chrome enterprise

Startleitfaden: Erweiterungen in Google Chrome für Unternehmen verwalten

Einführung

Es gibt Tausende Chrome-Erweiterungen, von denen viele sehr nützlich sind. Man kann damit Zeit sparen, Geschäftsabläufe verbessern und effizienter arbeiten. Durch sie lässt sich beispielsweise die RAM-Auslastung optimieren, die Browsergeschwindigkeit erhöhen oder eine Rechtschreibprüfung automatisch durchführen – das erhöht die Produktivität insgesamt. Damit Erweiterungen nicht zum Unternehmensrisiko werden, müssen sie richtig verwaltet werden. Deshalb müssen IT-Teams die Nutzererwartungen in puncto Produktivität und die Sicherheitsanforderungen des Unternehmens vernünftig gegeneinander abwägen.

Bei der Verwaltung von Erweiterungen haben IT-Teams in Unternehmen drei Hauptprioritäten:

1. Nutzer- und Unternehmensdaten schützen
2. Die Installation von Erweiterungen mit schädlichem Code verhindern
3. Nutzern den Zugriff auf die Erweiterungen ermöglichen, mit denen sie produktiver arbeiten können

Mithilfe von Best Practices können Administratoren alle neuen und vorhandenen Chrome-Erweiterungen der Nutzer sowie die ständigen Updates überwachen, verwalten und sichern.

In diesem technischen Leitfaden werden verschiedene Möglichkeiten zur Verwaltung von Erweiterungen erläutert und für welche Anforderungen sie am besten geeignet sind.

Zu berücksichtigende Kriterien

Für die Verwaltung von Erweiterungen ist es wichtig zu wissen, nach welchen Kriterien Ihre Organisation diese bewertet und genehmigt. Stellen Sie sich dafür die folgenden Fragen:

- Welche Sicherheitsbestimmungen und Compliance-Auflagen müssen wir erfüllen?
- Welche Nutzer- und Unternehmensdaten werden auf den Geräten der Nutzer gespeichert?
- Welche durch Erweiterungen angeforderten Berechtigungen verstoßen möglicherweise gegen unsere Datenschutzrichtlinien?

Sobald Sie diese Fragen für sich selbst beantwortet haben, können Sie entscheiden, wie Sie Erweiterungen verwalten möchten.

Der herkömmliche Ansatz:

Lange Zeit bestand die einzige Möglichkeit zur Verwaltung von Browsererweiterungen darin, jede Erweiterung manuell zu bewerten und dann Zulassungs- und Sperrlisten zu erstellen, um festzulegen, welche Erweiterungen auf Nutzergeräten installiert werden dürfen. Einige Organisationen verwenden diesen Ansatz nach wie vor.

In der Admin-Konsole haben Sie folgende Möglichkeiten:

- Alle Erweiterungen zulassen und einzelne blockieren
- Alle Erweiterungen blockieren und einzelne zulassen
- Erweiterungen einzeln blockieren oder zulassen
- Die Installation von einer oder mehreren Erweiterungen erzwingen

Mit Microsoft[1]-Gruppenrichtlinien haben Sie dank der Vorlagen, die auf bestimmte Gruppen oder die gesamte Organisation angewendet werden können, ähnliche Möglichkeiten:

- Alle Erweiterungen zulassen und einzelne blockieren
- Erweiterungen einzeln blockieren oder zulassen
- Die Installation einer Erweiterung erzwingen

Beide Möglichkeiten funktionieren, haben aber gewisse Grenzen und sind nicht automatisiert, nehmen also viel Zeit in Anspruch.

Das kann sich negativ auf die Produktivität sowohl der Nutzer als auch des Administrators auswirken. Außerdem ist es möglich, dass Erweiterungen, die auf der Zulassungsliste stehen, von Personen oder Unternehmen verkauft und/oder aktualisiert werden, die Sie nicht überprüft haben – ein nicht unerhebliches Sicherheitsrisiko.

[2] Mac und macOS sind Marken von Apple Inc., die in den USA und/oder anderen Ländern registriert sind.

Ein moderner Ansatz: Erweiterungen anhand von Berechtigungen verwalten

Angeforderte Chrome-Erweiterungen lassen sich anhand von Berechtigungen verwalten. Diese Möglichkeit ist effizienter und zudem skalierbar und sicher. IT-Teams können den Nutzern damit die Erweiterungen zur Verfügung stellen, die sie benötigen – ohne Sicherheitsrisiko für die Unternehmensdaten. Das IT-Team von Google nutzt diese Methode und empfiehlt sie anderen Unternehmen.

Mit den entsprechenden Berechtigungen können Erweiterungen bestimmte Änderungen an Websites oder Geräten vornehmen. Damit eine Erweiterung erwartungsgemäß funktioniert, sind oft bestimmte Berechtigungen erforderlich.

Es gibt zwei Hauptkategorien: Websiteberechtigungen und Geräteberechtigungen. Für viele Erweiterungen werden beide verwendet.

Mit Websiteberechtigungen können Sie beispielsweise einer Erweiterung erlauben, Bilder zu blockieren oder zu steuern, wie weit sich eine Website heranzoomen lässt. Zu den Geräteberechtigungen zählen der Zugriff auf USB-Anschlüsse oder den Bildschirm und die Interaktion mit Programmen.

Noch weiter verringern können Sie Risiken, indem Sie Erweiterungen mithilfe der folgenden Richtlinien verwalten:

- **Blockierte/Zulässige Berechtigungen:** Bietet Schutz vor Berechtigungs-Updates bei Erweiterungen, die bereits auf der Zulassungsliste stehen. Sie können Erweiterungen, die Ihre Anforderungen nicht mehr erfüllen, nach der Installation deaktivieren.
- **Hosts mit Laufzeitsperrung:** Gibt an, auf welchen Websites Erweiterungen ausgeführt werden dürfen.
- **Mit erzwungener Installation:** Erweiterungen werden automatisch auf den Geräten der Nutzer installiert, sodass den Mitarbeitern alle Produktivitäts-Tools zur Verfügung stehen.
- **Zulassungsliste/Sperrliste:** Falls erforderlich

Diese Methode zur Verwaltung von Chrome-Erweiterungen ist sicherer, einfacher und lässt sich auch auf große Umgebungen anpassen. Sie schützt vor manipulierten Erweiterungen und spart der IT Zeit. Es müssen keine extrem langen Zulassungs- und Sperrlisten mehr manuell verwaltet und keine Updates geprüft werden. Sie müssen auch nicht mehr jede Erweiterung einzeln prüfen. Das ist eine wirkliche Win-win-Situation.

chrome enterprise

Einstieg: Erweiterungen anhand von Berechtigungen verwalten

Folgen Sie diesen Schritten, um Ihre Erweiterungen anhand von Berechtigungen zu verwalten:

Erstellen Sie eine Liste mit den Erweiterungen, die Ihre Nutzer bereits installiert haben. Verwenden Sie dazu die Berichtsfunktion in der Chrome-Verwaltung über die Cloud oder führen Sie eine Umfrage bei den Endnutzern durch.

1. Ermitteln Sie die Websites/Hosts, die geschützt werden müssen. Bestimmen Sie, welche Berechtigungen mit potenziellen Risiken verbunden sind und beschränkt werden müssen.

2. Erstellen Sie aus allen erfassten Daten eine Masterliste und lassen Sie sich diese von wichtigen Entscheidungsträgern bestätigen.

3. Testen Sie die neuen Richtlinien in einer Testumgebung oder innerhalb einer kleinen Pilotgruppe und führen Sie sie anschließend schrittweise für die Mitarbeiter ein.

4. Gehen Sie das Feedback der Nutzer durch.

5. Wiederholen und optimieren Sie diesen Vorgang monatlich, vierteljährlich oder jährlich, je nachdem, welcher Zeitraum für Ihre Organisation am besten geeignet ist.

Sie müssen die Richtlinien nur einmal festlegen, um eine Basis zulässiger Berechtigungen zu schaffen und damit vertrauliche Unternehmenswebsites zu schützen. So erhöhen Sie nicht nur automatisch die Sicherheit, sondern verbessern auch die Nutzererfahrung.

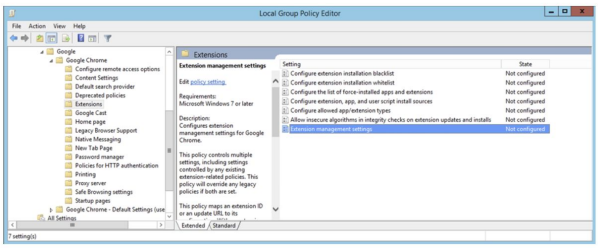
Die Mitarbeiter können auf diese Weise vielleicht sogar Erweiterungen installieren, die zuvor lockiert waren. Sie lassen sich nur nicht mehr auf vertraulichen Unternehmenswebsites ausführen.

Berechtigungen festlegen

Sie können ganz einfach steuern, welche Erweiterungen die Nutzer installieren dürfen. Sie müssen lediglich festlegen, welche Berechtigungen zulässig sind und welche nicht.

Admin-Konsole

Unter Windows, Chrome OS, Mac[2] und Linux können Sie das in der Admin-Konsole tun. Erweiterungen, die Zugriffs- oder andere Berechtigungen erfordern, die gegen Ihre Sicherheitsrichtlinien verstoßen, werden nicht installiert. So lassen sich beispielsweise Erweiterungen blockieren, die eine Verbindung zu USB-Speichermedien herstellen oder den Zugriff auf Cookies verhindern. Wenn eine bereits installierte Erweiterung eine nicht zugelassene Berechtigung erfordert, wird sie nicht ausgeführt. Sie wird nicht entfernt, sondern deaktiviert.



Gruppenrichtlinien

Viele Unternehmen verwalten ihre Erweiterungen in Windows auch mit der Richtlinie „ExtensionSettings“. Im Gruppenrichtlinienverwaltungs-Editor können Sie gleich mehrere Richtlinien über eine JSON-Zeichenfolge oder über die Windows-Registrierung festlegen. Mit der Richtlinie „ExtensionSettings“ können Sie Optionen festlegen wie etwa den Installationsmodus,

[2] Mac und macOS sind Marken von Apple Inc., die in den USA und/oder anderen Ländern registriert sind.

die Update-URL, blockierte Berechtigungen, Installationsquellen, zulässige Typen, blockierte Installationen sowie Hosts mit Laufzeitsperrung und zulässige Hosts. Sie können entweder alle Einstellungen für die Erweiterungsverwaltung hier festlegen oder mithilfe von einzelnen Richtlinien. Konfiguriert werden die Einstellungen über die Windows-Registrierung oder eine JSON-Zeichenfolge im Gruppenrichtlinien-Editor von Windows.

Zusätzliche Überlegungen

Einige Unternehmen bevorzugen eine eigene Website für den Download von Erweiterungen. Google empfiehlt diesen Ansatz jedoch nicht, da er möglicherweise nicht so sicher ist wie der Chrome Web Store, wo durch automatisierte und manuelle Code-Scans verhindert wird, dass schädlicher Code an die Nutzer gesendet wird.

Bei der Chrome-Verwaltung über die Cloud handelt es sich um eine neue Konsole, in der sich alle Chrome-Einstellungen für Windows-, Mac- und Linux-Geräte verwalten lassen. Hier haben Sie eine detaillierte Ansicht des Chrome-Status in Ihrer Umgebung mit folgenden Informationen:

- Aktuelle Chrome-Versionen auf allen Computer- und Laptop-Typen
- In den einzelnen Browsern installierte Erweiterungen
- Auf die einzelnen Browser angewendete Richtlinien

Außerdem können Sie in der Konsole mit nur einem Klick auf eine Schaltfläche eine verdächtige Erweiterung auf allen Geräten blockieren.

Chrome-Erweiterungen verwalten wie bei Google

Nachdem das IT-Team von Google die Erweiterungen für mehr als 300.000 Endpunkte jahrelang mithilfe der herkömmlichen Methode für Zulassungs- und Sperrlisten verwaltet hatte, suchte es nach einem weniger aufwendigen Ansatz, der weder in puncto IT-Anforderungen und Sicherheit des Unternehmens noch in Hinblick auf Mitarbeiterproduktivität Kompromisse vorsah. Schließlich fand das Team eine Lösung, die viel effizienter und zudem skalierbar und sicher ist: Erweiterungen anhand von Berechtigungen verwalten.

Wie Google können auch Sie von Zulassungs-und Sperrlisten zu der in diesem technischen Leitfaden beschriebenen Methode wechseln.
Damit erfüllen Sie die Sicherheitsanforderungen Ihres Unternehmens und bieten gleichzeitig Ihren Nutzern die Möglichkeit, Erweiterungen zu installieren, mit denen sie produktiver arbeiten können.

Verwalten auch Sie Ihre Erweiterungen anhand von Berechtigungen.

Weitere Informationen zur Verwaltung von Chrome-Erweiterungen finden Sie in den **folgenden Ressourcen**:

Leitfaden zur Verwaltung von Erweiterungen im Unternehmen
Google Cloud Next 19 Breakout Session: How Google Cloud IT Manages Enterprise Extensions (Wie das IT-Team von Google Cloud Erweiterungen verwaltet)
Optionen für die Chrome-Verwaltung über die Cloud
Chrome-Downloads für Ihr Unternehmen
Weitere Informationen zum Support für Google Chrome für Unternehmen
Richtlinienliste des Chrome-Browsers
Google Chrome Enterprise-Hilfe und Google Chrome-Hilfeforum