LastPass-Quellcode-Lücke: Sind Passwortmanager noch zu empfehlen?

Fünf Fragen von besorgten Usern und fünf Antworten vom Sophos Security-Evangelisten Paul Ducklin sorgen für mehr Klarheit.

Letzte Woche meldete der bekannte und weit verbreitete Passwortmanager LastPass eine Sicherheitslücke. Wie das Unternehmen mitteilte, ereignete sich der Sicherheitsverstoß bereits zwei Wochen zuvor, als Angreifer in das System eindrangen, in dem LastPass den Quellcode seiner Software speichert. Von dort stahlen die Angreifer Teile des Quellcodes und einige proprietäre technische Informationen von LastPass. Die Cyberkriminellen durchwühlten den geschützten Quellcode und das geistige Eigentum des Unternehmens, kamen aber offenbar nicht an Kunden- oder Mitarbeiterdaten heran.

Die Security-Experten von Sophos erhielten daraufhin viele Fragen von besorgten Anwendern. Die fünf wichtigsten Fragen und Antworten sind folgend zusammengefasst:

Wenn ich LastPass verwende, sollte ich dann alle meine Passwörter ändern?
Anwender können natürlich einige oder alle ihrer Passwörter ändern, wenn sie das möchten. Dem Vernehmen nach hat dieser Sicherheitsvorfall jedoch nichts damit zu tun, dass die Cyberkriminellen an persönlichen Daten gelangt sind, schon gar nicht an Passwörter, die ohnehin nicht in verwertbarer Form auf den Servern von LastPass gespeichert sind.

Sollte ich als LastPass-Anwender zu einer anderen Lösung wechseln?
Fakt ist laut LastPass, dass weder persönliche noch passwortbezogene Daten (verschlüsselt oder anderweitig) gestohlen wurden, sondern nur Quellcode und geschützte Informationen des Unternehmens selbst. Die Vertrauenswürdigkeit eines Unternehmens im Bereich der Cybersicherheit sollte darauf beruhen, wie es beim Auftreten eines Fehlers oder einer Sicherheitslücke reagiert, insbesondere wenn der Fehler des Unternehmens die Anwender nicht direkt und unmittelbar gefährdet hat. Es ist empfehlenswert, den LastPass-Vorfallbericht und die FAQ zu lesen und auf dieser Grundlage über das weitere Vertrauen zu entscheiden.

Bedeutet gestohlener Quellcode nicht, dass es zwangsläufig zu Hacks und Exploits kommt?
Quellcode ist viel leichter zu lesen und zu verstehen als ein kompiliertes, "binäres" Äquivalent, insbesondere wenn er gut kommentiert ist und aussagekräftige Namen für Dinge wie Variablen und Funktionen innerhalb der Software verwendet. Mit anderen Worten, dieses Quellcode-Leck könnte potenziellen Angreifern ein wenig helfen, aber erstens mit ziemlicher Sicherheit nicht so sehr, wie man zunächst denken könnte, und zweitens nicht in dem Maße, dass neue Angriffe möglich werden, die ohne den Quellcode niemals hätten herausgefunden werden können.

Sollte ich auf Passwort-Manager ganz verzichtet?
Grundsätzliche Bedenken wären berechtigt, wenn Passwortmanager exakte Kopien aller Passwörter auf ihren eigenen Servern speichern würden, wo sie von Angreifern ausgelesen oder von den Strafverfolgungsbehörden abgefragt werden könnten. Aber kein vernünftiger Cloud-basierter Passwort-Manager funktioniert auf diese Weise.

Warum sollte ich einen Passwort-Manager nutzen?

- Ein guter Passwortmanager vereinfacht die Verwendung von Passwörtern. Er löst das Problem, sich Dutzende oder vielleicht sogar Hunderte von Passwörtern zu wählen und zu merken – optional verstärkt durch 2FA.
- Ein guter Passwort-Manager lässt dasselbe Passwort nicht zweimal zu. Denn wenn Cyberkriminelle ein Passwort herausfinden, beispielsweise durch die Kompromittierung einer Website, nutzen sie dieses oder ähnliche Passwörter, um den Zugang auf andere Konten zu versuchen.
- Ein guter Passwort-Manager kann Hunderte oder sogar Tausende von langen, pseudozufälligen, komplexen und völlig unterschiedlichen Passwörtern generieren und speichern.
- Ein guter Passwort-Manager wird nicht zulassen, dass das richtige Passwort auf der falschen Seite eingeben wird. Dies schützt Anwender beispielsweise vor Phishing.

Ein detaillierter Blog-Beitrag vom Sophos Security-Evangelisten Paul Ducklin mit sehr ausführlichen Antworten auf die Fragen ist auf Sophos Naked Security zu finden.

Social Media von Sophos für die Presse

Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de