Google Chrome im Unternehmen verwalten

Chartstürmer in Serie

von Dr. Christian Knermann

Google Chrome steht unangefochten an der Spitze der Browser-Hitparade. Und je mehr Anwendungen von lokal installierten Clients auf Webinterfaces wechseln, desto wichtiger wird der Browser als Fenster zur Welt. IT-Administrator widmet sich in diesem Workshop der zentralen Konfiguration von Chrome mittels Gruppenrichtlinien sowie per Chrome Browser Cloud Management.

Die frei verfügbare Statistik von Statcounter sieht Googles Chrome-Browser mit ungefähr 65 Prozent weltweitem Marktanteil auf dem ersten Platz der Charts. Mit deutlichem Abstand folgt Apple Safari bei etwas mehr als 18 Prozent, während sich Microsofts Internet Explorer sowie Edge, Mozilla Firefox und Opera unter "ferner liefen" einreihen. Bezogen auf Europa ändert sich das Bild kaum. Mit Blick auf den deutschen Markt verliert Chrome zwar etwas gegenüber Safari und Firefox, verteidigt aber mit immerhin knapp der Hälfte der Browser-Instanzen auch hierzulande den ersten Platz [1].

Über alle Hersteller hinweg steigt die Bedeutung des Browsers, entwickeln sich doch immer mehr Dienste weg von lokal zu installierenden Clientapplikationen in Richtung webbasierter Bedienung. Mit Erweiterungen, Plug-ins und Add-ons aufgebohrt, gewinnen Browser zunehmend an Funktionalität. Grund genug also, der Frage nachzugehen, wie sich eine Vielzahl an Browser-Installationen im Unternehmensumfeld zentral verwalten lässt.

Im Fokus dieses Workshops steht dabei Google Chrome. Der basiert auf dem maßgeblich von Google unterstützten Open-Source-Projekt Chromium [2], wartet aber im Gegensatz zu seiner quelloffenen Basis mit zusätzlichen Funktionen auf. So spendiert Google dem Browser automatische Updates und unterstützt für Windows, Linux sowie macOS jeweils Methoden zur zentralen Konfiguration. Plattformübergreifend kümmert sich zudem das Chrome Browser Cloud Management (CBCM) um die Pflege von Einstellungen und Erweiterungen. Doch widmen wir uns zunächst der Installation unter Windows und der Verwaltung auf klassischem Weg per Gruppenrichtlinien.

Separates Setup für Unternehmen

Die Setuproutine, die Google standardmäßig zum Download anbietet, richtet sich

eher an Endanwender, die den Browser in Eigenregie auf einem nicht verwalteten Endpunkt installieren möchten. Diese Variante kommt auch ohne lokale Admin-Rechte aus und richtet den Browser in diesem Fall einfach im persönlichen Profil des installierenden Anwenders ein. Auf den Unternehmenseinsatz zielt stattdessen das "Chrome Browser for Enterprise-Bundle", das Google in Varianten für 32- und 64-Bit-Systeme bereitstellt [3]. Insbesondere die Einrichtung und Verwaltung unter Windows beschreibt Google zudem im Bereitstellungshandbuch für Chrome [4].

Im Enterprise-Bundle finden Sie alle Elemente, die Sie für eine zentrale Verteilung und Konfiguration von Chrome benötigen. Insgesamt liefert Google drei MSI-Pakete, darunter neben dem eigentlichen Browser auch den sogenannten "Legacy Browser Support". Letzterer ist inzwischen aber nicht mehr als separate Installation erforderlich, da aktuelle Versionen von Chrome diese Funktion bereits ab Werk mitbringen. Sie hilft Ihnen dabei, bestimmte ältere Webseiten, die in Chrome nicht funktionieren, automatisch in einem anderen Browser zu öffnen.

Dabei beschränkt sich Chrome nicht auf Microsofts Internet Explorer oder den neueren IE-Modus von Microsoft Edge, sondern übergibt per frei definierbarem Pfad Webseiten auch an Mozilla Firefox oder Apple Safari.

Optional ist die "Endpoint Verification". Bei dieser Prüfung handelt es sich um eine Cloudfunktion, die Ihnen dabei hilft, den Zugriff auf Daten Ihres Unternehmens basierend auf dem Standort des Geräts, dem Sicherheitsstatus oder anderen Attributen kontextsensitiv zu steuern. Die Basisfunktionalität ist kostenfrei verfügbar. Sobald Sie aber gerätespezifische Regeln verwenden möchten, benötigen Sie eine kostenpflichtige Lizenz – entweder die Premiumversion von Google Cloud Identity oder eine Edition von Google Workspace (ehemals G-Suite).

Installation und Erstkonfiguration

Den Browser installieren Sie unbeaufsichtigt mittels

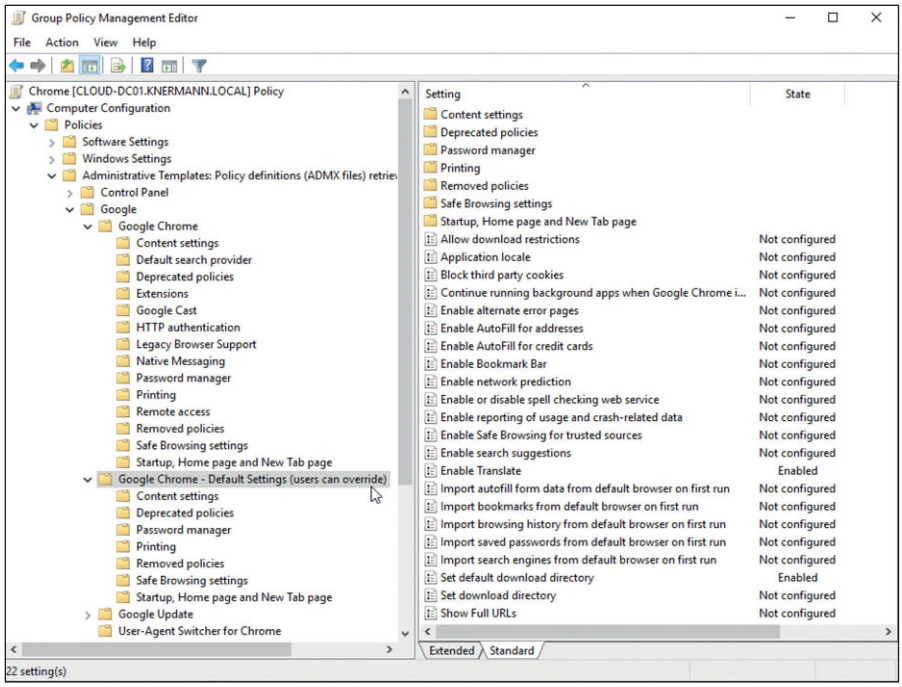

Bild 1: Googles Gruppenrichtlinien geben Einstellungen für den Browser fix vor oder erlauben den Nutzern, sie zu ändern.

```
msiexec /i GoogleChromeStandaloneEn-
  terprise64.msi /qn
```

und verfahren nach Bedarf ebenso mit der Endpunktprüfung. Die Installationen bringen Sie entsprechend auch per Gruppenrichtlinien, mittels Microsoft Endpoint Configuration Manager oder einer anderweitigen Softwareverteilung zentral auf Ihre Clients aus. Passen Sie im Rahmen der Installation die JSON-Datei "master_ preferences" im Pfad "%programfiles%\ Google\ Chrome \ Application" an, können Sie dem Browser Voreinstellungen mitgeben, die Ihre Anwender später ändern dürfen. So definieren Sie etwa die Startseite des Browsers und veranlassen auf Wunsch sogar die Installation von Erweiterungen beim ersten Start des Browsers [5]. Voraussetzung hierfür ist, dass die Anwender Zugriff auf die Erweiterungen im Chrome Web Store oder auf eine andere URL haben, die zur gewünschten Chrome-Erweiterung in Form einer CRX-Datei führt.

Der Vorteil der JSON-Datei ist, dass Sie dem Browser so auch auf Systemen, die keiner AD-Domäne angehören, eine Erstkonfiguration mitgeben können. Doch bedenken Sie den Nachteil, dass die Vorgaben der "master_preferences" nur einmal beim ersten Start des Browsers ins Benutzerprofil einfließen und sich auf diesem Weg nachträglich keine Änderungen mehr verteilen lassen. Das Management per Gruppenrichtlinien oder CBCM ist folglich der flexiblere und komfortablere Ansatz.

Verwaltung per Gruppenrichtlinien

Die passenden Gruppenrichtlinienvorlagen und Sprachdateien finden Sie ebenfalls im Enterprise-Bundle unter ".\Google ChromeEnterpriseBundle64\Configuration\admx". Kopieren Sie die ADMX-Dateien an den zentralen Ablageort der Windows-Gruppenrichtlinienvorlagen unter "\\<Domain-Name>\SYSVOL\<Domain-Name>\Policies\PolicyDefinitions". Die zugehörigen ADML-Files befördern Sie je nach Sprache in die passenden Unterordner, mindestens in den Ordner "en-US" und auf einem deutschen System auch nach "de-DE".

Sollte es einen Ordner namens "PolicyDefinitions" in der SYSVOL-Freigabe Ihrer Domäne noch nicht geben, kopieren Sie ihn dorthin aus dem Pfad "C:\Windows\ PolicyDefinitions" von einem Domaincontroller oder einem anderen System, auf dem die Gruppenrichtlinienverwaltung (Group Policy Management Console, GPMC) installiert ist. Das hat den Vorteil, dass von nun an alle Instanzen der GPMC in Ihrer Domäne die identischen Vorlagen

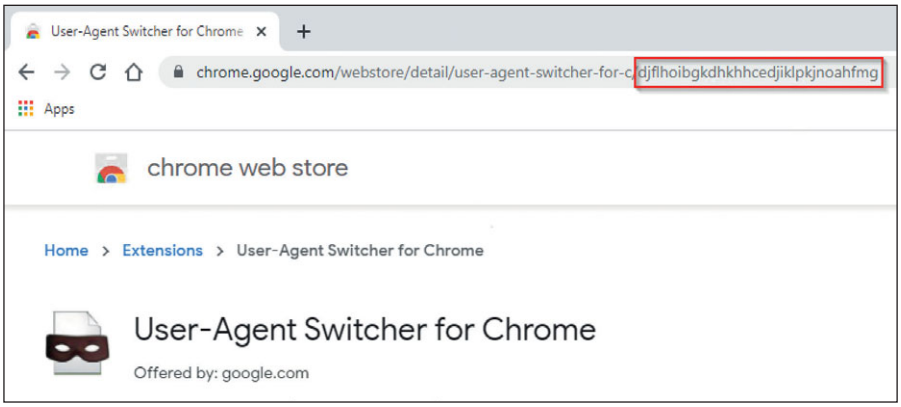

Bild 2: Die URL zu einer Extension im Chrome Web Store endet mit ihrer ID.

aus dem zentralen Speicher verwenden. Google liefert insgesamt sechs Vorlagendateien für Gruppenrichtlinien mit. Die Datei "google.admx" hat lediglich eine kosmetische Funktion. Sie sorgt dafür, dass der Gruppenrichtlinieneditor die Einstellungen aller weiteren Vorlagen in einem gemeinsamen Ordner zusammenfasst (Bild 1).

Zentrales Element ist die Datei "chrome.admx" mit über 200 Richtlinien zur Konfiguration des Browsers. Im Bereitstellungshandbuch beschreibt Google einige Beispielszenarien für Unternehmen unterschiedlicher Größenordnung und mit verschiedenen Anforderungen etwa an Einstellungen zu Datenschutz und Privatsphäre.

Diese finden Sie im Gruppenrichtlinieneditor sowohl im Bereich der Computerkonfiguration als auch unterhalb der Benutzerkonfiguration. Sie dürfen somit wählen, ob Sie die Einstellungen des Browsers pauschal pro Computer vornehmen oder auf Basis einzelner Benutzer oder Gruppen unterscheiden möchten.

Die Mehrzahl der Einstellungen liegt im Ordner "Google Chrome" und gibt die Konfiguration des Browsers fix vor, sodass Benutzer nicht davon abweichen können. Gegenüber dieser üblichen Funktionsweise von Gruppenrichtlinien ist aber eine Besonderheit erwähnenswert. Einige Einstellungen finden sich zusätzlich noch einmal unterhalb des Ordners "Google Chrome – Default Settings (users can override)". Ähnlich der Datei "master_preferences" können Sie Nutzern darüber für den ersten Start empfohlene Voreinstellungen mitgeben, von denen die Nutzer anschließend dann aber abweichen dürfen, indem Sie etwa den als Startseite definierten Webauftritt des Unternehmens durch ihren persönlichen Favoriten ersetzen.

Erweiterungen per Richtlinie verwalten

Ebenfalls eine Erwähnung wert sind die Optionen zur Verwaltung von Erweiterungen. Das umfangreiche Angebot an Extensions von Google selbst sowie von Drittanbietern im Chrome Web Store bietet reichlich Gelegenheit, den Browser um Funktionen zu ergänzen. Hier sollten Unternehmen steuern, was erlaubt ist und was nicht, und diese Richtlinien helfen ihnen dabei.

Sie legen über diese fest, ob Nutzer überhaupt Extensions installieren dürfen. Falls ja, schließen Sie unerwünschte Extensions anhand einer Block-List aus oder erlauben ausschließlich von Ihnen freigegebene Extensions mittels Allow-List. Unternehmenskritische Erweiterungen können Sie auf Wunsch zwangsweise installieren. Google empfiehlt, die Erweiterungen online aus dem offiziellen Chrome Web Store zu beziehen. Alternativ übergeben Sie auch hier eine eigene Quelle, die die gewünschte Chrome-Erweiterung als CRX-Datei bereitstellt. Die gesperrten, erlaubten oder sogar erzwungenen Erweiterungen tragen Sie mit ihrer jeweiligen ID in die mehrzeiligen Eingabemasken der entsprechenden Einstellungen im Gruppenrichtlinienobjekt ein.

Die ID finden Sie, indem Sie die jeweilige Erweiterung auf einem Referenzsystem installieren, im Browser die interne URL "chrome://extensions/" aufrufen und dann den Entwicklermodus aktivieren. Noch einfacher gelangen Sie an die ID, indem Sie die Webseite der Erweiterung im Chrome Web Store besuchen. Der 32 Zeichen lange String am Ende der URL entspricht der ID (Bild 2).

Pauschaler regeln Sie den Zugriff auf Erweiterungen mittels der Einstellung "Configure allowed app/extension types", die bestimmte Klassen erlaubt, etwa nur Themes. Die Einstellung "Extension management settings" gestattet oder verbietet Erweiterungen basierend auf den Rechten, die sie einfordern. So sperren Sie etwa alle Erweiterungen, die Zugriff auf USB-Schnittstellen verlangen. Bereits vorhandene Erweiterungen würde Chrome damit zwar nicht deinstallieren, aber deaktivieren. Die Syntax der entsprechenden Re-

Apple macOS und Linux

Im Fall von Windows-Endpunkten innerhalb einer AD-Domäne sind Gruppenrichtlinien der optimale Weg zur zentralen Konfiguration. Doch wie steht es um Instanzen des Chrome-Browsers unter Apple macOS oder verschiedenen Linux-Distributionen? Google unterstützt offiziell macOS für x86- und ARM-Prozessoren sowie Linux in 64-Bit-Varianten als DEB-Paket für Debian- und Ubuntu-Plattformen sowie als RPM-Paket für Fedora- und OpenSUSE-Plattformen. Auch für diese Endpunkte stellt Google Installationspakete des Browsers mitsamt passenden Kurzanleitungen bereit.

Die Beispiele für entsprechende Konfigurationsdateien sind allerdings im ZIP-Archiv des Chrome Browser for Enterprise-Bundles für Windows versteckt. Darin finden Sie für macOS die Property-List-Beispieldatei "com.google.Chrome.plist", deren XML-Code Sie nach Ihren Wünschen anpassen können. Anschließend wandeln Sie die Datei mit einem Konvertierungstool Ihrer Wahl in ein Konfigurationsprofil um, das Sie schließlich in eine MDM-Lösung einbinden.

Für Linux-Systeme dient die bereits erwähnte Datei "master_preferences" als Vorlage. Sie können daraus für jede Richtlinie, die Sie festlegen möchten, eine separate JSON-Datei erzeugen und anschließend auf Ihre Endpunkte kopieren. Richtlinien im Ordner "/etc/opt/chrome/policies/recommended" wirken als Empfehlung, von der ein Anwender abweichen darf. Vorgaben aus dem Ordner "/etc/opt/chrome/policies/managed" sind verpflichtend, Benutzer können sie nicht ändern.

geln beschreibt Google detailliert in einem separaten Dokument [6].

Updates und weitere Funktionen

Die übrigen ADMX-Vorlagen kümmern sich um optionale Funktionen. So versorgt der Dienst "Google Update", ebenfalls im Computerkontext, mit allen Einstellungen aus der "GoogleUpdate.admx" längst nicht nur den Browser Chrome, sondern auch diverse andere Produkte, wie etwa Google Drive oder Google Earth. Da Google ab Chrome 92 von einem sechswöchigen auf einen vierwöchigen Veröffentlichungszyklus für neue Versionen wechselt, empfiehlt der Hersteller, die automatischen Updates zu nutzen. Die Größe eines initialen Installationspakets gibt Google mit ungefähr 56 MByte an, während eine Aktualisierung der Hauptversion 10 bis 15 MByte und kleinere Patches lediglich zwischen 0,5 und 3 MByte beanspruchen.

Die Datei "LegacyBrowserSupport.admx" ist nur noch aus Gründen der Kompatibilität mit älteren Versionen im Paket enthalten. Sie benötigen diese für aktuelle Versionen von Chrome nicht mehr, da die Funktionen des Legacy Browser Supports inzwischen fester Bestandteil des Browsers und die zugehörigen Einstellungen in der Datei "chrome.admx" enthalten sind. Lassen Sie "LegacyBrowserSupport.admx" daher einfach weg, um Verwirrung im Gruppenrichtlinieneditor zu vermeiden. Die zugehörigen Einstellungen existieren nur im Computerkontext und steuern, wann Chrome Webseiten in alternativen Browsern öffnet.

Auch die Settings für den User-Agent Switcher for Chrome aus "ChromeUASwitcher.admx" beziehen sich auf die Computerkonfiguration und funktionieren nur, wenn Sie zusätzlich die entsprechende Erweiterung installieren.

Zu guter Letzt sind die Einstellungen aus "PasswordAlert.admx" nur im Benutzerkontext der Gruppenrichtlinien verfügbar. Sie steuern die erweiterte Passwortwarnung, eine Open-Source-Lösung zum Schutz vor Phishing-Angriffen. Die setzt allerdings eine weitere Chrome-Extension

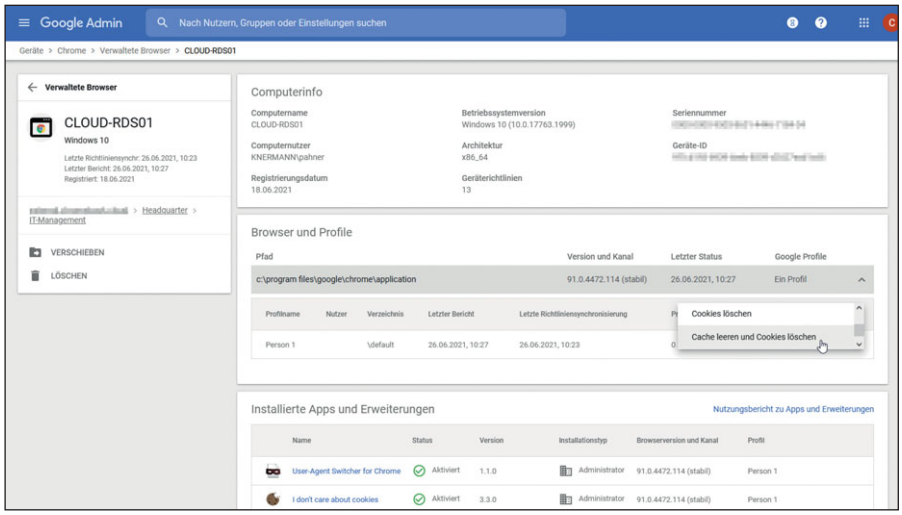

Bild 3: Die optionalen Nutzerberichte liefern detaillierte Informationen zu Browser-Instanzen mitsamt Apps und Erweiterungen.

sowie im Backend Googles Server für Passwortwarnungen voraus.

Mittels eines solchen Servers können Sie Alarme per E-Mail versenden und Anwender veranlassen, das Passwort ihres Google-Accounts zu ändern, falls sie es versehentlich auf einer nicht vertrauenswürdigen Website eingegeben haben [7].

Plattformübergreifend aus der Cloud

Gruppenrichtlinien sind praktisch, wenn ein AD den Rahmen bildet. Möchten Sie jedoch auch Endpunkte außerhalb einer Domäne verwalten und kommen in heterogenen Umgebungen macOS oder Linux hinzu, wird die Verwaltung schnell mühsam und unübersichtlich. Dem möchte Google mit dem Chrome Browser Cloud Management (CBCM) begegnen, einem kostenlosen Dienst, mit dem Sie Instanzen des Browsers plattformübergreifend konfigurieren können. Schaltzentrale ist die webbasierte "Google Admin Console", die uns schon beim Management von Chromebooks begegnet ist [8]. Mit Hilfe der Konsole konfigurieren Sie den Browser, Apps und Erweiterungen.

Ihre Anwender können sich optional mittels ihrer E-Mail-Adresse im Browser authentifizieren. Im Rahmen der Registrierung an der Konsole müssen Sie daher mindestens eine Domain verifizieren. Für viele größere Provider erledigt die Konsole dies halbautomatisch. Ansonsten fordert Google Sie auf, einen bestimmten TXT-Record als Eigentumsnachweis im DNS einzutragen [9].

Die Konsole verwaltet Benutzer und Browser hierarchisch in Organisationseinheiten (OE), die wahlweise die Aufbauorganisation, die logische oder geografische Struktur Ihres Unternehmens abbilden. Nutzerkonten legen Sie im einfachsten Fall direkt in der Konsole an. Alternativ synchronisiert der Google Cloud Directory Sync (GCDS) einen generischen LDAP-Server oder ein AD mit der Cloud. Außerdem versteht sich die Google Admin Console auch auf die Bereitstellung von Identitäten aus sowie den Single Sign-On (SSO) an einem Azure AD.

Clients registrieren

Unser Interesse gilt dem Bereich "Geräte/Chrome / Verwaltete Browser". Dort finden Sie links die Struktur Ihrer OEs und können pro OE über das gelb umrandete Plus-Zeichen unten rechts auf der Seite ein Registrierungs-Token generieren. Das bietet Ihnen die Konsole im Klartext, als Reg-Datei für Windows-Clients sowie als Textdatei für macOS und Linux an. Das Token finden Sie anschließend auch im Bereich "Geräte / Chrome / Registrierungstokens" wieder.

Dieses Token verwenden Sie anschließend, um Ihre Client-Browser in der gewünschten OE zu registrieren. Unter Windows importieren Sie nach der Installation von Chrome die REG-Datei oder verteilen die darin enthaltenen Informationen per

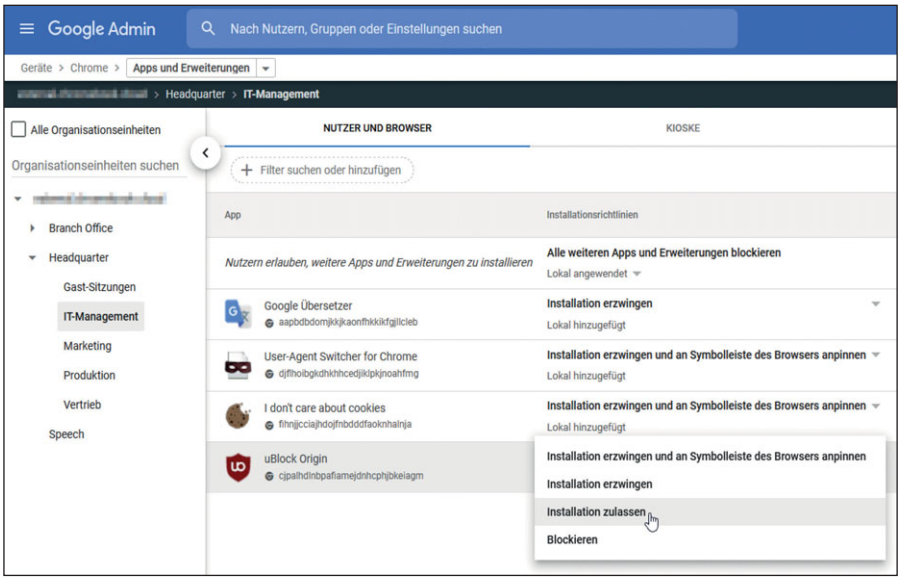

Bild 4: Die Google Admin Console verwaltet Erweiterungen komfortabel mit grafischem Frontend.

Gruppenrichtlinie. Einem Computer unter macOS weisen Sie das Token per MDM-Profil zu oder einfach, indem Sie die zugehörige Text-Datei im lokalen Pfad "/Library/Google/Chrome/" ablegen. Für Linux-Clients lautet der Pfad "/etc/opt/chrome/policies/registration".

Sobald Sie den Browser nun starten, registriert er sich automatisch in der gewünschten OE innerhalb der Google Admin Console. Das Registrierungstoken ist nur einmalig erforderlich. Sie können es später gefahrlos zurückrufen und durch ein anderes ersetzen. Die Browser bleiben jeweils mit einer individuellen Geräte-ID, ihrem Computernamen, Betriebssystem sowie der Betriebssystemversion in der Konsole registriert.

Einstellungen setzen, Berichte erstellen

Pro OE nehmen Sie im Bereich "Geräte / Chrome / Einstellungen" Ihre Konfiguration vor, die sich von oben nach unten über die OEs vererbt. Um in der Vielzahl an Optionen nicht den Überblick zu verlieren, filtern Sie hier auf die Plattform "Chrome für Computer". Dann zeigt Ihnen die Konsole sämtliche Einstellungen, die den Desktop-Browser betreffen. Im Gegensatz zu Gruppenrichtlinien setzen die Clients Einstellungen, die Sie hier vornehmen, praktisch ohne Zeitverzögerung sofort um.

Zu beachten ist, dass Clients in der Gegenrichtung standardmäßig keine Informationen an die Google Admin Console übermitteln. Möchten Sie sich zentral einen Überblick darüber verschaffen, welche Versionen von Chrome und welche Erweiterungen auf den Clients vorhanden sind, müssen Sie dies explizit aktivieren. Navigieren Sie dazu auf der Registerkarte "Nutzer- und Browsereinstellungen" zum Bereich "Nutzerberichte" und wählen Sie dort die Option "Cloud-Berichterstellung für verwaltete Browser aktivieren".

Daraufhin erhalten Sie detaillierte Sichten pro Client und sehen, welche Version von Chrome aus welchem Update-Kanal installiert ist, welches Benutzerprofil aktiv ist und auch welche Apps und Erweiterungen installiert sind. Die Admin-Konsole liefert Ihnen außerdem eine Liste der Apps und Erweiterungen über alle Clients hinweg. Weiterhin können Sie einer Chrome-Instanz Kommandos schicken und sie veranlassen, ihren Cache zu leeren, Cookies zu löschen oder beides (Bild 3).

Extensions verwalten

Extensions verwalten Sie im separaten Bereich "Geräte / Chrome / Apps und Erweiterungen". Gegenüber den Gruppenrichtlinien und Textdateien gelingt die Konfiguration hier deutlich intuitiver (Bild 4). Über das Plus-Zeichen unten rechts wählen Sie erwünschte oder zu blockierende Erweiterungen in einem grafischen Dialog mit Suchfunktion direkt aus dem Chrome Web Store.

Die globale Einstellung zuoberst blockiert auf Wunsch alle weiteren Extensions. Alternativ können Sie über das Zahnrad-Symbol am Ende der Zeile Extensions detaillierter anhand der von Ihnen angeforderten Berechtigungen sperren. Zukünftig plant Google, einen Workflow zu ergänzen, mit dem Benutzer sich Erweiterungen wünschen können, die der Admin dann zentral freigibt oder auch nicht.

Fazit

Google stellt seinem Chrome-Browser umfangreiche Funktionen zur zentralen Verwaltung zur Seite, und das sogar kostenlos. Mittels Gruppenrichtlinien oder Textdateien bleibt die Konfiguration komplett lokal, erfordert aber, Einstellungen ganz oder teilweise in JSON und XML zu notieren. Gerade in heterogenen Umgebungen gerät dies schnell komplex und unübersichtlich. Wer extern gehostete Cloudanwendungen nicht scheut, greift stattdessen zur Google Admin Console und dem Chrome Browser Cloud Management. Das erledigt die Konfiguration zahlreicher Chrome-Instanzen mitsamt Erweiterungen komfortabel grafisch und plattformübergreifend. *(ln)*

Link-Codes

[1] Browser-Marktanteile in Deutschland
l9za1

[2] Chromium-Projekt
l9za2

[3] Download Google Chrome für Unternehmen
l9za3

[4] Bereitstellungshandbuch für Chrome (Windows)
l9za4

[5] Chrome-Extensions vorinstallieren
l9za5

[6] Chrome-Extensions im Unternehmen verwalten
l9za6

[7] Phishing-Angriffe auf Nutzer verhindern
l9za7

[8] IT-Administrator 05/2021: Google Chrome OS im Unternehmen verwalten
l7z76

[9] Chrome-Verwaltung über die Cloud
l9za9