So erholen Sie sich von einer Offenlegung Ihrer Passwörter

Es gibt viele Möglichkeiten, wie Ihre Passwörter in unbefugte Hände gelangen können:

1. Weil es praktischer ist, werden Passwörter manchmal offen in elektronischen Dokumenten gespeichert oder auf Papier notiert. Wenn das Dokument verloren geht oder gestohlen wird bzw. das elektronische Dokument abgerufen wird, ist das Passwort offengelegt.
2. Bei einem Phishing-Angriff versucht man Sie dazu zu bringen, Ihr Passwort freiwillig auf einer Website einzugeben. Anschließend wird es verkauft oder verwendet. Wenn Sie den Angriff nicht erkennen, wird Ihr Passwort offengelegt.
3. Sie, Ihr Arbeitgeber und jedes Unternehmen, mit dem Sie digital interagieren, können von einem Verstoß betroffen sein.
4. Technologien, die mit Passwörtern arbeiten, darunter Browser, die Passwörter speichern, Browser-Erweiterungen, Passwortmanager oder sogar der Schlüsselbund von Apple, können einen Verstoß erleiden.

Von Verstößen, die Sie betreffen, erfahren Sie normalerweise über traditionelle oder digitale Nachrichtenmedien oder direkt vom Unternehmen, bei dem sich der Verstoß ereignet hat, sofern dieses verpflichtet ist, Sie zu benachrichtigen. Außerdem können Sie verschiedene Darknet-Überwachungsdienste erwerben, um Benachrichtigungen zu erhalten. Mit einigen kostenlosen Tools und Diensten können Sie selbst überprüfen, ob Sie betroffen sind, oder sich in diesem Falle benachrichtigen lassen, beispielsweise:

- ';--have i been pwned? ermöglicht Ihnen das Durchsuchen von Informationen zu zahlreichen Verstößen, um herauszufinden, ob Ihre E-Mail-Adresse darunter ist.
- Apple kann Benachrichtigungen an iPhone- (siehe Funktion Kompromittierte Passwörter erkennen) und Safari-Browserbenutzer senden.
- Google kann Benachrichtigungen an Chrome-Benutzer senden und bietet das Tool Passwortcheck als Ressource zur anschließenden Überprüfung.

Dieser Blog konzentriert sich auf Verstöße, die möglich sind, wenn bei einem Passwortmanager-Tool ein Sicherheitsvorfall auftritt und Passwortdaten von Benutzern offengelegt werden.

Im August 2022 ereignete sich bei LastPass, einem beliebten Passwortmanager, ein Datensicherheitsverstoß. Während das Unternehmen den Benutzern versichert, dass verschlüsselte Passwort-Vaults weiterhin sicher sind, wurden Quellcodes und technische Informationen gestohlen. Der Vorfall warf bei vielen Benutzern Bedenken auf und ließ sie an der Sicherheit der Plattform zweifeln.

Wenn Sie derzeit ein Passwortmanager-Tool verwenden und über einen Wechsel nachdenken, sollten Sie Folgendes berücksichtigen:

Verstöße verstehen

LastPass räumt ein, dass die Angreifer mit den gestohlenen Informationen aus dem ersten Vorfall auf Speicher-Volumes zugreifen konnten, die als ausreichend geschützt betrachtet wurden. Dadurch steigt das Risiko, dass zugehörige Passwörter kompromittiert wurden. Das Unternehmen versicherte seinen Kunden zwar, dass keine Kundendaten direkt abgerufen wurden, doch der Verstoß unterstreicht, wie wichtig es ist, Passwörter so gut wie möglich zu schützen.

Bei einem Verstoß gegen jegliche Bestimmungen müssen Sie wissen, was genau passiert ist. Kontaktieren Sie Ihren aktuellen Anbieter über dessen Kundensupport-Kanäle, um Antworten auf Ihre Fragen zu erhalten.

Was sollten Sie als Nächstes tun?

1. **Anforderungen und Risikotoleranz beurteilen:** Informieren Sie sich über alternative Passwortmanager. Beliebte Optionen sind 1Password, Bitwarden, Dashlane und andere. Berücksichtigen Sie Funktionen wie Unterstützung für mehrere Geräte, Sicherheitsmaßnahmen, Unterstützung für Zwei-Faktor- oder Multi-Faktor-Authentifizierung, Verfahren zur Kontowiederherstellung und Benutzerfreundlichkeit. Besonders wichtig: Bewerten Sie Ihre Risikotoleranz für verschiedene Kontotypen.

   Hinweis: Dies sind nur Beispiele. Bewerten Sie die Risiken anhand Ihrer eigenen Anforderungen und Toleranz:

   - **Geringes Risiko:** Social-Media-Konten und Shopping-Websites, die Sie selten nutzen und für die Sie keine Zahlungsdaten hinterlegt haben.
   - **Mittleres Risiko:** Eigenständige E-Mail-Adressen, die nicht für Single Sign-on oder die Verwaltung von Diensten mit höherem Risiko genutzt werden.
   - **Hohes Risiko:** Bankkonten, Finanzanwendungen, Gesundheitsportale, Cloud-Speicher und sonstige Konten, die mit Ihren Finanzdaten interagieren.
   - **Extremes Risiko:** Konten, die beliebte Single Sign-on-Dienste unterstützen, darunter Ihre Apple-ID, Microsoft-ID oder Ihr Google-Konto.

2. **Priorität basierend auf Risiko:** Basierend auf Ihrer Risikobewertung sollten Sie Maßnahmen für Ihre kritischsten Konten priorisieren.

Sicherheitsmaßnahmen basierend auf Risiken

- **Grundsätzlich (unabhängig davon, ob Sie zu einem neuen Tool wechseln):**
  - Verwenden Sie ein sicheres Passwort für Ihr Passwortmanager-Tool und ändern Sie es regelmäßig.
  - Aktivieren Sie für das Tool selbst die stärkste verfügbare Methode zur Multi-Faktor-Authentifizierung:

        - Zu den schwächeren Methoden gehört die Verifizierung per E-Mail, SMS oder Anruf.
        - Zu den stärkeren Methoden gehören biometrische oder Einmal-Passcode-Authentifizierungs-Apps oder -Geräte wie Google Authenticator oder Microsoft Authenticator.
        - Zu den stärksten verfügbaren Methoden gehören Passkeys und Zertifikate.
    - Sofern dies unterstützt wird, sollten Sie die Verschlüsselungsschlüssel steuern.
    - Löschen Sie alle Cookies und Passwörter aus Ihrem Browser.
- **Gut:**
    - Sollten Sie zu einem neuen Tool migrieren, beachten Sie folgende Anweisungen.
    - Verwenden Sie das gewünschte Tool, um die Passwörter für Ihre Konten zu ändern.
    - Vernichten Sie bei Bedarf alle Dateien, die Sie für den Export der alten Passwörter von Ihrem alten Passwortmanager-Tool verwendet haben.
- **Besser:**
    - Dieses Vorgehen sorgt für noch mehr Sicherheit.
    - Sollten Sie zu einem neuen Tool migrieren, beachten Sie folgende Anweisungen.
    - Erwägen Sie, die zugehörige Benutzer-ID oder E-Mail-Adresse zu ändern, nachdem Sie mit Ihrem gewünschten Tool sichere Passwörter für alle Konten mit HOHEM oder EXTREMEM Risiko festgelegt haben.
    - Vernichten Sie bei Bedarf alle Dateien, die Sie für den Export der alten Passwörter aus Ihrem alten Passwortmanager-Tool verwendet haben.
    - Sie können auch mehrere Browser-Profile ohne Plug-ins oder Erweiterungen (außer den für Ihr Passwortmanager-Tool erforderlichen) einrichten, die als Container zur direkten Nutzung mit Ihren Konten mit EXTREMEM Risiko fungieren.
- **Am besten:**
    - Dieses Vorgehen ist noch sicherer, aber äußerst zeitaufwendig.
    - Sollten Sie zu einem neuen Tool migrieren, beachten Sie folgende Anweisungen.
    - Sie können mithilfe des neuen Tools die Passwörter für alle Ihre Konten (unabhängig von Risiko) ändern und JEDEM Konto mit HOHEM oder EXTREMEM Risiko eine neue, eigene zugehörige Benutzer-ID oder E-Mail-Adresse zuweisen.
    - Bei diesem Vorgehen erstellen Sie separate Anmeldedaten für Ihre kritischsten Konten und minimieren dadurch die Auswirkungen eines Verstoßes bei einem davon.
    - Der Nachteil dieses Ansatzes ist, dass Sie für Ihre Hochrisikokonten möglicherweise keine gängigen Single Sign-on-Dienste nutzen können.
    - Vernichten Sie bei Bedarf alle Dateien, die Sie für den Export der alten Passwörter von Ihrem alten Passwortmanager-Tool verwendet haben.
    - Sie können auch mehrere Browser-Profile ohne Plug-ins oder Erweiterungen (außer den für Ihr Passwortmanager-Tool erforderlichen) einrichten, die als Container zur direkten Nutzung mit Ihren Konten mit HOHEM und EXTREMEM Risiko fungieren.

Nicht vergessen:

- Fallen Sie nicht auf Phishing-Versuche herein.
- Speichern Sie Ihre Passwörter niemals als Klartext, ob in elektronischer Form oder auf Papier.
- Verwenden Sie sichere, einzigartige Passwörter für alle Ihre Konten. Mit einem Passwortmanager können Sie diese sicher generieren und speichern.
- Aktivieren Sie überall die stärkste verfügbare Methode zur Multi-Faktor-Authentifizierung.
- Denken Sie auch an andere sensible Daten, die Sie vielleicht in einem Passwortmanager-Tool gespeichert haben, beispielsweise Finanzdaten, Kontowiederherstellungen oder Informationen zu Kryptowährungs-Wallets. Auch wenn dies in diesem Blog-Beitrag nicht direkt behandelt wird, müssen Sie eine Risikoanalyse durchführen, um zu ermitteln, welche Wiederherstellungsmaßnahmen Sie ergreifen sollten. Dazu gehört beispielsweise, Finanzkonten oder Kredit-/Debitkartennummern zu ändern oder zu einem neuen Kryptowährungs-Wallet zu migrieren.

Der erwähnte Verstoß soll daran erinnern, wie wichtig es ist, in Bezug auf die Cybersecurity wachsam zu sein. Wenn Sie Ihre Anforderungen und Risikotoleranz bewerten und entsprechend handeln, können Sie dafür sorgen, dass Ihre Online-Konten selbst vor gewieften, entschlossenen Cyberkriminellen sicher sind.