Deaktivierung von HP (Wolf/Sure) Security

Bei aktuellen HP-Business-Notebooks wie dem HP EliteBook 8 G1a 14 ist „HP Wolf Security“ teilweise Windows-Software und teilweise mit Firmware-/UEFI-Sicherheitsfunktionen von HP verbunden (z. B. Sure Start, Sure Admin, Secure Platform). Es gibt daher meist keinen einzigen Schalter „HP Wolf Security deaktivieren“ im UEFI.

Hintergrundinformationen

Woran Sie versteckte oder aktive HP-Security-Module erkennen

Bei HP-Wolf-/Sure-Systemen gibt es mehrere Ebenen:

1. HP Sure Start aktiv

Erkennbar an:

- Bootmeldung:
  - „Protected by HP Sure Start“
  - oder „HP Sure Start Recovery“
- BIOS-Menü:
  - Security → HP Sure Start
- Optionen wie:
  - Runtime Intrusion Detection
  - Boot Block Verification

Das bedeutet:
Ein separater Sicherheitscontroller überwacht permanent das BIOS.

2. Endpoint Security Controller (ESC) aktiv

Das ist die eigentliche Hardware-Komponente hinter HP Wolf/Sure.

Hinweise darauf:

- Menüpunkt:
  - Secure Platform Management
- Optionen wie:
  - Provisioned
  - Endpoint Security Controller
  - Deprovision Device

Wenn dort „Provisioned“ erscheint, ist das Gerät noch in einer HP-Sicherheitsdomäne eingebunden.

Bei neueren EliteBooks läuft ein Teil der Sicherheitslogik in einem separaten Mikrocontroller außerhalb des eigentlichen BIOS.

3. Firmware-Selbstheilung aktiv

Typische Anzeichen:

- BIOS-Änderungen werden nach Neustart rückgängig gemacht
- Secure-Boot-Keys werden automatisch wiederhergestellt
- BIOS reflasht sich selbst

- Meldungen wie:
  - „unauthorized BIOS change“
  - „Secure Boot Keys restored“

Das deutet auf aktive Sure-Start-/ESC-Überwachung hin.

Vorgehensweise

Falls das Gerät nicht unter Unternehmensverwaltung steht, funktioniert häufig folgende Reihenfolge:

Schritt 1

Security → Secure Boot Configuration

- Secure Boot = Disable

Schritt 2

Security → TPM Embedded Security

- TPM Device = Hidden oder Disable
- optional:
  - Clear TPM

Schritt 3

Security → HP Sure Start

Falls möglich:

- Runtime Intrusion Detection = Disable
- Verify Boot Block = Disable
- Sure Start Secure Boot Protection = Disable

Schritt 4

Security → Secure Platform Management

Falls vorhanden:

- Deprovision Device
- anschließend:
  - Reset Security Settings

Danach speichern und vollständig ausschalten.

Wichtiger technischer Hintergrund

Die aktuellen EliteBooks besitzen oft einen separaten „HP Endpoint Security Controller“, der:

- BIOS-Integrität überwacht,
- Änderungen erkennt,
- und Firmware automatisch wiederherstellen kann.

Das erklärt, warum bei manchen Geräten:

- CMOS-Reset nichts bringt,

- BIOS-Flash rückgängig gemacht wird,
- oder Einstellungen „wie von selbst“ zurückkehren.

Bei der G1a-Serie von HP (inklusive HP EliteBook 8 G1a 14) ist die **UEFI-/Security-Struktur** gegenüber älteren EliteBooks etwas erweitert worden. Die Menüs können je nach BIOS-Version leicht abweichen, typischerweise sieht die Struktur jedoch ungefähr so aus:

Main

├─ System Information

├─ Update System BIOS

└─ Restore Defaults

Security

├─ Administrator Password

├─ Power-On Password

├─ TPM Embedded Security

│ ├─ TPM Device

│ ├─ TPM State

│ └─ Clear TPM

│

├─ Secure Boot Configuration

│ ├─ Secure Boot

│ ├─ Legacy Support

│ ├─ Clear Secure Boot Keys

│ └─ Restore Factory Keys

│

├─ HP Sure Start

│ ├─ Sure Start

│ ├─ Runtime Intrusion Detection

│ ├─ Verify Boot Block on Every Boot

│ └─ Sure Start Secure Boot Keys Protection

│

- Secure Platform Management
  - Device Provisioning
  - Deprovision Device
  - Reset Security Settings
  - Endpoint Security Controller
- HP Sure Recover
  - Sure Recover
  - Network Recovery
- System Security
  - Virtualization Technology
  - TXT
  - DMA Protection

Advanced

- Boot Options
- USB Configuration
- Power Management

Exit

- Save Changes
- Ignore Changes
- Restore Defaults