NACHRICHTEN AG

12. April 2025

Achtung! Gefälschte Captchas gefährden Ihre Daten – So schützen Sie sich!

Das BSI warnt vor gefälschten Captchas, die Malware verbreiten. Schützen Sie sich mit diesen Tipps vor Cyberkriminalität.

Deutschland - Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schlägt Alarm: Cyberkriminelle nutzen gefälschte Captchas, um ahnungslose Nutzer in die Falle zu locken. Diese gefälschten Sicherheitsabfragen, die sich als legitime CAPTCHA-Technologie tarnen, fordern die Benutzer auf, schädliche Tastenkombinationen einzugeben. Diese Kombinationen können potenziell schädliche Befehle auslösen und somit die Sicherheit der Geräte gefährden, warnt das BSI. **Ruhr24 berichtet**.

Besonders gefährlich ist es, wenn nach dem ersten Klick auf „Ich bin kein Roboter“ ein zusätzliches Banner mit weiteren Anweisungen erscheint. Echte Captchas verlangen nie von den

Nutzern, bestimmte Tasten auf ihrer Tastatur zu drücken. Daher sollten Internetnutzer erhöhte Vorsicht walten lassen.

Schutzmaßnahmen und Handlungsempfehlungen

Das BSI gibt einige Empfehlungen, um sich vor solchen betrügerischen Captchas zu schützen. Insbesondere die Nutzung von Adblockern wird empfohlen, um Schadcode in Werbebannern zu vermeiden. Zudem ist es ratsam, beim Surfen keine Administratorrechte zu verwenden, um die Installation von Malware zu erschweren. Nutzer sollten auch misstrauisch bleiben, wenn sie zu ungewöhnlichen Interaktionen mit ihrem Gerät aufgefordert werden.

Wenn der Verdacht besteht, dass das Gerät durch ein gefälschtes Captcha infiziert wurde, sollten betroffene Personen folgende Schritte in Betracht ziehen:

- Betriebssystem neu installieren.
- Daten von externen Backup-Datenträgern wiederherstellen.
- Wichtige Daten sichern, falls keine aktuelle Datensicherung existiert.
- Passwörter von Onlinekonten, besonders E-Mail-Accounts, ändern.

Regelmäßige Backups sind entscheidend, um im Ernstfall gewappnet zu sein und Datenverluste zu vermeiden.

Das Risiko bei beliebten Inhalten

Die Gefahr wird durch die Tatsache verstärkt, dass Hacker eine Methode entwickelt haben, um reCAPTCHAs auszunutzen, um die Zwischenablage der Benutzer zu kapern und Malware zu installieren. Angreifer locken die Nutzer häufig auf schadhafte Seiten, die beliebte Inhalte wie Filme oder Musik anbieten.

Nutzer werden dann mit einer CAPTCHA-Abfrage konfrontiert, deren Legitimität sie oft nicht in Frage stellen.**Tom’s Guide informiert**.

Das Klicken auf die entsprechende Checkbox führt zumeist zu weiteren Bestätigungsschritten, in denen Befehle wie Windows-Taste + R, Strg + V und Enter eingegeben werden müssen. Diese Befehle können in der Tat zur Installation von Malware führen, da die schadhafte Seite einen Befehl in die Zwischenablage kopiert. Malwarebytes hat diese Technik identifiziert und nennt unter anderem den Lumma Stealer und SecTopRat als Beispiele für die über diese Methode verbreitete Malware.

Um sich vor solchen Angriffen zu schützen, sollten Nutzer besonders vorsichtig sein, wenn sie dazu aufgefordert werden, CAPTCHAs auf weniger bekannten Websites zu lösen. Eine Kombination aus Antivirensoftware und Browsererweiterungen zur Blockierung schadhafter Seiten kann zusätzliche Sicherheit bieten. Zudem könnte das Deaktivieren von JavaScript den Zugriff auf die Zwischenablage verhindern, allerdings kann dies die Funktionalität vieler Websites beeinträchtigen.

Schließlich ist es von entscheidender Bedeutung, stets über die neuesten Betrugsmaschen informiert zu bleiben und grundlegende Prinzipien der Cybersicherheit zu befolgen, um im Internet sicher zu agieren.

Details	
Vorfall	Cyberkriminalität
Ort	Deutschland
Quellen	• **www.ruhr24.de** • **www.tomsguide.com**