# Was ist ein API-Schlüssel, und was passiert, wenn er gestohlen wird?

**Kurzantwort:** Ein API-Schlüssel ist eine geheime Zeichenfolge, die ein Programm – und nicht eine Person – identifiziert und autorisiert, wenn es einen Dienst aufruft. Ein gestohlener Schlüssel ermöglicht es einem Angreifer, Anfragen im Namen Ihrer Anwendung zu stellen, oft ohne Benutzerinteraktion, ohne MFA und ohne offensichtliches Anzeichen dafür, dass etwas nicht stimmt.

## Warum sie attraktive Ziele sind

- **Kein Mensch beteiligt.** Schlüssel sind für automatisierte, unbeaufsichtigte Nutzung konzipiert, sodass keine MFA-Aufforderung stört.
- **Häufig weit gefasste Berechtigungen.** Schlüssel werden oft mit mehr Rechten ausgestellt, als für die Aufgabe erforderlich ist.
- **Langlebig.** Viele werden nie rotiert, sodass ein heute gestohlener Schlüssel möglicherweise noch Monate später funktioniert.
- **An vorhersehbaren Orten gespeichert.** Konfigurationsdateien, Umgebungsvariablen und Zugangsdatenspeicher – allesamt Orte, die Automatisierung durchsuchen kann.

## Typische Folgen

Je nachdem, wofür der Schlüssel autorisiert: Lesen oder Exportieren von Kundendaten, Versenden von Nachrichten im Namen Ihrer Organisation, Ausgeben von Geld über ein Cloud-Konto oder das Vordringen in andere verbundene Systeme.

Da die Anfragen ordnungsgemäß authentifiziert sind, erscheinen sie in Protokollen meist als normaler Anwendungsverkehr. Die Entdeckung erfolgt in der Regel erst deutlich später, etwa durch eine Rechnung oder ein Audit.

## Verringerung der Angriffsfläche

Beschränken Sie Schlüssel eng auf ihren Zweck, rotieren Sie sie regelmäßig, und halten Sie sie aus der Versionsverwaltung fern. Dies sind sinnvolle Maßnahmen, die jedoch den möglichen Schaden begrenzen, statt den Diebstahl zu verhindern.

Cyber Crucible setzt beim Diebstahl selbst an. Speicherorte für Zugangsdaten und Konfigurationen werden geschützt, und ein Programm, das darauf zugreift, wird im jeweiligen Kontext bewertet: gefälschte Daten oder Verweigerung bei legitimer, aber übermäßiger Zugriffsanforderung, Ablehnung oder Aussetzung bei unbekannten oder kompromittierten Prozessen. Der Schlüssel wird in beiden Fällen nicht preisgegeben.

---

Revision #1
Created 2026-07-24 04:29:27 UTC by Dennis Underwood
Updated 2026-07-24 04:29:28 UTC by Dennis Underwood