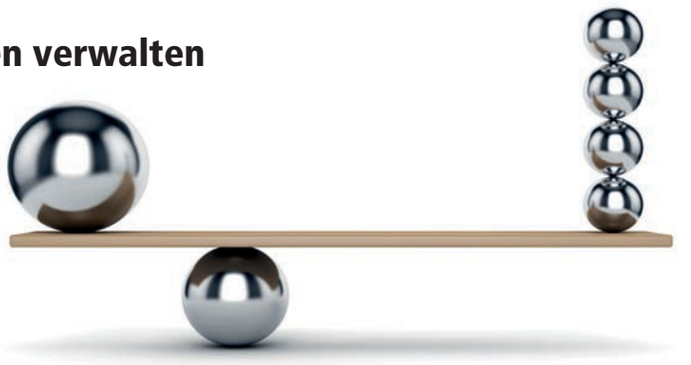
Google Chrome OS im Unternehmen verwalten

Glänzend aufgestellt



Quelle: Konstantin Faraktinov – 123RF

von Dr. Christian Knermann

Geräte mit Googles Betriebssystem Chrome OS haben sich vom spartanischen Webclient zu einer Plattform entwickelt, die sich inzwischen über den Bildungssektor hinaus steigender Beliebtheit in Unternehmen erfreut. Dazu tragen eine breite Palette an Hardware sowie ein umfangreiches Angebot an Erweiterungen und Apps bei. IT-Administrator hilft, das Chrome-Ökosystem und dessen Verwaltung im Unternehmen auf eine solide Basis zu stellen.

Mit der Vision eines modernen und sicheren Betriebssystems für die Cloudära ist Google vor nunmehr zehn Jahren angetreten und hat das erste Chromebook mit Chrome OS vorgestellt. Schaffte es der damalige Prototyp "Cr-48" – in der Chemie das Chrom-Isotop mit der Nukleonenzahl 48 – nicht in den europäischen Markt, ist heutzutage ein breites Spektrum unterschiedlicher Hardware von mehreren Herstellern verfügbar. Zu den Chromebooks in Form von Notebooks, Convertibles und Tablets diverser Größen gesellen sich Chromebases genannte All-in-one-Systeme sowie als Chromeboxen bezeichnete Mini-PCs.

Anfangs etablierten sich die Chromebooks vor allem als günstige Alternative im Bildungssektor, wo sie auch heute noch sehr verbreitet sind. Das Angebot startet mit Geräten auf Basis von ARM-Prozessoren bereits bei Preisen unter 300 Euro, während Business-Geräte mit Intel- oder AMD-Prozessoren sowie üppiger Ausstattung an RAM und SSD-Speicher Preisschilder jenseits von 1000 Euro tragen.

Mit dem hauseigenen Pixelbook tritt Google selbst als Hardware-Anbieter in Erscheinung, vermarktet die Geräte hierzulande jedoch offiziell nicht, sondern setzt auf Drittanbieter. So haben viele namhafte Hersteller inzwischen Geräte mit Chrome OS im Programm – darunter Acer, Asus, Dell, HP, Lenovo oder auch Samsung. Allen gemeinsam ist, dass sie die Geräte entsprechend der Spezifikation von Google fertigen. Äußerlich fällt auf, dass die Geräte ohne Funktionstasten auskommen und auch auf die Feststelltaste verzichten. An deren Stelle tritt eine Such-Taste und die oberste Reihe der Tastatur bilden einige Sondertasten für Aktionen innerhalb des Browsers sowie Funktionen der Hardware wie Helligkeit und Lautstärke.

Ein Titan sorgt für Sicherheit

Deutlich spannender ist aber der Blick unter die Haube, wo sich in allen seit Anfang 2019 vorgestellten Chromebooks der "Titan C"-Sicherheitschip findet [1]. Der ist vergleichbar mit dem Trusted Platform Module (TPM) in herkömmlichen Endgeräten und geht doch über dessen Funktionalität hinaus.

Titan C verifiziert den kompletten Bootvorgang und sorgt dafür, dass ein Gerät ausschließlich das von Google signierte, unveränderte Chrome OS startet und nur ebenso signierte Betriebssystemupdates akzeptiert. Dazu errechnet das System einen Hash-Wert über den Firmware-Code und überprüft, ob dieser mit dem von Google bereitgestellten signierten Hash-Wert übereinstimmt. Die derart verifizierte Firmware überprüft auf dieselbe Art den Kernel, der wiederum allen weiteren Code und den Chrome-Browser verifiziert.

Betriebssystem ohne Altlasten

Wer erstmals mit Chrome OS in Berührung kommt, wird zuerst die Geschwindigkeit bemerken, mit der das System startet. Ein Chromebook ist bereits nach sechs bis sieben Sekunden einsatzbereit. Neustarts benötigen selbst mit der Installation von Updates nicht viel länger.

Dies liegt darin begründet, dass der Hersteller Chrome OS grundlegend neu und anders als alle bisherigen Betriebssysteme entwickelt hat. So blickt Microsoft bei Windows, beginnend bei den Wurzeln von Windows NT, inzwischen auf eine über dreißigjährige Geschichte zurück. Linux-Derivate sind nicht viel jünger und auch Apples macOS feierte in diesem Jahr bereits seinen zwanzigsten Geburtstag seit dem Neustart auf UNIX-Basis. Zwar finden sich in den Entwicklungsgeschichten all dieser Systeme Einschnitte, die teilweise mit der Kompatibilität zu früheren Versionen brechen, doch tragen alle ihr Erbe mit sich.

Demgegenüber hat Google Chrome OS von Grund auf neu konzipiert mit Fokus auf Webanwendungen und die Sicherheit im Hinblick auf Admin-Rechte sowie die Installation von Anwendungen und Updates. So wie der Browser Chrome auf dem Open-Source-Projekt Chromium aufsetzt, basiert auch Chrome OS auf einem maßgeblich von Google gepflegten Open-Source-System, dem Chromium OS [2]. Im Gegensatz zu Letzterem ist Chrome

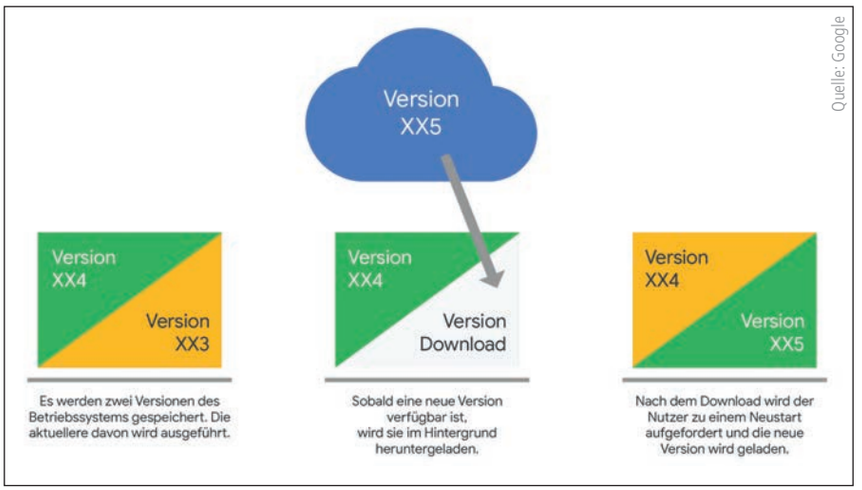


Bild 1: Chrome OS minimiert Downtimes, indem es Updates im Hintergrund in eine zweite, inaktive Partition installiert.

OS aber ein proprietäres System, das Google zwar aus der Entwicklung von Chromium OS ableitet, jedoch um Closed-Source-Komponenten ergänzt, insbesondere die Verknüpfung mit der Firmware und dem Sicherheitschip nach der eigenen Hardwarespezifikation.

Nur verifizierte Updates möglich

Die Architektur des Systems besteht aus mehreren Schichten, beginnend mit der Firmware über das Betriebssystem bis hin zu Browser, Apps und Datenhaltung. Auf der Anwendungsschicht laufen jede App, jeder Tab des Browsers Chrome und auch jede einzelne Domain innerhalb der Tabs in einer isolierten Sandbox [3].

Das Betriebssystem ist grundsätzlich schreibgeschützt und aus der Anwendungsschicht heraus nicht direkt veränderbar. Um trotzdem Updates zu ermöglichen, residieren jeweils zwei Versionen von Chrome OS in separaten Partitionen. Die Firmware bootet das aktuellere dieser beiden Betriebssysteme.

Stehen Betriebssystemupdates an, was typischerweise alle sechs Wochen der Fall ist, installiert das System diese in der inaktiven Partition und überschreibt damit die ältere Version von Chrome OS. Beim nächsten Neustart bootet das System dann von der aktualisierten Partition (Bild 1). Hierbei wacht der Titan-Chip darüber, dass ausschließlich von Google signierte, nicht kompromittierte Updates ihren Weg auf das System finden.

Google-Account nach wie vor obligatorisch

Der Schwerpunkt lag zunächst darauf, das System als Client für die hauseigenen Webanwendungen des Google Workspace (ehemals G-Suite genannt), wie Google Docs, Präsentationen und Tabellen, zu verwenden. E-Mail-Dienst und -client der Wahl war dabei natürlich Gmail und die bevorzugte Plattform zum Speichern, Synchronisieren und Teilen von Daten Google Drive.

Die Benutzeroberfläche zeigte sich entsprechend minimalistisch und bestand aus nicht vielmehr als dem Browser für eine rein weborientierte Arbeitsweise, die sich deutlich von allen übrigen Betriebssystemen unterschied und eine dauerhafte Onlineverbindung voraussetzte.

Wer heutzutage als einzelner Benutzer ein Chromebook einsetzen möchte, sollte weiterhin eine gewisse Affinität zum Portfolio von Google mitbringen, denn abseits einer temporären Gastsitzung, die zu nicht viel mehr als Browsen taugt, ist ein Google-Account obligatorisch. Das System ist aber längst nicht allein auf die Dienste und Anwendungen von Google beschränkt.

Zusammenspiel mit Android und Linux

Das Betriebssystem bedient sich inzwischen gleich mehrerer Quellen, um seinen Funktionsumfang auszubauen. Zunächst sind dabei die nativen Erweiterungen für Chrome OS aus dem Chrome Web Store und Progressive Web Apps (PWA) zu nennen. Also Anwendungen, die im Kern auf HTML5, CSS und JavaScript setzen, sich aber trotzdem wie native Apps verhalten und in Grenzen auch offline verwendbar sind. Zusätzlich hat Google 2016 seinen Play Store in Chrome OS integriert und das System so für Android-Apps ertüchtigt. Viele Apps im Play Store, von Google selbst und auch von Drittanbietern, sind aber unter der Haube inzwischen PWAs. Diese sind schneller und benötigen weniger Speicherplatz als ihre nativen Android-Pendants.

PWAs und Android-Apps laufen im Vollbild oder in unterschiedlich dimensionierten Fenstern und vertragen sich auch mit Touchscreen, Tastatur und Trackpads der Geräte – jedoch nur sofern die Entwickler dafür Sorge tragen. Das kann dazu führen, dass manche Apps von kleineren Software-Anbietern sich auf dem Chromebook nicht so verhalten wie gewünscht. Gängige Android-Apps sowie PWAs fügen sich aber sehr gut unter Chrome OS ein und bieten den Anwendern so viele Freiheiten. Wer Dokumente lieber in Microsoft Word bearbeiten, seine Notizen Evernote anvertrauen oder Dateien in Dropbox speichern möchte, ist mittels der entsprechenden Apps nicht auf das Google-Ökosystem festgelegt, wie in Bild 2 gezeigt.

Eine derzeit noch als Beta deklarierte Option erlaubt zudem die Ausführung von Linux-Anwendungen in einer auf Debian 10 (Buster) basierenden virtuellen Umgebung, ähnlich dem von Windows 10 bekannten Windows Subsystem for Linux (WSL). In diesem Fall greift allerdings das ansonsten konsequente Sandboxing von Chrome OS nicht vollends. Alle Linux-Applikationen teilen sich eine Sandbox und sind nicht gegeneinander abgeschottet [4].

Zentrales Verwalten mit Chrome Enterprise

Individuellen Nutzern öffnet Chrome OS somit bereits viele Anwendungsmöglichkeiten. Für den Unternehmenseinsatz in größerem Maßstab stellt sich aber die Frage, ob und wie sich hunderte oder gar hunderttausende Chromebooks in ein

zentrales Management einfügen. Dazu hat Google im Rahmen des "Chrome Enterprise"-Programms in der Cloud die passende Lösung parat.

Mittels der "Google Admin Console" in der Cloud verwalten Sie nahezu beliebig viele Endpunkte zentral [5]. Als Administrator verteilen Sie WLAN- und VPN-Konfigurationen, Systemeinstellungen, Chrome-Erweiterungen und Apps auf Ihre Geräte. Die Konsole selbst ist kostenlos, setzt allerdings voraus, dass die Geräte über die passende Enterprise-Lizenz verfügen. Die erhalten Sie auf zwei Wegen:

- Für den Unternehmenseinsatz konzipierte Geräte, typischerweise erkennbar am Begriff "Enterprise" im Produktnamen und am vergleichsweise höheren Kaufpreis, bringen die passende Option bereits ab Werk mit. In diesem Fall können Sie sich selbst für ein Unternehmenskonto und die Verwendung der Konsole bei Google registrieren, Ihre Domain verifizieren und anschließend Endgeräte einbinden [6].
- Günstigere Geräte ohne die Enterprise-Option registrieren sich nicht ohne Weiteres in der Adminkonsole. In diesem Fall müssen Sie sich zusätzlich pro Gerät ein Enterprise-Upgrade über einen Reseller beschaffen. Dabei richtet der Reseller auch den Adminzugang zur Konsole für Sie ein. Nur um das Registrieren der Geräte in Ihrem Unternehmenskonto müssen Sie sich dann noch selbst kümmern.

Eine dauerhafte Kauflizenz des Enterprise-Upgrades ist für 113 Euro erhältlich und gilt, solange das Endgerät lebt. Auf Mietbasis kostet die Lizenz 36 Euro pro Jahr. Sobald ein Gerät drei Jahre oder länger im Einsatz ist, empfiehlt sich folglich der Kauf.

Strukturen schaffen, Benutzer verwalten

Ohne weitere Vorbereitungen würde die Admin Console all Ihre Benutzer und Geräte innerhalb einer einzigen Organisationseinheit (OE) verwalten. Alle Einstellungen, die Sie vornehmen, wirken sich entsprechend auf diese OE und damit auf alle Objekte darin aus. Bevor Sie Benutzerkonten anlegen und Geräte registrieren, empfiehlt es sich daher, im ersten Schritt Ihre Organisation in der Google Admin Console abzubilden. So können Sie – ganz ähnlich der Anwendung von Gruppenrichtlinien im AD – bestimmten Benutzern und Endgeräten unterschiedliche Einstellungen zuweisen. Untergeordnete OEs erben dabei die Einstellungen von höheren Ebenen der Hierarchie, sofern Sie diese Vererbung nicht bewusst unterbrechen.

Wählen Sie auf der Startseite der Adminkonsole die Kachel "Organisationseinheiten" und erstellen Sie über das "+"-Symbol eine oder mehrere OEs sowie nach Bedarf weitere untergeordnete OEs darin. Die OEs können Sie auch nachträglich nach Belieben verschieben.

Navigieren Sie nun zurück zur Startseite und dann in den Bereich "Nutzer", wo Sie manuell neue Benutzerkonten hinzufügen können. Die Konsole fragt obligatorisch nach Vornamen, Nachnamen sowie E-Mail-Adresse und OE. Hierbei ist die oberste Hierarchieebene voreingestellt. Sie können den neuen Nutzer jedoch auch direkt in eine Ihrer zuvor erstellten Unter-OEs einsortieren. Weiterhin dürfen Sie ein initiales Passwort automatisch generieren oder manuell setzen und festlegen, ob der Nutzer bei der nächsten Anmeldung zur Passwortänderung aufgefordert wird.

Anfänglich hat nur Ihr primärer Nutzer, mit dem Sie sich zur Verwendung der Konsole bei Google registriert haben, die Rolle "Super Admin" inne und damit die volle Kontrolle. Rufen Sie aus der Liste

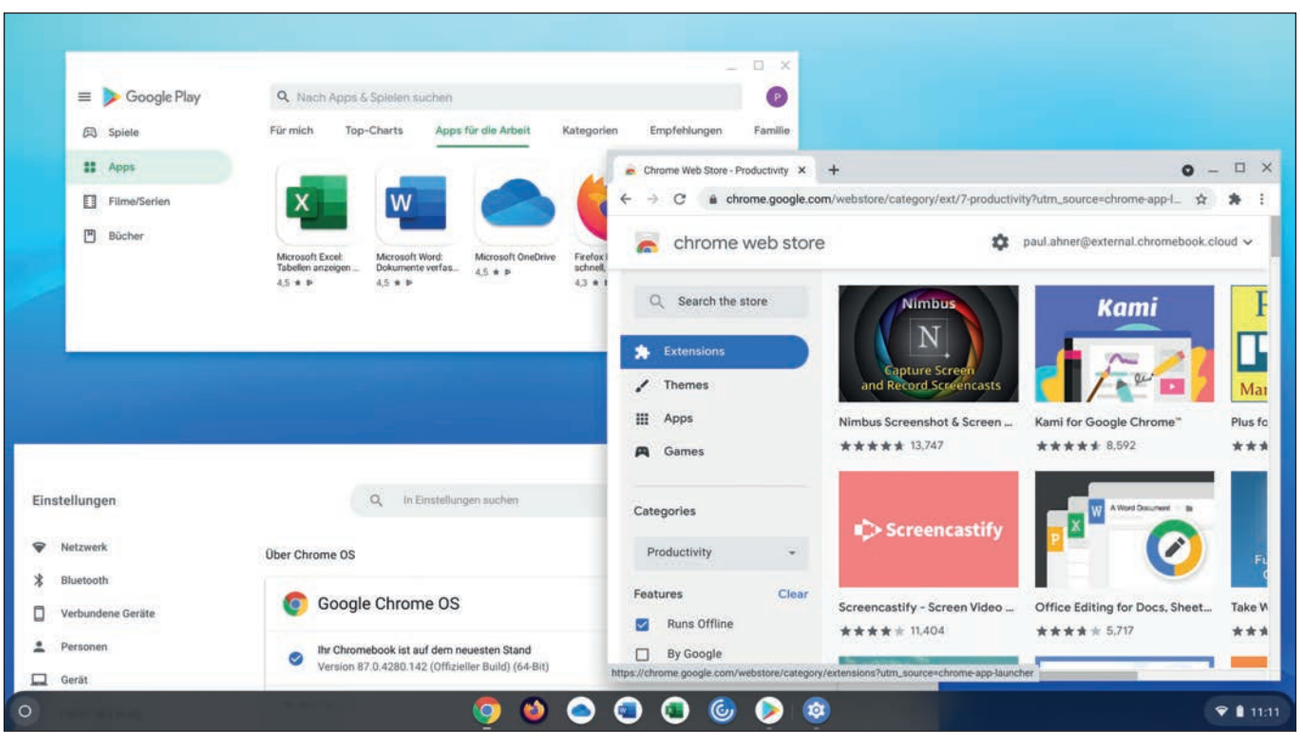


Bild 2: Erweiterungen aus dem Chrome Web Store sowie native Android-Apps und PWAs aus dem Google Play Store bauen den Funktionsumfang von Chrome OS aus.

aller Benutzer die Eigenschaften eines einzelnen Kontos auf, so können Sie dem Nutzer nach Bedarf Administratorrollen und -berechtigungen zuweisen. Dazu dürfen Sie aus einer Reihe an vordefinierten Rollen wählen oder auch benutzerdefinierte Rollen erstellen [7].

Über die Funktion "Bulk-Update für Nutzerliste" legen Sie massenhaft neue Nutzer an und aktualisieren ebenso mehrere bestehende Accounts in nur einem Arbeitsgang. Dazu bietet Ihnen die Konsole an, wahlweise alle bereits existierenden Benutzer zu exportieren oder eine leere Vorlage als CSV-Datei herunterzuladen. Nehmen Sie nach Bedarf Änderungen vor oder fügen Sie der Datei Zeilen mit neuen Benutzern hinzu. Anschließend laden Sie die Datei wieder hoch und die Konsole führt automatisch alle Änderungen aus, was laut Google für bis zu 150.000 Nutzer in einem Durchlauf funktioniert.

Wie Sie alternativ Benutzerkonten aus einem Azure Active Directory in die Welt von Google provisionieren und per Single-Sign-On (SSO) authentifizieren, beschreibt Google in einem Support-Artikel unter [8].

Geräte registrieren

Damit sind nun alle Voraussetzungen geschaffen, um Chromebooks zentral zu verwalten. Insbesondere zu Zeiten der Corona-Pandemie haben sich für Unternehmen die sogenannten "Zero Touch"-Geräte als praktisch erwiesen. Diese schicken Reseller auf Wunsch passend vorkonfiguriert zu den Endanwendern nach Hause. Sofern Sie nicht von einem Reseller Geräte beziehen, die schon ab Werk für Ihr Unternehmen vorkonfiguriert sind, erledigen Sie das im Zuge der Erstkonfiguration [9].

Ein Gerät unter Chrome OS, das erstmals startet, bietet Ihnen prominent in der Mitte des Bildschirms platziert an, das System für Sie persönlich oder mit passenden Spielregeln versehen für ein Kind zu konfigurieren. Eher unscheinbar in der unteren linken Ecke des Bildschirms positioniert finden Sie die Möglichkeit, das Gerät ohne Anmeldung als temporärer Gast zu nutzen, und daneben die "Enterprise-Registrierung" (in der englischen Benutzeroberfläche "Enterprise Enrolment").

Verbinden Sie das Gerät nun mit einem WLAN und melden Sie sich mit einem entsprechend berechtigten Nutzer an dem Gerät an. Das System registriert sich daraufhin in der Admin Console, wo es im Bereich "Geräte / Chrome-Geräte" erscheint. Es befindet sich zunächst auf der obersten Ebene Ihrer OE-Struktur, von wo Sie es nach Belieben in eine andere OE verschieben.

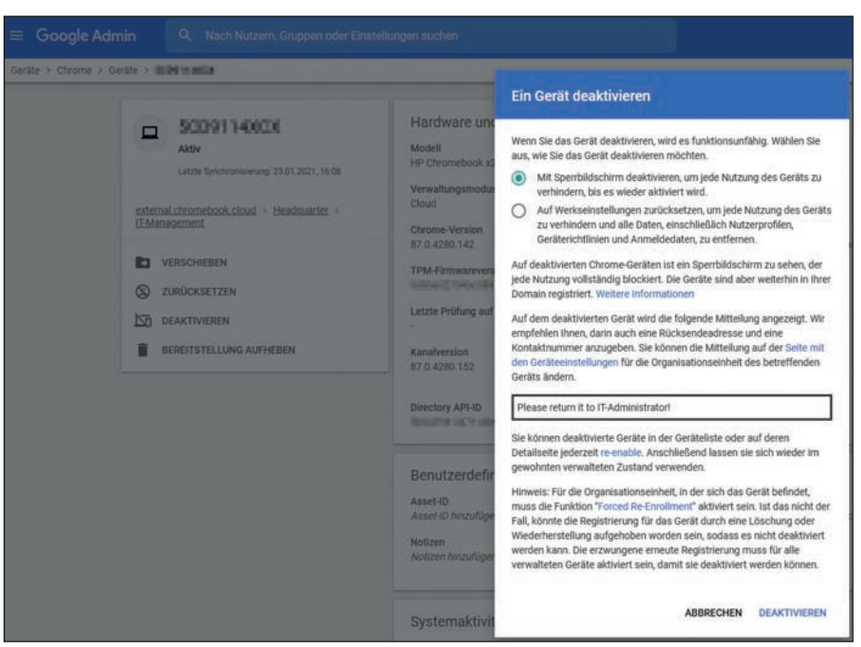


Bild 3: Keine Chance für Langfinger: Die Google Admin Console deaktiviert oder löscht Geräte bei Verlust.

Lokal präsentiert das Gerät nach erfolgreicher Registrierung einen weiteren Log-in-Prompt. Hier dürfen sich nun beliebige Nutzer aus Ihrer Organisation anmelden, um mit dem Gerät zu arbeiten. Vorher wollen wir aber Nutzern und Geräten innerhalb der Konsole Richtlinien zuweisen.

Netzwerke und VPN konfigurieren

Zurück in der Geräte-Ansicht der Admin-Konsole wählen Sie in der Hierarchie links im Bild die OE, für die Sie im Folgenden eine Konfiguration erstellen möchten. Am Ende des Pfades zuoberst auf der Seite finden Sie ein Dropdown-Menü. Hier sind insbesondere die Bereiche "Einstellungen", "Apps und Erweiterungen" sowie "Netzwerke" interessant.

In Letzterem verwalten Sie WLAN- und Ethernet-Verbindungen. Beide dürfen Sie sowohl an Geräte als auch an Nutzer zuweisen. Neben einfacher WEP-/WPA-/WPA2-Authentifizierung mittels Preshared-Key (PSK) versteht sich die zentrale Verwaltung auch auf Enterprise-Verschlüsselung (802.1x). Ebenso konfigurieren Sie an dieser Stelle VPN-Verbindungen für Nutzer und rollen manuell oder automatisiert mittels Simple Certificate Enrolment Protocol (SCEP) Zertifikate auf Ihre Geräte aus [10]. So wäre es denkbar, dass Sie ein separates WLAN mit einfachem Schutz per WPA2-PSK und direktem Internetzugriff nur zur Registrierung und Erstkonfiguration Ihrer Geräte verwenden und weitere Einstellungen für sichere Verbindungen ins Firmennetz dann über die Konsole ausrollen.

Kiosk für Gäste

Ist das Gerät im passenden Netz, geht es weiter im Bereich "Einstellungen". Die verteilen sich auf die drei Registerkarten "Nutzer- und Browsereinstellungen", "Geräteeinstellungen" sowie "Einstellungen für verwaltete Gastsitzungen". Letztere sind besonders praktisch etwa für öffentliche Rechner in Bibliotheken oder im Empfangsbereich.

Sie können eine solche Gastsitzung nicht nur zulassen, sondern auch deren automatischen Start erzwingen. Innerhalb der Gastsitzung belegen Sie dann den Browser

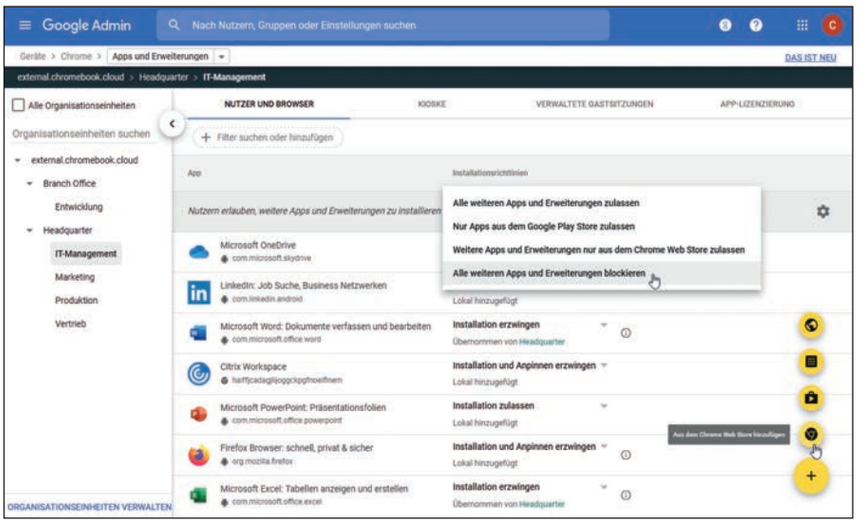


Bild 4: Die Google Admin Console verwaltet zentral sämtliche Erweiterungen sowie Apps und pinnt diese auf Wunsch auch gleich in der Taskleiste der Chrome-Geräte an.

mit restriktiven Voreinstellungen. Alternativ geben Sie im Bereich "Apps und Erweiterungen / Kioske" den Start einer beliebigen anderen App verbindlich vor, sodass Gäste nur bestimmte Seiten aufrufen oder die festgelegte Anwendung benutzen dürfen.

Diebstahl zwecklos

Auf der Registerkarte "Geräteeinstellungen" passen Sie die Computerkonfiguration umfassend an Ihre Anforderungen an. Hier steuern Sie den Zugriff auf USB-Geräte, Bluetooth-Verbindungen, sämtliche Einstellungen des Anmeldebildschirms und wie das System mit Updates umgeht. So können Sie Updates generell aktivieren oder deaktivieren, auf eine bestimmte Major-Version von Chrome OS beschränken und auch einen Zeitplan für die gestaffelte Einführung von Updates vorgeben. Ein solcher Plan sieht vor, dass nach einer wählbaren Frist von Tagen nur ein gewisser Prozentsatz aller Geräte in der OE die Updates installiert und erst nach einer weiteren Frist alle übrigen Geräte die Updates erhalten. Weiterhin dürfen Sie entscheiden, ob Geräte automatische Neustarts zur Installation der Updates ausführen sollen.

Besonders erwähnenswert sind die Einstellungen zu "Registrierung und Zugriff". Hier können Sie erzwingen, dass sich Systeme nach dem Löschen der Gerätedaten automatisch wieder in Ihrer Organisation registrieren. Zusätzlich dürfen Sie unter "Information zur Rückgabe deaktivierter Geräte" einen Freitext von bis zu 512 Zeichen eingeben für den Fall, dass ein Gerät verloren gehen sollte. In diesem Fall können Sie das System in der Geräte-Ansicht deaktivieren. Dabei bietet die Konsole an, das Gerät mit einem Sperrbildschirm zu versehen, um jede Nutzung des Geräts zu verhindern, bis es wieder aktiviert wird, oder es komplett auf Werkseinstellungen zurückzusetzen. So unterbinden Sie jede Nutzung des Geräts und entfernen alle Daten, einschließlich Nutzerprofilen, Geräterichtlinien und Anmeldedaten (Bild 3). Doch Vorsicht, wenn der betroffene Computer online ist, greift diese Einstellung umgehend und das Gerät ist unbrauchbar, bis Sie es wieder entsperren. Damit sind zentral verwaltete Geräte unter Chrome OS für Diebe völlig uninteressant.

Erweiterungen und Apps verteilen

Im Bereich "Geräte / Chrome / Apps und Erweiterungen" steuern Sie pro OE den weiteren Funktionsumfang, der Nutzern zur Verfügung steht. Hier legen Sie zunächst global fest, ob Nutzer selbsttätig Apps und Erweiterungen installieren dürfen. Das erlauben oder verbieten Sie pauschal. Alternativ bestimmen Sie, dass Nutzer entweder nur native Chrome-Erweiterungen aus dem Chrome Web Store oder nur Android-Apps sowie PWAs aus dem Google Play Store installieren dürfen.

Über das "+"-Symbol unten rechts auf der Seite fügen Sie der Konfiguration gezielt Chrome-Erweiterungen und Android-Apps hinzu. Dabei dürfen Sie die jeweilige Anwendung explizit blockieren oder Benutzern erlauben, sie im Self-Service zu installieren. Erweiterungen und Apps von besonderer Relevanz für Ihr Unternehmen installieren Sie automatisch und pinnen Sie optional auch gleich in der Startleiste von Chrome OS an (Bild 4).

Fazit

Geräte unter Chrome OS sind längst nicht mehr auf Anwendungen und Dienste aus dem Angebot von Google beschränkt und haben sich für viele Anwendungsfälle zu einer praxistauglichen Alternative entwickelt. Die Geräte sind mit minimalem Aufwand eingerichtet, im Fall von "Zero Touch" auch gänzlich ohne manuelle Interaktion. Chrome-Erweiterungen, native Android-Apps und PWAs bauen den Funktionsumfang aus und schlagen die Brücke zu Infrastrukturen abseits der Google-Welt. Mithilfe der Google Admin Console verwalten Sie auch eine größere Flotte an Chrome-Geräten, versorgen diese zentral mit Konfigurationen sowie Anwendungen und deaktivieren oder löschen die Systeme im Bedarfsfall aus der Ferne. *(jp)* IT

Link-Codes

[1] **Titan C**
l5p21

[2] **Chromium OS**
l5p22

[3] **Chromebook-Sicherheit durch Sandboxing**
l5p23

[4] **Linux auf einem Chromebook einrichten**
l5p24

[5] **Google Admin Console (Google Workspace-Konto erforderlich)**
l5p25

[6] **Bereitstellungshandbuch für Chrome-Geräte**
l5p26

[7] **Vordefinierte Administratorrollen**
l5p27

[8] **Google-Tutorial zu Single Sign-on über Azure AD**
l5p29

[9] **Zero-Touch-Registrierung**
l5p20

[10] **Netzwerke für verwaltete Geräte einrichten**
l5p2a