SecureVibe IT Solutions GmbH
USt-IdNr: DE361138481 | HRB 180978
Securevibe.de
contact@securevibe.de
+49 40 5555 5195
Anne-Frank-Straße 25, 22587 Hamburg

SecureVibe
IT Solutions

# IT-Sicherheitsbericht

Anonymisierte Fassung für eine Fallstudie

Kunde anonym

Datum:

Dokument erstellt von:

# Inhaltsverzeichnis

1 Einleitung 1

2 Laptop 1: 3

3 Laptop 2: 8

4 Installations-Sticks 12

5 Auswertung der Bitcoin-Wallets 15

6 Anhang 17

# 1 Einleitung

## Hinweis zu dieser Fassung

- Dies ist eine anonymisierte Fassung des IT-Sicherheitsberichts zur Verwendung in einer Fallstudie.
- Entfernt oder grau hinterlegt ersetzt sind alle Namen, Benutzer- und Rechnernamen, E-Mail-Adressen, Konto- und Ticketnummern, Seriennummern, MAC-Adressen und BSSIDs, WLAN-Namen, Ortsangaben sowie alle Wallet-Adressen, Fingerabdrücke, Beträge und Transaktionsdaten.
- Nicht enthalten sind die Angaben des Kunden zu seinen Geräten, der Verlauf der Salden, die Bilanz und die Transaktionslisten des Anhangs.

## Zweck und Ziel

- Dieser Bericht dokumentiert die Untersuchung von zwei Laptops und vier USB-Sticks des Kunden, von denen Rechner installiert wurden.
- Anlass war der Verdacht, dass Rechner des Kunden, auf denen unter anderem Bitcoin verwaltet wurden, angegriffen und kompromittiert wurden.
- Ziel ist die nachvollziehbare Dokumentation des festgestellten Zustands und die Bewertung möglicher Sicherheitsvorfälle.
- Die Feststellungen beruhen ausschließlich auf den durchgeführten Prüfungen. Nicht belegbare Aussagen sind als solche gekennzeichnet.

## Untersuchte Geräte

| | **Laptop 1** | **Laptop 2** |
|---|---|---|
| Gerät | Acer Aspi | t |
| | chnername entfernt | Rechnername entfernt |
| Betriebssystem | Windows 11 Home 25H2, Build 26200.9457 | Linux Mint 22.3 „Zena“, Kernel 7.0.0-38 |
| Anlass | Verdacht auf Kompromittierung, Bitcoin-Verwaltung (laut Kunde) | Verdacht auf Kompromittierung, Bitcoin-Verwaltung (laut Kunde) |
| Zugriff | Fernzugriff über Hardware-KVM (PiKVM) | Fernzugriff über Hardware-KVM (PiKVM) |

Tabelle 1: Übersicht der untersuchten Geräte

## Vorgehen

- Laptop 1 wurde in einer separaten Sitzung über einen Hardware-KVM untersucht. Der Zugang erfolgte über ein Rettungssystem, die Prüfung danach lesend.

- Laptop 2 wurde über einen Hardware-KVM untersucht, am laufenden System und lesend: zunächst ohne, dann mit Administratorrechten, in einer zweiten Sitzung ohne Administratorrechte.
- Die vier USB-Sticks wurden an Laptop 2 schreibgeschützt untersucht und mit dem offiziellen Linux-Mint-Image verglichen (Abschnitt 4).
- **Beide Laptops wurden vollständig offline untersucht.** Während der Prüfungen bestand keine Verbindung zum Internet.
- Die Wallet-Daten wurden mit der öffentlichen Bitcoin-Blockchain abgeglichen (mempool.space). Stand der Abfrage: Bloc 10.2026.

# 2 Laptop 1:

## Ausgangslage

- Windows-Laptop des Kunden. Laut Kunde wurde auch dieser Rechner zur Verwaltung von Bitcoin genutzt. Der Kunde vermutet, dass er angegriffen wurde.
- Geprüft wurde ein Acer-Laptop mit Windows 11 (Hostname entfernt). Der Zugang wurde über ein Rettungssystem hergestellt.
- Die Prüfung erfolgte über eine Hardware-KVM (PiKVM) in einer Administrator-PowerShell. Die Ausgaben wurden per Bildschirmfoto gesichert (109 Aufnahmen mit SHA-256-Prüfsummen).
- **Das Gerät wurde vollständig offline untersucht.** Während der gesamten Prüfung bestand keine Verbindung zum Internet.

## Gerätedaten

| Merkmal | Wert |
|---|---|
| Hersteller / Modell | Acer A |
| nnummer | entfernt (BIOS und Produkt identisch) |
| SKU | 0000000000000000 (vom Hersteller nicht hinterlegt) |
| System-UUID | entfernt |
| BIOS | Insyde Corp., Version V1.07, |
| | RPL Toffee_ |
| U / RAM | Intel Core i5-1342 |
| äger | Micron 2500 NVMe MTF t, Firmware V8MA000 |
| Datenträger- | HealthStatus *Healthy*, OperationalStatus *OK*, Temperatur 60 °C, Verschleiß 0; Betriebsstunden und Fehlerzähler vom Treiber nicht geliefert |
| MAC WLAN | entfernt (MediaTek Wi-Fi MT7902) |
| M | (MediaTek Bluetooth Adapter |
| | verbaut; virtuell: McAfee-VPN-TAP entfernt, Wi-Fi Direct entfernt |
| TPM | vorhanden, aktiviert, bereit; Hersteller INTC, Version 600.18.35.2557 |
| Secure Boot | aktiv |
| | werk C: vollständig verschlüsselt (XTS-AES 128), **Schutz deaktiviert** (nur Wiederherstellungskennwort, keine TPM-Schutzvorrichtung) |
| Windows | Windows 11 Home 64 Bit, Version 25H2, Build 26200.9457 |
| Werks-Image | 07.04.2026 13:37 MESZ (Hostname entfernt) |
| Ersteinrichtung | 10.10.2026 ca. 11:10 MESZ (Windows meldet 17:04:35, weil die Uhr beim ersten Start vorging; Korrektur auf 11:11:22 belegt) |
| Hostname | entfernt |
| Benutzerkonto | Acer, verknüpft mit Microsoft-Konto E-Mail-Adresse entfernt, Administrator |

| Merkmal | Wert |
|---|---|

Tabelle 2: Gerätedaten Laptop 1

## Durchgeführte Prüfungen

| Bereich | Ergebnis |
|---|---|
| Zeitraum der Systemdaten | Frühestes Ereignis in allen 134 Ereignisprotokollen: 07.04.2026 13:37 MESZ (Werks-Image). Ersteinrichtung durch den Nutzer am 10.10.2026. |
| Konten | Aktiv: `Acer` (Microsoft-Konto, Administrator). `Administrator`, `Gast`, `DefaultAccount` und `WDAGUtilityAccount` sind deaktiviert. Kontoereignisse bei der Einrichtung am 10.10.2026 um 13:03 MESZ. |
| Anmeldungen | Security-Protokoll lückenlos ab 10.10.2026 12:14 MESZ. Nur lokale Anmeldungen (Typ 2, 7, 11) an den Tagen 10.10., 11.10. und 20.10.2026. **Keine Netzwerk- oder RDP-Anmeldungen** (Typ 3/10) für Benutzerkonten. Automatische Anmeldung eingerichtet (`AutoLogonSID` = Konto Acer). |
| Fernzugriff | RDP deaktiviert (`fDenyTSConnections`=1), WinRM gestoppt, kein OpenSSH-Server. Remoteunterstützung erlaubt (`fAllowToGetHelp`=1, Windows-Standard). |
| Fernwartungssoftware | AnyDesk, TeamViewer, RustDesk, ScreenConnect, Splashtop, VNC u. a.: nicht vorhanden (Programme, Dienste, Store-Apps, Prefetch, Firewallregeln). Quick Assist 2.0.29.0 ist als Windows-Bestandteil vorhanden, laut Prefetch nie gestartet. |
| Persistenz | Run-Schlüssel nur OneDrive, Firefox, Edge und SecurityHealth. Geplante Aufgaben nur Acer, McAfee, Google Updater, Mozilla und OneDrive. Alle 177 Dienstinstallationen (Ereignis 7045) ab 10.10.2026 stammen von McAfee, Google, Microsoft, Intel, Mozilla oder Acer. WMI-Abonnements nur Windows-Standard; IFEO, Winlogon, AppInit und LSA unverändert. |
| Programme in AppData, ProgramData, Temp | Nur signierte Acer-, Microsoft- und Mozilla-Komponenten sowie SweetLabs „App Explorer“ (Acer-Beigabe, gültig signiert). `Desktop\Firefox.exe` ist der signierte Mozilla-Desktop-Launcher. |
| Installierte Software | 28 Programme (Acer-OEM, Microsoft 365, McAfee, Firefox 157.0.1, Google Play Spiele). **Keine Krypto-Software** ( edger Live, Trezor Suite, Exodus, Electrum, Atomic, Trust Wallet, MetaMask u. a.). |
| Ausführungsspuren | Prefetch (369 Dateien), ShimCache und UserAssist zeigen nur Einrichtung, Acer-/Microsoft-Updates, Firefox und Edge. Der einzige `certutil.exe`-Lauf (10.10.2026 18:30 MESZ) importierte das Acer-Zertifikat `localhost.pfx`; kein Download. Keine PowerShell-Historie im Profil Acer. |
| Browser Firefox | [redacted] |

| Bereich | Ergebnis |
|---|---|
| Browser Edge | Verlauf: 10.10.2026 13:10 MESZ Firefox-Download (offizielle Mozilla-Quelle); „ Nur Standard-Erweiterungen, keine gespeicherten Logins, kein Autofill. |
| | |
| | |
| WLAN | Sechs Profile, alle offene öffentliche Netze: WLAN 1, WLAN 2, WLAN 3, WLAN 4, WLAN 5, WLAN 6. Verbindungen nur am 10.10. und 11.10.2026; letzte am 11.10.2026 11:11 MESZ. **Das WLAN WLAN X ist nicht vorhanden**, auch nicht im Verbindungsprotokoll. |
| Netzwerkkonfiguration | Firewall in allen Profilen aktiv; `hosts` ohne Einträge; kein Proxy, keine PAC-Datei; DNS auf Windows-Standard; keine VPN-Verbindungen (McAfee-VPN-Adapter getrennt, ExpressVPN nur als Acer-Installer-Helfer). Keine aktiven Verbindungen, keine ungewöhnlichen offenen Ports. |
| Zertifikate | Zusätzlich zu den öffentlichen Stammzertifizierungsstellen zwei Acer-Zertifikate: `CN=localhost` (Fingerabdruck `88043BF573ECE6707F8CBDADE9ED8AD2F69D54E8`) und `CN=F5240129-3993-455E-8347-B5A9BDDF4B89` (`EC011F245205A2332ACC8CD564C79E09FF8E37D0`, Herausgeber der AcerSense-App). |
| Virenschutz und Updates | McAfee ist der aktive Virenschutz; `detection.log` leer, Quarantäne unverändert. Defender 4.18.26080.4 im passiven Modus, Signaturen 1.459.655.0, keine Funde, keine Ausschlüsse. Letzte erfolgreiche Windows-Update-Installation am 10.10.2026 16:30 MESZ. |
| USB-Verlauf | Ab Werks-Image vollständig: Yubico Security Key (`VID_1050&PID_0402`) und YubiKey 5 (`VID_1050&PID_0407`), beide am 10.10.2026 zwischen 13:27 und 16:43 MESZ; USB-Maus (`VID_1C4F&PID_0048`). **Keine USB-Speicher**, **keine** ( ), kein Ledger oder Trezor. Keine Bluetooth-Kopplungen. |

Tabelle 3: Prüfumfang und Ergebnisse Laptop 1

## Bezug zum Vorfall

- **E-Mail:** E-Mail-Anbieter wurde am 10.10.2026 um 13:13 Uhr aufgerufen. Eine Anmeldung am Postfach und gespeicherte Zugangsdaten sind nicht nachweisbar. Das Microsoft-Konto des Geräts lautet E-Mail-Adresse entfernt.
- **Wallets:** Keine Wallet-Software, keine Wallet-Dateien, keine Seed-Phrasen oder privaten Schlüssel. Eine Bi VI war nie angeschlossen.

suchten Dateien vor.

## Identifizierte Schwachstellen

- **BitLocker ohne Schutz.** Laufwerk C: ist verschlüsselt, der Schutz ist aber deaktiviert (`manage-bde`: „Der Schutz ist deaktiviert", keine TPM-Schutzvorrichtung). Ursache: Die automatische Geräteverschlüsselung konnte den Wiederherstellungsschlüssel nicht im Microsoft-Konto sichern (BitLocker-Ereignisse 898 und 4103, 11.10.2026 11:01 bis 11:11 MESZ). Dadurch sind die Daten offline lesbar und das System manipulierbar; genau so war der Zugang über ein Rettungssystem möglich.
- **Sitzung dauerhaft offen.** Das Konto Acer blieb ab 20.10.2026 15:32 MESZ im Standby angemeldet. Für das Konto ist die automatische Anmeldung eingerichtet (`AutoLogonSID` gesetzt). *Annahme:* Nach Standby wird kein Kennwort verlangt bzw. die automatische Wiederanmeldung (ARSO) ist aktiv. Wer das Gerät öffnet, hat damit Zugriff auf das Administratorkonto.
- **Alltagskonto mit Administratorrechten.** Das Microsoft-Konto E-Mail-Adresse entfernt ist lokaler Administrator. Schadsoftware erhielte so volle Systemrechte.
- **Nutzung offener WLANs für sicherheitskritische Vorgänge.** Alle sechs bekannten Netze
- **Zusätzliche OEM-Stammzertifikate.** `CN=localhost` und `CN=F5240129-3993-455E-8347-B5A9BDDF4B89` stehen im vertrauenswürdigen Stammspeicher. Ist der private Schlüssel auf allen Geräten gleich, sind Zertifikatsfälschungen denkbar.
- **OEM-Beigaben.** SweetLabs „App Explorer" (Updater in `AppData`), Acer Jumpstart, ExpressVPN-Installer-Helfer, McAfee-Testversion und Booking.com-Verknüpfung vergrößern die Angriffsfläche.

## Fazit

- Auf Laptop 1 wurden **keine Hinweise auf eine Kompromittierung** gefunden: keine Schadsoftware, keine Fernwartung, keine fremden Anmeldungen, keine verdächtige Persistenz und keine Funde der Virenschutzprogramme.

- Laptop 1 ist nach derzeitigem Stand nicht kompromittiert. Er ist damit voraussichtlich nicht an der Kompromittierung des E-Mail-Kontos beteiligt. Das Windows-Werks-Image entstand am 07.04.2026, die Ersteinrichtung durch den Nutzer erfolgte am 10.10.2026.
- Auf dem Gerät gibt es keine Wallet-Software, keine Seed-Phrasen, keine privaten Schlüssel und keine der Fallbezugs-Adressen. Eine  war nie angeschlossen.

# 3 Laptop 2:

## Ausgangslage

- Auf dem Gerät wurde laut Kunde Bitcoin verwaltet. Der Kunde vermutet, dass der Rechner angegriffen wurde.
- Auf dem Gerät läuft Linux Mint 22.3. Das System wurde am **08.10.2026** gegen 19:35 bis 19:44 Uhr vom USB-Stick S1 installiert (Abschnitt 4). Ältere Daten sind nicht mehr vorhanden.
- Einziger Benutzer ist Benutzer A. Installierte Zusatzsoftware: Brave, , 4.52.0. Firefox ist vorinstalliert.
- Nutzungszeiträume laut Systemprotokoll: 08.10.2026 (ab 19:45 Uhr), 09.10.2026 (ca. 14:20 bis 16:16 Uhr), 10.10.2026 (ca. 04:35 bis 06:38 Uhr) sowie 14.10.2026 (ab ca. 17:25 Uhr) bis 15.10.2026 (07:30 Uhr).
- Die Hardware-Uhr enthält UTC, wird vom System aber als Ortszeit gelesen. Bis zur Zeitsynchronisierung über das Netz zeigt das System deshalb Zeiten an, die 2 Stunden zu früh sind. Die Nutzung am 10.10.2026 beginnt laut Protokoll um 02:35 Uhr, tatsächlich gegen 04:35 Uhr. Die Zeitangaben in diesem Bericht sind entsprechend korrigiert, soweit die Synchronisierung protokolliert ist.
- Die Untersuchung erfolgte in zwei Sitzungen über PiKVM, zunächst ohne, dann mit Administratorrechten, in der zweiten Sitzung ohne Administratorrechte (Gerätedaten, Browser, Netzwerk, Installationsprotokoll und Prüfung der USB-Sticks).
- **Das Gerät wurde vollständig offline untersucht.** Während der gesamten Prüfung bestand keine Verbindung zum Internet.

## Gerätedaten

| Merkmal | Wert |
|---|---|
| Hersteller / Modell | Acer S uk 0000000000000001 |
| Mainboard | `LNL Arte` n V1.23 |
| BIOS | Insyde Corp., Version `V1` |
| | Intel Core aut System |
| Datenträger | WD PC SN5000 ntfernt, Firmware `34230100` |
| TPM | vorhanden |
| Secure Boot | deaktiviert |
| UEFI-Starteinträge | `ubuntu` (`\EFI\ubuntu\shimx64.efi`, an erster Stelle), `Windows Boot Manager` (`\EFI\Microsoft\Boot\bootmgfw.efi`), USB, CD, Netzwerk |
| MAC WLAN | entfernt |
| Weitere Netzwerkschnittstelle | USB-Netzwerkadapter Kennung entfernt, ohne Verbindung |
| Betriebssystem | Linux Mint 22.3 „Zena“, Kernel 7.0.0-38 |

| Merkmal | Wert |
|---|---|
| Installation | 08.10.2026, ca. 19:35 bis 19:44 Uhr, Installer `ubiquity 24.04.3+mint19`, Medium: Stick S1 |
| Rechnername / Benutzer | entfernt / Benutzer A |

Tabelle 4: Gerätedaten Laptop 2

## Durchgeführte Prüfungen

| Bereich | Ergebnis |
|---|---|
| Netzwerk | Keine offenen Ports nach außen, keine aktiven Fremdverbindungen, Firewall (ufw) aktiv mit Voreinstellung „eingehend sperren“ |
| Fernwartung | Keine Fernwartungs-Software, kein SSH-Zugang, keine SSH-Schlüssel |
| Anmeldungen | Nur lokale Anmeldungen. Fünf Fehlversuche am eigenen Bildschirm (Tippfehler), keine Zugriffe von außen |
| Konten und Rechte | Nur Benutzer A mit Passwort, `root` gesperrt, sudo-Regeln nur Standard |
| Autostart und Persistenz | Cron, Autostart, systemd-Dienste und -Timer, udev, Login-Skripte, Preload: nur Standardeinträge |
| Systemintegrität | Alle Programme, Bibliotheken, Kernel und PAM-Module unverändert gegenüber den offiziellen Paketen (`dpkg -V`) |
| Dateien ohne Paket-Herkunft | Rund 7.550 Dateien, ausschließlich automatisch erzeugte Caches und Verknüpfungen. Die 11 ausführbaren Dateien darunter sind identisch mit den Paketvorlagen bzw. automatisch erzeugt |
| Rootkit-Indikatoren | Kernel nicht „tainted“, keine fremden oder versteckten Kernelmodule, keine versteckten Prozesse, `LD_PRELOAD` in keinem Prozess gesetzt |
| Paketverwaltung | Nur offizielle Quellen (Linux Mint, Ubuntu, Brave, ), nur Standard-Hooks |
| DNS, Hosts, Proxy, Zertifikate | Keine Umleitungen, kein Proxy, keine zusätzlich installierten Stammzertifikate |
| Installationsprotokoll | `/var/log/installer` stimmt mit dem Protokoll auf Stick S1 überein: gleiche Firmware-Kennung, gleiches WLAN, gleiche Zeitkorrektur, gleicher Benutzer. Die Medienprüfung bei der Installation meldete eine Abweichung in `/boot/grub/efi.img`. Ursache ist ein von Windows angelegter Ordner (Abschnitt 4) |
| Bootkette | Secure Boot aus. Start über `shimx64.efi`. Im UEFI-Speicher steht zusätzlich ein Eintrag „Windows Boot Manager“. Der Inhalt der EFI-Partition war ohne Administratorrechte nicht lesbar |
| Browser Brave | Ohne Erweiterungen und ohne Wallet. Beim Beenden werden Verlauf, Cache, Cookies, Downloads, Formular- und Website-Daten gelöscht. Verlauf, Cookies, gespeicherte Logins, Downloads, Formulardaten und Lesezeichen sind leer. Einzige Spur ist die letzte Sitzung vom 14.10.2026 mit der Suchmaschine `startpage.com` |

| Bereich | Ergebnis |
|---|---|
| Browser Firefox | Mit uBlock Origin und Decentraleyes aus dem offiziellen Store. Dauerhafter Privatmodus (`browser.privatebrowsing.autostart`). Im Verlauf stehen nur 13 Adressen vom 08.10.2026, 20:34 bis 20:35 Uhr: Mozilla-Startseiten und der Download von Brave über `brave.com`. Keine Cookies, Formulardaten, gespeicherten Logins oder Zertifikatsausnahmen. Website-Speicher nur der beiden Erweiterungen |
| Schlüsselbund, GPG, Dateien | Schlüsselbund `login.keyring` vom 08.10.2026, 20:37 Uhr, zeitgleich mit dem ersten Start von Brave (Inhalt nicht ausgelesen). GPG enthält nur den Signaturschlüssel von ( ). Zuletzt geöffnet wurden nur die , ihre Signatur und dieser Schlüssel. Kein Papierkorb |
| | Echt: SHA-256-Prüfsumme und GPG-Signatur des Herstellers stimmen. Eingetragen sind nur die Server des Herstellers (`btc1` bis `btc4.` ), kein Proxy, keine Lightning-Konten, keine Notizen. Im Protokoll stehen keine Signier- oder Sendevorgänge |
| WLAN | Profile: WLAN H (zuletzt 10.10.2026, 06:38 Uhr) und WLAN P (nie verbunden). WLAN H war vom 08.10. bis 10.10.2026 über mehrere Zugangspunkte desselben Routers verbunden (BSSIDs entfernt). Das Profil WLAN X wurde am 10.10.2026 um 06:22 Uhr neu angelegt und später gelöscht (Details unter Schwachstellen) |
| | Version 2026.5, Konto entfernt. Automatisches Verbinden und Sperre ohne VPN sind ausgeschaltet. Verbindungen am 09.10.2026 von 14:32 bis 16:20 Uhr (sechs verschiedene VPN-Server) und am 10.10.2026 von 04:36 bis 06:22 Uhr (ein VPN-Server). Danach meldete „offline“ |
| USB-Geräte (gesamte Laufzeit) | Mäuse, Webcam, USB-Audio-Adapter, zwei , zwei YubiKeys. Vor der Untersuchung war nie ein USB-Massenspeicher angeschlossen. Kein verdächtiges Gerät |
| Bluetooth | Keine gekoppelten Geräte |

Tabelle 5: Prüfumfang und Ergebnisse Laptop 2

## Identifizierte Schwachstellen

- **Secure Boot ist deaktiviert.** Bei physischem Zugriff könnte ein veränderter Bootloader oder Kernel unbemerkt gestartet werden.
- **Der Datenträger ist nicht verschlüsselt.** Bei Verlust oder Diebstahl sind alle Daten, darunter die Wallet-Metadaten, direkt lesbar.
- **Verbindung mit einem offenen WLAN.** Das Gerät war mit dem unverschlüsselten WLAN WLAN X verbunden: am 10.10.2026 von 06:22 bis 06:28 Uhr und am 14.10.2026 laut Systemuhr von 15:28 bis 15:32 Uhr. Am 14.10. war die Uhr nicht synchronisiert, tatsächlich also vermutlich 17:28 bis 17:32 Uhr. Das Profil wurde anschließend gelöscht. **Zugangspunkt:** BSSID x, 2,4 GHz (2437 und 2447 MHz). Die Adresse ist lokal vergeben und deshalb keinem Hersteller direkt zugeordnet. Ohne das Lokal-Bit ergibt sich die Herstellerkennung A, die laut IEEE-Register **.** gehört. Voraussichtlicher Hersteller ist damit

Google, etwa ein Pixel-Smartphone als Hotspot oder ein Google-WLAN-Gerät. Dasselbe Ableitungsschema zeigt der Router von WLAN H: x ist die lokal vergebene Variante von x, dessen Kennung y gehört.

- **VPN nicht dauerhaft aktiv.** Automatisches Verbinden und die Sperre ohne VPN sind ausgeschaltet. Im WLAN WLAN X bestand keine VPN-Verbindung, d meldete ab 10.10.2026, 06:22 Uhr „offline“.
- **Eingeschränkte Nachvollziehbarkeit.** Firefox läuft dauerhaft im Privatmodus, Brave löscht seine Daten beim Beenden. Besuchte Webseiten lassen sich nicht rekonstruieren.

## Fazit

- Es wurden **keine Hinweise auf eine Kompromittierung** des Systems gefunden.
- Das System wurde vom Stick S1 installiert. Dessen Image stimmt mit dem offiziellen Linux-Mint-Image überein (Abschnitt 4).
- Die festgestellten Schwachstellen erhöhen das Risiko, sind aber kein Beleg für einen erfolgten Angriff.

# 4 Installations-Sticks

## Ausgangslage

- Zur Untersuchung lagen vier USB-Sticks vor, von denen laut Kunde Laptops aufgesetzt wurden. Laut Notiz wurden die Linux-Geräte mit „silbernen“ und „schwarzen“ Sticks eingerichtet. Die Farbe der Sticks war über die KVM nicht zu erkennen. Die Sticks sind im Folgenden nach Modell und Seriennummer bezeichnet.
- Ein manipuliertes Installationsmedium könnte Schadsoftware schon bei der Einrichtung eines Rechners einbringen. Geprüft wurde deshalb, ob die Sticks das unveränderte Original-Image enthalten und welche Rechner mit ihnen eingerichtet wurden.
- Laptop 1 (Windows) wurde nicht mit diesen Sticks eingerichtet. Er läuft mit dem Werks-Image, und an ihm war nie ein USB-Speicher angeschlossen.

## Vorgehen

- Die Sticks wurden über einen USB-Hub an Laptop 2 angeschlossen. Linux Mint band dabei die Persistenz- und FAT-Partitionen automatisch beschreibbar ein. Vor der Prüfung wurden alle Partitionen ausgehängt und schreibgeschützt neu eingebunden. Danach wurde nur noch gelesen.
- Als Vergleich diente das offizielle Image `linuxmint-22.3-cinnamon-64bit.iso`. Es wurde vom Kernel.org-Spiegel der Linux-Mint-Downloads geladen und als virtuelle CD über den PiKVM eingebunden. Seine SHA-256-Prüfsumme `a081ab202cfda17f6924128dbd2de8b63518ac0531bcfe3f1a1b88097c459bd4` stimmt mit der veröffentlichten Prüfsummenliste von Linux Mint überein.
- Geprüft wurden:
  - jede Datei gegen die Prüfsummenliste `md5sum.txt` des Sticks
  - diese Liste und die Dateiliste gegen das Original
  - Abweichungen Byte für Byte
  - die Bootdateien in `efi.img` und auf der EFI-Partition
  - die Persistenz-Partitionen mit den dort abgelegten Installationsprotokollen
- Arbeitsdateien und Kopien entstanden auf Laptop 2 unter `/tmp/sticks`.

## Übersicht der Sticks

| Nr | Modell / Größe | Seriennummer | Aufbau |
|---|---|---|---|
| S1 | , 14,6 GB | entfernt | Linux-Mint-Image (2,9 GB), EFI-Partition (5 MB), Persistenz-Partition „writable“ (11,8 GB) |
| S2 | , 14,6 GB | entfernt | Eine FAT-Partition „LINUX MINT“, am 29.09.2026 von 13:40 bis 13:42 Uhr mit unter Windows erstellt |
| S3 | , 58,6 GB | entfernt | Linux-Mint-Image (2,9 GB), EFI-Partition (5 MB), Persistenz-Partition „writable“ (55,7 GB) |
| S4 | , 58,6 GB | entfernt | Linux-Mint-Image (2,9 GB), EFI-Partition (5 MB), Persistenz-Partition „writable“ (55,7 GB) |

Tabelle 6: Untersuchte USB-Sticks

Alle vier Sticks enthalten Linux Mint 22.3 „Zena“ Cinnamon, Release amd64 vom 08.01.2026. Die Persistenz-Partition „writable“ wurde jeweils unmittelbar vor dem ersten Installationsprotokoll angelegt, also beim ersten Start des Live-Systems. Dort hat der Installer seine Protokolle abgelegt.

## Installationen laut Protokollen auf den Sticks

| Stick | Zeitpunkt | Gerät laut Firmware | Benutzer | Netz und Medienprüfung |
|---|---|---|---|---|
| S4 | 22.02.2026, ca. 14:33 | nicht feststellbar | – | Protokolle leer, vermutlich abgebrochener Lauf |
| S4 | 22.02.2026, 13:47 bis 14:02 (Geräteuhr) | ( , ) | Benutzer B | keine WLAN-Verbindung protokolliert; Medienprüfung ohne Fehler |
| S4 | 24.02.2026, 14:00 bis 14:11 (Geräteuhr) | ( , ) | Benutzer C | keine WLAN-Verbindung protokolliert; Medienprüfung ohne Fehler |
| S3 | 18.08.2026, ca. 16:35 | nicht feststellbar | – | Protokolle leer, vermutlich abgebrochener Lauf |
| S3 | 26.09.2026, ca. 16:55 bis 17:04 MESZ | ( , ) | Benutzer D | WLAN WLAN 7 |
| S1 | 08.10.2026, ca. 19:35 bis 19:44 MESZ | ( , ) = Laptop 2 | Benutzer A | WLAN WLAN H |

Tabelle 7: Mit den Sticks durchgeführte Installationen

## Fazit

- **Alle vier Sticks enthalten das unveränderte offizielle Linux-Mint-22.3-Image.** Es gibt keine Hinweise auf manipulierte Installationsmedien.
- Die einzigen Abweichungen sind ein von Windows angelegter Ordner in der EFI-Partition von S1 und S3 sowie Kopierfehler in sieben Paketen auf S2. Keine davon betrifft Bootdateien oder das Live-System.
- Laptop 2 wurde am 08.10.2026 mit Stick S1 eingerichtet.
- Mit Stick S4 wurden **am 22. und 24.02.2026 zwei** eingerichtet (Benutzer
- Mit Stick S3 wurde am 26.09.2026 ein eingerichtet (Benutzer Benutzer D).

# 5 Auswertung der Bitcoin-Wallets

## Ausgangslage

- Der Kunde nutzt zwei Hardware-Wallets vom Typ [redacted]: eine **Bitcoin-only**-Ausführung und eine **Multi**-Ausführung.
- Bei einer Hardware-Wallet verbleiben die privaten Schlüssel auf dem Gerät. Jede Überweisung muss am Gerät selbst bestätigt werden.
- Beide Geräte waren an Laptop 2 nur am **09.10.2026 zwischen 15:43 und 16:12 Uhr** angeschlossen. Beide bestanden die Echtheitsprüfung der [redacted]. Die Firmware beider Geräte wurde dabei aktualisiert.
- Die B[redacted]hat bei diesem Anschluss den vollständigen Transaktionsverlauf aus der Blockchain geladen. Die Transaktionen selbst stammen nicht von diesem Rechner.

## Zuordnung der Wallets

Jede [redacted] meldet einen eindeutigen Fingerabdruck ihrer Wallet. Laut Protokoll der [redacted]-App:

| Gerät | Fingerabdruck | Konten mit Bewegungen |
|---|---|---|
| [redacted] Bitcoin-only | entfernt | „Bitcoin“, „Bitcoin 2“, „Bitcoin 3“ |
| [redacted] Multi | entfernt | „Bitcoin“ (Litecoin und Ethereum ohne Bewegungen) |

Tabelle 8: Zuordnung der Wallets

Die Fingerabdrücke unterscheiden sich. Es handelt sich um zwei getrennte Wallets mit unterschiedlichen Seed-Phrasen.

## Verwendete Kürzel

| Kürzel | Adresse | Bedeutung |
|---|---|---|
| K1 | entfernt | Multi, Konto „Bitcoin“ |
| K2 | entfernt | Bitcoin-only, Konto „Bitcoin“ |
| K3 | entfernt | Bitcoin-only, Konto „Bitcoin 2“ |
| K4 | entfernt | „Bitcoin 2“, Wechselgeld |
| K5 | entfernt | Bitcoin-only, Konto „Bitcoin 3“ |
| K6 | entfernt | „Bitcoin 3“, Wechselgeld |
| Z | entfernt | [redacted] |
| S | entfernt | [redacted] |

Tabelle 9: Adressen und Kürzel

Eine **Wechselgeld-Adresse** entsteht automatisch: Ein Bitcoin-Guthaben wird immer vollständig ausgegeben, der nicht benötigte Rest geht an eine neue eigene Adresse zurück.

## Verlauf der Salden und Bilanz

In der Originalfassung stehen hier die Salden aller Konten nach jeder der 15 Bewegungen und eine Bilanz der Ein- und Abgänge. Beide Tabellen sind in dieser Fassung entfernt.

## Feststellungen



- Keine der beteiligten Adressen ist in der öffentlichen Ransomware-Datenbank Ransomwhere verzeichnet. Diese Datenbank wird seit Oktober 2024 nicht mehr gepflegt.

# 6 Anhang

## Anhang A: Zeitachse Laptop 2 und Installations-Sticks

| Zeitpunkt | Ereignis |
|---|---|
| [redacted] | [redacted] |
| 22.02. und 24.02.2026 | Einrichtung zweier [redacted] ([redacted] [redacted] mit Stick S4 |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| 18.08.2026 | Start des Live-Systems von Stick S3, keine Protokolle |
| 26.09.2026, ca. 16:55 bis 17:04 | Einrichtung eines [redacted] mit Stick S3 |
| 29.09.2026, 13:40 bis 13:42 | Stick S2 mit Rufus unter Windows erstellt |
| 08.10.2026, ca. 19:35 bis 19:44 | Installation Linux Mint 22.3 auf Laptop 2 vom Stick S1 |
| 08.10.2026, ab 19:45 | Einrichtung, Download und Installation von Brave und [redacted] |
| 09.10.2026, 14:32 bis 16:20 | [redacted] zeitweise verbunden |
| 09.10.2026, 14:53 bis 15:14 | Download der [redacted] 4.52.0 samt Signatur, Prüfung per GPG |
| 09.10.2026, 15:43 bis 16:12 | Beide [redacted] angeschlossen, Echtheitsprüfung bestanden, Firmware-Update, Synchronisierung des Verlaufs |
| 10.10.2026, ca. 04:35 bis 06:38 | Nutzung (Systemuhr zunächst 02:35): Firefox-Erweiterungen installiert, Paketquellen geprüft, YubiKeys angeschlossen; [redacted] verbunden von 04:36 bis 06:22 |
| 10.10.2026, 06:22 bis 06:28 | WLAN-Profil WLAN X angelegt und verbunden (voraussichtlich Google), ohne VPN |
| 14.10.2026, ca. 17:28 bis 17:32 | Verbindung mit offenem WLAN WLAN X (Systemuhr: 15:28 bis 15:32), Profil danach gelöscht |
| 14.10. bis 15.10.2026 | Letzte Nutzung vor der Untersuchung |
| 20.10.2026 | Gerät laut Kunde mitgenommen (Notiz, nicht überprüft) |

Tabelle 10: Zeitachse der relevanten Ereignisse

## Anhang B: Zeitachse Laptop 1

Zeitangaben bis 24.10.2026 in MESZ, ab 25.10.2026 in MEZ.

| Zeitpunkt | Ereignis |
|---|---|
| 07.04.2026, 13:20 | Erster Eintrag im Setup-API-Log (Werks-Image) |
| 07.04.2026, 13:37 | Frühestes Ereignis aller 134 Ereignisprotokolle (Werks-Image, Rechnername entfernt) |
| 07.04.2026, 13:45 | Neustart des Werks-Image |
| 10.10.2026, 11:10 | Erster Start beim Nutzer, die Systemuhr zeigt fälschlich ca. 17:04 |
| 10.10.2026, 11:11 | Uhr von 17:06:01 auf 11:11:22 korrigiert, Ersteinrichtung beginnt |
| 10.10.2026, 11:13 | WLAN WLAN 1 verbunden (bis 15:36) |
| 10.10.2026, 11:58 | Defender-Echtzeitschutz aus, McAfee übernimmt |
| 10.10.2026, 12:14 | Rechnername entfernt, Beginn des Sicherheitsprotokolls |

| Zeitpunkt | Ereignis |
|---|---|
| 10.10.2026, 13:03 | Konto `Acer` angelegt, Administrator |
| 10.10.2026, 13:10 | Edge: Download des Firefox-Installers aus offizieller Quelle |
| 10.10.2026, 13:12 | |
| 10.10.2026, 13:13 | Firefox: E-Mail-Anbieter |
| 10.10.2026, 13:27 bis 13:30 | Yubico Security Key und YubiKey 5 erstmals angeschlossen |
| 10.10.2026, 13:42 | |
| 10.10.2026, 14:54 | Microsoft-Konto mit dem Konto `Acer` verknüpft |
| 10.10.2026, 15:36 bis 16:04 | Wechsel in die WLANs WLAN 2, WLAN 3 und WLAN 4 |
| 10.10.2026, 16:05 | WLAN WLAN 5 (bis 11.10.2026, 10:24) |
| 10.10.2026, 16:30 | Letzte erfolgreiche Windows-Update-Installation |
| 10.10.2026, 16:37 bis 16:43 | YubiKeys erneut angeschlossen |
| 10.10.2026, 17:23 | |
| 10.10.2026, 18:11 | |
| 10.10.2026, 18:15 bis 18:27 | Firefox über den Desktop-Starter geöffnet, letzte Firefox-Aktivität des Tages |
| 10.10.2026, 18:30 | `certutil` importiert das Acer-Zertifikat `localhost` |
| 10.10.2026, 18:33 | Herunterfahren |
| 11.10.2026, 10:24 | Start, 10:26 bis 11:11 WLAN WLAN 6 |
| 11.10.2026, 11:00 bis 11:12 | |
| 11.10.2026, 11:01 bis 11:11 | BitLocker: Sicherung im Microsoft-Konto fehlgeschlagen, Geräteverschlüsselung nicht aktiviert |
| 11.10.2026, 11:11 | Letzte WLAN-Verbindung überhaupt |
| 11.10.2026, 11:13 | Standby |
| 20.10.2026, 15:28 bis 15:32 | Kurz aufgeweckt (offline), Firefox gestartet, danach Standby |

Tabelle 11: Zeitachse der relevanten Ereignisse auf Laptop 1

Alle Angaben ohne Gewähr. Es gelten die Allgemeinen Geschäftsbedingungen der SecureVibe IT Solutions GmbH unter `https://securevibe.de/agb`.