// KI-Hub VON STRUKTURAFLOW

IT-SECURITY

Der Algorithmus aus 1991, der heute Ihre Passwörter knackt

60 % Ihrer Passwörter werden in unter einer Minute geknackt — schuld ist ein Algorithmus aus dem Jahr 1991. Wer noch auf MD5 setzt, betreibt grobe Fahrlässigkeit.

AUTOR
Natascha Reiner

VERÖFFENTLICHT
15. Mai 2026

ONLINE LESEN
https://wissen.strukturaflow.it.com/der-algorithmus-aus-1991-der-heute-ihre-passwoerter-knackt/

60 % Ihrer Passwörter werden in unter einer Minute geknackt — schuld ist ein Algorithmus aus dem Jahr 1991.

Eine aktuelle Kaspersky-Studie zeigt: Nicht Ihr Passwort ist das eigentliche Problem. Es ist das Verfahren, mit dem Ihr IT-Dienstleister Passwörter speichert. Wer noch auf MD5 setzt, betreibt grobe Fahrlässigkeit — und weiß es oft nicht einmal.

Die Zahlen aus der Studie:

- **60 %** aller getesteten Passwörter in unter einer Stunde geknackt
- **48 %** sogar in unter 60 Sekunden — mit einer einzigen GPU
- **220 Mrd.** MD5-Hashes pro Sekunde schafft eine aktuelle RTX 5090

Kaspersky hat im Mai 2026 eine Datenbank mit 231 Millionen geleakten Passwörtern analysiert — mit genau diesem Ergebnis. Das ist kein theoretischer Laborwert. Diese Passwörter stammten aus echten Datenlecks; die Hardware ist frei käuflich. Die Bedrohungslage hat sich durch KI-gestützte Angriffe weiter verschärft. Der entscheidende Punkt: Die meisten Betroffenen hatten Passwörter, die auf den ersten Blick „okay" aussahen. Keine einfachen Wörter, keine reinen Zahlenfolgen.

Das Problem war nicht das Passwort selbst. Das Problem war, wie es gespeichert war.

Was Hashing ist – und warum es existiert

Kein seriöser Dienst speichert Ihr Passwort als lesbaren Text in einer Datenbank. Wenn Sie sich bei einem Portal registrieren, läuft Ihr Passwort durch eine mathematische Funktion — einen sogenannten Hash-Algorithmus. Das Ergebnis ist eine scheinbar zufällige Zeichenkette fixer Länge. Diese Zeichenkette, der Hash, wird gespeichert.

So funktioniert Hashing:

Ihr Passwort `Murtal2024!` wird zu einem Hash wie `5f4dcc3b5aa765d61d8327deb882cf99`. Beim Login tippen Sie Ihr Passwort erneut ein — das System berechnet den Hash erneut und vergleicht ihn mit dem gespeicherten Wert. Stimmen sie überein, werden Sie eingeloggt. Das Originalpasswort verlässt dabei nie die Datenbank, weil es dort gar nicht vorliegt.

Hashing ist Einbahnstraße: Aus dem Hash lässt sich das Originalpasswort mathematisch nicht zurückrechnen. Das ist die Theorie. Die Praxis sieht anders aus — und hängt vom gewählten Algorithmus ab.

Solange niemand die Datenbank stiehlt, spielt die Qualität des Algorithmus kaum eine Rolle. Sobald eine Datenbank kompromittiert ist, entscheidet exakt dieser Algorithmus darüber, ob ein Angreifer in Minuten oder in Jahrzehnten an verwertbare Passwörter kommt.

Warum moderne GPUs das Spielfeld grundlegend verändert haben

Grafikkarten wurden ursprünglich entwickelt, um Millionen einfacher Rechenoperationen parallel durchzuführen — für 3D-Grafik. Exakt diese Architektur ist ideal, um in kürzester Zeit Milliarden von Passwortversuchen zu berechnen und mit einem gestohlenen Hash zu vergleichen. Das nennt sich Brute-Force: einfach alle Kombinationen durchprobieren, bis eine passt.

MD5-Hashes pro Sekunde — Geschwindigkeitsentwicklung:

GPU	JAHR	HASHES/SEK.
RTX 4090	2024	164 Mrd.
RTX 5090	2025/26	220 Mrd.

Die Geschwindigkeit stieg in einem Jahr um 34 %. Passwortgewohnheiten blieben gleich. Diese Lücke wächst jedes Jahr.

Die niedrige Einstiegshürde:

Kriminelle müssen sich keine RTX 5090 um 3.500 Euro kaufen. Leistungsstarke GPUs lassen sich heute für wenige Euro pro Stunde in der Cloud mieten. Die Einstiegshürde für professionelle Passwort-Angriffe ist praktisch verschwunden.

MD5 vs. bcrypt vs. Argon2 – der Unterschied, der alles entscheidet

Nicht jeder Hash-Algorithmus ist gleich. Es gibt einen fundamentalen Unterschied zwischen Algorithmen, die für Geschwindigkeit optimiert wurden, und solchen, die explizit für Passwortspeicherung entwickelt wurden.

ALGORITHMUS	ENTWICKELT FÜR	GESCHWINDIGKEIT	BEWERTUNG
MD5 (1991)	Dateiprüfung, Checksums	220 Mrd. Hashes/Sek.	❌ Niemals für Passwörter
SHA-256 (2001)	Digitale Signaturen, Blockchain	Mehrere Mrd. Hashes/Sek.	❌ Nicht für Passwörter
bcrypt (1999)	Passwortspeicherung	Absichtlich langsam (einstellbar)	⚠ Akzeptabel ab Kostenfaktor 12
Argon2id (2015)	Passwortspeicherung	Langsam + RAM-intensiv	✅ Aktueller Goldstandard

Der Unterschied ist kein Detail. MD5 wurde entwickelt, um so schnell wie möglich einen Hash zu erzeugen — eine sinnvolle Eigenschaft für Dateiprüfungen, eine katastrophale für Passwörter. Bcrypt und Argon2 dagegen sind bewusst so gebaut, dass jeder einzelne Hash-Vorgang Zeit und Rechenleistung kostet. Was für den Login-Prozess 100 Millisekunden bedeutet, bedeutet für einen Angreifer: statt 220 Milliarden Versuche pro Sekunde nur noch ein paar Hundert.

Der Argon2-Vorteil im Detail

Argon2id belegt bei jedem Hash-Vorgang gezielt Arbeitsspeicher (RAM). GPUs sind extrem gut im parallelen Rechnen — aber RAM ist begrenzt und teuer zu skalieren. Argon2id macht GPU-basierte Angriffe dadurch drastisch unwirtschaftlicher als bcrypt. Für neue Systeme ist Argon2id heute die einzig sinnvolle Wahl.

Was Unternehmen jetzt konkret tun müssen

Sie müssen kein Kryptographie-Experte sein. Aber Sie müssen die richtigen Fragen stellen — an Ihren IT-Dienstleister, Ihre Softwareanbieter und Ihre interne IT.

IT-Security Checkliste: Passwort-Hashing im Betrieb

☐ **Überprüfen Sie alle eingesetzten Webanwendungen und Portale**

Jedes System, das Passwörter speichert — CRM, ERP, Kundenportal, Intranet — muss diesen Standard erfüllen. Ein einziges schwaches Glied reicht für ein Datenleck.

Fragen Sie Ihren IT-Dienstleister direkt: „Welchen Hash-Algorithmus nutzen Sie für die Passwortspeicherung?“ Wenn die Antwort MD5 oder SHA-256 lautet — oder wenn niemand spontan antworten kann — haben Sie ein Problem.

☐ **Aktivieren Sie überall Zwei-Faktor-Authentifizierung (2FA)**

Selbst wenn ein Passwort geknackt wird: Mit 2FA bleibt der Zugang gesperrt. Das ist die wichtigste Sofortmaßnahme, die Sie ohne IT-Kenntnisse umsetzen können.

☐ **Führen Sie einen Passwort-Manager ein — für das gesamte Unternehmen**

Lange, einzigartige Passwörter pro Dienst sind der einzige sichere Weg. Passwort-Manager wie Bitwarden (Open Source, selbst hostbar) oder 1Password machen das umsetzbar.

☐ **Definieren Sie interne Mindeststandards schriftlich**

Mindestlänge, Komplexitätsregeln, 2FA-Pflicht und Passwort-Manager-Nutzung gehören in eine interne IT-Sicherheitsrichtlinie — nicht als Empfehlung, sondern als Voraussetzung.

☐ **Haben Sie ein Datenleck-Monitoring?**

Services wie Have I Been Pwned oder professionelle Monitoring-Lösungen informieren Sie, sobald Mitarbeiterdaten in bekannten Leaks auftauchen. Mit Bug-Bounty-Programmen können Unternehmen zusätzlich aktiv Schwachstellen identifizieren. Frühe Reaktion verhindert Folgeschäden.

Passwortlänge allein reicht nicht

Passwortlänge schützt Sie nur dann, wenn der Algorithmus dahinter ebenfalls stimmt. Ein 20-stelliges Passwort, das mit MD5 gespeichert ist, fällt schneller als ein 10-stelliges, das mit Argon2id geschützt wird. Beide Ebenen müssen stimmen.

Rechtliche Einordnung: DSGVO-Relevanz

Für Unternehmen, die personenbezogene Daten verarbeiten, gilt die DSGVO. Ähnliche Sorgfaltspflichten gelten auch für kritische Infrastrukturen unter NIS2. Schwache Passwort-Speicherung — insbesondere der Einsatz veralteter Algorithmen wie MD5 — kann als Verstoß gegen Artikel 32 (technische Sicherheitsmaßnahmen) gewertet werden. Auch bei KI-Tools im Unternehmen gelten strenge DSGVO-Anforderungen. Meldepflichtige Datenpannen, die auf vermeidbare Schwachstellen zurückzuführen sind, ziehen Bußgelder nach sich.

Nächste Schritte

Wenn Sie sich nicht sicher sind, welche Hash-Algorithmen Ihre Systeme nutzen — kein Problem. Wir nehmen uns gerne die Zeit und werfen gemeinsam einen Blick auf Ihre aktuelle Situation. Strukturaflow prüft Ihre IT-Infrastruktur auf genau diese Schwachstellen und liefert klare Handlungsempfehlungen.

→ IT-Security Check anfragen: strukturaflow.com/kontakt

Natascha Reiner — Gründerin & CEO, Strukturaflow IT-Systemhaus, Steiermark