ACCCF / BIBLIOTHEK FÜR ANGEWANDTES WISSEN

13

BAND

Sichere Entscheidungen, bevor gelöscht oder beschuldigt wird

Spanische Ausgabe · 2026

Verdacht auf digitale Überwachung: Leitfaden zur Prüfung und Beweissicherung mit Zero Breach Toolkit

Krise, falsche Indizien, überprüfter Download, Datenschutz, Berichtsinterpretation und forensische Übergabe

Einer besorgten Person helfen, Indizien zu prüfen, ohne Beweismaterial zu vernichten oder ein zusätzliches Risiko einzubringen – mit einfachen Schritten und einem reproduzierbaren Anhang für die Fallprüfung.

Für alle, die sich wegen ihres Telefons oder Computers Sorgen machen, und für Sachverständige, die solche Fälle übernehmen. Kenntnisse über Intrusion, physische Extraktion, JTAG oder Chip-off sind nicht erforderlich. Die lokale Prüfung ist optional; Hilfe zu erhalten hängt niemals von ihrer Durchführung ab.

Redaktionelle Koordination: Jocsan Laguna · Amerikanischer Rat für Cybersicherheit und digitale Forensik

Allgemeiner technischer Leitfaden und offenes Bildungsmaterial. Er stellt keine Rechtsberatung oder forensisches Gutachten dar und enthält keine Anleitung zum unbefugten Zugriff auf Systeme. Beispiele und Daten sind fiktiv; die Abbildungen sind redaktionelle Rekonstruktionen.

Inhalt

Die sichtbare Seitennummerierung entspricht der PDF-Ausgabe. Word kann dieses Inhaltsverzeichnis beim Öffnen des Dokuments aktualisieren; die Überschriften ermöglichen weiterhin die interne Navigation.

1. Bevor du etwas anfasst: Sicherheit und Ruhe 3

2. Normale Verhaltensweisen, die wie Spionage wirken können 4

- **2.1 Ein Signal ist keine Erklärung** 4
- **2.2 Falsch positiv bedeutet nicht Einbildung** 4

3. Was Zero Breach leistet und wann es nicht eingesetzt werden sollte 5

- **3.1 Lokale Prüfung veröffentlichter Indikatoren** 5
- **3.2 Wann abbrechen und Hilfe holen** 5

4. Paket herunterladen und überprüfen 6

- **4.1 Offizielles Repository statt weitergeleiteter Links** 6
- **4.2 Überprüfung der Windows-Programmdatei** 7
- **4.3 Alternative: Quellcode und reproduzierbarer Vergleich** 7

5. Datenschutz und Vorbereitung vor der Ausführung 7

- **5.1 Lokal bedeutet nicht harmlos** 7
- **5.2 Ordner und Untersuchungsumfang vorbereiten** 8
- **5.3 Vorschau und Beschreibung** 8

6. Schrittweise Ausführung 8

- **6.1 Zuerst ohne ein echtes Gerät üben** 8
- **6.2 Danach: autorisierte lokale Prüfung** 9
- **6.3 Wenn du ein Telefon auswählst** 9

7. Den Bericht vor dem Teilen richtig lesen 9

- **7.1 Ergebnis, Grad, Untersuchungsumfang und Lücken** 9
- **7.2 Codes und operative Bedeutung** 10
- **7.3 „Worth a look“ ist kein Urteil** 10

8. Die vier Laborszenarien 11

- **8.1 `spyware`: sechs Befunde, keine voreiligen Schlüsse** 11
- **8.2 `worth-a-look`: Anlass für Fragen, nicht für Anschuldigungen** 11
- **8.3 `clean`: keine Übereinstimmungen, aber vier Lücken** 12
- **8.4 `cellebrite`: forensischer Zugriff, keine Spyware** 12

9. Sichere Übergabe an Sachverständige oder Reaktionsteams 16

- **9.1 Zuerst die Zusammenfassung, dann das vollständige Dossier** 16
- **9.2 Hash und EML für eine überprüfbare Übergabe** 17
- **9.3 Die Erklärung, die eine zweite Krise verhindert** 17

Anhang A. Reproduzierbares Protokoll für Sachverständige 18

- **A.1 Umgebung und Herkunft dokumentieren** 18
- **A.2 Formular für eine autorisierte reale Ausführung** 18
- **A.3 Interpretationsmatrix** 18

Anhang B. Rechtsrahmen, Datenschutz und Abschlusskontrolle 19

1. Bevor du etwas anfasst: Sicherheit und Ruhe

Wenn du glaubst, dass jemand dein Telefon oder deinen Computer überwacht, ist der erste Schritt nicht, ein Programm herunterzuladen. Vermeide zunächst, durch voreiliges Handeln Informationen zu verlieren oder ein weiteres Problem zu verursachen. Lösche keine Dateien, setze das Gerät nicht zurück, installiere keine angeblichen Wunderpakete und erlaube Unbekannten keinen Fernzugriff auf das Gerät. Eine Sorge kann durch etwas Legitimes, eine Konfiguration oder einen tatsächlichen Vorfall entstehen. Das wissen wir noch nicht und müssen es nicht in dieser Minute entscheiden.

Bei körperlicher Bedrohung, Gefahr für Minderjährige, aktiver Verfolgung oder wenn jemand entdecken könnte, dass du Hilfe suchst, haben deine Sicherheit und die örtlichen Notfallkanäle Vorrang. Führe eine Prüfung nicht nur deshalb durch, weil dieser Leitfaden existiert. Eine Analyse kann Protokolle verändern, Speicherplatz belegen oder indirekt jemanden warnen, der die Umgebung kontrolliert. Hole zunächst über ein sicheres Gerät und einen sicheren Kanal Hilfe, bevor du fortfährst.

Erstelle eine kurze Liste: Was hast du beobachtet, wann begann es, was hat sich verändert, was wurde installiert, wer hatte physischen Zugriff und welche Konten könnten kompromittiert sein? Verwende ungefähre Uhrzeiten, wenn du dich nicht genau erinnerst. Fertige keine Aufnahmen intimer Inhalte an und leite sie nicht weiter, um Hilfe zu erhalten. Eine Nachricht, eine URL, eine Einstellung, ein App-Name und ein Datum sind häufig nützlicher als ein ganzer Ordner aus deinem Privatleben.

> **Das Erforderliche vor dem Möglichen**
> Atme durch. Lösche nichts, verfolge nicht den mutmaßlichen Angreifer und gib weder Passwörter noch Codes weiter. Bei Gefahr hole jetzt Hilfe. Wenn Zeit bleibt, bewahre das Nötigste auf und prüfe ohne Dramatisierung. Duriva wird dir diese Frage mehrmals stellen: Was kannst du beweisen und was erscheint lediglich möglich?



Abbildung 1. Vermeide vor der Prüfung, die Quelle zu verlieren. Vorrang hat nicht der Beweis, dass du recht hattest. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

2. Normale Verhaltensweisen, die wie Spionage wirken können

2.1 Ein Signal ist keine Erklärung

Eine andere MAC-Adresse, eine getrennte Verbindung, ein sich schnell entladender Akku, eine unerwartete Benachrichtigung, eine unbekannte Anwendung oder eine neue IP-Adresse beweisen für sich allein nicht, dass jemand dich überwacht. Datenschutzfunktionen, Aktualisierungen, Empfang, Synchronisierung, eine legitime Anwendung oder ein gemeinsam genutztes Konto können die Ursache sein. Sie können auch Teil eines schwerwiegenderen Vorfalls sein. Der Fehler besteht darin, die alarmierendste Erklärung zu wählen, bevor die Quelle geprüft wurde.

Apple dokumentiert, dass seine Geräte je nach Netzwerk unterschiedliche private WLAN-Adressen verwenden und diese im Modus Rotating auf kompatiblen Systemen alle zwei Wochen ändern können. Diese Funktion soll Tracking verringern, nicht Spionage beweisen. Eine getrennte Verbindung ist eine andere Frage: Router, Empfang, Aktualisierung, Kompatibilität, Energieverwaltung, Software oder Unternehmenskonfiguration können daran beteiligt sein. Schreibe ihr nicht ohne Prüfung eine einzige Ursache zu.[1]

Was du beobachtest	Erste ruhige Prüfung	Was für die Prüfung aufzubewahren ist
Die MAC-Adresse hat sich geändert	Prüfe die Einstellung der privaten Adresse für jedes Netzwerk sowie Modell und System.	Screenshot der Konfiguration, des Netzwerks und des Datums; nicht des gesamten Verlaufs.
Die Verbindung wird getrennt	Notiere Häufigkeit, andere Geräte, Empfang, Uhrzeit und kürzliche Änderungen.	Modell, System, Router, Muster und Fehler; kein WLAN-Passwort.
Der Akku entlädt sich schnell	Prüfe Verbrauch nach App, Signalstärke, Temperatur und Aktualisierungen.	Systemstatistiken und Zeitraum; keine Chat-Inhalte.
Doppelte Nachricht	Prüfe Synchronisierung, andere Geräte und verknüpfte Konten.	Anwendung, Version, Uhrzeit, Konten und Kontextnachricht.
Sicherheitswarnung	Lies, welche Datei oder welches Verhalten erkannt wurde und welche Version des Werkzeugs vorliegt.	Vollständige Warnung, Pfad, Datum und Erklärung; führe die Datei nicht aus.
Nächtliche Aktivität	Unterscheide Aktualisierungen, Sicherungen, geplante Aufgaben und physischen Zugriff.	Protokolle, Sperrstatus und wer das Gerät hatte.

2.2 Falsch positiv bedeutet nicht Einbildung

Ein falsch positives Ergebnis ist eine Warnung, die nicht das befürchtete Problem darstellt. Jedoch ist nicht jedes ungewöhnliche Verhalten falsch positiv und nicht jedes Ergebnis ohne Befunde ebenfalls falsch positiv. Die Person braucht nicht zu hören, dass sie sich Dinge einbildet; sie muss wissen, welche Prüfung die Interpretation ändern würde. Erklärt eine Konfiguration die Beobachtung, wird dies dokumentiert. Erklärt sie die Beobachtung nicht, wird ohne Schuldzuweisung und ohne voreilige Schlüsse weiter untersucht.

[1] Apple Support. Use private Wi-Fi addresses on Apple devices: Die private Adresse kann je nach Netzwerk variieren und sich mit Rotating auf kompatiblen Systemen alle zwei Wochen ändern. Die Funktion soll Tracking verringern; sie ist kein Beweis für Spionage und erklärt nicht jede getrennte Verbindung. Offizielle Online-Quelle

Die passende Formulierung

„Dafür kann es eine normale Erklärung geben. Ich werde sie prüfen, bevor ich es Spionage nenne.“ Und außerdem: „Wenn die Erklärung nicht passt, bewahre ich die Quelle auf, damit eine qualifizierte Person sie prüfen kann.“

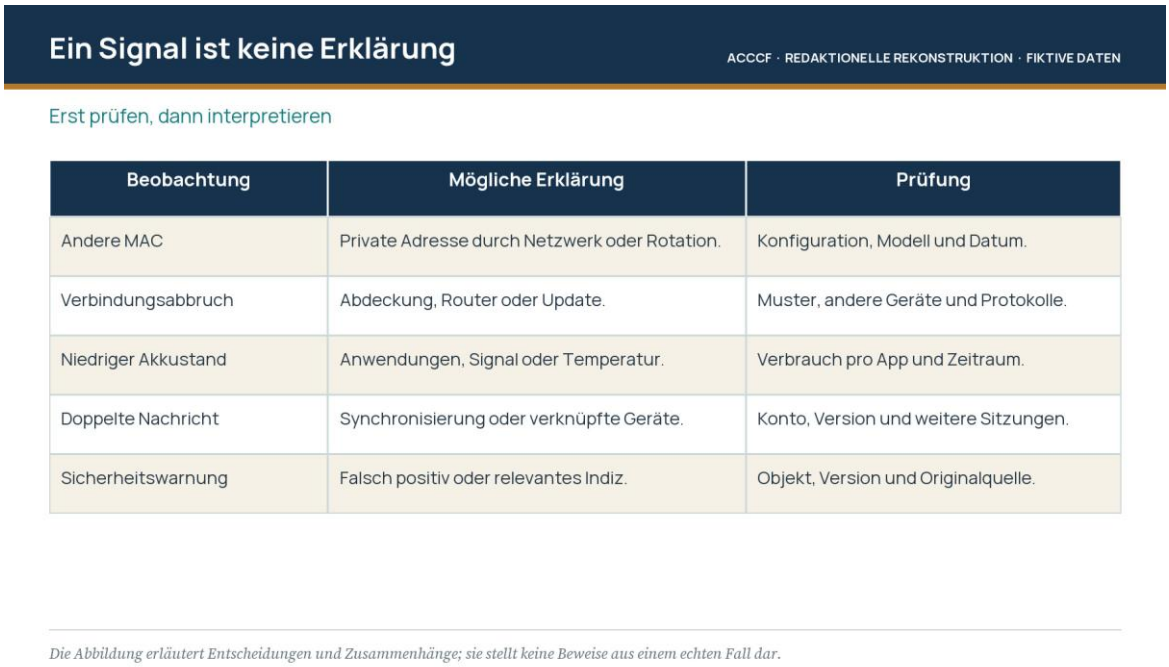


Abbildung 2. Ein Signal ist keine Erklärung. Zuerst wird geprüft, dann interpretiert. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

3. Was Zero Breach leistet und wann es nicht eingesetzt werden sollte

3.1 Lokale Prüfung veröffentlichter Indikatoren

Zero Breach Toolkit ist ein kostenloses Open-Source-Werkzeug, das auf Computern, in Android-Datensammlungen und iPhone-Sicherungen nach dokumentierten Indikatoren bestimmter Spyware sucht. Es kann Dateien, Browser, Persistenzeinträge und andere unterstützte Artefakte prüfen. Es ist keine vollständige forensische Untersuchung, erkennt nicht jede Überwachung und beweist nicht, dass eine Person sicher ist, nur weil es nichts findet.[2][3]

Das Werkzeug ist besonders nützlich für eine erste lokale Auswertung bekannter Indizien und eine ausdrückliche Liste dessen, was nicht geprüft werden konnte. Sein Wert liegt nicht darin zu sagen: „Es gibt keine Kobolde“, sondern darin, Übereinstimmungen, schwache Referenzen, Lücken und Fragen für Fachleute voneinander zu trennen. Neue oder unbekannte Quellen erscheinen nicht wie von selbst in einer veröffentlichten Indikatordatenbank, und einige Spuren verschwinden mit der Zeit.

3.2 Wann abbrechen und Hilfe holen

Führe keine Prüfung durch, wenn sie dich gefährden kann, du keine Berechtigung für das Gerät oder die Dateien hast, eine andere Person den Vorgang beobachten kann oder du den Bericht nicht schützen

[2]Zero Breach Toolkit, Repository interplains/Zero-Breach-Toolkit. Lokale Prüfungen veröffentlichter Spyware-Indikatoren, mit Code unter Apache 2.0 und Dokumentation von Untersuchungsumfang und Grenzen. Offizielle Online-Quelle

[3]Zero Breach Toolkit. Abdeckung nach Prüfungsfamilien und Grenzen: Dateien, Browser, Persistenz, Protokolle, Android und iPhone-Sicherungen. Es werden weder Erkennungsraten noch Falsch-Positiv-Raten gemessen. Offizielle Online-Quelle

kannst. Nutze sie auch nicht, um ohne Erlaubnis das Gerät deines Partners, eines Beschäftigten, eines Kunden oder eines Angehörigen zu prüfen. Die Möglichkeit, eine Datei zu lesen, macht dich nicht zum berechtigten Inhaber ihres Inhalts.

Liegt bereits eine glaubwürdige Sicherheitsmeldung, eine bestätigte Extraktion oder ein Verdacht auf gezielte Überwachung vor, suche spezialisierte Hilfe, ohne zuvor deine eigene Prüfung vollständig durchzuführen. Journalisten, Aktivisten, Menschenrechtsverteidiger und die Zivilgesellschaft können sich an die Hilfshotline von Access Now oder an Amnesty International Security Lab wenden; die Links dazu enthält der Bericht. Für alle anderen ist ein Incident Responder oder ein qualifizierter Sachverständiger der geeignete Weg.[4]

Situation	Was zuerst zu tun ist	Was zu vermeiden ist
Neugier aufgrund ungewöhnlichen Verhaltens	Konfiguration und Chronologie vor einem Scan prüfen.	Viele Werkzeuge wahllos installieren.
Begründeter Verdacht und sichere Umgebung	Lokale Prüfung mit festgelegtem Untersuchungsumfang und Datenschutz.	Den vollständigen Bericht in einer Gruppe teilen.
Gefahr oder aktive Überwachung	Spezialisierte Hilfe sowie sicheres Gerät und sicherer Kanal.	Tests ausführen, die die Hilfsanfrage verraten könnten.
Gerät einer anderen Person	Ausdrückliche Berechtigung und dokumentierter Untersuchungsumfang.	Inhalte nur deshalb lesen, weil sie zugänglich sind.
Test im Rahmen einer Anleitung oder eines Kurses	Integrierte synthetische Szenarien, keine echten Geräte.	Training als echte Erkennung ausgeben.

Du musst nicht zum Hacker werden

Es ist weder erforderlich, einen Test Point zu setzen, über den Prozessor einzudringen noch Chip-off durchzuführen. Beantwortet eine einfache Prüfung die Frage nicht, wird gesichert und an Fachleute eskaliert. Technische Komplexität ist keine Voraussetzung, um Hilfe zu erhalten.

4. Paket herunterladen und überprüfen

4.1 Offizielles Repository statt weitergeleiteter Links

Die in diesem Leitfaden verwendete Quelle ist `github.com/interplains/Zero-Breach-Toolkit`. Dort wird der Bereich Releases geöffnet, um das Paket für Windows, macOS oder Linux oder den Quellcode herunterzuladen. Lade keine gleichnamige Datei aus einem Video, über einen URL-Kürzer, aus einem Screenshot oder einem Kommentar herunter. Ein identischer Name beweist nicht identischen Inhalt.[5]

Die Projektdokumentation weist darauf hin, dass das Windows-Programm nicht mit einem Code-Signing-Zertifikat signiert ist. SmartScreen oder ein Antivirus kann daher eine Warnung anzeigen. Deaktiviere keine Schutzfunktionen und akzeptiere die Datei nicht blindlings. Das Projekt bietet eine Attestierung des Build-Ablaufs und für neuere Programme signierte SHA-256-Manifeste. Überprüfe dies vor der Ausführung.[6]

[4] Zero Breach Toolkit. Leitfaden für synthetische Trainingsszenarien: spyware, worth-a-look, clean und cellebrite. Die Indikatoren sind erfunden, und die Beispiele lesen weder das Gerät noch reale Listen; sie erlauben keine Rückschlüsse auf den Zustand eines realen Geräts. Offizielle Online-Quelle

[5] Zero Breach Toolkit, Repository interplains/Zero-Breach-Toolkit. Lokale Prüfungen veröffentlichter Spyware-Indikatoren, mit Code unter Apache 2.0 und Dokumentation von Untersuchungsumfang und Grenzen. Offizielle Online-Quelle

[6] Zero Breach Toolkit. Leitfaden zur Versionsüberprüfung: Attestierung von durch GitHub Actions erstellten Programmen, SHA-256-Manifeste und Signatur; das Windows-Paket verfügt über keine Windows-Code-Signatur. Offizielle Online-Quelle

4.2 Überprüfung der Windows-Programmdatei

Bei installiertem GitHub CLI und einer in den aktuellen Ordner heruntergeladenen Programmdatei schlägt die Dokumentation folgende Herkunftsprüfung vor:

Prüfung der Attestierung, nicht der Abwesenheit von Malware

```
gh attestation verify zero-breach-toolkit-windows-x64.exe --repo interplains/Zero-Breach-Toolkit
```

Eine gültige Attestierung verknüpft diese Bytes mit einem öffentlichen Build-Ablauf und einem Commit. Sie beweist weder, dass das Programm fehlerfrei ist, noch dass es für deine Situation geeignet ist. Du kannst auch die vom Projekt beschriebenen signierten SHA-256-Manifeste verwenden. Verwende keinen Hash von einer anderen Seite, als wäre es der Hash deiner Datei: Berechne deinen eigenen und vergleiche ihn mit der offiziellen Quelle für diese Version.

4.3 Alternative: Quellcode und reproduzierbarer Vergleich

Der andere Weg besteht darin, das Repository zu klonen, den Code zu prüfen und die erzeugte Python-Datei mit der erwarteten Version zu vergleichen. Das Projekt beschreibt den deterministischen Build der Einzeldatei und die Veröffentlichungsprüfungen. Nicht technisch versierte Personen müssen nicht selbst kompilieren: Sie können Hilfe bei der Paketprüfung erhalten oder die Übungsoption im Menü verwenden. Aus Zeitdruck darf jedoch die Identität der Quelle nicht ungeprüft bleiben.

Beispiel für das Abrufen des offiziellen Quellcodes

```
git clone --depth 1 https://github.com/interplains/Zero-Breach-Toolkit.git
```

> **Duriva fragt**
> Woher stammt diese Programmdatei genau? Wenn du das nicht mit Repository, Version und Prüfung beantworten kannst, ist es noch nicht Zeit, sie auszuführen.

5. Datenschutz und Vorbereitung vor der Ausführung

5.1 Lokal bedeutet nicht harmlos

Die gewöhnliche Analyse ist so konzipiert, dass sie deine Daten nicht hochlädt und keine Indikatoren aufruft. Das Aktualisieren von Listen verwendet dagegen das Netzwerk; die Android-Erfassung lädt mit Einwilligung einen separaten Kollektor herunter und verändert den Zustand des Telefons. Außerdem ist die interne Netzwerksperre keine Sandbox des Betriebssystems: Netzwerk-Mounts, andere Anwendungen und Synchronisierung bestehen weiterhin. Wenn du strikte Isolation benötigst, entscheide dies mit Fachleuten.[7]

Der Bericht kann Benutzernamen, Profile, Pfade, Verläufe, SMS-Absender und Nachrichtenauszüge enthalten. Die Zusammenfassung zum Teilen enthält weniger Informationen, ist aber keine vollständige forensische Untersuchung und darf nicht ungeprüft veröffentlicht werden. Wähle einen lokalen, nicht synchronisierten Ordner, vermeide OneDrive, iCloud, Dropbox und freigegebene Ordner und lege fest, wer den Bericht öffnen darf. Sende keine Schlüssel, Cookies, Passwörter oder persönlichen Dateien an das Repository.

[7] Zero Breach Toolkit. PRIVACY: Die gewöhnliche Analyse führt konstruktionsbedingt keine Uploads durch; Aktualisierung und Android-Akquisition sind unterschiedliche Vorgänge. Berichte können sensible Daten enthalten, und die Zusammenfassung zum Teilen ersetzt nicht den vollständigen Bericht. Offizielle Online-Quelle

5.2 Ordner und Untersuchungsumfang vorbereiten

Entscheidung	Auswahl	Begründung
Ausgabeordner	Lokal, neu, nicht synchronisiert und mit eingeschränktem Zugriff.	Vermeidet die Offenlegung von Verläufen und Pfaden.
Erste Ausführung	Übungsszenario oder begrenzter Untersuchungsumfang.	Macht mit dem Bericht vertraut, ohne einen echten Fall vorzutäuschen.
Aktualisierung der Indikatoren	Separater, bewusster Schritt; nicht mit einem Scan verwechseln.	Netzwerk und Quellen verändern sich.
Geöffnete Anwendungen	Schließe Browser und Messaging-Apps, wenn das Verfahren dies verlangt.	Verringert gesperrte Dateien und gleichzeitige Änderungen.
Berechtigungen	Nur die erforderlichen; nicht aus Gewohnheit erweitern.	Vermeide die Prüfung anderer Konten und Änderungen an der Konfiguration.
Empfangende Person	Empfänger und sicheren Kanal vor der Dateierstellung festlegen.	Vermeidet späteres impulsives Teilen.

5.3 Vorschau und Beschreibung

Vor der Analyse realer Daten kannst du eine Ansicht des Untersuchungsumfangs und der verfügbaren Prüfungen anfordern. `--preview` zeigt den Untersuchungsumfang ohne Scan; `--describe` gibt in JSON aus, welche Lesevorgänge vorhanden sind und welche Grenzen sie haben. Diese Schritte helfen zu entscheiden, ob eine Prüfung die Frage beantwortet und ob es eine weniger intrusive Alternative gibt.[8]

Beschreibung von Untersuchungsumfang und Lesevorgängen

```
python -X utf8 scan/zero-breach-toolkit.py --preview
python -X utf8 scan/zero-breach-toolkit.py --describe
```

> **Bevor du fortfährst**
> Wenn der Untersuchungsumfang Daten enthält, die du nicht teilen musst, reduziere die Auswahl. Wenn dein Anliegen Hilfe erfordert, verschiebe sie nicht, um diese Schritte abzuschließen. Das Werkzeug ist eine Option, keine Pflicht.

6. Schrittweise Ausführung

6.1 Zuerst ohne ein echtes Gerät üben

Das Projekt enthält Lernszenarien: `spyware`, `worth-a-look`, `clean` und `cellebrite`. Sie verwenden ein erfundenes Telefon und erfundene Indikatoren mit `.invalid`-Domains, die zu keiner realen Infrastruktur gehören können. Der Bericht enthält eine deutlich sichtbare Trainingswarnung, und das temporäre Verzeichnis wird am Ende gelöscht. Sie erzeugen weder eine Zusammenfassung zum Teilen noch ein Beweispaket, damit niemand sie mit einem echten Fall verwechselt.[9]

Vier Übungsszenarien

```
python scan/zero-breach-toolkit.py --training spyware
python scan/zero-breach-toolkit.py --training worth-a-look
python scan/zero-breach-toolkit.py --training clean
```

[8] Zero Breach Toolkit. Ergebnis- und Abdeckungsvertrag: Codes 0, 1, 2, 3 und 4; Unterscheidung zwischen Befund, Referenz, Lücke, Beenden ohne Scan und begrenztem Untersuchungsumfang. Ein Ergebnis ohne Übereinstimmungen ist niemals eine Sicherheitsgarantie. Offizielle Online-Quelle

[9] Zero Breach Toolkit. Leitfaden für synthetische Trainingsszenarien: spyware, worth-a-look, clean und cellebrite. Die Indikatoren sind erfunden, und die Beispiele lesen weder das Gerät noch reale Listen; sie erlauben keine Rückschlüsse auf den Zustand eines realen Geräts. Offizielle Online-Quelle

```
python scan/zero-breach-toolkit.py --training cellebrite
```

Wenn du den Windows-Starter verwendest, suche die Übungsoption im Menü; die Dokumentation bezeichnet sie als `Practise`. Bei Verwendung des Quellcodes führe die Befehle im Ordner des Repositorys aus. Kombiniere `--training` nicht mit Dateien, Telefonen, Aktualisierungen oder realen Listen: Das Programm lehnt dies konstruktionsbedingt ab. Mache dich zuerst damit vertraut, wo Ergebnis, Beweisgrade und Lücken angezeigt werden.

6.2 Danach: autorisierte lokale Prüfung

Wenn die Quelle überprüft, die Berechtigung eindeutig und der Ausgabeordner geschützt ist, kannst du eine Prüfung des gewählten Untersuchungsumfangs ausführen. Verwende `--quick` nicht, wenn du eine bewusst unvollständige Abdeckung vermeiden willst. Wenn du ein bestimmtes Ziel auswählst, tue dies bewusst: Eine gezielte Prüfung ist nicht gleichbedeutend mit der Prüfung des gesamten Geräts.

Ausführungsbeispiel mit Bericht, JSON und minimaler Zusammenfassung

```
python -X utf8 scan/zero-breach-toolkit.py --report reporte.txt --json reporte.json --share-json
resumen.json
```

Der Textbericht dient zum Lesen, JSON zur Prüfung der Struktur und die Zusammenfassung zu einem ersten Gespräch mit geringerer Offenlegung. Keine dieser Ausgaben beweist die Authentizität des Geräts oder dass das gesamte System untersucht wurde. Kombiniere das Training weder mit `--share-json` noch mit einem Beweispaket: Beide werden nur für eine autorisierte reale Prüfung erzeugt.

6.3 Wenn du ein Telefon auswählst

Eine Android-Datensammlung und die Prüfung einer iPhone-Sicherung sind nicht dasselbe. Das Werkzeug liest verfügbare Artefakte und weist aus, worauf es nicht zugreifen kann. Eine Akquisition verändert den Zustand des Telefons und speichert private Informationen; führe sie nicht ohne ausdrückliche Einwilligung, ein sicheres Ziel und Verständnis der Abdeckung durch. Die lokale Kopie kann ein separates Passwort oder eine gesonderte Entschlüsselung erfordern; teile sie nicht und lade sie nicht zu Analysediensten hoch.[10][11]

> **Es gibt keine Schaltfläche für die Wahrheit**
>
> Wenn du nicht weißt, welchen Untersuchungsumfang du gerade gewählt hast, halte an. Die Antwort liegt nicht darin, „full“ auszuwählen, sondern zu wissen, was geprüft wurde und was nicht geprüft werden konnte.

7. Den Bericht vor dem Teilen richtig lesen

7.1 Ergebnis, Grad, Untersuchungsumfang und Lücken

Achte vor jeder Zahl auf vier Dinge: was das Ergebnis aussagt, welchen Beweisgrad es hat, welcher Untersuchungsumfang geprüft wurde und was außen vor blieb. Dieselbe Zahl kann je nach Quelle unterschiedliche Bedeutungen haben. Sechs Befunde sind nicht sechs Infektionen, null Befunde bedeuten keine Abwesenheit von Überwachung, und eine Referenz ist keine ausgeführte Schaddatei.

[10] Zero Breach Toolkit. Abdeckung nach Prüfungsfamilien und Grenzen: Dateien, Browser, Persistenz, Protokolle, Android und iPhone-Sicherungen. Es werden weder Erkennungsraten noch Falsch-Positiv-Raten gemessen. Offizielle Online-Quelle

[11] Zero Breach Toolkit. PRIVACY: Die gewöhnliche Analyse führt konstruktionsbedingt keine Uploads durch; Aktualisierung und Android-Akquisition sind unterschiedliche Vorgänge. Berichte können sensible Daten enthalten, und die Zusammenfassung zum Teilen ersetzt nicht den vollständigen Bericht. Offizielle Online-Quelle

Element	Was es dir sagt	Vermiedener Fehler
Ergebnis und Code	Was in der ausgewählten Ausführung geschehen ist.	Daraus eine absolute Kategorie machen.
Beweisgrad	Ob es sich um Datei, Registrierungseintrag, Referenz, Protokoll oder Infrastruktur handelt.	Alles als Beweis einer Ausführung behandeln.
Untersuchungsumfang	Welches Telefon und welche Dateien, Konten und Optionen einbezogen sind.	Auf das gesamte Gerät verallgemeinern.
Lücken	Was nicht gelesen oder geprüft werden konnte und warum.	Ungeprüftes als sauber bezeichnen.
Indikatoren und Datumsangaben	Welche Quellen verwendet wurden und ob sie aktuell sind.	Eine kürzlich erstellte Kopie mit einem aktuellen Indikator verwechseln.
Nächster Schritt	Je nach Fall sichern, Lücken schließen oder Hilfe holen.	Reflexartig löschen oder „bereinigen“.

7.2 Codes und operative Bedeutung

Code / Situation	Richtige Interpretation	Nächste Entscheidung
0: keine maßnahmenrelevanten Ergebnisse oder Lücken	In diesem Untersuchungsumfang wurden keine maßnahmenrelevanten Übereinstimmungen gefunden.	Nicht als sicheres Gerät bezeichnen; Untersuchungsumfang und Grund der Sorge prüfen.
1: Fehler	Die Ausführung oder die Ausgabe ist fehlgeschlagen.	Eingabe oder Ziel korrigieren; nicht als Abwesenheit interpretieren.
2: maßnahmenrelevante Übereinstimmungen	Es liegen Indizien vor, die Interpretation und Sicherung erfordern.	Nichts löschen, ausführen oder verfolgen; Hilfe holen.
3: Daten oder Quellen fehlen	Es gibt Lücken; dies ist kein sauberes Ergebnis.	Abdeckung vervollständigen und erneut prüfen.
4: ohne Scan beendet	Es fand weder eine Prüfung noch eine Bewertung statt.	Nicht behaupten, dass keine Spyware vorhanden ist.
Zurückgezogene Referenzen oder Indikatoren	Der Ursprung des Indikators verändert seine aktuelle Bedeutung.	Kontext und Quelle prüfen, keine Anschuldigung erzwingen.

Quellen der Tabelle:[12]

7.3 „Worth a look“ ist kein Urteil

Eine außerhalb des Stores installierte Anwendung, Zugriff auf Bedienungshilfen, eine alte Version oder eine deaktivierte Überprüfungseinstellung kann Anlass für eine Frage sein. Für sich allein ist dies kein Befund. Bedienungshilfen, Bildschirmleseprogramme, Passwortmanager und Automatisierungsanwendungen können legitim sein. Die Person, die das Gerät kennt, kann diese Erklärungen mit weiteren Informationen bestätigen oder ausschließen.

> **Duriva durchbricht die vierte Wand**
> Wenn du nur „sechs Übereinstimmungen“ liest, wirkt dies wie ein Urteil. Wenn du auch „vier Prüfungen nicht ausgeführt“ liest, erkennst du, dass der Fall weiterhin offen ist. Das ist der Unterschied zwischen Reagieren und Prüfen.

[12] Zero Breach Toolkit. Ergebnis- und Abdeckungsvertrag: Codes 0, 1, 2, 3 und 4; Unterscheidung zwischen Befund, Referenz, Lücke, Beenden ohne Scan und begrenztem Untersuchungsumfang. Ein Ergebnis ohne Übereinstimmungen ist niemals eine Sicherheitsgarantie. Offizielle Online-Quelle



Abbildung 3. Der Bericht wird schichtweise gelesen. Untersuchungsumfang und Lücken verändern die Bedeutung. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

8. Die vier Laborszenarien

8.1 `spyware`: sechs Befunde, keine voreiligen Schlüsse

Das synthetische Szenario `spyware` erzeugte sechs Übereinstimmungen: fünf Beweise auf dem Gerät und eine im Registrierungseintrag. Es enthält eine Anwendung, einen Datei-Fingerabdruck, ein Zertifikat, eine Eigenschaft, einen Pfad und eine Referenz auf erfundene Infrastruktur. Außerdem blieben vier Lücken: keine Datei-Fingerabdrücke, kein Akkuverlauf, kein Absturzbericht und keine SMS-Sicherung. Das Ergebnis war `INDICATORS_FOUND`, Code 2 und `scan_state: partial`.[13]

Die Lehre daraus ist nicht „du hast Spyware“, sondern wie unterschiedliche Objekte gruppiert werden und warum jedes einzelne interpretiert werden muss. Die Ausgabe selbst weist darauf hin, dass eine Übereinstimmung eine Untersuchung erfordert, nicht die Erklärung einer Kompromittierung oder eine Bereinigung. Das Vorhandensein einer Datei oder Konfiguration beweist allein keine Ausführung, und eine Infrastrukturreferenz beweist keinen erfolgreichen Kontakt. Das gesamte Telefon und alle Indikatoren sind fiktiv.

8.2 `worth-a-look`: Anlass für Fragen, nicht für Anschuldigungen

Das Szenario `worth-a-look` fand keine bekannten Indikatoren, zeigte jedoch vier Anlässe für Fragen: eine direkt installierte Anwendung mit Zugriff auf Bedienungshilfen, veraltete Aktualisierungen, einen aktivierten Bedienungshilfedienst und eine deaktivierte App-Überprüfung. Das Ergebnis war `NO_KNOWN_INDICATORS_WITH_GAPS`, Code 3, mit denselben vier Abdeckungslücken.[14]

Diese Elemente beweisen weder eine Infektion noch eine Täuschung. Sie laden zu Fragen ein: Erkennst du die Anwendung? Warum hast du sie installiert? Hast du diese Berechtigung erwartet? Stehen

[13] Lokales ACCCF-Labor. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, Ausführung der vier synthetischen Szenarien. Dateien spyware, worth-a-look, clean und cellebrite in TXT/JSON. Es wurden weder persönliche Informationen noch reale Geräte untersucht.

[14] Lokales ACCCF-Labor. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, Ausführung der vier synthetischen Szenarien. Dateien spyware, worth-a-look, clean und cellebrite in TXT/JSON. Es wurden weder persönliche Informationen noch reale Geräte untersucht.

Aktualisierungen aus? Was änderte sich vor dem Verhalten? Das Handbuch behauptet weder, dass die besitzende Person im Unrecht ist, noch dass alles normal ist. Ziel ist es, erst Fragen zu stellen und nicht vorschnell zu beschuldigen.

8.3 `clean`: keine Übereinstimmungen, aber vier Lücken

Das Szenario `clean` erzeugte keine bekannten Übereinstimmungen, behielt jedoch vier Lücken und Code 3. Die Ausgabe stellt ausdrücklich klar, dass dies keine Bestätigung eines einwandfreien Zustands ist. Sie zeigt, dass sich „nichts gefunden“ nur auf den geprüften Bereich und die bekannten Indikatoren beziehen kann. Dies beweist weder die Abwesenheit neuer, verborgener, gezielt eingesetzter oder undokumentierter Spyware noch, dass alle Bereiche untersucht wurden.[15]

Wenn eine Person einen konkreten Grund zur Sorge hat, beseitigt das Ergebnis diese Sorge nicht. Der nächste Schritt kann darin bestehen, die Abdeckung zu vervollständigen, Protokolle zu prüfen, Fachleute zu konsultieren oder lediglich zu dokumentieren, dass die erste Prüfung keine maßnahmenrelevanten Indizien lieferte. Ein falsch positives Ergebnis muss nicht erzwungen werden, damit sich die Person verstanden fühlt.

8.4 `cellebrite`: forensischer Zugriff, keine Spyware

Das Szenario `cellebrite` erzeugte eine Übereinstimmung im USB-Registrierungseintrag und Code 2. Es zeigt, wie das Werkzeug einen Hinweis auf forensischen Zugriff erkennt und wie sich die Empfehlungen verändern: sichern, Anwendungen im zeitlichen Umfeld prüfen und, wenn der Kontext es rechtfertigt, Passwörter von einem anderen Gerät aus ändern. Der Registrierungseintrag und die Seriennummer sind erfunden; weder eine reale Person noch ein reales Gerät steht dahinter.[16]

Bei diesem Fall handelt es sich nicht um Spyware, und er allein erlaubt auch nicht die Aussage, dass eine vollständige Extraktion stattgefunden hat. Forensisch ist zu fragen, wer wie lange und mit welcher Berechtigung Zugriff auf das Telefon hatte und was davor und danach geschah. Die Schlussfolgerung muss einen Hinweis auf eine Verbindung von der Bedeutung unterscheiden, die der Kontext belegen kann.

> **Vier unterschiedliche Lehren**
> Übereinstimmungen bedeuten keine Infektion; prüfenswerte Elemente bedeuten kein falsch positives Ergebnis; null Übereinstimmungen bedeuten keine Sicherheit; und ein forensischer Hinweis beweist keine vollständige Extraktion. Der Bericht ist der Anfang einer Prüfung, kein Urteil.

[15] Lokales ACCCF-Labor. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, Ausführung der vier synthetischen Szenarien. Dateien spyware, worth-a-look, clean und cellebrite in TXT/JSON. Es wurden weder persönliche Informationen noch reale Geräte untersucht.

[16] Lokales ACCCF-Labor. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, Ausführung der vier synthetischen Szenarien. Dateien spyware, worth-a-look, clean und cellebrite in TXT/JSON. Es wurden weder persönliche Informationen noch reale Geräte untersucht.

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · spyware

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: spyware. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:33   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: SERIOUS FINDING - seek expert help promptly.

  WHAT WAS FOUND
    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       org.example.training.spyapp  [artifact]
          Where: app org.example.training.spyapp

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       e36c3fee5d43ffb61b91fbee792cd8b7b4ebd9076f77e9002a9eaa0ea5648a84  [sample]
          The file fingerprint of a published spyware sample (its family
          is named where the source gives one). A match here is
          conclusive, not circumstantial.
          Where: app org.example.training.spyapp (/data/app/training-spyapp/base.apk)

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       d472b7c9d957a9e55ce56bd80388b97be9e2132644c0a51cac03aa618905e6d2  [artifact]
          Where: app org.example.training.spyapp

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       persist.training.spy.flag  [artifact]
          Where: system property persist.training.spy.flag

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       /data/local/tmp/training-spy-daemon  [artifact]
          Where: /data/local/tmp/training-spy-daemon

    >> THE PHONE'S SYSTEM LOGS NAME THIS SPYWARE INFRASTRUCTURE
       training-spyware-server[.]invalid  [infrastructure]
          A server the cited researchers attribute to the named spyware
          family. Its exact role - delivering an exploit, controlling an
          implant or receiving stolen data - is not stated in the source,
          so treat contact as serious but unspecified. A domain can change
          hands after a campaign ends: compare the date of the evidence
          with the date of the research.
          the phone's own system logs name it - it may have been a
          connection, a lookup, or only text an app wrote to the log
          Where: phone log dumpsys.txt, line 1

  WHAT TO DO
    Seek expert help promptly. Preserve this report and the named
    files or registrations. Do NOT delete, move, run or try to clean
    them. A file match establishes presence; a registration
    establishes configuration. Neither alone establishes that spyware
    executed.

    Contact a qualified incident responder or your organisation's
    security team. You do not need to finish investigating first.
    Support options are at the end of this report.
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

Abbildung 4. Tatsächlicher Trainingsbericht des Szenarios spyware. Wörtlicher Auszug; sämtliche Daten sind synthetisch. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · worth-a-look

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: worth-a-look. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:33   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: no known indicator was found in anything that could be
          checked.

  This is NOT a clean bill of health. See the two sections below for
  what was searched and, more importantly, what could not be.

  ALSO: 4 items under "WORTH A LOOK" further down. They are NOT
  a finding; each comes with its usual, ordinary explanation.

  WHAT COULD NOT BE CHECKED  (4 gaps, grouped)
    - android/android:file-hashes: the collection has no file
      fingerprints (AndroidQF's "hash files" option was off), so files
      were checked by path and name only
    - android/android:history: no battery history in the collection
    - android/android:crashes: bug report missing or unreadable; crash
      records were not checked
    - android/android:messages: no SMS backup in the collection, so
      links in messages were not checked
    (The full report lists them again at its end.)

  Before you share this report: it can contain your Windows username,
  browser profile names, file paths and browsing details, SMS senders
  and message excerpts. --share-json writes a minimal summary without
  artifact text. Ask a responder how to share evidence securely; do
  not post the full report publicly.
========================================================================

Indicator set : 6 indicators, unknown age
  ** WARNING: one or more source dates are unknown; copying files does not refresh indicators. **

DETAIL  —  what was examined, and the evidence behind the summary

--- android-intrusion check  [NOT_APPLICABLE] ---
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

Abbildung 5. Tatsächlicher Trainingsbericht des Szenarios worth-a-look. Wörtlicher Auszug; sämtliche Daten sind synthetisch. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · clean

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: clean. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:34   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: no known indicator was found in anything that could be
          checked.

  This is NOT a clean bill of health. See the two sections below for
  what was searched and, more importantly, what could not be.

  WHAT COULD NOT BE CHECKED  (4 gaps, grouped)
    - android/android:file-hashes: the collection has no file
      fingerprints (AndroidQF's "hash files" option was off), so files
      were checked by path and name only
    - android/android:history: no battery history in the collection
    - android/android:crashes: bug report missing or unreadable; crash
      records were not checked
    - android/android:messages: no SMS backup in the collection, so
      links in messages were not checked
    (The full report lists them again at its end.)

  Before you share this report: it can contain your Windows username,
  browser profile names, file paths and browsing details, SMS senders
  and message excerpts. --share-json writes a minimal summary without
  artifact text. Ask a responder how to share evidence securely; do
  not post the full report publicly.
========================================================================
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

Abbildung 6. Tatsächlicher Trainingsbericht des Szenarios clean. Wörtlicher Auszug; sämtliche Daten sind synthetisch. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · cellebrite

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: cellebrite. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:34   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: SERIOUS FINDING - seek expert help promptly.

  WHAT WAS FOUND
    >> SIGNS THIS PHONE WAS UNLOCKED WITH A PHONE-FORENSICS TOOL (CELLEBRITE)
       cellebrite usb 04f2:b071  [forensic]
          A trace of Cellebrite, the phone-forensics tool police and
          security services use to unlock seized phones and copy their
          contents. It is not spyware: it shows the phone was unlocked, or
          an unlock was attempted, while it was out of its owner's hands.
          the phone's own system logs name it - it may have been a
          connection, a lookup, or only text an app wrote to the log
          Where: phone log logcat.txt, line 2

  WHAT TO DO
    Someone unlocked this phone, or tried to, with Cellebrite: the
    phone-forensics tool police and security services use to copy
    everything on a seized phone. Assume what was on the phone then -
    messages, photos, contacts, saved passwords and the accounts
    signed in - was copied. Change the passwords of important accounts
    from another device, sign out other sessions, and tell the people
    whose conversations were on it. In documented cases spyware was
    installed after such an unlock, so check the apps installed around
    that time and get expert help.

    Seek expert help promptly. Preserve this report and the named
    files or registrations. Do NOT delete, move, run or try to clean
    them. A file match establishes presence; a registration
    establishes configuration. Neither alone establishes that spyware
    executed.

    Contact a qualified incident responder or your organisation's
    security team. You do not need to finish investigating first.
    Support options are at the end of this report.

    Do NOT open, visit or look up indicator addresses. Keep the [.]
    spelling when sharing them.

  WHAT COULD NOT BE CHECKED  (4 gaps, grouped)
    - android/android:file-hashes: the collection has no file
      fingerprints (AndroidQF's "hash files" option was off), so files
      were checked by path and name only
    - android/android:history: no battery history in the collection
    - android/android:crashes: bug report missing or unreadable; crash
      records were not checked
    - android/android:messages: no SMS backup in the collection, so
      links in messages were not checked
    (The full report lists them again at its end.)

  Before you share this report: it can contain your Windows username,
  browser profile names, file paths and browsing details, SMS senders
  and message excerpts. --share-json writes a minimal summary without
  artifact text. Ask a responder how to share evidence securely; do
  not post the full report publicly.
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

Abbildung 7. Tatsächlicher Trainingsbericht des Szenarios cellebrite. Wörtlicher Auszug; sämtliche Daten sind synthetisch. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

9. Sichere Übergabe an Sachverständige oder Reaktionsteams

9.1 Zuerst die Zusammenfassung, dann das vollständige Dossier

Bevor du alles sendest, frage die Person, die den Fall übernehmen wird, was sie benötigt und über welchen Kanal. Das erste Gespräch kann sich auf Grund der Sorge, Gerät, Untersuchungsumfang, Datum, Ergebnis und Lücken beschränken. Die minimale Zusammenfassung hilft bei der Entscheidung, ob der vollständige Bericht erforderlich ist, und vermeidet die Übermittlung von Verläufen oder Nachrichten, die zur Frage nichts beitragen.

Wird der vollständige Bericht benötigt, erfolgt die Übergabe über einen sicheren Kanal und nicht als öffentliche Datei. Arbeitsversion und Version zum Teilen werden getrennt. Die empfangende Person kann Originalobjekte benötigen, dies wird jedoch ausdrücklich vereinbart. Android-Datensammlungen, iOS-

Sicherungen und Berichte werden nicht zu unbekannten Diensten, Chatgruppen oder allgemeinen Analyseseiten hochgeladen.[17]

9.2 Hash und EML für eine überprüfbare Übergabe

Wird der Bericht per E-Mail gesendet, bewahre die vollständige EML-Datei mit Inhalt, Kopfzeilen und Anhängen auf. Der Nachrichtentext kann Algorithmus und Hash jeder Datei enthalten. Der Empfänger berechnet eigene Werte und vergleicht sie. Die Übereinstimmung belegt die Identität mit der bei dieser Übergabe angegebenen Datei, nicht die Authentizität des Geräts oder die Richtigkeit der Befunde. Ein später berechneter Hash belegt die Integrität nur ab diesem Zeitpunkt.

E-Mail-Verschlüsselung, Signatur und Hash lösen unterschiedliche Probleme. Verschlüsselung begrenzt, wer lesen kann; die Signatur hilft, Herkunft und Veränderung zu prüfen; der Hash vergleicht Objekte. Keines dieser Elemente beweist, dass die schreibende Person diejenige ist, die sie vorgibt zu sein, oder dass der Inhalt wahr ist. Sende weder den privaten Schlüssel noch das Dateipasswort in derselben Nachricht. Verwende einen separaten vereinbarten Kanal.

Objekt	Was aufgezeichnet wird	Was nicht bewiesen wird
EML der Übergabe	Inhalt, Kopfzeilen, Anhänge und Empfang.	Dass der menschliche Absender den Inhalt geschrieben hat.
TXT-/JSON-Bericht	Name, Größe, Hash, Datum und Version.	Dass der Untersuchungsumfang vollständig oder das Gerät authentisch war.
Zusammenfassung zum Teilen	Ergebnis, Untersuchungsumfang, Lücken und nächster Schritt.	Eine vollständige forensische Untersuchung oder die Abwesenheit von Risiken.
Schlüssel oder Passwort	Separater Kanal und bestätigter Empfänger.	Dass die Übergabe durch einen beliebigen Empfänger autorisiert worden wäre.
Ursprüngliche Datensammlung	Berechtigung, Abdeckung, Verwahrung und Hash je Objekt.	Dass jedes Werkzeug alle Artefakte lesen kann.

9.3 Die Erklärung, die eine zweite Krise verhindert

Kurzer Text für die Fallübergabe

```
Grund der Sorge: [beobachtetes Verhalten und Datum]
Gerät und Berechtigung: [Typ, Inhaber und Erlaubnis]
Werkzeug und Version: [Herkunft und Überprüfung]
Untersuchungsumfang: [was geprüft wurde und was nicht]
Ergebnis: [Übereinstimmungen, Referenzen und Lücken]
Bereits durchgeführte Maßnahmen: [ohne Löschen oder Bereinigen]
Übergebene Objekte: [Zusammenfassung / Bericht / Originale]
Hash jeder Datei: [Algorithmus und Wert]
Was ich benötige: [Überprüfung des Untersuchungsumfangs, Interpretation und nächster Schritt]
Nicht einbezogene Daten: [Schlüssel, Passwörter, intime oder irrelevante Inhalte]
```

> **Es geht nicht darum, eine Auseinandersetzung zu gewinnen**
>
> Die sachverständige Person braucht nicht den Beweis, dass die betroffene Person recht hatte. Sie braucht eine Quelle, eine Chronologie und eine Erklärung der durchgeführten Schritte. Gut dokumentierte Ungewissheit ist nützlicher als erzeugte Gewissheit.

[17] Zero Breach Toolkit. PRIVACY: Die gewöhnliche Analyse führt konstruktionsbedingt keine Uploads durch; Aktualisierung und Android-Akquisition sind unterschiedliche Vorgänge. Berichte können sensible Daten enthalten, und die Zusammenfassung zum Teilen ersetzt nicht den vollständigen Bericht. Offizielle Online-Quelle

Anhang A. Reproduzierbares Protokoll für Sachverständige

A.1 Umgebung und Herkunft dokumentieren

Aufzeichnung zur Erstellung der Beispiele in diesem Leitfaden

```
Repository: https://github.com/interplains/Zero-Breach-Toolkit
Commit: 10ceaba497e40da1f327916a0a3fe0af0ff5994f
Angezeigte Version: Zero Breach Toolkit 2.0.6
JSON-Schema: 1.6
Datei: scan/zero-breach-toolkit.py
SHA-256: 4f7294b0d72ae901552e3ac44f64148c0059d43d587a1638654ab00e7c80e627
Szenarien: spyware, worth-a-look, clean und cellebrite
Datenart: vollständig synthetisch
Personenbezogene Informationen: nicht untersucht
Reale Geräte: nicht verwendet
```

Diese Aufzeichnung beschreibt das Klonen des Repositorys und Trainingsausführungen; sie ist weder eine Attestierung der Windows-Programmdatei noch eine Überprüfung der neuesten Version. Die heruntergeladene Programmdatei muss anhand ihrer eigenen Version und ihres Build-Ablaufs überprüft werden. Die vier Szenarien wurden tatsächlich ausgeführt und erzeugten TXT und JSON sowie eine JSON-Ausgabe von `--describe`.

A.2 Formular für eine autorisierte reale Ausführung

Vorlage für die forensische Aufzeichnung

```
Fall und Berechtigung: [Kennung, Inhaber, Untersuchungsumfang und Ausschlüsse]
Grund der Prüfung: [Verhalten und Frage]
Gerät und Ausgangszustand: [Modell, System, Datum, Zeitzone]
Paket: [Repository, Version, Datei und Überprüfung]
Hash des Pakets und der Indikatoren: [Werte und Datum]
Umgebung: [Analysegerät, Isolation und Synchronisierung]
Untersuchungsumfang: [default / full / targeted / browser / phone]
Befehl und Parameter: [ohne Geheimnisse]
Beginn und Ende mit Zeitzone: [im Wortlaut]
Ausgaben: [TXT, JSON, Zusammenfassung, manifest und Hashes]
Ergebnis und Code: [im Wortlaut]
Befunde: [Grad, Objekt, Quelle und Kontext]
Lücken: [nicht ausgeführte Prüfungen und Gründe]
Vorkommnisse: [Fehler, Grenzen und nicht verfügbare Dateien]
Sicherung und Verwahrung: [Speicherort, Zugriff und Übergaben]
Überprüfung: [Person, Datum und nächste Prüfung]
```

A.3 Interpretationsmatrix

Frage	Quelle der Antwort	Was nicht behauptet werden darf
Was wurde gefunden?	Treffer, Grad und Objekt.	Dass eine Infektion vorliegt oder wer der Angreifer ist.
Was konnte nicht geprüft werden?	Coverage.not_checked und scan_state.	Dass die ausgelassenen Bereiche sauber sind.
Welche Quellen wurden verwendet?	Indikatoren, Versionen und Datumsangaben.	Dass eine kürzlich erstellte Kopie aktuelles Beweismaterial sei.
Was kann eine normale Erklärung haben?	Konfiguration, Anwendung und Kontext der besitzenden Person.	Dass es sich ohne Bestätigung um ein falsch positives Ergebnis handelt.
Was fehlt für eine Attribuierung?	Berechtigung, Sitzungen, Gerät und Chronologie.	Eine bestimmte Person aufgrund einer IP, App oder MAC.
Was wird geteilt?	Je nach Bedarf Zusammenfassung oder vollständiger Bericht.	Dass die Veröffentlichung des Berichts harmlos sei.

Abnahmekriterium

Der Bericht muss es einer anderen Person ermöglichen, den Untersuchungsumfang zu reproduzieren, jeden Befund zu lokalisieren, jede Lücke zu verstehen und zu erkennen, was nicht bewiesen wurde. Enthält er lediglich die Bezeichnung „sauber“ oder „infiziert“, ist die Prüfung noch nicht vollständig.

Anhang B. Rechtsrahmen, Datenschutz und Abschlusskontrolle

Eine Sicherheitsprüfung betrifft ebenfalls personenbezogene Daten. In Mexiko gelten die Grundsätze Zweckbindung, Verhältnismäßigkeit, Sicherheit und Vertraulichkeit sowie die Bestimmungen zu Sicherheitsverletzungen der aktuellen LFPDPPP. Peru, Chile, Argentinien, Kolumbien, Ecuador und Spanien/EU enthalten gleichwertige, aber nicht identische Regelungen zu Datenminimierung, Sicherheit, Rechten und Anbietern. In Chile tritt die Modernisierung durch die Ley 21.719 erst am 1. Dezember 2026 in Kraft und darf nicht als bereits vollständig geltendes Regime dargestellt werden. Es gibt keine allgemeine Berechtigung, ein fremdes Gerät auszulesen.[18][19][20][21][22][23][24]

Kontrolle vor dem Abschluss	Erforderliche Antwort
War die Sicherheit der Person gewährleistet und lag eine Berechtigung vor?	Es wurde keine Prüfung aus Neugier oder ohne Erlaubnis durchgeführt.
Wurde das Paket überprüft?	Repository, Version und Herkunft dokumentiert.
Wurde die Ausgabe geschützt?	Lokaler Ordner, Zugriff und Synchronisierung kontrolliert.
Wurden Befund, Referenz und Lücke voneinander unterschieden?	Aufgrund einer Bezeichnung wurde weder eine Infektion noch Sicherheit behauptet.
Wurden normale Erklärungen geprüft, ohne Schwerwiegenderes auszuschließen?	Konfiguration und Kontext wurden überprüft.
Wurde der Bericht mit Datenminimierung geteilt?	Zusammenfassung zuerst; vollständiges Dossier über einen sicheren Kanal.
Kann die sachverständige Person den Vorgang reproduzieren?	Version, Untersuchungsumfang, Befehle, Hashes, Lücken und Verwahrung sind vorhanden.

[18] Mexiko. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Text veröffentlicht am 20-03-2025 und Reform vom 14-11-2025. Artikel 5–9, 18–20 und 31: Grundsätze, Sicherheit, Vertraulichkeit, Sicherheitsverletzungen und Wahrnehmung von Rechten. Die derzeitige Bundesbehörde ist die Secretaría Anticorrupción y Buen Gobierno. Offizielle Online-Quelle

[19] Peru. Ley 29733 und ihr durch DS 016-2024-JUS verabschiedetes Reglamento. Grundsätze der Zweckbindung, Verhältnismäßigkeit, Sicherheit und Vertraulichkeit; das neue Reglamento regelt Vorfälle, die vorbeugende Bewertung und die schrittweise Einführung der Aufgaben des Datenschutzbeauftragten. Offizielle Online-Quelle

[20] Chile. Ley 21.719, die die Ley 19.628 zum Schutz personenbezogener Daten ändert. Die Fassung mit dem neuen Regime tritt erst am 01-12-2026 in Kraft; vor diesem Datum ist die dann geltende Vorschrift zu prüfen, und künftige Pflichten dürfen nicht als bereits geltend dargestellt werden. Offizielle Online-Quelle

[21] Argentinien. Ley 25.326, aktualisierter Text. Artikel 4–6, 9–10, 14–16 und 25: Datenqualität, Information, Sicherheit, Vertraulichkeit, Rechte der betroffenen Personen und Erbringung von Datenverarbeitungsdiensten im Auftrag Dritter. Offizielle Online-Quelle

[22] Kolumbien. Ley Estatutaria 1581 de 2012, Artikel 4, 8, 12, 17–18 und 26: Grundsätze, Rechte, Information, Pflichten von Verantwortlichen und Auftragsverarbeitern sowie Übermittlung in Drittländer. Offizielle Online-Quelle

[23] Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021. Artikel 10, 37–44: Grundsätze, Sicherheitsmaßnahmen, Datenschutz durch Technikgestaltung, Risiken und Vorgehen bei Vorfällen. Offizielle Online-Quelle

[24] Europäische Union. Verordnung (EU) 2016/679, Artikel 5, 25, 28 und 32–34: Grundsätze, Datenschutz durch Technikgestaltung, Auftragsverarbeiter, Sicherheit sowie Meldung und Benachrichtigung bei Sicherheitsverletzungen. Für Spanien ist zusätzlich das anwendbare nationale und sektorielle Recht zu prüfen. Offizielle Online-Quelle

Abschluss

Die richtige Frage lautet nicht „Bin ich paranoid?“, sondern „Was kann ich prüfen, ohne mir weiteren Schaden zuzufügen?“. Die Antwort kann eine Konfiguration, eine Übereinstimmung, eine Lücke oder eine fachkundige Prüfung sein. Alle sind hilfreicher als eine Anschuldigung ohne Quelle.