

BitLocker: Die unendliche Geschichte?

DMA, Bitpixie, YellowKey, ... wie verliert man als Verteidiger nicht den Überblick?

KLASSIFIZIERUNG: PUBLIC

Kurz zu mir



Martin Grottenthaler

Gründer & Penetration Tester, VidraSec · OSCP · CISSP

- Pentester seit 2017, VidraSec 2024 gegründet
- Schwerpunkt: Windows, Active Directory, Entra ID
- Speaker auf Sicherheitskonferenzen (u.a. Troopers, Hacktivity, IT-SECX)
- BitLocker in echten Kundenprojekten geknackt, mit Bitpixie und YellowKey

Rückblick: IT-SECX 2021

Utilman is back - BitLocker und Windows Logon über DMA umgehen



Warum die unendliche Geschichte?

- 5 Jahre später, gleiches Thema
- Ich prophezeie: das Thema ist auch in 5 Jahren noch relevant
- Ich geb’s zu: ich hab das Buch nicht gelesen
- Zusammenfassung: irgendwas mit Virtualisierung und Sandbox Escapes

Warum das überhaupt wichtig ist

- Diebstahl ohne Verschlüsselung: nicht nur Hardware weg, auch Daten
- Hardware weg: ärgerlich. Daten weg: Sicherheitsvorfall und Datenschutzverletzung
- Dazu: lokale Rechteausweitung (LPE)
- **Verschlüsselung ist nur so gut, wie sie konfiguriert ist**

Laufwerksverschlüsselung in 60 Sekunden

1. Etablierte Algorithmen verschlüsseln die Daten
2. Zum Entschlüsseln braucht es einen Schlüssel
3. Wer den Schlüssel nicht hat, hat keinen Zugriff auf die Daten
4. ???
5. Profit? Nein, aber Probleme!

Probleme mit dem Setup

Brute-Force kurzer Schlüssel

- Schlüssel muss bei jedem Boot eingegeben werden
  - Lange, zufällige Schlüssel sind mühsam
- Kein echter Brute-Force-Schutz möglich (Angreifer hat Festplatte)

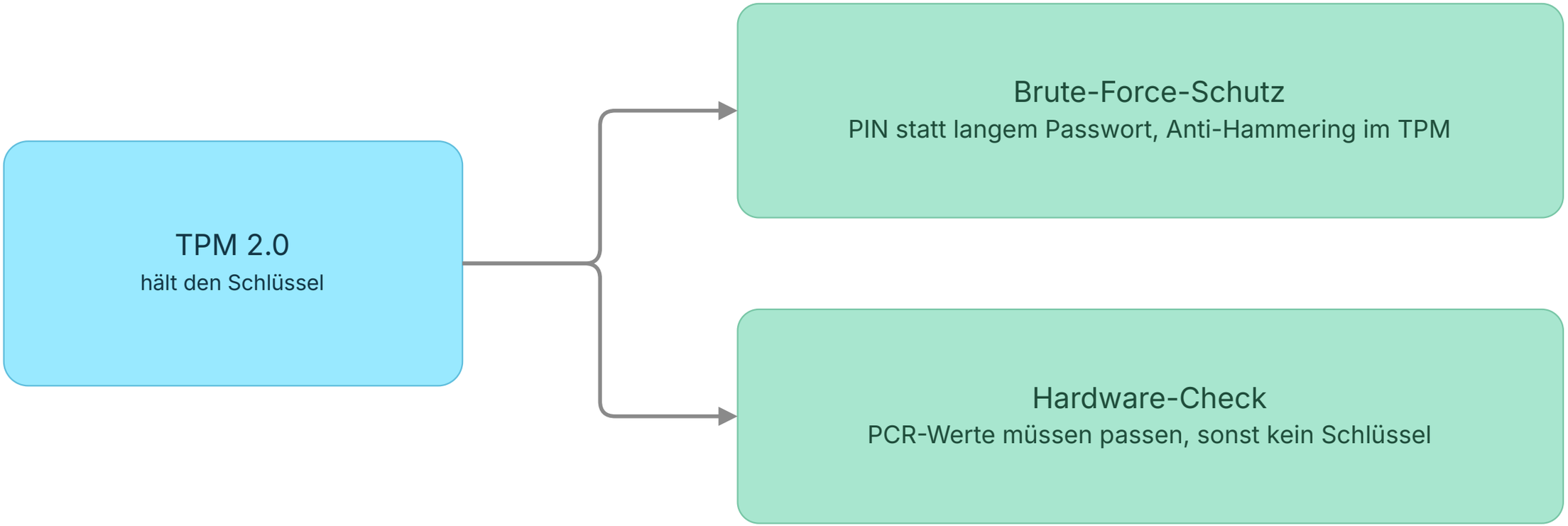
Gerät muss vertraut werden

- z. B.: manipulierte Bootreihenfolge zeigt eine Fake-Passworteingabe

Die Antwort drauf: Trusted Platform Module (TPM)

- Hardware-Modul für kryptografische Operationen
- Nach Common Criteria oder FIPS 140-2 zertifiziert
- Speichert unter anderem BitLocker-Schlüssel sicher
  - genauer: BitLocker Schlüssel, sind nicht im TPM, werden aber vom TPM entschlüsselt
- Schlüssel nicht extrahierbar, nur benutzbar
- TPM 2.0 ist Pflicht für Windows 11 → jedes moderne System hat eins

Zwei Features, die daraus folgen



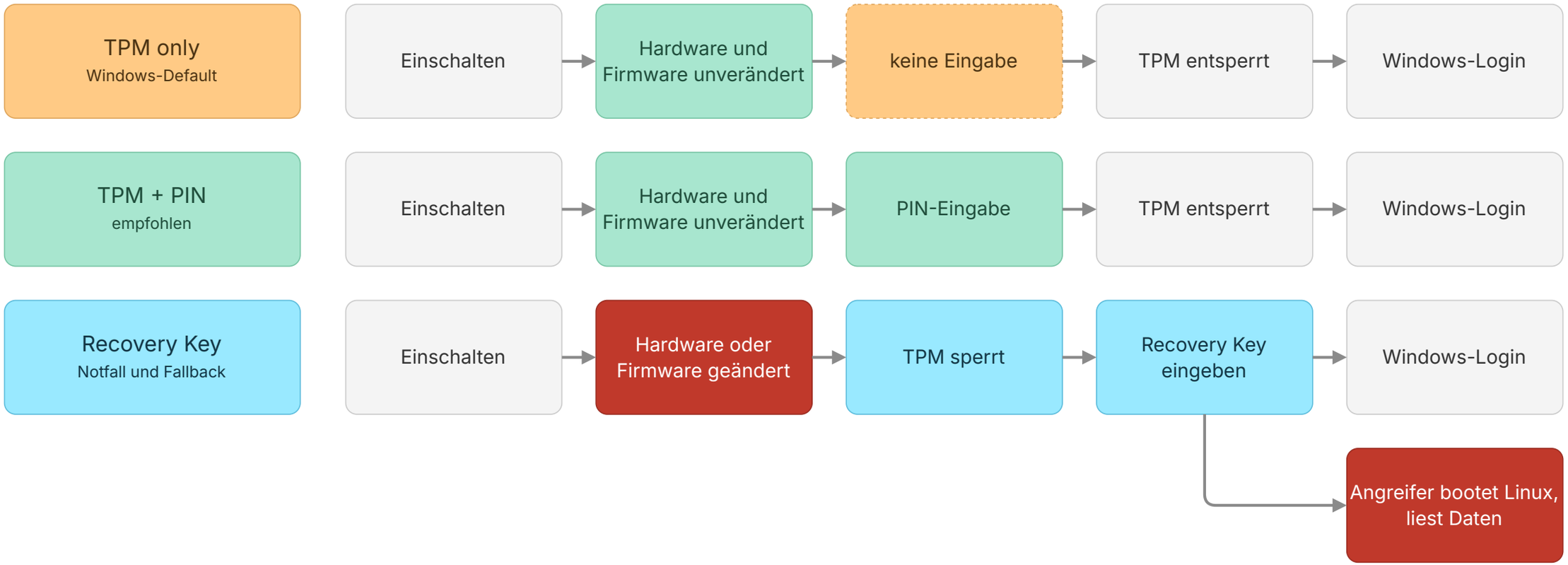
Microsoft weicht das an zwei Stellen auf

1. Zentral gespeicherte Recovery Keys
2. TPM-only-Modus ← **darüber reden wir heute**

Recovery Keys

- Passwort statt TPM-PIN, für Recovery-Fälle
- Ausgedruckt im Safe, im Microsoft-Konto, oder zentral in AD bzw. Entra ID und Intune
- In Unternehmen Standard: Leute vergessen PINs, UEFI-Updates gehen schief
- Eher Feature als Schwachstelle
  - Wie ist dein Threat Model?
  - Wo liegen sie, wer darf sie auslesen?

Key Protectors



„TPM only“ klingt schlimmer als es ist

- Checks auf Hard- und Firmware laufen trotzdem: fremdes OS → kein Schlüssel
- Ohne Windows-Passwort kommt niemand an Daten

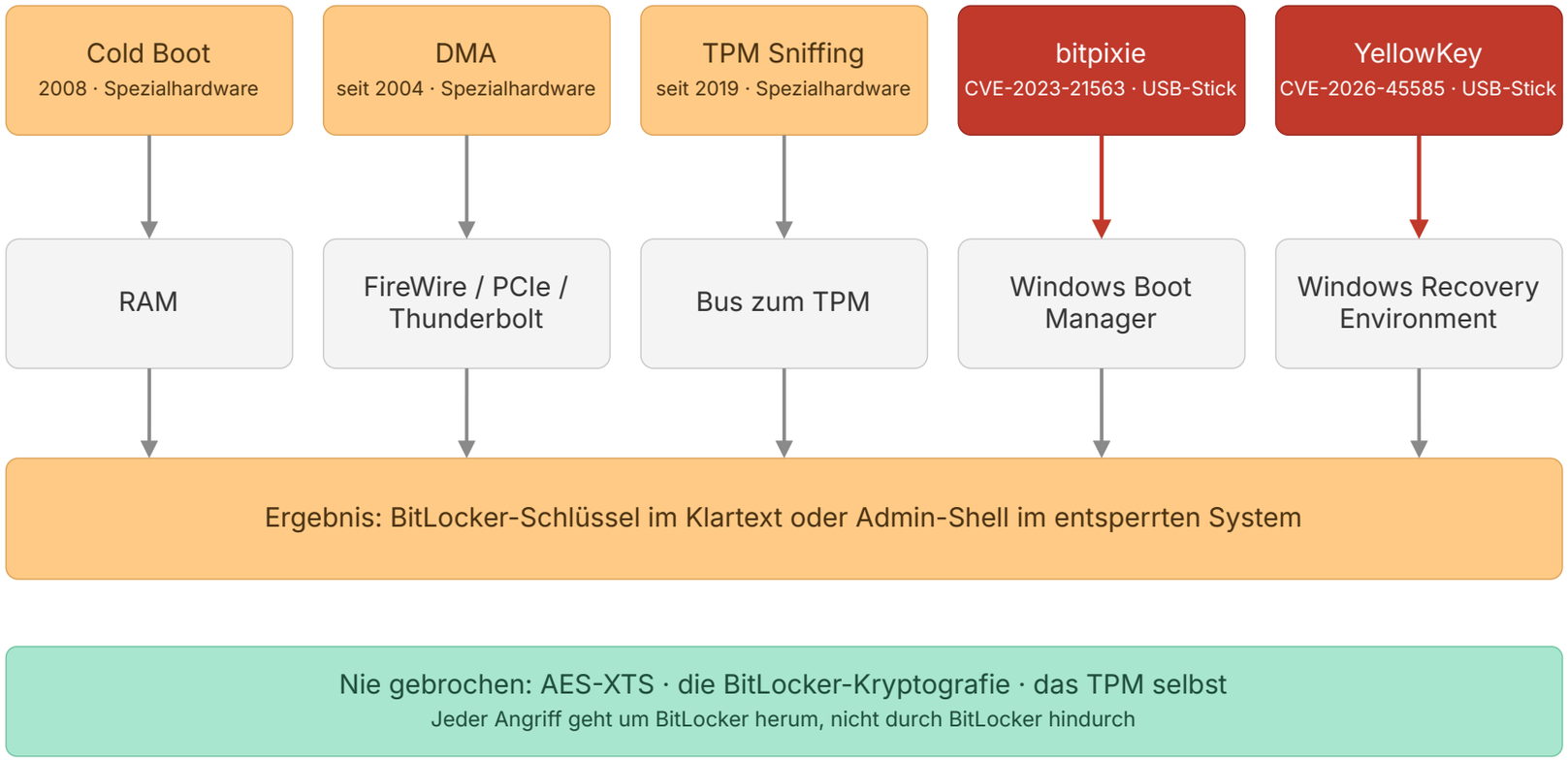
Großes „Aber“

- Jeder Angriff, den ich kenne, zielt auf die TPM-only-Konfiguration
- Und keiner greift BitLocker an, immer andere Komponenten

Die Angriffsfläche

Kein Angriff bricht AES oder BitLocker. Anfällig sind immer andere Komponenten.

Überblick



Eine größere Liste pflegt Wack0: `github.com/Wack0/bitlocker-attacks`

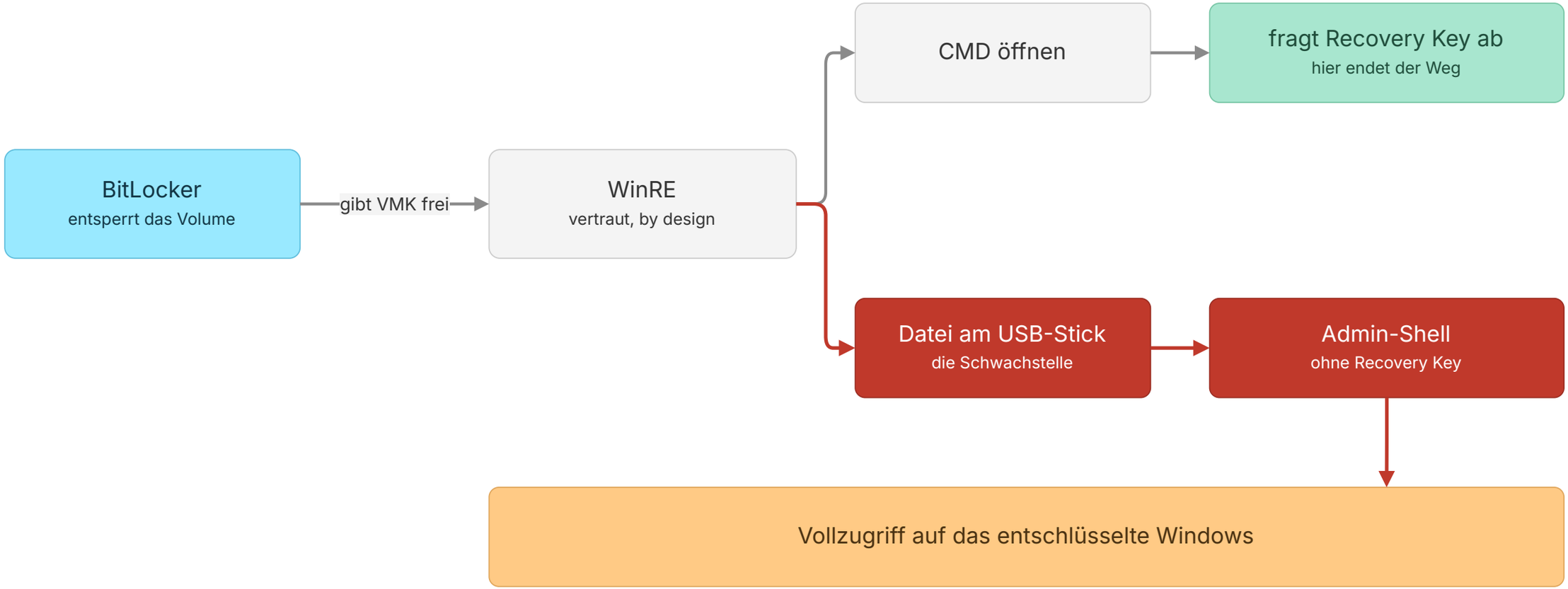
YellowKey

Ein USB-Stick, ein paar Dateien, 5 Minuten

Live-Demo

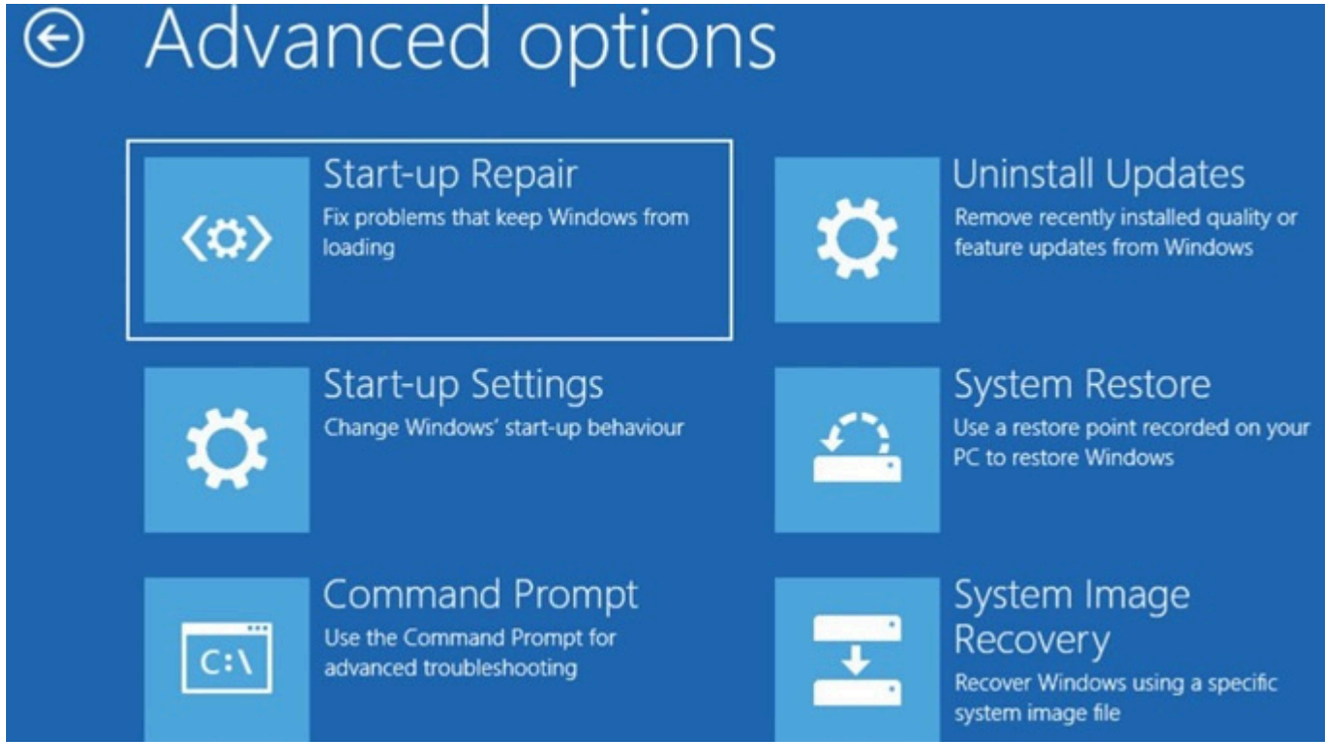
YellowKey in der Praxis

Und wieder: kein BitLocker-Bug



- Betroffen ist das **Windows Recovery Environment**, nicht BitLocker

WinRE: was ist das?



WinRE: was ist das?

- Mini-Windows in einer eigenen Partition, bei jedem Windows dabei
- Startet automatisch nach fehlgeschlagenen Boots, oder **per Shift + Reboot**
- Von Microsoft signiert und Teil der gemessenen Bootkette
- BitLocker vertraut ihm und entsperrt das Laufwerk

Die Eingabeaufforderung fragt deshalb den Recovery Key ab

Patch

- Erste Gegenmaßnahme: WinRE deaktivieren. Inzwischen gibt es einen Patch
- Aber: WinRE-Image wird nicht immer mit dem OS mitgepatcht

Nach dem Patchday prüfen: `reagentc /info`

Was gerade passiert ist

- BitLocker gibt Key korrekt an das vertraute Recovery Environment frei
- Recovery Environment war anfällig
- Schwachstelle öffnet Admin-Shell, ohne BitLocker zu sperren

Zusätzliches Detail

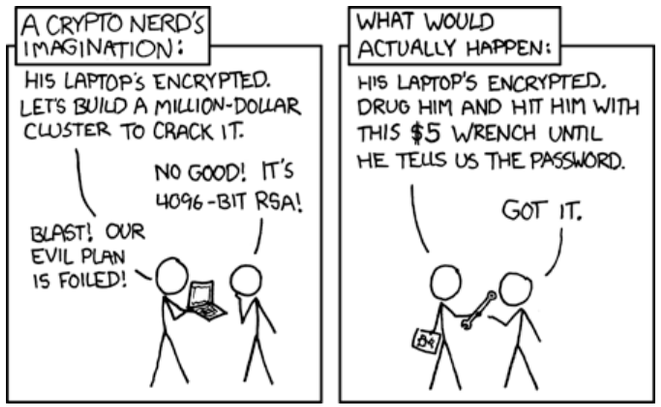
- YellowKey-Autor hat angeblich auch einen Exploit für BitLocker mit TPM
- **Aber:** Notebook muss vorher im entsperrten Zustand präpariert werden
- Nicht veröffentlicht, dazu nachher mehr

Gegenmaßnahmen

Und ihre Grenzen

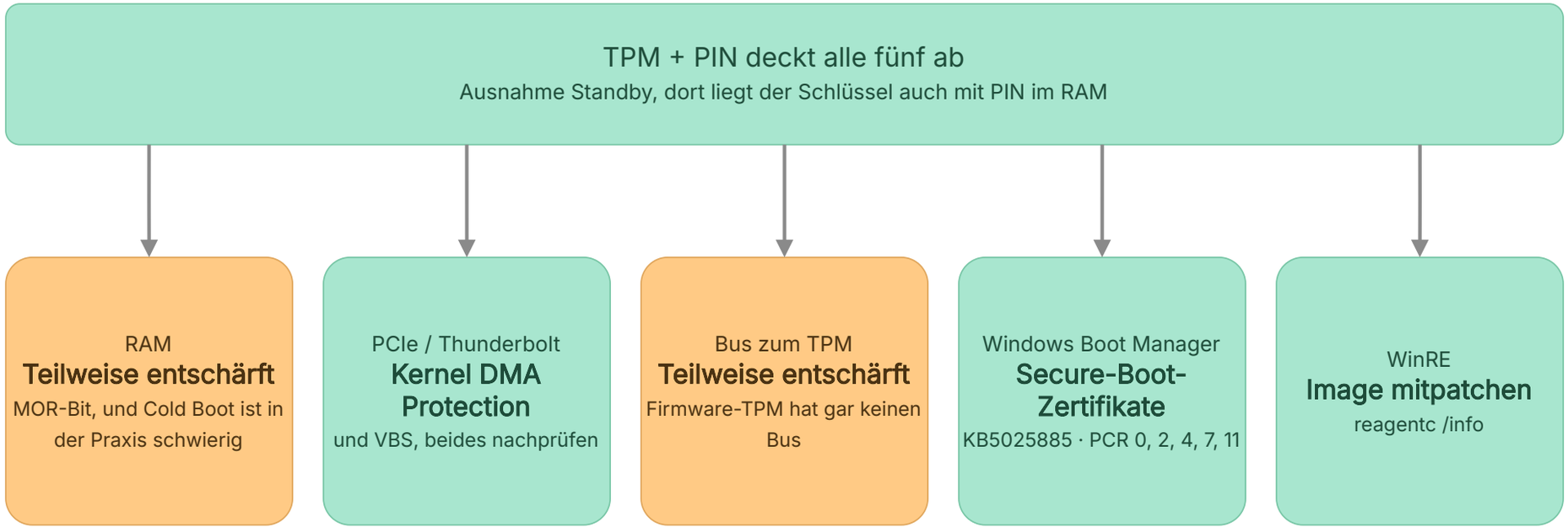
Die eine Maßnahme: Pre-Boot-Authentication

- **TPM + PIN**: PIN-Eingabe beim Booten, zusätzlich zum Windows-Login
- Schränkt Angriffsfläche deutlich ein
- Schützt bisher gegen fast alle bekannten Angriffe
- Bleiben: gewisse Evil-Maid-Angriffe und ein 5-Dollar-Schraubenschlüssel



- **Aber:** TPM ohne PIN ist eine Risikoabwägung, für manche Geräte vertretbar

Wo welche Maßnahme greift



Selbst-Check

```
# genereller Status
manage-bde -status C:
# TPM + PIN oder nur TPM? Welche PCR Validation Profiles?
manage-bde -protectors -get C:
# Empfohlen:
# PCR Validation Profile:
# 0, 2, 4, 7, 11

# WinRE-Image aktuell?
reagentc /info
# VBS aktiv? funktioniert nur im englischen Windows
systeminfo | findstr /I "Virtualization-based security"
# aktuelle Secure-Boot-Zertifikate?
[System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI db).bytes) -match 'Windows UEFI CA 2023'
```

Ist die Geschichte jemals zu Ende?

- Kein Angriff geht gegen BitLocker selbst, immer gegen das Drumherum
- Das „Drumherum“ ist groß und komplex (danke Microsoft)
- 🔮: gibt sicher bald eine neue Schwachstelle

- **Wichtig**: meine Konfiguration muss nicht nur heute sicher sein, sonst wartet der Dieb einfach auf die nächste Schwachstelle

YellowKey-Autor über BitLocker

Warum er den Exploit für TPM + PIN nicht veröffentlicht hat

> *I didn’t release the PoC because I rely on bitlocker myself, bitlocker is great, the issue is it have to rely on retarded software to function which is a huge flaw.*

Ich selbst nutze BitLocker mit TPM + PIN, in meiner empfohlenen Konfiguration.

Zum Schluss

- TPM+PIN ist die einzig sichere Konfiguration.
- TPM only nur nach Risikoabschätzung und sauberer Konfiguration

Alle Details: https://www.vidrasec.com/de/blog/bitlocker-the-neverending-story/

Vielen Dank!



Martin Grottenthaler

Gründer & Penetration Tester, VidraSec
OSCP · CISSP

martin@vidrasec.com

+43 670 3081275

linkedin.com/in/mgrottenthaler

vidrasec.com

LinkedIn