chrome enterprise

Datenpannen und Identitätsdiebstahl im Unternehmen durch die Passwort-Warnung in Google Chrome verhindern

Einführung

Welche Auswirkungen hat es auf die Sicherheit Ihrer Organisation und auf Ihre Daten, wenn die meisten Mitarbeiter ihre geschäftlichen Passwörter auch auf anderen Seiten verwenden?

In einer Google/Harris-Umfrage von 2019 wurden 3.000 Erwachsene gefragt, ob sie ihre Passwörter wiederverwenden. 65 % der Befragten gaben an, dass sie entweder für mehrere oder sogar *für all ihre Konten* das exakt gleiche Passwort hätten.

Die Wiederverwendung von Passwörtern ist noch immer eine gängige Praxis

52 % verwenden dasselbe Passwort für mehrere (wenn auch nicht alle) Konten

35 % verwenden ein unterschiedliches Passwort für alle Konten

13 % verwenden dasselbe Passwort für all ihre Konten

chrome enterprise

Hacker benötigen lediglich *ein einziges geschäftliches Passwort eines Mitarbeiters*, um auf die Geräte dieser Person sowie auf das Netzwerk und die Daten Ihres Unternehmens zugreifen zu können. Dabei verfolgen sie zahlreiche Wege, um an solch ein Passwort zu gelangen. Die drei gängigsten Methoden sind Brute-Force-Angriffe, Social Engineering und Phishing.

Was, wenn Chrome die Wiederverwendung von geschäftlichen Passwörtern proaktiv verhindern könnte?
Damit würden Ihre Organisation und Ihre Mitarbeiter von der zusätzlichen Sicherheitsebene profitieren – und Sie von einem besseren Gefühl.

Passwort-Warnung in Google Chrome

Die Passwort-Warnung in Google Chrome ist eine Richtlinie, die Unternehmen bei der Vermeidung von Identitätsdiebstahl und dem Schutz personenbezogener und geschäftlicher Daten unterstützt. Wenn ein Mitarbeiter seine geschäftlichen Anmeldedaten auf einer anderen Website eingibt, wird das automatisch erkannt.

Erweiterte Funktionen und zusätzliche Sicherheit für Unternehmenskonten und -daten bietet die Richtlinie durch den Schutz von Anmeldedaten sowohl von Google- *als auch* von Drittanbieter-Konten. Die IT hat die Möglichkeit, Richtlinien für die Passwort-Warnung auf allen wesentlichen Betriebssystemen wie ChromeOS, Windows[1], Mac[2] und Linux zu verwalten.

Datenschutz

Google nimmt den Datenschutz für Nutzer sehr ernst. Wir speichern ausschließlich nicht-reversible Fingerabdrücke von Passwörtern auf der Festplatte. Niemand kann die Anmeldedaten Ihrer Nutzer sehen und **sie werden ausschließlich lokal gespeichert. Darüber hinaus werden die Daten nicht an Google gesendet oder mit Dritten geteilt**. So können Sie sicher sein, dass die Passwort-Warnung den Schutz und die Sicherheit Ihrer Nutzer nicht beeinträchtigt.

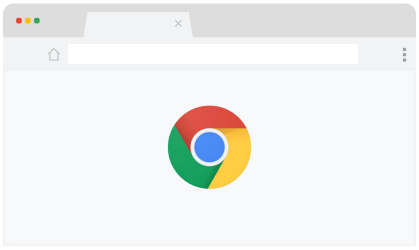
[1] Microsoft®, Windows® und Internet Explorer® sind eingetragene Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

[2] Mac und macOS sind Marken von Apple Inc., eingetragen in den USA und anderen Ländern.

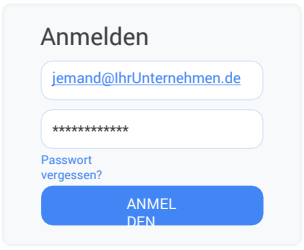
chrome enterprise

Funktionsweise der Passwort-Warnung

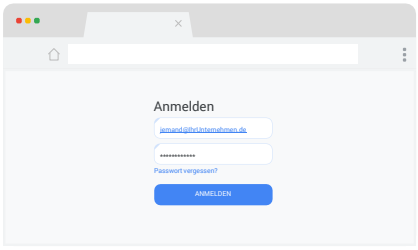
Zuerst sehen wir uns die Passwort-Warnung aus der Endnutzerperspektive an. Sobald Ihre IT diese Richtlinie aktiviert hat, fügt sie sich nahtlos ein.



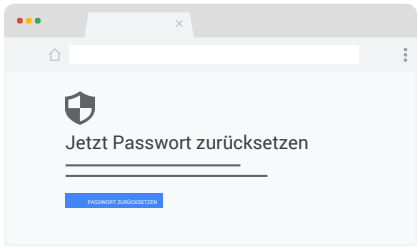
1. Der Nutzer öffnet Google Chrome… . .



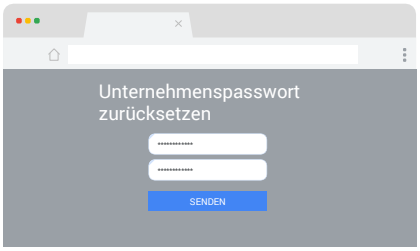
2. . . …und meldet sich über seinen geschäftlichen Standard-Log-in im Unternehmensnetzwerk an, um anschließend… . .



3. . . …eine Seite aufzurufen, auf der er dasselbe Passwort (wenn auch einen anderen Benutzernamen) verwendet.



4. Die Passwort-Warnung benachrichtigt den Nutzer darüber, dass er ein identisches Passwort verwendet. Der Nutzer kann nun wählen, ob… . .



5. . . …er auf die Seite „Passwort zurücksetzen“ weitergeleitet werden soll.

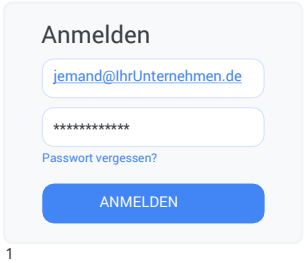
Wenn ein Nutzer seine geschäftlichen Anmeldedaten auf einer Website eingibt, die nicht zum Unternehmen gehört, erhält er eine Warnmeldung und wird zu einer Seite weitergeleitet, auf der er sein Passwort ändern kann.

Das passiert im Back-End, wenn die Passwort-Warnung aktiviert wird:

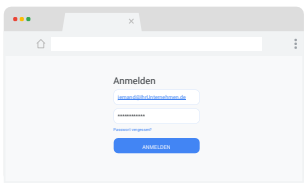
1. Der Nutzer meldet sich über seinen geschäftlichen Standard-Log-in im Unternehmensnetzwerk an.

2. (Unsichtbar für den Nutzer) Die Passwort-Warnung erfasst und speichert das Passwort lokal als Hash, ohne dass der Nutzer dazu aufgefordert werden muss.

3. Der Nutzer fährt ganz normal mit seiner Arbeit fort.



1



3

Sie können die Passwort-Warnung in zwei verschiedenen Modi nutzen.

Passive Überwachung: Ereignisse, in denen Passwörter wiederverwendet wurden, werden im lokalen Dateisystem oder im Windows-Ereignisprotokoll erfasst, ohne dem Nutzer eine Warnung anzuzeigen. Damit verschaffen Sie sich einen Überblick über die Wiederverwendung von Passwörtern in Ihrem Unternehmen.

Aktive Erkennung: Dem Nutzer wird eine Warnung angezeigt, wenn er seine geschäftlichen Anmeldedaten auf Phishing- oder solchen Websites eingibt, die nicht zum Unternehmen gehören. Diese Ereignisse können auch im lokalen Dateisystem oder im Windows-Ereignisprotokoll erfasst werden.

chrome enterprise

Die Passwort-Warnung aktivieren

Die Richtlinie für die Passwort-Warnung ist in den Google-Vorlagen für Unternehmen enthalten. Sie können sie auf allen Betriebssystemen in der Konsole für die Chrome-Verwaltung über die Cloud oder über die Gruppenrichtlinien in Microsoft-Umgebungen aktivieren.

Erste Schritte mit der Passwort-Warnung in Google Chrome

Das Einrichten der Passwort-Warnung ist ganz einfach – sowohl für Google Workspace-Kunden mit oder ohne Einmalanmeldung (SSO) als auch für Kunden, die Google Workspace nicht nutzen. Diese Richtlinie kann auf jedem Chrome Enterprise-Browser aktiviert werden, der über Gruppenrichtlinienobjekte oder die Cloud verwaltet wird. Weitere Informationen zur Verwaltung Ihres Chrome Enterprise-Browsers in der Cloud oder über Gruppenrichtlinien finden Sie im technischen Whitepaper für die Passwort-Warnung in Google Chrome – hier lernen Sie die einzelnen Schritte für jede Konfigurationsoption kennen.

Fazit

Die Passwort-Warnung in Google Chrome bietet Ihnen eine zusätzliche Sicherheitsebene für den Schutz Ihres Unternehmens. Nutzer erhalten eine Warnmeldung, wenn sie ihr geschäftliches Passwort auf nicht-genehmigten bzw. Phishing-Websites eingeben. In der heutzutage global vernetzten Welt, in der Phishing- und andere Angriffe zwar verheerend, aber auch Teil des Alltags geworden sind, ist die Passwort-Warnung ein unerlässliches Tool für die Sicherheit in Ihrem Unternehmen.

Um Ihr Wissen über die Passwort-Warnung in Google Chrome zu vertiefen, **empfehlen wir Ihnen außerdem das folgende Infomaterial:**

Video über die Passwort-Warnung von Google Chrome

Weitere Informationen zur Passwort-Warnung in Google Chrome

Admin-Hilfe für Google Workspace-Nutzer: FAQs zum Schutz vor Phishing durch die Passwort-Warnung

Weitere Informationen zum Schutz vor Phishingangriffen auf Nutzer

Chrome-Browser für Ihr Unternehmen herunterladen

Weitere Informationen zum Support für Google Chrome für Unternehmen

Liste der Richtlinien für Google Chrome

Versionshinweise für Chrome Enterprise und Education

Mit dem Chrome Releases-Blog immer über die neuesten Aktualisierungen auf dem Laufenden bleiben

Offizieller Google-Blog zu Sicherheit und Schutz

Die Chrome Enterprise und Education-Hilfe und das Google Chrome-Hilfeforum

Öffentlicher Tracker für Programmfehler in Google Chrome