsel zu Maus
- Wechsel zu USB Netzwerkkarte



Rubber Ducky

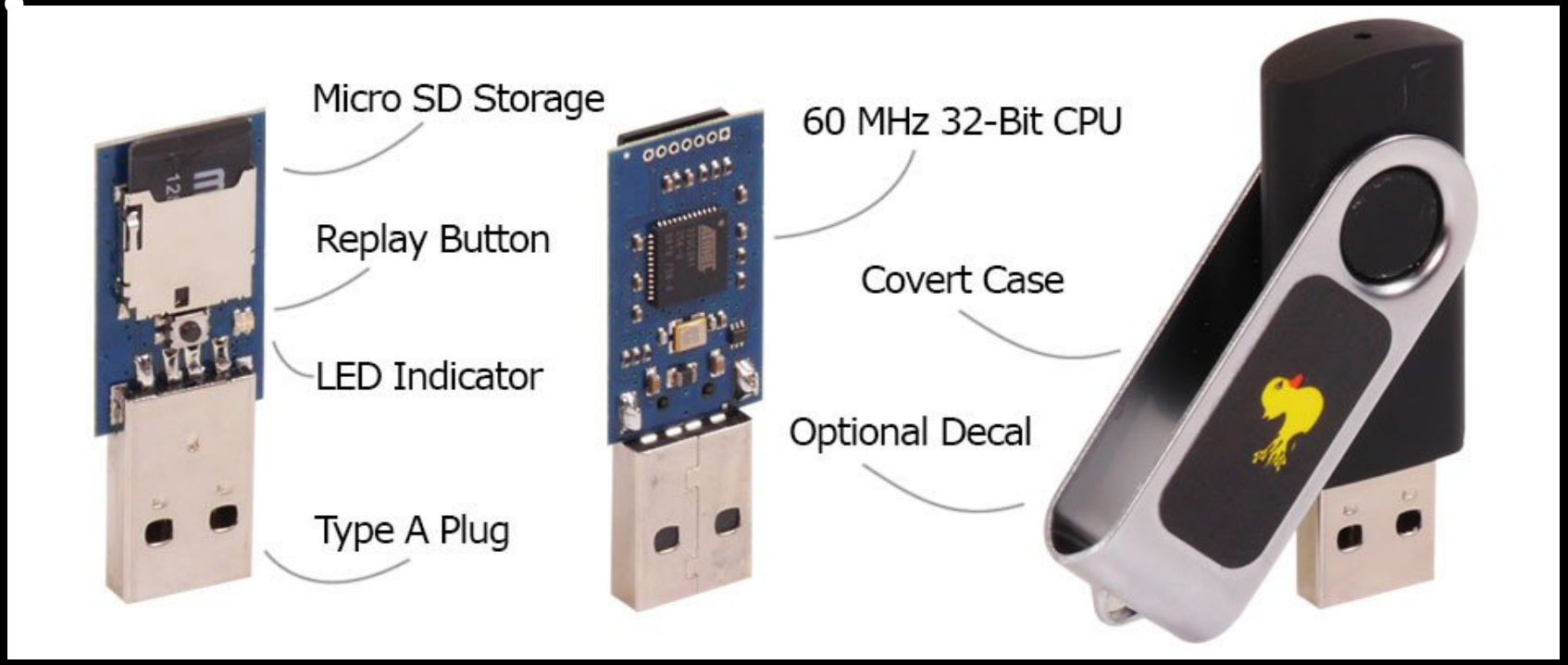


Bild von https://hakshop.com/products/usb-rubber-ducky-deluxe

Rubber Ducky

- Toolchain Rubber Ducky
  - DuckyScript

```
REM First Hello World Payload

WINDOWS r

DELAY 100

STRING notepad.exe

ENTER

DELAY 200

STRING Hello World
```

Rubber Ducky

- Toolchain Rubber Ducky
  - DuckEncoder.jar
  - Generiert Payload (.bin) aus Script Datei
  - Payload wird auf SD Karte übertragen

Rubber Ducky

- Toolchain Rubber Ducky
  - Diverse Online Ressourcen
  - Sammlung von Payloads
  - Online Payload Generator
  - Alternative Firmware
  - Usw.

Rubber Ducky

Demo!

Arduino Rubber Ducky

Arduino Rubber Ducky

- Arduino Bibliothek Keyboard.h
- Emulation von USB-Tastatur

- Arduino mit Onboard USB:
  - Arduino Leonardo, Due und Micro

Arduino Rubber Ducky

- Beispielcode:

```
#include "Keyboard.h"
void setup() {
  delay(1000);
  Keyboard.begin();
  delay(1000);
  Keyboard.println("Hello World");
  delay(100);
  Keyboard.end();
}
```

Arduino Rubber Ducky

- Probleme:
  - BlÃ¼de Sonderzeichen
  - Eingeschränkte Funktionalität
  - Keine Fehler beim Programmieren machen

Arduino Rubber Ducky

- Lösung:
  - Alternative Bibliotheken
    - https://github.com/NicoHood/HID
    - https://github.com/donid/akuhell

Arduino Rubber Ducky

- Lösung:
  - Alternative Bibliotheken
    - https://github.com/NicoHood/HID
    - https://github.com/donid/akuhell
  - Workarounds:
    - Darstellung über US-Layout
    - Nachladen von Payload in richtiger Sprache
    - Programmatisches Umstellen des Tastaturlayouts

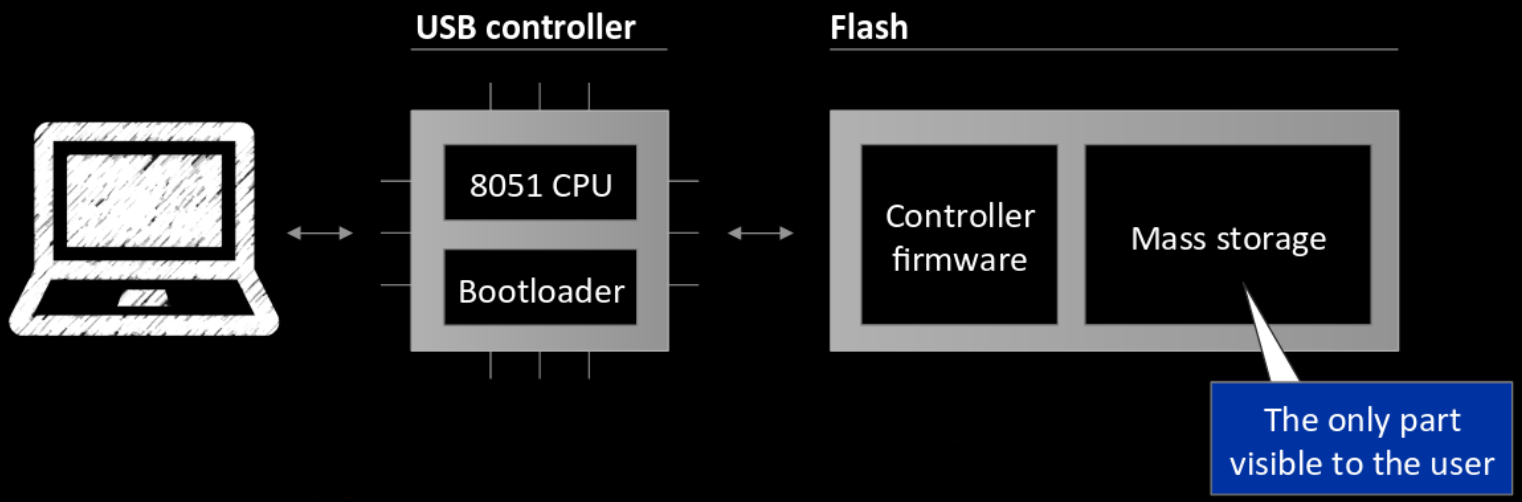
Arduino Rubber Ducky

Demo!

BADUSB

BADUSB

- Neu-Programmierung von eingebetteten USB Controllern
- Ziel: Handelsübliche USB Geräte



https://web.archive.org/web/20160521102051/https://srlabs.de/blog/wp-content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf

BADUSB

- Laut Nohl und Lell sind ca. 50% aller Geräte anfällig
- Grundsätzlich ist Reverse Engineering nötig
  - Doku, Firmware, Update, usw.

→ Aufwändig und nicht praktikabel

BADUSB

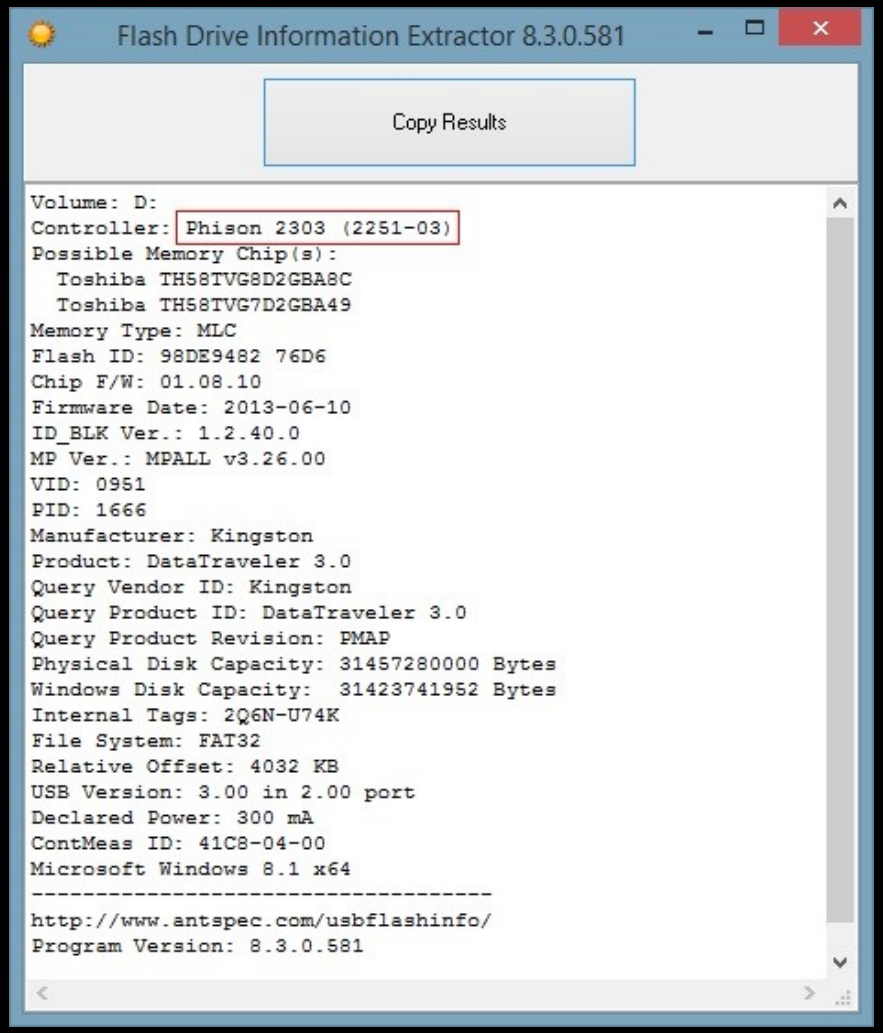
- Mögliche Szenarien
  - Mehrere USB Geräte gleichzeitig (Mass Storage + Keyboard)
  - Vervielfältigung auf andere USB Geräte
  - OS-Detection
  - Daten beim Lesen/Schreiben ändern
  - USB Netzwerkkarte

BADUSB

- Tools für verbreiteten Phison veröffentlicht[1]
  - Keine/wenig Aufwand
  - USB Keyboard auf normalem USB Stick
  - Injection von Rubber Script Payload möglich

[1]:https://github.com/brandonlw/Psychson

BADUSB

- 

BADUSB

1) IDE einrichten
   - DriveCom
   - EmbedPayload
   - Injector
   - Duck Encode
   - Burner Image

BADUSB

1)Firmware kompilieren (build.bat)

2)Duckyscript schreiben

3)Payload generieren (duckencoder)

4)Payload in Firmware einbetten (EmbedPayload)

5)Firmware flashen (DriveCom)

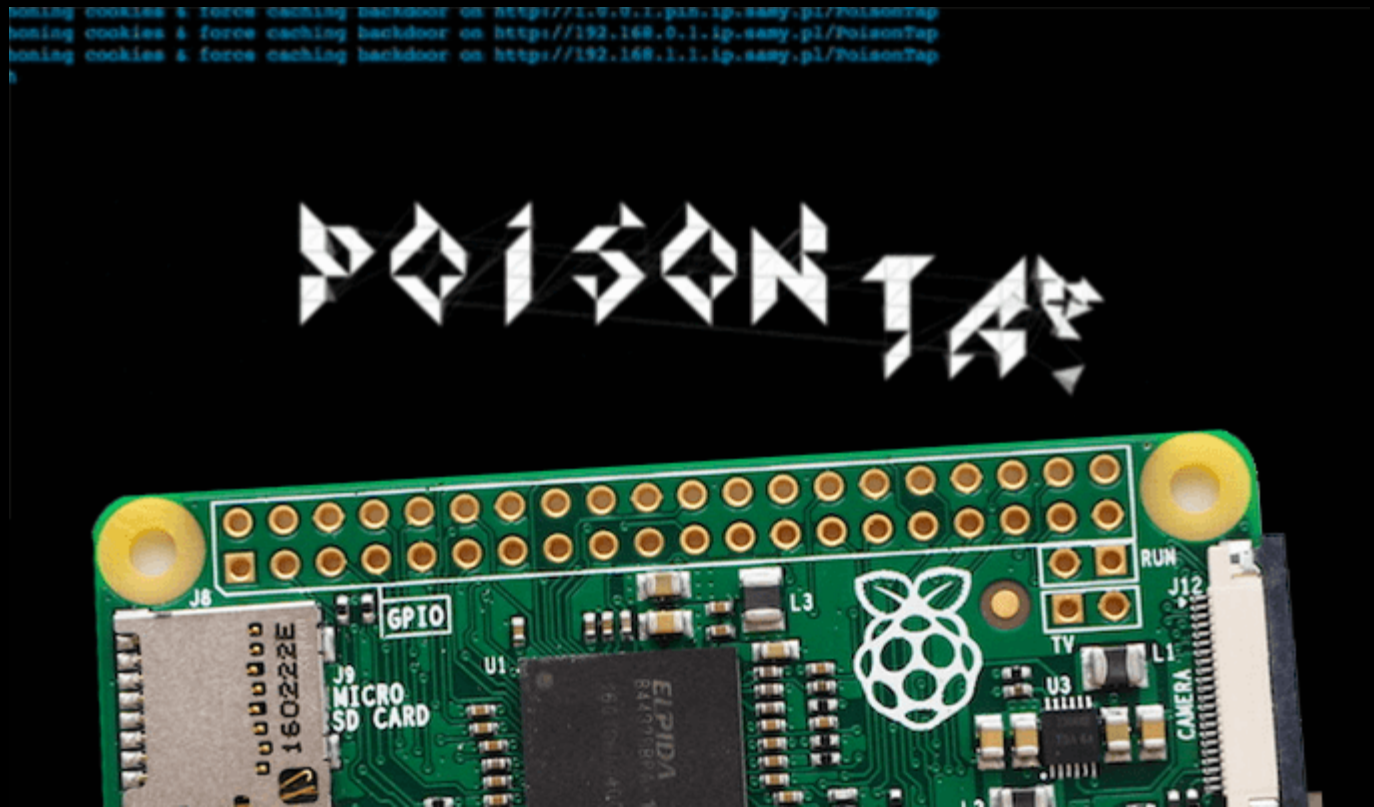
Bootmode erzwingen

BADUSB

Demo!

Poison TAP

https://threatpost.com/files/2016/11/poisontap.png



HSB
Hochschule Bremen
City University
of Applied Sciences

Poison TAP

- Firmware für Raspberry Pi (Zero)
- Übernimmt Computer über emulierten USB-Netzwerkadapter (MITM)
- Funktioniert auch bei gesperrten Bildschirmen

Poison TAP

- PoisonTap sendet falschen DHCP Adressraum
  - Adresse 1.0.0.10
  - Netmask: 128.0.0.0
  - Gateway 1.0.0.1

Anderes

- Teensy
- DroidDucky (Android Smartphone als Tastatur)
- Nethunter/Duckhunter (Android Smartphone)
- Android als Ethernet Adapter (slrlabs BADUSB Talk)

Gegenmaßnahmen

Gegenmaßnahmen

http://spoonfulofimagination.com/wp-content/uploads/2013/03/Hot-Glue-Gun.jpg

Gegenmaßnahmen

- Nutzer:
  - Heißkleber / Blockieren im BIOS
  - Misstrauen gegenüber USB
  - Whitelist für USB Geräte
    - Was ist während des Boot?
  - Bildschirm sperren/Stand-By
  - Separate Maschine für USB
  - Tools (z.B. Gdata Keyboard Guard)

Gegenmaßnahmen

- Hersteller:
  - Signierung von Firmware
  - keine Firmware Updates

Vielen Dank für ~~Ihre~~ deine Aufmerksamkeit!