# Sicherheitslücken bei Browserweiterungen im Chrome Web Store

*Bericht: CISPA Helmholtz Center for Information Security*

**Millionen von User:innen nutzen täglich Browser-Erweiterungen, etwa um Werbung auf Websites zu blockieren. Aber ist die Nutzung der von Drittanbietern zur Verfügung gestellten Erweiterungen überhaupt sicher? CISPA-Faculty Dr. Aurore Fass hat dies nun anhand von Erweiterungen für Chrome, den Web-Browser von Google, zusammen mit ihren Studentinnen Sheryl Hsu und Manda Tran untersucht und damit zum ersten Mal eine große Studie über den Chrome Web Store vorgelegt. Ihr zugehöriges Paper „What is in the Chrome Web Store?“ wurde von der ACM ASIA Conference on Computer and Communications Security akzeptiert.**

Wenn Nutzer:innen auf das Internet zugreifen wollen, benötigen sie dafür einen Web-Browser wie Chrome, Safari, Mozilla Firefox oder Microsoft Edge. Wenn die Standard-Features der Browser nicht ausreichen, können Erweiterungen von Drittanbietern genutzt werden. „Browser-Erweiterungen sind sehr nützlich, um die Funktionalität des Browsers zu erweitern. Fügt man zum Beispiel Erweiterungen wie einen Ad-Blocker hinzu, lässt sich damit Werbung auf Websites blockieren oder einschränken“, erklärt CISPA-Faculty Dr. Aurore Fass. Die Erweiterungen lassen sich über die Browser downloaden und mit wenigen Klicks installieren. Da alle gängigen Web-Browser Erweiterungen anbieten, entschied sich die CISPA-Faculty, den Chrome Web Store zu untersuchen. „Wir verwenden Chrome, weil es der beliebteste Browser ist“, erläutert die Faculty. „Und Chrome hat eine Web-Erweiterungs-API, die browserübergreifend funktioniert. Aus Entwicklerperspektive sind also Erweiterungen für Chrome oder Firefox sehr ähnlich.“ Ein weiterer wichtiger Faktor war, dass ein Tool namens „Chrome-Stats“ den Datenzugang zu Chrome erleichtert. „Chrome-Stats sammelt Längsschnittdaten für Erweiterungen im Chrome Webstore. Das war sehr wichtig, denn sobald eine Erweiterung aus dem Store entfernt wird, haben wir keinen Zugriff auf die Metadaten oder den Quellcode dieser Erweiterungen“, so Fass weiter.

## Das Feld der sicherheitskritischen Erweiterungen

Für ihre Untersuchung arbeitet die Forscherin mit der Unterscheidung von harmlosen und sicherheitskritischen Erweiterungen, auf Englisch „Security Noteworthy Extensions (SNE)“ genannt, die sie in drei Kategorien unterteilt. „Zunächst gibt es Erweiterungen, die Malware enthalten“, erklärt Fass. „Diese Erweiterungen sind bösartig, da sie speziell von Leuten entwickelt wurden, die Benutzer:innen schaden wollen. Die zweite Kategorie sind Erweiterungen, die gegen die Datenschutzrichtlinien von Google verstoßen. Und die dritte Kategorie sind si-

cherheitskritische Erweiterungen.“ Letztere wurden zwar von Entwickler:innen in guter Absicht entwickelt, aber sie enthalten Fehler, die Sicherheitslücken zur Folge haben können. Die Gefahr von SNEs ist, dass diese von Angreifer:innern genutzt werden, um Malware zu versenden, User:innen zu tracken und auszuspionieren oder Daten zu stehlen. Untersucht wurden von Fass und ihren Kolleg:innen Erweiterungen, die zwischen Juli 2020 und Februar 2023 im Chrome Web Store verfügbar waren.

## Lebensdauer und Sicherheitsrisiken von Erweiterungen

Die erste wichtige Erkenntnis von Fass war, dass Erweiterungen sehr kurze Lebenszyklen haben. „60 Prozent bleiben weniger als ein Jahr im Chrome Webstore“, erklärt Fass. „Das ist verrückt! Damit braucht es regelmäßige Analysen, um zu wissen, was im Store vorhanden ist.“ Die zweite Erkenntnis bezieht sich auf die Präsenz von sicherheitskritischen Erweiterungen. „Wir haben im Chrome Web Store viele sicherheitskritische Erweiterungen analysiert, die Hunderte von Millionen von Nutzer:innen betreffen“, so Fass weiter. „Einige davon bleiben zehn Jahre lang im Store und beeinträchtigen die Sicherheit und die Privatsphäre der Nutzer:innen für eine sehr lange Zeit.“ Die dritte Erkenntnis bezieht sich auf Ähnlichkeiten zwischen Erweiterungen. „Mit Hilfe von Clustering-Prozesse konnten wir Erweiterungen erkennen, die eine ähnliche Code-Basis haben“, erläutert Fass. „Das hilft, um sicherheitskritische Erweiterungen aufzuspüren. Denn wenn eine Erweiterung einer sicherheitskritischen Erweiterungen ähnelt, können wir stark davon ausgehen, dass sie ebenfalls sicherheitskritisch ist. Das kann helfen, bis dato unbekannte sicherheitskritische Erweiterungen zu erkennen.“ Die letzte Erkenntnis hängt mit der mangelnden Wartung des Chrome Web Store zusammen. „60 Prozent der Erweiterungen wurden seit ihrer Veröffentlichung im Store nicht aktualisiert. Das bedeutet, dass keine neuen APIs oder Funktionen von Chrome verwendet werden, die die Ausführung der Sicherheits- und Privatsphäre verbessern, wie zum Beispiel das neue Manifest V3“, so Fass.

## Erkenntnisse zum Quellcode der Erweiterungen

In einem weiteren Schritt hat Fass auch den Quellcode der Erweiterungen im Chrome Web Store näher untersucht. Dahinter stand die Annahme, dass die Suche nach ähnlichem Quellcode dabei helfen kann, SNEs einfacher und schneller zu entdecken. Und tatsächlich entdeckte Fass tausende Cluster mit ähnlichem Quellcode. „30 Prozent der Browser-Erweiterungen haben eine verwundbare Bibliothek in ihrem Quellcode“, erklärt Fass. „Wir haben zwar nicht untersucht, ob dies tatsächlich ausgenutzt werden kann, aber wir halten es trotzdem für eine schlechte Praxis, diese anfälligen Bibliotheken zu verwenden. Denn sie warten darauf, dass etwas Schlimmes passiert.“ Die Gründe, warum ähnlicher Quellcode Verwendung findet, liegt in der Praxis vieler Entwickler:innen, bestehende Codes aus frei zugänglichen Onlinebibliotheken wiederzuverwenden. „Das Problem besteht darin, dass der Code von Drittanbietern, den sie verwenden, nicht gewartet wird. Dies führt dazu, dass sie einen veralteten, nicht ge-

warteten Code verwenden, der Sicherheitslücken enthalten könnte“, so Fass. Besonders häufig nutzten Entwickler:innen Quellcode aus einem Tool namens Extensionizr.

## Was können Nutzer:innen, Entwickler:innen und Google tun?

Danach gefragt, was Entwickler:innen tun könnten, um ihre Erweiterungen sicherer zu machen, antwortet Fass: „Entwickler:innen mit guten Intentionen sollten sich darüber bewusst werden, was bei Erweiterungen schiefgehen kann. Gut wäre es, wenn sie Bedrohungsmodelle im Kopf haben und darüber nachdenken würden, was Einfallstore für Angreifer:innen sein könnten.“ Auch regelmäßige Updates sind ein wichtiger Faktor. Schwieriger ist es für die Nutzer:innen von Erweiterungen. „Für die gibt es nur wenige Möglichkeiten herauszufinden, ob eine Erweiterung gefährlich ist oder nicht“, erklärt Fass. „Theoretisch kann man sich die Berechtigungen von Erweiterungen ansehen, aber die meisten haben sich damit nicht beschäftigt und verstehen die Details nicht.“ Umso wichtiger ist eine bessere Kontrolle durch Google. „Google hat ein Überprüfungssystem, in dem Erweiterungen vor der Veröffentlichung im Chrome Web Store überprüft werden“, so die Faculty weiter. Fass hat auch eine Idee, wie sich das Überprüfungssystem verbessern ließe: „In einem älteren Paper zeige ich, wie anfällige Erweiterungen automatisch erkannt werden könnten. Dies könnte in die Pipeline von Google aufgenommen werden.“

**Originalpublikatio**n:
Hsu, Sheryl and Tran, Manda and Fass, Aurore (2024) What is in the Chrome Web Store? Conference: ASIACCS ACM ASIA Conference on Computer and Communications Security

---

*16.02.2024*
*Felix Koltermann*
*Unternehmenskommunikation*
*CISPA Helmholtz Center for Information Security*
*www.cispa.de*