// KI-Hub VON STRUKTURAFLOW

IT-SECURITY

Mein Chrome-Browser checkt Passwörter auf Kompromittierung - reicht das?

Chrome prüft Browser-Passwörter auf Leaks – doch Windows-Domänenkonten bleiben außen vor. Wie KMU die AD-Lücke schließen und was rechtlich gilt.

AUTOR
Natascha Reiner

VERÖFFENTLICHT
11. Juni 2026

ONLINE LESEN
https://wissen.strukturaflow.it.com/mein-chrome-browser-checkt-passwoerter-auf-kompromittierung-reicht-das/

Kurze Antwort: Nein.

Chrome, Firefox und Edge prüfen gespeicherte Passwörter automatisch gegen bekannte Datenlecks. Das ist gut – aber es schützt das Falsche.

Denn die kritischsten Passwörter Ihres Unternehmens – Windows-Domänenkonten, Admin-Zugänge, VPN – liegen im Active Directory. Und dort findet dieser Check nicht statt.

Was der Browser prüft - und was nicht

Der Browser-Check greift nur bei Passwörtern, die Mitarbeitende aktiv im Browser gespeichert haben. Webdienste, Online-Shops, SaaS-Tools.

Was er nicht prüft: das Domänen-Passwort, das morgens beim Windows-Login eingegeben wird. Das Passwort, das Zugriff auf Firmenlaufwerke, E-Mails und interne Systeme gibt.

Das Active Directory prüft von Haus aus gar nichts

Windows Active Directory ist in den meisten österreichischen KMU das Herzstück der Benutzerverwaltung. Es prüft bei Passwortänderungen Mindestlänge, Komplexität und Passworthistorie – aber keinen Abgleich gegen kompromittierte Passwörter.

Ergebnis: `Sommer2024!` kommt durch. Es erfüllt formal alle Anforderungen. Und steht gleichzeitig in Millionen Datenlecks.

Das ist keine Lücke, die Microsoft übersehen hat. Es ist eine Design-Entscheidung – die voraussetzt, dass Unternehmen selbst für diesen Check sorgen.

Die Lösung: kostenlos, lokal, DSGVO-konform

Es gibt ein kostenloses Open-Source-Tool namens Lithnet Password Protection, das direkt auf dem Domain Controller läuft — eine souveräne IT-Lösung, die ohne Cloud-Abhängigkeit auskommt. Bei jeder Passwortänderung prüft es automatisch gegen über 900 Millionen bekannte kompromittierte Hashes – vollständig lokal, kein Datentransfer, kein Cloud-Dienst. Einmal eingerichtet läuft es im Hintergrund.

Das Problem: Die Einrichtung setzt Zugang zum Domain Controller voraus und braucht jemanden, der weiß, was er dort tut.

Wenn Sie nicht sicher sind, ob diese Lücke bei Ihnen offen ist – das ist genau das, was wir in einem ersten Gespräch klären.

→ **Beratungsgespräch vereinbaren**

Was rechtlich gilt

Die DSGVO Art. 32 verpflichtet jedes österreichische Unternehmen zu technischen Schutzmaßnahmen „entsprechend dem Stand der Technik„. Die Behördenplattform onlinesicherheit.gv.at (A-SIT) empfiehlt mindestens 12 Zeichen für normale Konten, Passphrasen statt komplexer Einzelwörter – und Passwortänderungen nur bei konkretem Verdacht, nicht auf Zeitbasis.

Drei Maßnahmen, die wirklich helfen

Lithnet installieren – schließt die AD-Lücke, kostenlos, halber Tag Setup.

MFA aktivieren – für Admin-Konten, VPN und E-Mail. Selbst ein kompromittiertes Passwort reicht dann nicht mehr aus.

Passwortmanager einführen – damit Mitarbeitende nicht dasselbe Passwort für AD, E-Mail und zehn SaaS-Tools verwenden. Vaultwarden läuft selbst gehostet, DSGVO-konform, auf eigener Infrastruktur.

Quellen: - onlinesicherheit.gv.at – Passwort-Auswahl (A-SIT) - sicherheitshandbuch.gv.at