



DayBlock – Sicherheitsbericht

Internes Sicherheits-Audit, verständlich aufgeschrieben

Oktober 2026 · von René · dayblock.de

Das Wichtigste in Kürze

- Ich habe DayBlock im Oktober 2026 vollständig auf Sicherheitslücken geprüft – von der Anmeldung über die Verschlüsselung bis zu jeder einzelnen Schnittstelle.
- Ergebnis: keine kritische Lücke. Niemand konnte an verschlüsselte Inhalte, Passwörter oder fremde Konten gelangen.
- Drei Stellen konnten vorsichtiger sein – alle drei habe ich noch während der Prüfung verbessert.
- Dieser Bericht ist ein internes Audit und ersetzt nicht die unabhängige externe Prüfung. Die bleibt Pflicht vor dem öffentlichen Start.

1

Warum dieser Bericht

DayBlock ist ein Tagesplaner, und ein Tagesplaner weiß viel über dich: wann du zum Arzt gehst, mit wem du dich triffst, wie es dir an einem Dienstagabend ging. Darum wird bei DayBlock alles Inhaltliche auf deinem Gerät verschlüsselt, bevor es dein Gerät verlässt. Der Server speichert nur Zeichensalat.

Ein solches Versprechen ist nichts wert, wenn es niemand überprüft. Deshalb habe ich DayBlock systematisch angegriffen – so, wie es jemand mit schlechten Absichten tun würde – und schreibe hier auf, was dabei herauskam. Veröffentlicht wird nur, was bereits behoben ist: Fände ich eine offene Lücke, würde ich sie zuerst schließen und erst danach darüber berichten.

Dieser Bericht richtet sich an alle, nicht nur an Fachleute. Wo ein Fachbegriff nötig ist, erkläre ich ihn. Wer tiefer einsteigen will, findet das vollständige Bedrohungsmodell als eigenen Artikel im DayBlock-Magazin.

2

Was geprüft wurde

Die Prüfung ging einmal durch alles, was zwischen deinem Browser und der Datenbank liegt:

- **Anmeldung und Konto** das Anmeldeverfahren, bei dem dein Passwort dein Gerät nie verlässt; Sitzungen und ihre Cookies; die Wiederherstellung mit den 24 Wörtern; Abmelden und Kontolöschung.
- **Verschlüsselung** die Schlüssel, die auf deinem Gerät entstehen; das Einwickeln des Hauptschlüssels; die Verschlüsselung jedes Datensatzes; die Frage, ob der Server wirklich nie Klartext sieht.

- **Abgleich zwischen Geräten** ob sich beim Hin- und Herschicken der verschlüsselten Umschläge etwas einschleusen, vertauschen oder wiederherstellen lässt.
- **Gruppen und Teilen** private Gruppen, deren Schlüssel nur im Einladungslink steht; öffentliche Gruppen; die Melde-Funktion.
- **Kalender abonnieren** ob sich der Abruf fremder Kalender als Brücke ins interne Netz missbrauchen lässt (eine bekannte Angriffsklasse, die ich gezielt durchgespielt habe).
- **Magazin und Verwaltungsbereich** ob sich über Artikel fremder Code in die Seite schmuggeln lässt; ob der Zugang zur Verwaltung dicht ist.
- **Mails, Begrenzungen, Kopfzeilen** Bestätigungs- und Wiederherstellungs-Mails; Bremsen gegen das Durchprobieren von Passwörtern; die Sicherheits-Kopfzeilen, die der Browser auswertet.
- **Bibliotheken** alle verwendeten Fremdbibliotheken, automatisch geprüft auf bekannte Schwachstellen.

3 Das Ergebnis

Ich habe keine kritische Lücke gefunden. Es gab keinen Weg, an verschlüsselte Inhalte zu kommen, Passwörter abzufangen, fremde Konten zu übernehmen oder den Server als Werkzeug gegen andere zu benutzen.

Gefunden habe ich drei Stellen, an denen DayBlock vorsichtiger sein konnte, als es war. Keine davon war nach meiner Einschätzung ausnutzbar – es waren Gurte, die fehlten, keine offenen Türen. Alle drei habe ich noch während der Prüfung verbessert. Sie stehen im nächsten Abschnitt, denn genau dafür ist dieser Bericht da.

4 Drei Verbesserungen, sofort umgesetzt

1. Der Browser besteht jetzt dauerhaft auf einer verschlüsselten Verbindung.

DayBlock war immer nur verschlüsselt erreichbar. Neu ist eine Kopfzeile, mit der sich dein Browser das für ein ganzes Jahr merkt: Er versucht danach gar nicht mehr erst, eine unverschlüsselte Verbindung aufzubauen – selbst wenn jemand im selben WLAN ihn dorthin umleiten wollte. Fachwort: HSTS.

2. Absenderangaben wird weniger geglaubt.

Anfragen erreichen DayBlock über eine vorgeschaltete Verteilstation, die dem Server mitteilt, von welcher Adresse eine Anfrage kommt. Dieser Angabe vertraut der Server jetzt nur noch genau eine Station weit. Vorher hätte – in einer ungünstigen Konstellation – jemand eine erfundene Absenderadresse mitschicken und so die Bremsen austricksen können, die das Durchprobieren von Passwörtern verhindern. Die eingesetzte Verteilstation verwirft solche erfundenen Angaben zwar selbst; Sicherheit soll aber nicht an einer einzigen Stelle hängen.

3. Auch ein Nebendienst der Testumgebung bekommt die strengen Kopfzeilen.

Ein kleiner Dienst, den es nur in der internen Testumgebung gibt, lief ohne die Sicherheits-Kopfzeilen, die Website und App längst haben. Das war kein Risiko für Nutzerdaten – in der Testumgebung gibt es nur Spieldaten –, aber Einheitlichkeit ist die bessere Gewohnheit.

5 Was dem Test standgehalten hat

Eine Prüfung findet nicht nur Schwächen, sie bestätigt auch Stärken. Diese Punkte haben sich bewährt:

- **Das Passwort bleibt bei dir.** Es verlässt dein Gerät nie – auch nicht bei der Anmeldung. Der Server kann es weder sehen noch aufschreiben. Selbst wer die Datenbank stiehlt, kann Passwörter nicht einfach durchprobieren, weil dazu ein weiteres Geheimnis nötig wäre, das dort nicht liegt.
- **Verschlüsselte Datensätze lassen sich nicht vertauschen.** Jeder Datensatz ist kryptografisch an seine eigene Kennung gebunden. Wer in der Datenbank Umschläge umsortiert, erzeugt Fehlermeldungen, keine falschen Einträge.
- **Der Kalender-Abruf ist kein Hintertürchen.** DayBlock prüft bei jedem Abruf, dass die Zieladresse öffentlich ist – auch nach Umleitungen, auch bei ausgetrickster Namensauflösung.
- **Artikel können keinen Code einschleusen.** Texte fürs Magazin werden Zeichen für Zeichen entschärft, bevor sie zur Webseite werden; Links sind auf harmlose Formen begrenzt.
- **Die Datenbank nimmt keine Befehle von außen an.** Alle Zugriffe sind so gebaut, dass Eingaben immer Daten bleiben und nie zu Befehlen werden.
- **Fremde Seiten können nicht in deinem Namen handeln.** Ändernde Anfragen brauchen eine Kennung, die nur die echte App setzen kann; die Sitzung reist nie zu fremden Seiten mit.
- **Die Bibliotheken sind sauber.** Die automatische Prüfung aller Fremdbibliotheken meldet keine bekannte Schwachstelle.

6 Ehrliche Grenzen

Diese Punkte ändert auch eine gute Prüfung nicht – du sollst sie kennen:

- **Der Server liefert den Code.** Das Grundproblem jeder verschlüsselten Web-App: Wer den Server kontrolliert, könnte veränderten Code ausliefern, der mitliest. Darum werbe ich mit „auf deinem Gerät verschlüsselt“ – nicht mit „ich kann technisch niemals mitlesen“. Geplant: nachprüfbare Fassungen mit veröffentlichten Prüfsummen, öffentlicher Code der App, später Apps mit eingebautem Code.
- **Zwei-Faktor-Anmeldung fehlt noch.** Bis sie da ist, bleibt ein kurzes oder wiederverwendetes Passwort das größte Risiko – das kannst nur du klein halten.
- **Wer registriert ist, lässt sich erraten.** Wie bei fast jedem Dienst verrät der Versuch, ein Konto mit einer fremden E-Mail-Adresse anzulegen, ob es schon eins gibt. Wiederherstellung und erneutes Senden der Bestätigung antworten dagegen bewusst neutral.
- **Verlierst du Passwort und Wiederherstellungsschlüssel, sind deine Daten weg.** Niemand kann sie zurückholen – auch ich nicht. Das ist der Preis echter Verschlüsselung, und DayBlock sagt ihn dir bei der Registrierung klar.

7 Wie geprüft wurde – und was dieser Bericht nicht ist

Dieses Audit war ein internes: Ich habe es selbst durchgeführt, systematisch und mit Unterstützung von KI-Analysewerkzeugen – jede Schnittstelle, jede Prüfung von Eingaben, jede kryptografische Operation

gegen die eigene Spezifikation und gegen bekannte Angriffsklassen. Das ist ehrlicher Fleiß, aber es ist nicht dasselbe wie vier fremde Augen.

Darum gilt: Vor dem öffentlichen Start wird DayBlock von unabhängigen Fachleuten geprüft – Verschlüsselung, Anmeldung und Abgleich. Dieser Bericht ersetzt diese Prüfung nicht, er bereitet sie vor. Auch der externe Bericht wird veröffentlicht.

Bewusst nicht in diesem Bericht: Adressen von Servern, Einstellungen des Betriebs und alles, was eine noch offene Schwachstelle wäre. Solche Angaben kämen erst nach einer Behebung dazu.

8 Wie es weitergeht

In dieser Reihenfolge sind die nächsten Schritte geplant – Geplantes heißt hier geplant, nicht fertig:

- **Nachprüfbare Fassungen** jede ausgelieferte Version lässt sich aus dem Quellcode exakt nachbauen, die Prüfsummen werden veröffentlicht.
- **Zwei-Faktor-Anmeldung** per Code-App oder Passkey.
- **Öffentlicher Code der App** damit das Versprechen „der Server sieht nie deine Inhalte“ von jedem nachgelesen werden kann.
- **Externe Sicherheitsprüfung** mit veröffentlichtem Bericht, verpflichtend vor dem öffentlichen Start.

9 Schwachstelle gefunden?

Dann schreib mir bitte an hallo@dayblock.de mit dem Betreff „Sicherheit“. Beschreib, was du gefunden hast und wie es sich nachvollziehen lässt. Ich antworte, behebe die Lücke so schnell ich kann – und nenne dich danach gern mit Namen, wenn du das möchtest. Bitte teste nur mit deinem eigenen Konto und greif nicht auf Daten anderer zu.

Mehr zum Aufbau von DayBlock: der Artikel „Bedrohungsmodell“ im Magazin auf dayblock.de und die Seite „Was René sieht“. Dieser Bericht trägt das Datum Oktober 2026; jedes weitere Audit bekommt einen neuen, datierten Bericht.

DayBlock · Sicherheitsbericht Oktober 2026 · Oktober 2026 · von René · dayblock.de