SecureVibe

IT-Sicherheitsbericht

Kompromittierungsprüfung und Bereinigung

Anonymisierter Kundenfall

Kunden- und Gerätekennungen wurden entfernt.

Gerät: Windows-Rechner

Windows-Arbeitsplatzrechner, Zugriff über KVM-Offline-Werkzeug

Stand:

Prüfung und Bereinigung

Erstellt und durchgeführt von:

Klassifizierung: **Anonymisierte Fassung**

Inhaltsverzeichnis

Einleitung 1

Zusammenfassung 3

Analyse des Systems und Handlungsempfehlungen 5
- Betriebssystem und Patchstand . . . 5
- Browser und Erweiterungen . . . 6
- Installierte Software und Adware . . . 7
- Lizenzierung: Office, KMS und OInstall . . . 8
- Konten und Berechtigungen . . . 9
- Netzwerk und Fernzugriff . . . 10
- Schutzsoftware . . . 10

Zeitleiste 12

Durchgeführte Bereinigung 15

Empfehlungen und Maßnahmenplan 23

Anhang: Indikatoren (IOC-Liste) 28
- Dateien . . . 28
- Signaturzertifikate . . . 30
- Browser-Erweiterungen . . . 30
- Domains . . . 30
- Geplante Aufgaben . . . 31
- Registry, Ordner und Verknüpfungen . . . 31

Einleitung

Zweck und Ziel

Der Arbeitsplatzrechner Rechnername entfernt wurde geprüft und bereinigt. Dieser Bericht dokumentiert die Befunde, die durchgeführten Maßnahmen und die Empfehlungen für den weiteren Betrieb. Untersucht wurden Verbindungen, Downloads, installierte Programme, Browser und weitere mögliche Angriffswege. Der Bericht umfasst außerdem die Folgearbeiten vom 01.11.2026: das Windows-Upgrade, die Ablösung von Avira durch Microsoft Defender, die Installation von Office LTSC Professional Plus 2024 und das Einspielen der verfügbaren Updates.

- Feststellung, ob Schadsoftware, unerwünschte Programme, Fernzugriffe oder Manipulationen an Browsern und Systemeinstellungen vorliegen.
- Nachvollziehbare Dokumentation aller Befunde mit Belegen wie Pfaden, Signaturen, Hashwerten und Zeitpunkten.
- Bewertung der Risiken und Ableitung priorisierter Maßnahmen.
- Dokumentation der durchgeführten Bereinigung und des verbleibenden Handlungsbedarfs.

Untersuchungsgegenstand

Merkmal	Angabe
Kundenbezug	Anonymisiert; Kundennamen und Kontaktdaten entfernt
Gerät	Windows-Rechner (Windows-Arbeitsplatzrechner, Zugriff über KVM-Offline-Werkzeug)
Betriebssystem	Windows 11 Home, Version 21H2, Build 22000.2538, installiert am 18.11.2022; seit 01.11.2026 Version 26H2, Build 26300.9711
Office	bis 31.10.2026 Office LTSC Standard 2021 aus einem Raubkopie-Werkzeug (entfernt); seit 01.11.2026 Office LTSC Professional Plus 2024, Volumenlizenz
Schutzsoftware	bis 01.11.2026 Avira Prime (Avira Security, System Speedup, Phantom VPN); seitdem Microsoft Defender
Hardware	Älterer All-in-One-Rechner, Prozessor von 2015, 4 GB RAM, kein TPM
Benutzerkonto	Benutzer (einziges aktives Konto, lokaler Administrator)
Zugriff	KVM-Offline-Werkzeug: Bildschirm, Tastatur und virtuelles Laufwerk, kein Agent auf dem Rechner
Prüf- und Bereinigungszeitraum	
Durchführung	SecureVibe IT Solutions GmbH

Tabelle 1: Untersuchungsgegenstand

Vorgehen und Methode

- Für die Analyse und Bereinigung wurden KI-gestützte Systeme eingesetzt.
- Die Prüfung wurde manuell in einer Administrator-PowerShell durchgeführt, die über die Tastatur des KVM-Offline-Werkzeugs bedient wurde. Während der Analyse wurden ausschließlich lesende Befehle ausgeführt.
- Ergebnisse von Virenscannern wurden bewusst nicht als Beleg verwendet. Alle Befunde beruhen auf der eigenen Auswertung des Systems.
- Verdächtige Dateien wurden nur gelesen (Hashwert, digitale Signatur, Versionsinformationen, Klartext-Zeichenketten) und nie ausgeführt.
- Öffentliche Einstufungen der gefundenen Programme wurden per Webrecherche ergänzt.
- Vor der anschließenden Bereinigung wurden ein Wiederherstellungspunkt und Sicherungen aller betroffenen Registry-Schlüssel, Aufgaben und Browser-Einstellungen angelegt.

Geprüft wurden folgende Bereiche:

- Netzwerkverbindungen, lauschende Ports, Proxy, hosts-Datei, DNS, Firewall-Regeln und Stammzertifikate
- Laufende Prozesse mit Pfad und Signatur, Dienste und Treiber
- Autostart-Einträge, geplante Aufgaben (inklusive versteckter Aufgaben), WMI, Winlogon, AppInit und IFEO
- Installierte Programme, Downloads mit Herkunftsvermerk (Mark-of-the-Web) und eine Zeitleiste neu angelegter Programmdateien
- Browser Chrome, Edge, Pulse Browser und OneBrowser: Erweiterungen, Installationsart, Richtlinien, Suchmaschine und Verlauf
- Konten, Anmeldungen und Ereignisprotokolle (System, Security, Defender, PowerShell)
- Lizenzierung von Windows und Office, Defender-Ausnahmen, Patchstand

Zusammenfassung

Ergebnis

Bei der Prüfung am 31.10.2026 wurde festgestellt, dass der Rechner Rechnername entfernt **mit Adware und Browser-Hijackern befallen war**. Es gab **keine Hinweise auf einen gezielten Angriff**, auf Fernzugriff oder auf klassische Schadsoftware wie Trojaner, Backdoor oder Keylogger.

- In Microsoft Edge war die Erweiterung „SearchShield“ aktiv. Sie leitete Suchanfragen auf fremde Server um und lief auf jeder aufgerufenen Webseite mit, auch beim Onlinebanking.
- In Chrome waren die Startseiten auf Werbe-Weiterleitungen umgestellt (F10). Das wurde erst während der Bereinigung festgestellt.
- Vier unerwünschte Programme waren installiert und zum Teil dauerhaft im Autostart verankert: Cookie A.Q., Pulse Browser, OneBrowser und My PDF Software (GooPDF).
- Das Betriebssystem Windows 11 21H2 hat seit dem 11.10.2023 keine Sicherheitsupdates mehr erhalten.
- Office war über das Raubkopie-Werkzeug „OInstall“ installiert. Dafür waren Ausnahmen in Microsoft Defender eingetragen, und als Aktivierungsserver diente der inoffizielle KMS-Server `kms.03k.org`.
- Die installierte Schutzsoftware Avira Prime meldete zum selben Zeitpunkt „Virenfrei“ und zeigte keinen dieser Befunde an.

Am selben Abend wurden die Befunde F1 und F3 bis F10 vollständig bereinigt. Office LTSC wurde deinstalliert. In der Nacht zum 01.11.2026 wurde Windows ohne Internetverbindung auf die aktuelle Version 26H2 mit dem Sicherheitsupdate vom Oktober 2026 aktualisiert (F2). Dabei zeigte sich, dass der Rechner die Hardwareanforderungen von Windows 11 nicht erfüllt (F11). Avira wurde durch Microsoft Defender ersetzt. Nach dem Anschluss an das Netzwerk wurde Office LTSC Professional Plus 2024 installiert und aktiviert. Alle verfügbaren Updates für Windows, Defender, Browser und Store-Apps wurden eingespielt. Die Endkontrolle am 01.11.2026 war ohne Befund. Offen sind die Passwortänderungen, die erneute Anmeldung am Microsoft-Konto und mittelfristig der Ersatz des Rechners (siehe „Empfehlungen und Maßnahmenplan“).

Befunde und Risikobewertung

Nr.	Befund	Zustand am 31.10.2026	Risiko	Nach Bereinigung
F1	Edge-Erweiterung „SearchShield“ (Browser-Hijacker)	aktiv	hoch	entfernt
F2	Windows 11 21H2, letztes Sicherheitsupdate am 11.10.2023	aktiv	hoch	erledigt
F3	Chrome-Erweiterung „SearchProtect“ (Browser-Hijacker)	deaktiviert, vorhanden	mittel	entfernt
F4	Cookie A.Q. (Galaxy Dynamics): Updater-Prozess und Chrome-Erweiterung	Prozess läuft	mittel	entfernt
F5	Pulse Browser (Alabama Technology USA, LLC)	Autostart aktiv	mittel	entfernt
F6	OneBrowser / OneBUpdate (Work Product Inc.)	Prozess läuft, stündlich	mittel	entfernt
F7	My PDF Software / GooPDF mit zugehörigem Installer	installiert, inaktiv	mittel	entfernt
F8	OInstall-Ausnahmen in Defender und KMS-Server `kms.03k.org` (Office-Raubkopie)	aktiv	mittel	erledigt
F9	Weitere Downloads und Altlasten (TotalAV, PDFDocReader, Soda PDF, Lavasoft u. a.)	inaktiv	gering	entfernt
F10	Gekaperte Chrome-Startseiten (`swiftverdict.com`, `smartingly.com`), bei der Bereinigung festgestellt	aktiv (Profil „Default“)	mittel	entfernt
F11	Hardware erfüllt die Windows-11-Anforderungen nicht (kein TPM, Prozessor von 2015), Upgrade nur mit Umgehung der Hardwareprüfung	vorhanden	mittel	offen

Tabelle 2: Befunde, Risiko und Bearbeitungsstand

Gesamtbewertung

- Der Rechner war durch unerwünschte Software kompromittiert. Die Programme stammen überwiegend aus einer Bündelinstallation am 24.09.2026. Innerhalb von fünf Minuten wurden dabei ein angeblicher PDF-Konverter, zwei Werbe-Browser und deren Aktualisierungsdienste installiert.
- Besonders kritisch war die aktive Edge-Erweiterung mit Lese- und Schreibzugriff auf alle Webseiten. Ein Abfluss von Zugangsdaten ist nicht belegt, lässt sich aber wegen des verschleierten Programmcodes nicht ausschließen.
- Alle unerwünschten Programme, Erweiterungen, Autostarts, gekaperten Browsereinstellungen, Raubkopie-Reste und Altlasten wurden entfernt. Die Nachkontrolle war ohne Befund.
- Betriebssystem, Office, Browser und Schutzsoftware sind seit dem 01.11.2026 auf dem aktuellen Stand. Avira wurde durch Microsoft Defender ersetzt. Der Schutz vor potenziell unerwünschten Anwendungen (PUA) ist eingeschaltet, und der Schnellscan war ohne Fund.
- Verbleibende Risiken sind möglicherweise abgeflossene Zugangsdaten und die Hardware, die die Anforderungen von Windows 11 nicht erfüllt (F11).
- Für einen gezielten Angriff, Fernzugriff, neue Benutzerkonten oder manipulierte Netzwerkeinstellungen ergaben sich keine Hinweise.

Analyse des Systems und Handlungsempfehlungen

Betriebssystem und Patchstand

Ausgangslage

- Auf dem Rechner läuft Windows 11 Home in der Version 21H2, Build 22000.2538, installiert am 18.11.2022.
- Die letzten installierten Updates stammen vom 11.10.2023 (KB5031358 Sicherheitsupdate, KB5031591).
- Der letzte Neustart erfolgte am 18.10.2026. Seitdem wurde der Rechner nur in den Standby versetzt und wieder aufgeweckt.
- Windows ist über eine OEM-Digitallizenz ordnungsgemäß aktiviert.
- Hardware: Älterer All-in-One-Rechner mit einem Prozessor von 2015 und 4 GB Arbeitsspeicher. Secure Boot ist aktiv, ein TPM ist nicht vorhanden. Festgestellt wurde das erst beim Upgrade am 01.11.2026.

Identifizierte Schwachstellen

- Die Version 21H2 erhält keine Sicherheitsupdates mehr. Seit über drei Jahren wurden keine Sicherheitskorrekturen installiert.
- Alle seit Oktober 2023 bekannt gewordenen Sicherheitslücken in Windows-Komponenten sind auf diesem Rechner offen.
- Der Rechner erfüllt die Mindestanforderungen von Windows 11 nicht (TPM 2.0, Prozessor ab der 8. Generation). Windows 11 lief darauf schon bisher nur an der Hardwareprüfung vorbei. Microsoft garantiert für solche Geräte keine Updates.

Fazit

- Der fehlende Patchstand war das größte strukturelle Risiko des Rechners. Der Patchstand wurde mit dem Upgrade am 01.11.2026 aktualisiert.
- Die Bereinigung der unerwünschten Software ändert daran nichts.

Lösungen

- erledigt Upgrade auf Windows 11 26H2 mit dem Sicherheitsupdate vom Oktober 2026 (Build 26300.9711) am 01.11.2026, siehe Abschnitt „Durchgeführte Bereinigung“.
- Mittelfristig Ersatz des Rechners durch ein Gerät, das die Anforderungen von Windows 11 erfüllt.
- Automatische Updates aktiviert lassen und den Rechner regelmäßig neu starten, damit Updates vollständig installiert werden.

Browser und Erweiterungen

Ausgangslage

- Standardbrowser ist Google Chrome mit den Profilen „Default“ und „Profile 1“. Zusätzlich sind Microsoft Edge, Pulse Browser und OneBrowser installiert, OneBrowser ohne Benutzerprofil.
- Für Chrome sind keine Richtlinien (Policies) gesetzt. Für Edge ist nur die unbedenkliche Richtlinie `ConfigureDoNotTrack` gesetzt, festgestellt bei der Bereinigung. Extern registrierte Erweiterungen stammen von Avira, Adobe und Cookie A.Q.
- Unauffällig sind die Erweiterungen von Avira, Adobe Acrobat, Google Docs Offline, die Chrome-Web-Store-Zahlungen und die Edge-eigenen Komponenten.

Identifizierte Schwachstellen

- **Edge, „SearchShield“** (`cajkghbacphcjgemgmmachjcgamkcacd`, Version 1.2.0.151): seit dem 30.09.2026, 11:30:40 Uhr aktiv. Die Erweiterung wurde direkt in das Browserprofil geschrieben und nicht aus einem Store installiert. Sie leitet die Standardsuche auf `searchraptor.com` um und hängt jeder Suche eine Installationskennung an (`iid=ENTFERNT`). Als neue Tab-Seite dient `shoutoutsearch.com`, im Edge-Verlauf stehen dazu 13 Einträge.
- **Chrome, „SearchProtect“** (`jnannpdmmiphnkpaooplhegabbghlplj`, Version 7.0.0.32): seit dem 28.09.2026, 10:48:18 Uhr vorhanden, zum Prüfzeitpunkt deaktiviert. Umleitungsziele sind `search-path.com` und `savvyfinder.com`. Die Chrome-Standardsuche steht auf Yahoo, dem typischen Endziel solcher Umleitungen.
- Beide Hijacker stammen aus derselben Familie (identische Symboldatei) und haben Berechtigungen für alle Webseiten. Ihr Skript läuft auf jeder Seite ab Ladebeginn. Der Code ist stark verschleiert, enthält Telemetrie-Aufrufe und beobachtet Tab-Wechsel. Im Klartext waren keine Zugriffe auf Cookies, Verlauf, Passwortfelder oder Tastatureingaben erkennbar.
- Beide Erweiterungen erschienen wenige Sekunden nach dem Aufwachen des Rechners aus dem Standby. Das spricht für eine Einschleusung durch einen bereits laufenden Hintergrundprozess. Welcher es war, ließ sich nicht mehr eindeutig feststellen.
- **Chrome, „Cookie A.Q.“** (`ogcodmabngepnhbcgeleiojgolkmpmpb`) in beiden Chrome-Profilen, mit Zugriff auf Browserdaten und alle Webseiten. Die Erweiterung war deaktiviert, wird aber über einen Registry-Eintrag immer wieder neu installiert.

Fazit

- Suchanfragen und aufgerufene Seiten gelangten mit hoher Wahrscheinlichkeit an die Betreiber der Hijacker.
- Weil auf dem Rechner Onlinebanking genutzt wird, ist ein weitergehender Datenabfluss das relevanteste Restrisiko. Belegt ist er nicht, ausschließen lässt er sich wegen der Verschleierung nicht.

Lösungen

- erledigt Entfernen der Erweiterungen SearchShield, SearchProtect und Cookie A.Q. einschließlich des Registry-Eintrags zur Neuinstallation.
- erledigt Zurücksetzen von Suchmaschine, Startseiten und neuer Tab-Seite in Edge und Chrome, Ausschalten des Entwicklermodus in beiden Browsern.
- Ändern der Passwörter für Onlinebanking, E-Mail und weitere wichtige Konten, die seit dem 28.09.2026 in Edge oder Chrome genutzt wurden, von einem sauberen Gerät aus.
- Begrenzung der Browser-Erweiterungen auf eine Freigabeliste per Browser-Richtlinie und Sperre des Entwicklermodus.

Installierte Software und Adware

Ausgangslage

- Neben regulärer Software (Office, Adobe Acrobat, PDF24, GIMP, Epson-Treiber, ABBYY FineReader, Avira, 7-Zip) waren vier unerwünschte Programme installiert.
- Cookie A.Q. kam am 24.10.2023 auf den Rechner. Am selben Tag lief die heute nicht mehr installierte Software Soda PDF Desktop 14.
- Pulse Browser, My PDF Software und OneBrowser wurden am 24.09.2026 zwischen 17:37 und 17:42 Uhr installiert, also innerhalb von fünf Minuten.

Identifizierte Schwachstellen

- **Cookie A.Q.** (Galaxy Dynamics Ltd): Der Prozess `cookieaq updater.exe` lief und lauschte auf `127.0.0.1:32259`. Er startete über eine von Avira angelegte verzögerte Startaufgabe. Öffentlich wird das Programm als Adware eingestuft.
- **Pulse Browser** (signiert von Alabama Technology USA, LLC): zwei geplante Aufgaben, davon eine als versteckt markiert und stündlich ausgeführt. Update-Server ist `pulseupdate.com`. Öffentlich wird der Browser als unerwünschtes Programm und Browser-Hijacker eingestuft.
- **OneBrowser** (signiert von Work Product Inc.): Der Dienst `OneBUpdateService.exe` lief stündlich. Das Programm hatte sich zusätzlich so eingetragen, dass es sich bei einem Windows-Upgrade selbst neu einrichtet. Öffentlich wird es als Adware eingestuft.
- **My PDF Software / GooPDF**: Das Programm ist unsigniert. Der Installer `PDFConvertSetup_279084.exe` ist von Net Sourcing Experts LLC (Kyjiw) signiert. Installer dieser Namensreihe werden teilweise heuristisch als Trojaner erkannt. Das Vorgehen entspricht bekannten Kampagnen mit gefälschten PDF-Werkzeugen.
- Die Herkunft der Installer ist nicht feststellbar: Sie tragen keinen Herkunftsvermerk, und im Verlauf von Chrome, Edge und Pulse Browser gibt es keinen Eintrag dazu.
- Weitere Downloads: `TotalAV_Setup.exe` kam über eine „Deal“-Weiterleitung, `PDFDocReader.exe` („Open PDF Studio“, signiert von Impertio Studio B.V.). Beide waren nicht installiert. Hinzu kommen Registry-Altlasten von Soda PDF, Lavasoft und Kaspersky.

Fazit

- Die Funde zeigen das typische Muster einer Bündelinstallation über einen angeblich kostenlosen PDF-Konverter.
- Die Adware war über geplante Aufgaben und Hintergrunddienste dauerhaft verankert. Hinweise auf eine darüber hinausgehende Schadfunktion ergaben sich nicht.
- Die Autostart-Optimierung von Avira hat Cookie A.Q. und den Pulse-Updater nur in verzögerte Startaufgaben verschoben, nicht entfernt.

Lösungen

- erledigt Deinstallation von Cookie A.Q., Pulse Browser, OneBrowser und My PDF Software.
- erledigt Entfernen der Restordner, geplanten Aufgaben, Registry-Einträge und Startmenü-Verknüpfungen (siehe Anhang).
- erledigt Löschen der Installer `PDFConvertSetup_279084.exe`, `PDFDocReader*.exe` und `TotalAV_Setup.exe`.
- Software nur von den Herstellerseiten beziehen. Für PDF-Aufgaben ist mit PDF24 bereits ein seriöses Werkzeug installiert.

Lizenzierung: Office, KMS und OInstall

Ausgangslage

- Installiert war Office LTSC Standard 2021, eine Volumenlizenz-Edition (Version 16.0.14334.20974, installiert am 21.11.2022 um 09:55 Uhr).
- Eine Minute zuvor, am 21.11.2022 um 09:54:33 Uhr, wurden in Microsoft Defender Ausnahmen für das Raubkopie-Werkzeug `OInstall.exe` und seinen Ordner `files` im temporären Verzeichnis eingetragen.
- Als Aktivierungsserver war systemweit der öffentliche, inoffizielle KMS-Server `kms.03k.org` (Port 1688) eingetragen.
- Office war nicht mehr aktiviert (Lizenzstatus 5, Benachrichtigungsmodus). Das Ereignisprotokoll zeigt wiederholte Aktivierungsfehler.
- Am 24.10.2026 wurden offizielle, von Microsoft signierte Installer für Office Home & Student und Microsoft 365 heruntergeladen.

Identifizierte Schwachstellen

- Die Office-Installation war nicht lizenziert und stammte aus einem Raubkopie-Werkzeug.
- Die Defender-Ausnahmen galten weiter, obwohl der Ordner nicht mehr existierte.
- Aktivierungsanfragen gingen an einen inoffiziellen Server.
- Raubkopie-Werkzeuge sind ein häufiger Verbreitungsweg für Schadsoftware. Weitere Spuren wie Hook-Bibliotheken, IFEO-Einträge oder KMS-Dienste wurden allerdings nicht gefunden.

Fazit

- Es wurde keine aktive Schadsoftware gefunden. Es bestanden aber ein Lizenzrisiko und eine unnötige Schwächung des Virenschutzes.

Lösungen

- erledigt Deinstallation von Office LTSC Standard 2021.
- erledigt Entfernen der Defender-Ausnahmen und des KMS-Eintrags `kms.03k.org`.
- erledigt Installation und Aktivierung von Office LTSC Professional Plus 2024 mit einem Volumenlizenzschlüssel (MAK) am 01.11.2026.

Konten und Berechtigungen

Ausgangslage

- Einziges aktives Konto ist Benutzer. Es ist lokaler Administrator und wird für die tägliche Arbeit genutzt. Das Passwort wurde zuletzt am 18.12.2024 gesetzt.
- Die Konten `Administrator`, `Gast`, `DefaultAccount` und `WDAGUtilityAccount` sind deaktiviert.
- Im ausgewerteten Zeitraum des Security-Protokolls (ab 24.09.2026) gab es keine neuen oder geänderten Konten, keine Gruppenänderungen und keine gelöschten Protokolle. Fehlgeschlagen sind fünf Anmeldungen, alle lokal oder über das Gastkonto.

Identifizierte Schwachstellen

- Die tägliche Arbeit mit Administratorrechten hat die unbemerkte Installation der Adware erleichtert.
- Alltags- und Verwaltungskonto sind nicht getrennt.

Fazit

- Die Konten selbst waren unauffällig. Das Berechtigungsmodell begünstigt aber den Befall mit unerwünschter Software.

Lösungen

- Ein Standardbenutzerkonto für die tägliche Arbeit einrichten und ein separates Administratorkonto mit starkem Passwort nur für Installationen verwenden.
- Das Passwort des bisherigen Kontos ändern.

Netzwerk und Fernzugriff

Ausgangslage

- Der Rechner ist per WLAN angebunden (IP entfernt Gateway und DNS ist der Router Router

- Zum Prüfzeitpunkt bestanden nur zwei ausgehende Verbindungen, beide von Avira. Die lauschenden Ports entsprachen dem Windows-Standard, hinzu kam der nur lokal erreichbare Port von Cookie A.Q.
- Es war kein Proxy gesetzt, die hosts-Datei enthielt keine Einträge, RDP war deaktiviert und die Firewall in allen Profilen aktiv.

Identifizierte Schwachstellen

- Keine. Es wurden keine Fernwartungsprogramme wie AnyDesk, TeamViewer, RustDesk oder ScreenConnect gefunden.
- Im ausgewerteten Zeitraum des Security-Protokolls (ab 24.09.2026) gab es keine Netzwerk- oder RDP-Anmeldungen von fremden Adressen.
- Es gab keine Firewall-Ausnahmen für die unerwünschten Programme und keine fremden Stammzertifikate. Ausnahme ist das erwartbare Zertifikat des Avira-Web-Schutzes.

Fazit

- Es gab keinen Hinweis auf Fernzugriff, Umleitung des Datenverkehrs oder Manipulation der Netzwerkeinstellungen.

Lösungen

- Keine Sofortmaßnahmen erforderlich.
- Der Router war nicht Gegenstand der Prüfung. Seine Firmware sollte aktuell gehalten werden.

Schutzsoftware

Ausgangslage

- Installiert ist Avira Prime mit Echtzeitschutz, Firewall, Web-Schutz und VPN. Microsoft Defender ist dadurch passiv bzw. abgeschaltet. In seiner Historie waren keine Funde abrufbar.
- Frühere Spuren deuten auf Verdacht hin: Am 10.07.2026 wurden AdwCleaner und Malwarebytes heruntergeladen, am 30.09.2026 wurde ein Microsoft-Defender-Offline-Scan vorbereitet.

Identifizierte Schwachstellen

- Der Avira Smart Scan meldete am 31.10.2026 „Virenfrei“ und „Programme sind aktuell“, obwohl die Befunde F1 bis F8 vorlagen. Die Erkennung unerwünschter Programme (PUA) war offenbar nicht wirksam.

- Die Autostart-Optimierung von Avira hat Cookie A.Q. und den Pulse-Updater nur in verzögerte Startaufgaben verschoben, statt vor ihnen zu warnen.
- Die Bereinigungsfunktion von Avira hat den Prefetch-Ordner geleert. Dadurch fehlten bei der Prüfung forensische Spuren.

Fazit

- Die Schutzsoftware allein bot keinen ausreichenden Schutz vor unerwünschten Programmen und Browser-Hijackern. Ihre Statusanzeige vermittelte eine trügerische Sicherheit.

Lösungen

- erledigt Avira am 01.11.2026 vollständig entfernt und durch Microsoft Defender ersetzt. Der PUA-Schutz ist eingeschaltet, die Signaturen sind aktuell, und der Schnellscan war ohne Fund.
- Erweiterungen und Autostarts regelmäßig manuell kontrollieren.

Zeitleiste

Die Zeitleiste fasst die rekonstruierten Ereignisse zusammen. Die Zeitpunkte stammen aus Dateizeitstempeln, Registry- und Aufgabendefinitionen, Herkunftsvermerken der Downloads sowie den Ereignisprotokollen.

Tabelle 3: Zeitleiste der Ereignisse

Zeitpunkt	Ereignis	Beleg
18.11.2022 13:22	Windows installiert	Systeminformationen
21.11.2022 09:54:33	Defender-Ausnahmen für `...\Temp\` Ordner `OInstall.exe` und `...\files` eingetragen	Defender-Ereignis 5007
21.11.2022 09:55:24	Office LTSC Standard 2021 installiert, KMS-Server `kms.03k.org` gesetzt	Programmordner, Registry
11.10.2023	Letztes Windows-Sicherheitsupdate (KB5031358)	Update-Verlauf
24.10.2023 ca. 13:39	Soda PDF Desktop 14 zuletzt gestartet (heute nicht mehr installiert)	Registry
24.10.2023 14:34:01	**Cookie A.Q. installiert**	Dateizeiten, Deinstallationseintrag
24.10.2023 18:45:28	Chrome-Erweiterung „Cookie A.Q.“ im Profil „Default“	Erweiterungsordner
29.09.2024 17:52	Avira verschiebt den Autostart von Cookie A.Q. in eine verzögerte Startaufgabe	Aufgabendefinition
14.10.2024 18:29:49	Chrome-Erweiterung „Cookie A.Q.“ im Profil „Profile 1“	Erweiterungsordner
10.07.2026 17:39	AdwCleaner und Malwarebytes heruntergeladen (heute nicht installiert)	Downloads, Herkunftsvermerk
23.08.2026 16:43	Zwei ZIP-Dateien mit Bankunterlagen aus einem Bank-Postfach (unbedenklich)	Herkunftsvermerk
24.09.2026 17:37:04–17:37:44	**Pulse Browser installiert**, geplante Aufgaben und Schnellstart-Verknüpfung angelegt	Dateizeiten, Aufgaben
24.09.2026 17:39:26	`PDFConvertSetup_279084.exe` in Downloads (ohne Herkunftsvermerk)	Dateizeit
24.09.2026 17:41:10 und 17:41:49	`PDFDocReader.exe` zweimal in Downloads (ohne Herkunftsvermerk)	Dateizeiten
24.09.2026 17:41:47	**My PDF Software (GooPDF) installiert**	Dateizeiten
24.09.2026 17:42:02–17:42:07	**OneBrowser installiert**, Aufgabe `\OneBUpdate` (stündlich) angelegt	Dateizeiten, Aufgabe
28.09.2026 10:48:12	Rechner wacht aus dem Standby auf	Systemprotokoll
28.09.2026 10:48:18	**Hijacker „SearchProtect“ in Chrome eingeschleust**	Erweiterungsordner, Profildaten
28.09.2026 10:48:52	Pulse Browser aktiv (Widevine-Komponente installiert)	Dateizeiten
28.09.2026 10:57:16	Avira legt eine verzögerte Startaufgabe für den Pulse-Updater an	Aufgabendefinition

Fortsetzung auf der nächsten Seite

Zeitpunkt	Ereignis	Beleg
28.09.2026 11:09:02	`TotalAV_Setup.exe` über `totalav.com/deal` geladen (nicht installiert)	Herkunftsvermerk
30.09.2026 11:30:33	Rechner wacht aus dem Standby auf	Systemprotokoll
30.09.2026 11:30:40	**Hijacker „SearchShield“ in Edge eingeschleust**, Edge-Suche seitdem über `searchraptor.com`	Erweiterungsordner, Profildaten
30.09.2026 11:30:56	Umleitungsregel für `searchraptor.com` angelegt	Regeldatei der Erweiterung
30.09.2026 11:33:22	Pulse-Software aktiv (WebView-Profil angelegt)	Dateizeiten
30.09.2026 12:07	Microsoft-Defender-Offline-Scan vorbereitet	Dateizeiten
24.10.2026 17:46:37	Avira-Bereinigung leert den Prefetch-Ordner	Avira-Protokolle, Prefetch
24.10.2026 18:19–20:35	Installer für Office Home & Student, Microsoft 365 und Outlook geladen und ausgeführt (von Microsoft signiert)	Downloads, Prefetch
25.10.2026 18:29	Pulse Browser zuletzt ausgeführt	Prefetch
31.10.2026 16:12:39	WLAN getrennt, die automatische Wiederverbindung um 16:12:54 Uhr schlägt fehl; der Rechner ist seitdem offline	WLAN- und Netzwerkprotokoll
31.10.2026 17:20:11	`cookieaq updater.exe` gestartet (verzögerte Avira-Startaufgabe)	Prozessliste
31.10.2026	Beginn der Prüfung	–
31.10.2026 17:42:42	`OneBUpdateService.exe` gestartet (stündliche Aufgabe)	Aufgabenstatus
31.10.2026	Ende der Analyse	–
31.10.2026	**Beginn der Bereinigung:** Wiederherstellungspunkt Nr. 169 angelegt	Systemwiederherstellung
31.10.2026	PUP-Prozesse beendet, fünf geplante Aufgaben entfernt	Durchgeführte Maßnahmen
31.10.2026	Pulse Browser und OneBrowser deinstalliert; Programmordner, Installer, Altordner und Registry-Reste entfernt	Durchgeführte Maßnahmen
31.10.2026	KMS-Einträge entfernt, Office LTSC Standard 2021 deinstalliert	Durchgeführte Maßnahmen
31.10.2026	Browser bereinigt: SearchShield und SearchProtect entfernt, gekaperte Startseiten, Suchmaschinen und Entwicklermodus korrigiert	Durchgeführte Maßnahmen
31.10.2026	Defender-Ausnahmen für OInstall entfernt	Durchgeführte Maßnahmen
31.10.2026	Registry- und Dateisystemreste entfernt, darunter 68 COM-Schlüssel und die Quellordner der Erweiterungen	Durchgeführte Maßnahmen
31.10.2026	**Nachkontrolle ohne Befund**	Durchgeführte Maßnahmen

Fortsetzung auf der nächsten Seite

Zeitpunkt	Ereignis	Beleg
01.11.2026	**Beginn des Windows-Upgrades:** Prüfung der Voraussetzungen, Übertragung und Prüfung der Update-Pakete	Durchgeführte Maßnahmen
01.11.2026	Setup für Windows 11 26H2 gestartet, ohne Internetverbindung und mit umgangener Hardwareprüfung	Durchgeführte Maßnahmen
01.11.2026	Upgrade abgeschlossen	Durchgeführte Maßnahmen
01.11.2026	KB5127648 und KB5127694 installiert, Neustart mit Verarbeitung der Updates	Durchgeführte Maßnahmen
01.11.2026	Avira System Speedup, Avira Phantom VPN und Avira Security deinstalliert	Durchgeführte Maßnahmen
01.11.2026	Avira-Reste und ein veralteter Kaspersky-Eintrag im Sicherheitscenter entfernt; Microsoft Defender ist einziger Virenschutz	Sicherheitscenter
01.11.2026	Defender-Signaturen 1.463.73.0 offline eingespielt, SHA256-Prüfsumme und Microsoft-Signatur geprüft	Durchgeführte Maßnahmen
01.11.2026	PUA-Schutz eingeschaltet, Defender-Schnellscan ohne Fund	Defender-Status
01.11.2026	Sieben Avira-Erweiterungen aus Chrome (beide Profile) und Edge entfernt	Browser
01.11.2026	Update-Pakete gelöscht, Avira-Registry entfernt, Kontrolle vor dem Netzanschluss	Durchgeführte Maßnahmen
01.11.2026	**Rechner per LAN-Kabel mit dem SecureVibe-LAN verbunden**	Netzwerkprofil
01.11.2026	**Office LTSC Professional Plus 2024 online installiert**, Kanal PerpetualVL2024, Build 16.0.17932.21056	Durchgeführte Maßnahmen
01.11.2026	Windows Update: drei Updates installiert, kein weiteres kumulatives Update verfügbar	Update-Verlauf
01.11.2026	Office aktiviert (MAK)	`OSPP.VBS`
01.11.2026	Defender-Signaturen online auf 1.463.76.0 aktualisiert	Defender-Status
01.11.2026	Edge, Chrome und Store-Apps aktualisiert	Browser, Microsoft Store
01.11.2026	**Neustart**	Durchgeführte Maßnahmen
01.11.2026	**Endkontrolle ohne Befund**	Endkontrolle

Durchgeführte Bereinigung

Grundlage waren die Befunde F1 bis F9. Office wurde deinstalliert. Die festgestellten Probleme wurden bereinigt. Alle Maßnahmen wurden über das KVM-Offline-Werkzeug durchgeführt, entweder in einer Administrator-PowerShell oder in den Oberflächen der Browser.

Vorbereitung und Sicherung

- **Wiederherstellungspunkt:** Nr. 169 „Vor PUP- und Office-Bereinigung 31.10.2026“, angelegt am 31.10.2026. Der Computerschutz war bereits aktiv, mit Punkten vom 06.10., 15.10. und 24.10.2026.
- **Sicherungen:** Vor jeder Änderung wurden alle betroffenen Registry-Schlüssel (24 Exporte), die Definitionen der fünf entfernten geplanten Aufgaben und die Einstellungsdateien von Chrome (beide Profile) und Edge gesichert.
- **Office vor der Deinstallation:** Der Lizenzstatus wurde dokumentiert:
  - Lizenz `Office21Standard2021VL_KMS_Client_AE`, Produktschlüssel anonymisiert
  - KMS-Eintrag `kms.03k.org:1688`
  - Status „Benachrichtigung“, Fehler `0xC004F00F`

  Es lief keine Office-Anwendung. Eine PST-Datei gab es nicht, nur eine leere OST-Datei (Cache eines E-Mail-Kontos). Durch die Deinstallation gingen also keine E-Mails verloren.

Durchgeführte Maßnahmen

Tabelle 4: Durchgeführte Maßnahmen am 31.10.2026

Maßnahme	Ergebnis
Wiederherstellungspunkt angelegt	erledigt Nr. 169
Registry-Sicherung von 20 Schlüsseln (Deinstallationseinträge, Herstellerschlüssel, Defender-Ausnahmen, KMS, Run, `HKCU\Software\Classes`)	erledigt gesichert
Aufgabendefinitionen und Browser-Einstellungen gesichert, Prozesse `cookieaq updater.exe` und `OneBUpdateService.exe` beendet	erledigt beendet
Geplante Aufgaben entfernt: `\OneBUpdate`, `\PulseSoftware\PulseBrowserStartup` SID entfernt, `\PulseSoftware\PulseBrowserUpdaterTaskUser135.0.7049.101{` ID entfernt , `\Avira\System Speedup\Delayed Startup\` Benutzer `2` und `\` Benutzer `4`	entfernt 5 Aufgaben
Pulse Browser mit dem eigenen Deinstallationsprogramm entfernt (`setup.exe --uninstall --force-uninstall`)	entfernt Exitcode 19 (erfolgreich)

Fortsetzung auf der nächsten Seite

Maßnahme	Ergebnis
OneBrowser mit dem eigenen Deinstallationsprogramm entfernt	entfernt Exitcode 19; Programmeintrag blieb wegen der unvollständigen Installation und wurde manuell entfernt
Ordner gelöscht: `AppData\Local\PulseSoftware`, `AppData\Local\OB`, `AppData\Roaming\cookieaq`, `AppData\Local\Programs\MyPdfSoftware`; Startmenü-Einträge „My PDF Software“ und `OneBrowser.lnk`; Installer `PDFConvertSetup_279084.exe`, `PDFDocReader.exe`, `PDFDocReader (1).exe` und `TotalAV_Setup.exe` im Download-Ordner	entfernt gelöscht
Altordner gelöscht, vorher auf Nutzerdateien geprüft: `AppData\Local\Avanquest_Software` (leer), `AppData\Roaming\Soda PDF Desktop 14` (nur Protokolle und Einstellungen, 0,3 MB), `ProgramData\Kaspersky Lab Setup Files` (alte Installer, 8,1 MB)	entfernt gelöscht
Registry-Einträge entfernt: Deinstallationseinträge `cookieaq`, `MyPdfSoftware` und `OB`; `Google\Chrome\Extensions\ogcodmabngepnhbcgeleiojgolkmpmpb` (Zwangsinstallation von Cookie A.Q.); {ID entfernt}; `OB`, `OneBrowser`, `OIBrowser`, `Chromium`, `Soda PDF Desktop 14`, `Avanquest`, `Lavasoft`, `KasperskyLab`	entfernt entfernt; die Pulse-Schlüssel waren bereits bei der Deinstallation gelöscht worden
Office: KMS-Produktschlüssel und KMS-Server über `OSPP.VBS` entfernt; Windows: KMS-Server mit `slmgr /ckms` gelöscht	erledigt kein Office-Produktschlüssel mehr
Office LTSC Standard 2021 still deinstalliert (`OfficeClickToRun.exe`, `DisplayLevel=False`)	entfernt Programmeintrag und Programmdateien entfernt
Edge: Erweiterung SearchShield entfernt, Entwicklermodus ausgeschaltet, Suchmaschine geprüft (wieder „Bing (Standard)“), Start- und Neuer-Tab-Seite geprüft	erledigt bereinigt
Chrome, Profil „Default“: SearchProtect entfernt, Cookie A.Q. von Chrome automatisch entfernt, Entwicklermodus ausgeschaltet, Suchmaschine von Yahoo auf Google umgestellt, gekaperte Startseiten entfernt (siehe F10)	erledigt bereinigt
Chrome, „Profile 1“: Cookie A.Q. automatisch entfernt, Entwicklermodus ausgeschaltet, Suche (Google) und Startverhalten geprüft; Benachrichtigungen in beiden Profilen geprüft (keine Freigaben)	erledigt bereinigt
Defender-Ausnahmen für OInstall entfernt	entfernt 0 Ausnahmen
Registry-Suche nach Resten (HKCU und `HKLM\SOFTWARE`), danach entfernt: 68 COM-Schlüssel der Pulse-/OneBrowser-Updater (4 CLSID, 31 TypeLib, 31 Interface, 2 ProgIDs), KMS-Eintrag in der 32-Bit-Sicht (`WOW6432Node`), 2 Einträge in der Avira-Startliste „Speedup DelayLoad“, 2 MAC-Reste der Erweiterungen, leere Aufgabenordner `\PulseSoftware`	entfernt entfernt, vorher zusätzlich gesichert

Fortsetzung auf der nächsten Seite

Maßnahme	Ergebnis
Quellordner der Hijacker-Erweiterungen gelöscht (Chrome `jnanndmmiphnkpaooplhegabbghlplj`, Edge `cajkghbacphcjgemgmmachjcgamkcacd`)	entfernt gelöscht
Nachkontrolle (siehe unten)	erledigt ohne Befund
Chrome, „Profile 1“: versteckte Start-URL `swiftverdict.com` entfernt	entfernt entfernt
Bereinigung abgeschlossen	erledigt abgeschlossen

Zusätzliche Feststellungen während der Bereinigung

- **F10, gekaperte Chrome-Startseiten:** Im Profil „Default“ stand Chrome beim Start auf „Bestimmte Seiten öffnen“. Hinterlegt waren zwei Werbe-Weiterleitungen mit identischem Tracking-Pfad, `swiftverdict.com/` entfernt `?...` und `smartingly.com/T` entfernt `?...`. Im „Profile 1“ war `swiftverdict.com` hinterlegt, aber nicht aktiv. Die Einstellung liegt in den geschützten Chrome-Einstellungen („Secure Preferences“) und wurde in der Analyse deshalb nicht erkannt. Beide Einträge sind entfernt.
- **Entwicklermodus:** In Chrome (beide Profile) und in Edge war der Entwicklermodus eingeschaltet. Er ist Voraussetzung für die eingeschleusten „entpackten“ Erweiterungen und ist jetzt überall ausgeschaltet.
- **Rückmeldung beim Entfernen:** Edge öffnete beim Entfernen von SearchShield die Deinstallationsseite der Erweiterung, `trueshields.com/ext/uni?iid=ENTFERNT&extVersion=1.2.0.151&extID=cajkghbacphcjgemgmmachjcgamkcacd`. Die Installationskennung bestätigt das Tracking. Wegen der fehlenden Netzwerkverbindung wurde die Seite nicht geladen.
- **Netzwerk:** Während der Bereinigung war der Rechner ohne Netzwerkverbindung. Das WLAN war bereits vor Prüfbeginn am 31.10.2026 getrennt worden; die automatische Wiederverbindung war fehlgeschlagen. Das geschah vor Prüfbeginn, an den Netzwerkeinstellungen wurde nichts geändert. Die Rückmeldungen der Hijacker erreichten deren Server deshalb nicht, und der leere DNS-Cache aus der Analyse ist damit erklärt.
- **Edge-Richtlinie:** Edge zeigt „Von Ihrer Organisation verwaltet“, weil die Richtlinie `ConfigureDoNotTrack = true` gesetzt ist. Sie ist datenschutzfreundlich und unbedenklich und wurde nicht verändert.
- **Ausführungsspuren:** Nutzungshistorie in der Registry (MuiCache, Programmkompatibilitäts-Assistent, FeatureUsage) belegt unter anderem zwei Starts von `CookieAQ_Install.exe` aus dem Temp-Ordner am 24.10.2023. Außerdem belegt sie einen Pulse-Installer unter `Temp\PulseSoftwareTEMP\bin\updater.exe`. Diese Einträge haben keine Funktion und wurden als Beleg belassen.
- **Platzhalter in den Browserdateien:** In den geschützten Einstellungsdateien von Chrome und Edge bleiben leere Platzhaltereinträge der entfernten Erweiterungen stehen. Sie haben keine Funktion. Ein manueller Eingriff würde die Prüfsummen der Browser verletzen.

Nachkontrolle

Prüfpunkt (31.10.2026)	Ergebnis
Installierte Programme	Keine PUPs, kein Office LTSC, kein TotalAV mehr. Es verbleibt das „Microsoft Teams Meeting Add-in“, das zu Teams gehört.
Prozesse der Funde	0
Geplante Aufgaben der Funde	0, Aufgabenordner `\PulseSoftware` entfernt
Run-Einträge der Funde	0
Defender-Ausnahmen	0
KMS-Eintrag (64- und 32-Bit)	leer
Lizenzen mit Produktschlüssel	nur Windows (Core edition, aktiviert)
Lauschende Ports außer Windows	nur OneDrive lokal (`::1:42050`); Port 32259 von Cookie A.Q. geschlossen
Dateisystem (Namen der Funde)	keine Treffer (ein Fehlalarm im Windows-Sprachpaket „PushToInstall“)
Registry (HKCU, `HKLM\SOFTWARE`)	nur noch Nutzungshistorie ohne Funktion
Chrome (beide Profile)	Suche Google, Start mit Neuer-Tab-Seite, keine Start-URLs, Entwicklermodus aus, keine Benachrichtigungsfreigaben
Edge	Suche Bing, Start mit Neuer-Tab-Seite, Entwicklermodus aus, keine Hijacker-Erweiterung

Tabelle 5: Ergebnis der Nachkontrolle

Windows-Upgrade ohne Internetverbindung (01.11.2026)

Windows wurde in der Nacht zum 01.11.2026 auf die aktuelle Version 26H2 aktualisiert, zusammen mit dem Sicherheitsupdate vom Oktober 2026 und dem zugehörigen .NET-Update. Der Rechner blieb dabei offline. Alle Installationsdateien stammen aus offiziellen Quellen von Microsoft.

- **Hardware:** Älterer All-in-One-Rechner mit einem Prozessor von 2015, 4 GB Arbeitsspeicher und aktivem Secure Boot. Ein **TPM ist nicht vorhanden**. Der Rechner erfüllt die Mindestanforderungen von Windows 11 nicht (TPM 2.0, Prozessor ab der 8. Generation). Das galt bereits für die Installation von 21H2 im November 2022.
- **Daten und Programme:** Es handelt sich um ein Inplace-Upgrade, Benutzerdaten, Programme und Einstellungen bleiben erhalten. Eine gesonderte Datensicherung wurde vorher nicht angelegt. Über „Einstellungen > System > Wiederherstellung“ ist zehn Tage lang die Rückkehr zu 21H2 möglich (Ordner `C:\Windows.old`).

Tabelle 6: Windows-Upgrade am 31.10.2026 und 01.11.2026

Maßnahme	Ergebnis
Offizielles Abbild `Windows11_Client_x64_de-de_26300_9457.iso` (Windows 11 26H2, Build 26300.9457, 9.052.962.816 Byte) von der Microsoft-Downloadseite auf das KVM-Offline-Werkzeug geladen	erledigt vollständig
Sicherheitsupdate KB5127648 (Build 26300.9711, 4.775.050.195 Byte) aus dem Microsoft Update-Katalog auf das KVM-Offline-Werkzeug geladen	erledigt vollständig

Maßnahme	Ergebnis
Voraussetzungen geprüft: 413 GB frei, BitLocker aus, Secure Boot an, kein TPM	erledigt geprüft
KB5127648 auf den Rechner übertragen, SHA1 `2B88D2D308ADC938FCD4D2876A68EE0B2A3C4C09`	erledigt Prüfsumme stimmt
.NET-Update KB5127694 (105.996.411 Byte) aus dem Update-Katalog auf das KVM-Offline-Werkzeug geladen und übertragen, SHA1 `A1A6F6D3C61E46A77278881FC5F7245BCF09CE3F`	erledigt Prüfsumme stimmt
Abbild auf dem virtuellen Laufwerk gegen die SHA256-Prüfsumme der Microsoft-Downloadseite geprüft, `193BBDE65EC84E298A1C798959489C8375ED501CF973C6D37FA52BB22EE8D43B`	erledigt Prüfsumme stimmt
Setup gestartet: `setup.exe /product server /auto upgrade /dynamicupdate disable /eula accept /compat ignorewarning /showoobe none`	erledigt keine Blockade
Erste Setup-Phase abgeschlossen, Neustart	erledigt
Upgrade abgeschlossen	erledigt ohne Rücksetzung
KB5127648 und KB5127694 installiert, anschließend Neustart	erledigt installiert
Neustart mit Verarbeitung der Updates	erledigt ohne Fehlermeldung

Installiert ist Windows 11 Home 26H2, Build 26300.9711. Beide Updates meldeten den Exitcode 3010 (erfolgreich, Neustart erforderlich). Installiert sind KB5127648, KB5127647 und KB5127694.

Ablösung von Avira durch Microsoft Defender (01.11.2026)

Avira Prime wurde vollständig entfernt und durch den in Windows enthaltenen Microsoft Defender ersetzt. Der Rechner war dabei noch ohne Netzwerkverbindung. Die Signaturen für Defender wurden deshalb über das virtuelle Laufwerk des KVM-Offline-Werkzeugs bereitgestellt.

Tabelle 7: Ablösung von Avira am 01.11.2026

Maßnahme	Ergebnis
Die fünf verzögerten Avira-Startaufgaben (Google Updater, Adobe Acrobat, Epson Download Navigator, PDF24, Realtek-Audio) gesichert, Browser-Erweiterungen erfasst	erledigt gesichert
Avira System Speedup 7.5.0.552 mit dem eigenen Deinstallationsprogramm entfernt	entfernt entfernt
Avira Phantom VPN 2.47.1.24783 entfernt	entfernt entfernt
Avira Security 1.1.116.3442 einschließlich Fallback Updater über das Avira-eigene Deinstallationsprogramm entfernt. Den angebotenen Neustart auf das Ende der Arbeiten verschoben	entfernt entfernt
Die zuvor von Avira verzögerten Autostarts, unter anderem PDF24, Epson, Adobe Acrobat und Google Updater, wurden bei der Deinstallation automatisch wieder regulär eingetragen	erledigt geprüft

Maßnahme	Ergebnis
Reste entfernt: Aufgaben `AviraSystemSpeedupRemoval` und `\Avira\System Speedup\SecurityTestScheduler`, Aufgabenordner `\Avira`, der tote Autostart „Avira Security startup helper“, die Ordner `C:\Program Files (x86)\Avira` und `C:\ProgramData\Avira` sowie die Prozesse des Avira-Meldewerkzeugs. Veralteten Kaspersky-Eintrag im Sicherheitscenter entfernt	entfernt 0 Avira-Aufgaben und -Prozesse; Defender einziger Virenschutz
Signaturpaket `mpam-fe.exe` 1.463.73.0 von Microsoft über das KVM-Offline-Werkzeug übertragen und eingespielt. SHA256 `7D2508677393923B249EE5368995BC37049CB8266BB95B919D83765779284010`, Signatur Microsoft Corporation gültig	erledigt Echtzeitschutz aktiv
Schutz vor potenziell unerwünschten Anwendungen (PUA) eingeschaltet	erledigt aktiv
Defender-Schnellscan	erledigt 0 Funde
Avira-Erweiterungen entfernt: in Chrome, Profile „Default“ und „Profile 1“, jeweils Avira Password Manager, Avira Safe Shopping und Avira Browser Safety; in Edge Avira Password Manager	entfernt 7 Erweiterungen
Registry-Schlüssel `HKLM\SOFTWARE\Avira`, `HKLM\SOFTWARE\WOW6432Node\Avira` und `HKCU\SOFTWARE\Avira` gesichert und entfernt. Avira-Treiber sind keine mehr registriert	entfernt entfernt
Kontrolle vor dem Netzanschluss: Firewall in allen Profilen aktiv, Remotedesktop deaktiviert, Echtzeit-, Verhaltens- und Download-Schutz von Defender aktiv	erledigt ohne Befund

Office LTSC Professional Plus 2024 (01.11.2026)

Office LTSC Professional Plus 2024 wurde mit dem Office Deployment Tool (ODT) von Microsoft installiert. Office wurde mit einem Volumenlizenzschlüssel (MAK) aktiviert. Konfiguration: 64 Bit, Deutsch, Update-Kanal `PerpetualVL2024`, automatische Aktivierung, ohne Skype for Business und ohne die Office-Variante von OneDrive (OneDrive ist Teil von Windows). Enthalten sind Word, Excel, PowerPoint, Outlook, OneNote und Access.

Tabelle 8: Office-Installation am 01.11.2026

Maßnahme	Ergebnis
Netzwerk geprüft: Ethernet, Profil „Öffentlich“, Server von Microsoft erreichbar.	erledigt geprüft
ODT `setup.exe` 16.0.20430.20146 von `officecdn.microsoft.com` geladen, Signatur Microsoft Corporation gültig	erledigt geprüft
Online-Installation	erledigt Build 16.0.17932.21056 (Version 2408)

Maßnahme	Ergebnis
Office aktiviert. Lizenzstatus laut `OSPP.VBS`: `Office24ProPlus2024VL_MAK_AE2`	erledigt `---LICENSED---`
Funktionstest: Word startet ohne Aktivierungsabfrage, unter „Konto“ steht „Produkt aktiviert – Microsoft Office LTSC Professional Plus 2024“	erledigt erfolgreich

Updates nach dem Netzanschluss (01.11.2026)

Am 01.11.2026 wurde der Rechner per LAN-Kabel mit dem SecureVibe-LAN verbunden. Die Verbindung wurde in Windows dem Profil „Öffentlich“ zugeordnet. Danach wurden alle verfügbaren Updates eingespielt.

- Das nächste Sicherheitsupdate von Microsoft erscheint am Patchday, dem 10.11.2026. Es kommt über die automatischen Updates.
- Das SecureVibe-LAN meldet sich bei Windows als getaktete Verbindung. Am Rechner ist Ethernet nicht als getaktet eingestellt. Store- und Edge-Updates wurden deshalb erst auf Anforderung gestartet.
- Nach Abschluss der Installationen wurde der Rechner neu gestartet. Damit ist auch die Deinstallation von Avira abgeschlossen.

Tabelle 9: Updates nach dem Netzanschluss

Bereich	Ergebnis	Stand
Windows Update	Suche über die Windows-Update-Schnittstelle, ohne optionale Updates. Installiert: Update der Microsoft-Defender-Antischadsoftwareplattform KB4052623 (4.18.26100.4), Update der Windows-Sicherheitsplattform KB5007651 (10.0.29680.1000) und der Microsoft-Audiotreiber AudioProcessingObject 1.0.4.7057. Kein Neustart erforderlich. Ein neues kumulatives Update gab es nicht, KB5127648 vom Oktober 2026 ist aktuell. Erneute Suche: nichts offen	erledigt
Defender-Signaturen	Online-Aktualisierung von 1.463.73.0 auf 1.463.76.0, die zu diesem Zeitpunkt aktuelle Version von Microsoft	erledigt
Microsoft Edge	156.0.4314.42 auf 156.0.4314.58	erledigt
Google Chrome	156.0.8078.79 auf 156.0.8078.80	erledigt
Microsoft Store	Alle angebotenen App-Updates installiert, darunter Store, App-Installer, Windows App Runtime, Medienerweiterungen, Fotos, Paint, Editor, Rechner und Copilot. Windows Terminal wurde nach dem Neustart aktualisiert	erledigt
Office	Installiert in der aktuellen Version des Kanals `PerpetualVL2024`, automatische Updates eingeschaltet	erledigt

Endkontrolle (01.11.2026)

Die Endkontrolle am 01.11.2026 war ohne Befund.

Prüfpunkt	Ergebnis
Windows	Windows 11 Home 26H2, Build 26300.9711, über die OEM-Digitallizenz aktiviert
KMS-Einträge	leer (Windows 64 und 32 Bit, Office)
Office	Office LTSC Professional Plus 2024, aktiviert (MAK, `---LICENSED---`)
Microsoft Defender	aktiv, Echtzeit- und PUA-Schutz an, Signaturen 1.463.76.0, Plattform 4.18.26100.4, keine Ausnahmen; einziger Virenschutz im Sicherheitscenter
Avira	keine Programme, Dienste, Treiber, Prozesse, Aufgaben, Autostarts oder Ordner
Unerwünschte Programme	keine Programme, Prozesse, Aufgaben oder Autostarts
Windows Update	keine offenen Updates, kein Neustart ausstehend
Microsoft Store	keine offenen Updates, Windows Terminal aktualisiert (1.24.12741.0)
Wiederherstellungspunkte	Nr. 169 wurde mit dem Upgrade entfernt, vorhanden ist nur Nr. 1 von Windows

Tabelle 10: Ergebnis der Endkontrolle

Empfehlungen und Maßnahmenplan

Empfehlung

Der akute Befall wurde durch die Bereinigung beseitigt. Entfernt wurden alle unerwünschten Programme und Browser-Hijacker, die gekaperten Browsereinstellungen, die Office-Raubkopie samt Defender-Ausnahmen und KMS-Eintrag sowie die Altlasten (siehe „Durchgeführte Bereinigung“). Seit dem 01.11.2026 sind zudem Windows (Version 26H2 mit dem Sicherheitsupdate vom Oktober 2026), Browser und Store-Apps auf dem aktuellen Stand. Avira wurde durch Microsoft Defender ersetzt. Office LTSC Professional Plus 2024 wurde installiert und aktiviert. Sicher betrieben werden kann der Rechner aber erst, wenn auch die Ursachen und die strukturellen Schwächen behoben sind. Empfohlen wird folgende Reihenfolge:

1. **Zugangsdaten erneuern (sofort):** Alle Passwörter, die seit dem 28.09.2026 in Edge oder Chrome verwendet wurden, sind als potenziell bekannt zu betrachten. Das gilt vor allem für Onlinebanking und E-Mail. Die Änderung erfolgt von einem sauberen Gerät aus, zusätzlich sind die Kontoumsätze zu prüfen.
2. **Microsoft-Konto (kurzfristig):** Die Endkontrolle am 01.11.2026 war ohne Befund. Das Microsoft-Konto muss erneut angemeldet werden, damit OneDrive und die Office-Anmeldung wieder funktionieren.
3. **Rechner ersetzen (mittelfristig):** Office ist seit dem 01.11.2026 installiert und aktiviert. Der Rechner erfüllt die Hardwareanforderungen von Windows 11 nicht (kein TPM, Prozessor von 2015) und sollte mittelfristig durch ein aktuelles Gerät ersetzt werden.
4. **Ursachen abstellen (mittelfristig):** Ein Standardbenutzerkonto für die tägliche Arbeit, eine Datensicherung und ein bewusster Umgang mit Software-Downloads verhindern einen erneuten Befall. Der PUA-Schutz von Defender ist seit dem 01.11.2026 eingeschaltet.

Der Patchstand wurde durch das Inplace-Upgrade vom 01.11.2026 aktualisiert. Die Restunsicherheit aus dem verschleierten Programmcode und dem früheren Einsatz eines Raubkopie-Werkzeugs bleibt, ebenso das Risiko, dass Microsoft für nicht unterstützte Geräte keine Updates mehr ausliefert. Beides wird durch ein **neues Gerät mit frisch installiertem Windows 11** beseitigt, auf das nur die Daten übernommen werden.

Phase 1: Analyse und Bestandsaufnahme (abgeschlossen)

Die Analyse am 31.10.2026 bildet die Grundlage aller weiteren Schritte. Die Ergebnisse stehen in den Abschnitten „Zusammenfassung“ bis „Zeitleiste“ und im Anhang.

- Prüfung von Netzwerkverbindungen, Prozessen, Autostarts, Aufgaben, Diensten, Registry, Dateisystem und Ereignisprotokollen
- Auswertung aller Browserprofile, Erweiterungen und Downloads
- Bewertung der Befunde F1 bis F9 und Erstellung der Indikatorenliste

Phase 2: Bereinigung (abgeschlossen am 31.10.2026)

Die Bereinigung ist im Abschnitt „Durchgeführte Bereinigung“ vollständig dokumentiert. Die Nachkontrolle war ohne Befund.

- erledigt Browser-Erweiterungen SearchShield, SearchProtect und Cookie A.Q. entfernt. Suchmaschinen, Startseiten (F10) und Entwicklermodus in Chrome und Edge korrigiert.
- erledigt Cookie A.Q., Pulse Browser, OneBrowser und My PDF Software deinstalliert, einschließlich Aufgaben, Ordnern, Registry-Einträgen (unter anderem 68 COM-Schlüssel) und Verknüpfungen.
- erledigt Office LTSC Standard 2021 deinstalliert. Defender-Ausnahmen und KMS-Einträge (64- und 32-Bit) entfernt.
- erledigt Verdächtige Installer und Altlasten von Soda PDF, Avanquest, Lavasoft und Kaspersky gelöscht.
- erledigt Vor der Bereinigung Wiederherstellungspunkt und vollständige Sicherungen angelegt.

Phase 3: Sofortmaßnahmen: Zugangsdaten, Nachprüfung und Netzwerk

Diese Maßnahmen sollten sofort umgesetzt werden. Passwortänderungen erfolgen von einem sauberen Gerät aus.

- Passwort für das Onlinebanking ändern, die Zwei-Faktor-Freigabe prüfen und die Kontoumsätze seit dem 28.09.2026 kontrollieren.
- Passwörter für E-Mail-Konten und weitere wichtige Dienste ändern, die seit dem 28.09.2026 in Edge oder Chrome genutzt wurden. Wo möglich, eine Zwei-Faktor-Anmeldung aktivieren.
- Die im Browser gespeicherten Passwörter nach der Änderung aktualisieren.
- erledigt Endkontrolle am 01.11.2026: ohne Befund.
- Das Microsoft-Konto erneut anmelden. Office meldet einen Kontofehler, Edge bittet um Bestätigung der Anmeldung.
- Das Kennwort des Kontos Benutzer nur regulär ändern, über „Strg+Alt+Entf“ und „Kennwort ändern“ mit dem bisherigen Kennwort. Ein Zurücksetzen durch einen Administrator macht gespeicherte Browser-Passwörter und Windows-Anmeldeinformationen unbrauchbar.
- erledigt Netzwerkverbindung am 01.11.2026 per LAN hergestellt, alle verfügbaren Updates eingespielt. Am Einsatzort das WLAN wieder verbinden, es ist seit dem 31.10.2026 getrennt.
- Bis zum Abschluss dieser Phase kein Onlinebanking auf diesem Rechner durchführen.

Phase 4: Systembasis erneuern (teilweise erledigt)

Betriebssystem

- erledigt Inplace-Upgrade auf Windows 11 26H2 mit dem Sicherheitsupdate KB5127648 und dem .NET-Update KB5127694 am 01.11.2026, ohne Internetverbindung.

- erledigt Am 01.11.2026 online geprüft: Ein weiteres kumulatives Update gab es nicht. Installiert wurden die Defender-Plattform, die Windows-Sicherheitsplattform und ein Audiotreiber. Das Sicherheitsupdate vom November 2026 (Patchday 10.11.2026) kommt über die automatischen Updates, die aktiviert bleiben.
- Mittelfristig den Rechner durch ein Gerät ersetzen, das die Anforderungen von Windows 11 erfüllt. Dabei Windows neu installieren und nur die Daten übernehmen. Vorher eine vollständige Datensicherung anlegen, insbesondere der wichtigen Benutzerdokumente.

Office

- erledigt Office LTSC Standard 2021 aus dem Raubkopie-Werkzeug am 31.10.2026 deinstalliert, KMS-Einträge und Defender-Ausnahmen entfernt.
- erledigt Office LTSC Professional Plus 2024 am 01.11.2026 installiert und mit einem Volumenlizenzschlüssel (MAK) aktiviert. Updates kommen automatisch über den Kanal `PerpetualVL2024`.
- erledigt Aktivierung bei der Endkontrolle bestätigt.

Phase 5: Härtung und nachhaltiger Betrieb

Konten und Berechtigungen

- Ein Standardbenutzerkonto für die tägliche Arbeit einrichten.
- Das Administratorkonto nur für Installationen und Änderungen verwenden und mit einem starken, eigenen Passwort schützen.
- Die Benutzerkontensteuerung auf der Standardstufe belassen und Rückfragen bewusst prüfen, insbesondere den angezeigten Herausgeber.

Schutzsoftware und Browser

- erledigt Avira am 01.11.2026 durch Microsoft Defender ersetzt, Schutz vor potenziell unerwünschten Anwendungen (PUA) eingeschaltet.
- Neben Defender keine weiteren Virenschutz- oder „Optimierungs“-Programme installieren. Zwei Virenschutzprogramme behindern sich gegenseitig.
- In Chrome und Edge Erweiterungen per Richtlinie auf eine Freigabeliste beschränken und den Entwicklermodus sperren.
- Nur benötigte Browser installiert lassen. Für PDF-Aufgaben das bereits vorhandene PDF24 nutzen.

Datensicherung

Eine Datensicherung war nicht Gegenstand der Prüfung. Da auf dem Rechner wichtige Benutzerdokumente liegen, wird eine einfache 3-2-1-Sicherung empfohlen.

- Regelmäßige Sicherung der Benutzerdaten auf einen externen Datenträger, der nur während der Sicherung angeschlossen ist.

- Zusätzliche Sicherung in einem Cloudspeicher mit Versionierung, etwa dem bereits installierten OneDrive.
- Gelegentliche Wiederherstellungstests einzelner Dateien.

Sensibilisierung

- Software nur von den offiziellen Herstellerseiten oder aus dem Microsoft Store beziehen, nicht über Werbeanzeigen oder Download-Portale.
- Vorsicht bei angeblich kostenlosen PDF-Konvertern, Treiber-Updatern und „Optimierungs"-Werkzeugen. Solche Angebote bündeln häufig unerwünschte Software.
- Pop-ups und Seiten, die vor angeblichen Infektionen warnen und zum Kauf von Schutzsoftware drängen, schließen und nicht folgen.
- Keine Aktivierungs- oder Crack-Werkzeuge einsetzen.

Regelmäßige Kontrolle

- Vierteljährlich die installierten Programme, Browser-Erweiterungen und Autostart-Einträge sichten.
- Den Update-Status von Windows, Office und Browsern prüfen.
- Bei Auffälligkeiten wie veränderter Suchmaschine, neuen Symbolleisten oder unbekannten Programmen frühzeitig eine Prüfung veranlassen.

Roadmap der Maßnahmen

Die Abbildung zeigt die Abfolge der Maßnahmen und ihre Dringlichkeit.

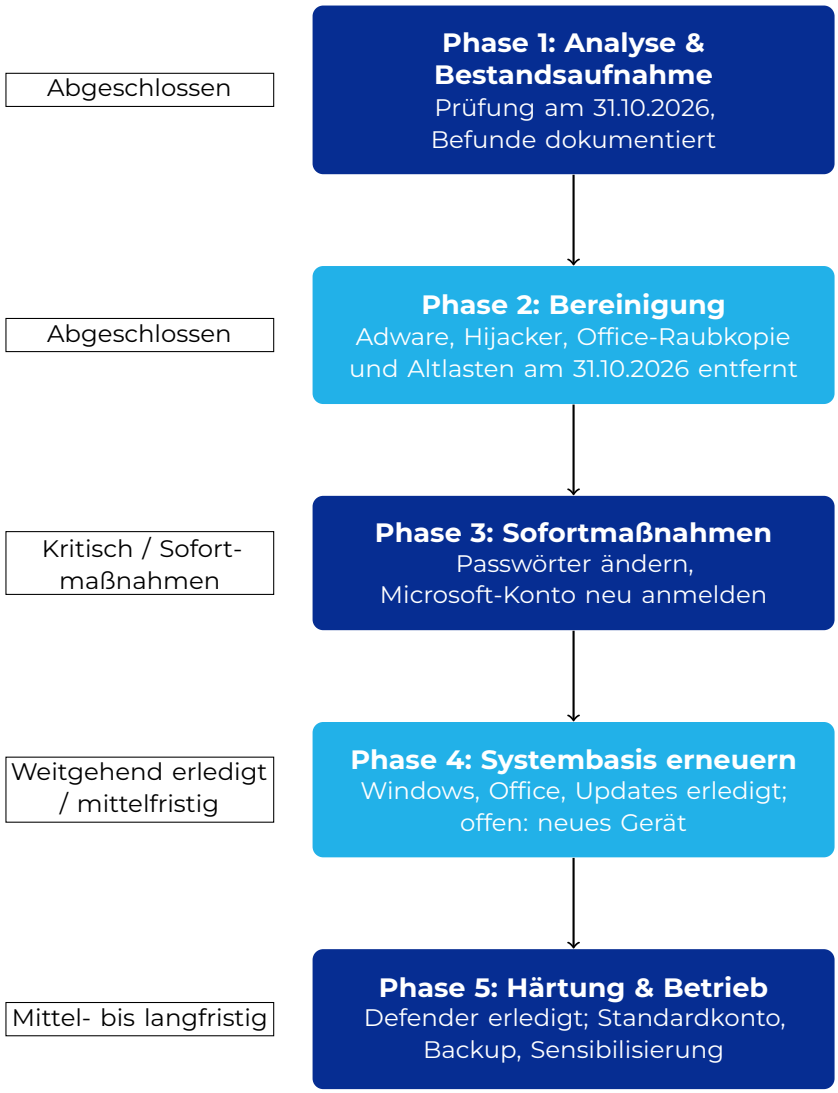


Abbildung 1: Roadmap der Maßnahmen für Windows-Rechner

Anhang: Indikatoren (IOC-Liste)

Die folgenden Indikatoren beschreiben den Befund zum Prüfzeitpunkt am 31.10.2026. Sie dienen zur Wiedererkennung auf diesem oder anderen Geräten und zum Abgleich mit Reputationsdiensten.

Hinweis: Die Hashwerte wurden vom Bildschirm abgelesen. Vor einer Weitergabe oder einem Abgleich, etwa mit VirusTotal, sind sie am Gerät mit `Get-FileHash -Algorithm SHA256 -Path <Pfad>` gegenzuprüfen.

Dateien

Tabelle 11: Dateien mit SHA256-Hashwert (Pfade relativ zu `C:\Users\` Benutzer)

Datei	Signatur	SHA256
`AppData\Roaming\cookieaq\updater\cookieaq updater.exe`	GALAXY DYNAMICS LTD	E7C5CE9D4A7000BFC7397B21DC9352024728F0C329D8A95ACCD987C6C455926F
`AppData\Roaming\cookieaq\cookieaq.exe`	GALAXY DYNAMICS LTD	01E1558918235DBE696070631F1E96895F59260AD02461ABDF179AEA78D01390
`AppData\Roaming\cookieaq\isrun.exe`	GALAXY DYNAMICS LTD	BD59352F99F7BC2358FE5AFF7C1206344FD92CE280EC03DE732CB9CF811DB924
`AppData\Roaming\cookieaq\iswaiter.exe`	GALAXY DYNAMICS LTD	0D1A84881A70F0B49DF7A237A22151B24554E68BF0E7297E2B2F214D15FF34A5
`AppData\Roaming\cookieaq\uninst.exe`	GALAXY DYNAMICS LTD	1745D817A00062C66B58213889289B3B2CA6C1E21D1922B4D5AD4342A6162DA9
`AppData\Local\PulseSoftware\PulseBrowser\Application\pulsebrowser.exe`	Alabama Technology USA, LLC	FE53E6C26F56E89C96828E28FF064267AA74E45A0F75508C60E66C4D864BD121
`AppData\Local\PulseSoftware\PulseBrowser\Application\149.0.7827.158\Installer\setup.exe`	Alabama Technology USA, LLC	7F79979ABF143A9B91CE0F77B936438CC4A04BCC7F5D871BB9643299C97E27B1
`AppData\Local\PulseSoftware\PulseBrowserUpdater\135.0.7049.101\updater.exe` (identisch mit `AppData\Local\PulseSoftware\Update\Pulse BrowserUpdate.exe`)	Alabama Technology USA, LLC	A8EC63229A801901D83120E5E108CBF01D70C21D05C4E5288F54FF80591944C6
`AppData\Local\OB\OneBUpdate\OneBUpdateService.exe`	Work Product Inc.	A4C8A47853734C4796F6DEE296640B30B1140113ECE41E07CAEDAB8C351CF776
`AppData\Local\OB\Application\OneBrowser.exe` (auch in `AppData\Local\OB\Temp\`)	Work Product Inc.	FEC95BA8075AAFC0CE71C25A566A472821EDD8B8E7CC32960A881992CE7AE957

Fortsetzung auf der nächsten Seite

Datei	Signatur	SHA256
`AppData\Local\OB\Application\chrome_proxy.exe` (auch in `AppData\Local\OB\Temp\`)	Work Product Inc.	66F52182E935EC861D03104230297C67C8733524DCF92B91C863E6CE12B71796
`AppData\Local\OB\Application\137.0.7151.69\Installer\setup.exe`	Work Product Inc.	493E6B44B84ACCFC38C05C9C1011B944E9AB4115830D8D8A3EFA35A76DD901B2
`AppData\Local\OB\Application\137.0.7151.69\chrome_pwa_launcher.exe`	Work Product Inc.	E01B01B15E3421AC9FC2D0E31D3C95B5F520185F4E336D7F1C56D74CAD66181A
`AppData\Local\OB\Application\137.0.7151.69\notification_helper.exe`	Work Product Inc.	7AD935F4E9A3022DFF7ADAB6E8961B1E7DCF896915D71E5DF22400046AB3FA53
`AppData\Local\Programs\MyPdf Software\GooPdf.exe`	**unsigniert**	25925DCA6C7292C650A64B4670B260815EE6E1310BB3C9784D8BC237F90CB825
`Downloads\PDFConvertSetup_279084.exe`	Net Sourcing Experts LLC	4365F595F7D9626EB25D229EFE2D4F8160D9FAFC2ED975505C1832DF3664C7DD
`Downloads\PDFDocReader.exe` und `Downloads\PDFDocReader (1).exe`	Impertio Studio B.V.	A98E908E2D380F2559E6199CBE90E34A89235C5DAB98272A199668D03F04ADEC
`Downloads\TotalAV_Setup.exe`	Total Security Limited	295118E51842D24D5680C43ABF4D55304CC7529A7489A77805B1A4B1D43E74F6

Erweiterung	Datei	SHA256
SearchShield (Edge)	`service_worker.js`	A49EDE8DE0A3C910BF4FAA3E6A73648ADB90079C6AB7C0B640F4E94F0664D4D0
SearchProtect (Chrome)	`service_worker.js`	45C5AC0CA2D46BAC356CA9155342DB51C37F9A7A359EABD6A3CF943C5C84CFB7
beide (identisch)	`favicon.ico`	DF03463E67363914131D79ACEF1018FD9BF2897F9EB54C99306186465036FF85

Tabelle 12: Dateien der Hijacker-Erweiterungen

Signaturzertifikate

Signaturgeber	Sitz	Thumbprint	Gültigkeit
GALAXY DYNAMICS LTD	Egham (GB)	02F7FE1AC86F9EA9D55D7AD803567F9EA4528535	05.05.2022–05.05.2025
Alabama Technology USA, LLC	Kalifornien (US)	CB7DD993165246E52B2CCB50DC8D4779711F68E7	17.04.2026–18.04.2027
Work Product Inc.	Golden, Colorado (US)	32A3AD63140B38D99176B3E0885903696A098D07	17.12.2025–17.12.2026
Net Sourcing Experts LLC	Kyjiw (UA)	98C987E4871012EEAD71CB5F351CE4E2357D9688	27.02.2026–27.02.2027
Impertio Studio B.V.	Dordrecht (NL)	3D7C65F5DE619E1616C0815BD09F5B21DBB25739	26.07.2026–29.07.2026
Total Security Limited	Fareham (GB)	789B36BF4478802CB02AA4D2AFA0BCD38AF9AA2E	30.06.2026–02.10.2027

Tabelle 13: Signaturzertifikate der gefundenen Dateien

Browser-Erweiterungen

Browser/Profil	Kennung	Name, Version	Zustand
Edge, Default	`cajkghbacphcjgemgmmachjcgamkcacd`	SearchShield 1.2.0.151	aktiv
Chrome, Default	`jnannpdmmiphnkpaooplhegabbghlplj`	SearchProtect 7.0.0.32	deaktiviert
Chrome, Default und Profile 1	`ogcodmabngepnhbcgeleiojgolkmpmpb`	Cookie A.Q. 1.1.0	deaktiviert
Pulse Browser, Default	`ddomlcjnbfakinihjhdnabiodnikomhm`	Pulse AI 2.6	–

Tabelle 14: Unerwünschte Browser-Erweiterungen (Zustand bei der Prüfung, inzwischen entfernt)

Domains

Domain	Zuordnung
`searchraptor.com`	Suchumleitung der Erweiterung SearchShield
`shoutoutsearch.com`	Neue Tab-Seite der Erweiterung SearchShield
`trueshields.com`	im Code der Erweiterung SearchShield
`search-path.com`	Suchumleitung der Erweiterung SearchProtect
`savvyfinder.com`	Neue Tab-Seite der Erweiterung SearchProtect
`safesearchinc.com`	im Code der Erweiterung SearchProtect
`pulsebrowser.com`, `pulseupdate.com`	Pulse Browser, Update-Server
`cookieaq.com`, `galaxy-dynamics.com`	Cookie A.Q., Hersteller
`install.protected.net`	Download-Quelle von `TotalAV_Setup.exe`
`kms.03k.org`	inoffizieller KMS-Aktivierungsserver

Tabelle 15: Domains der gefundenen Programme

Geplante Aufgaben

Tabelle 16: Geplante Aufgaben der unerwünschten Programme

Aufgabe	Auslöser	Aktion
`\OneBUpdate`	stündlich ab 24.09.2026 17:42	`AppData\Local\OB\OneBUpdate\OneBUpdateService.exe`
`\PulseSoftware\PulseBrowserStartup` SID entfernt	bei Anmeldung	`pulsebrowser.exe --win-start --no-startup-window`
`\PulseSoftware\PulseBrowserUpdater\PulseBrowserUpdaterTaskUser135.0.7049.101{` ID entfernt (als versteckt markiert)	bei Anmeldung und stündlich	`updater.exe --wake`
`\Avira\System Speedup\Delayed Startup\` Benutzer `2`	bei Anmeldung, 1:06 min verzögert	Pulse `updater.exe --wake`
`\Avira\System Speedup\Delayed Startup\` Benutzer `4`	bei Anmeldung, 1:10 min verzögert	`cookieaq updater.exe`

Registry, Ordner und Verknüpfungen

Registry

- Deinstallationseinträge unter `HKCU\Software\Microsoft\Windows\CurrentVersion\Uninstall\`: `cookieaq`, `MyPdfSoftware`, `OB`, `PulseSoftware PulseBrowser`
- `HKCU\Software\Google\Chrome\Extensions\ogcodmabngepnhbcgeleiojgolkmpmpb` (Neuinstallation der Cookie-A.Q.-Erweiterung)
- `HKCU\Software\{` ID entfernt mit dem Wert `cookieaq=1`
- `HKCU\Software\OB` (unter anderem `Commands\on-os-upgrade`, Neueinrichtung bei Windows-Upgrade)
- `HKCU\Software\OneBrowser`, `HKCU\Software\OIBrowser`, `HKCU\Software\PulseSoftware`, `HKCU\Software\Chromium`
- `HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths` mit zwei Ausnahmen für `OInstall.exe` und `files`
- `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform` mit `KeyManagementServiceName=kms.03k.org`

Ordner

- `C:\Users\` Benutzer `AppData\Roaming\cookieaq\`
- `C:\Users\` Benutzer `AppData\Local\PulseSoftware\`
- `C:\Users\` Benutzer `AppData\Local\OB\`

- `C:\Users\ Benutzer AppData\Local\Programs\MyPdfSoftware\`

Verknüpfungen

- Startmenü: `My PDF Software\Goopdf.lnk`, `OneBrowser.lnk`, `Pulse Browser.lnk`
- Schnellstart: `AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Pulse Browser.lnk`