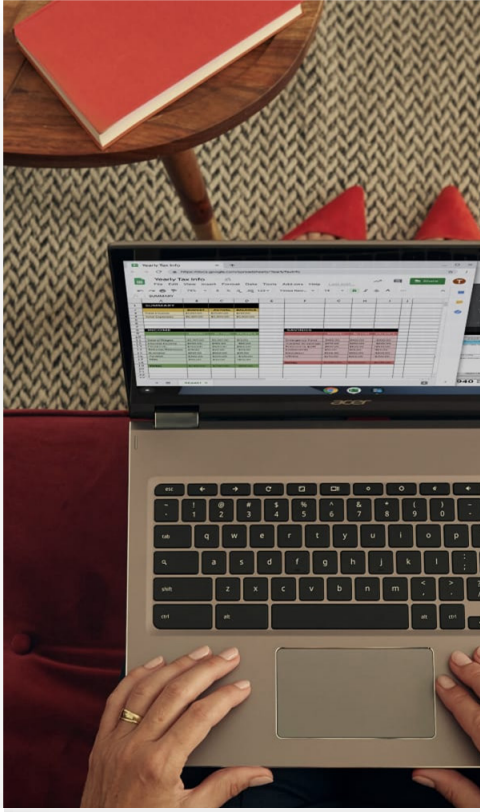
chrome

Konfigurationshandbuch für die Sicherheitseinstellungen von Google Chrome für Unternehmen

Basierend auf Chrome 90

chrome

Konfigurationshandbuch für die Sicherheitsein-stellungen von Google Chrome für Unternehmen



Basierend auf Chrome 90

Zuletzt aktualisiert: 20. Mai 2021

Ziel dieses Handbuchs

Obwohl die Ratschläge in diesem Dokument sich in erster Linie auf den Chrome-Browser unter Windows beziehen, treffen sie fast vollständig auch auf alle anderen Desktop-Plattformen zu. Gelegentlich müssen Administratoren die Vor- und Nachteile abwägen, wenn sie sich zwischen der Sicherheit ihrer Organisation und den von den Nutzern gewünschten Technologien und Funktionen entscheiden müssen.

Dieses Dokument beschreibt ausführlich die von Google Chrome bereitgestellten Sicherheitsrichtlinien sowie die Kompromisse, zwischen denen die Administratoren abwägen müssen, bevor sie die entsprechenden Richtlinien (de-)aktivieren.

Themen
Empfehlungen und wichtige Überlegungen für sicherheitsbewusste Organisationen beim (De-)Aktivieren von Sicherheitsrichtlinien in Google Chrome

Hauptzielgruppe
Administratoren von Microsoft® Windows® und Google Chrome

IT-Umgebung
Microsoft Windows 7 und höher

Kernpunkte
Abwägungen zwischen der Unternehmenssicherheit und den Auswirkungen auf die Nutzer bei der Konfiguration der Sicherheitsrichtlinien von Google Chrome

Einführung

Google Chrome ist als sicherer Browser konzipiert. Das Chrome-Team nimmt Sicherheit sehr ernst und kann mit Stolz behaupten, dass dieser Browser in Bereichen wie Sandbox-Funktionen, TLS-Standards und konfigurierbarer Sicherheit branchenführend ist.

Chrome ist sofort einsatzbereit – mit dem Ziel, ein Gleichgewicht aus Sicherheit und Nutzerfreundlichkeit zu bieten. Unternehmen haben leicht unterschiedliche Vorstellungen von der Sicherheit der Browser in ihren Organisationen. Dieses Dokument beschreibt einige Konfigurationsmöglichkeiten, mit denen Chrome diese individuellen Anforderungen erfüllen kann.

Die Standardeinstellungen von Chrome bieten ein ausgewogenes Verhältnis zwischen Sicherheit und Nutzerfreundlichkeit. Gelegentlich steht beides miteinander in Konflikt. In diesem Fall bietet Chrome Ihnen verschiedene Sicherheitsrichtlinien. Als IT-Administrator entscheiden Sie hierbei, welche Richtlinie sich für Ihren Zweck am besten eignet.

In diesem Dokument sind die Vor- und Nachteile in verschiedenen Situationen aufgeführt, in denen Sie zwischen Nutzerfreundlichkeit und Sicherheit wählen können. In all diesen Fällen sollten Sie beides gegeneinander abwägen und sich im Anschluss für diejenige Richtlinie entscheiden, die besser zu Ihrer Unternehmensumgebung passt.

Es werden drei verschiedene Sicherheitsanforderungen von Unternehmen beschrieben:

- Schutz vor Bedrohungen
- Datenschutz
- Verwaltung und Leistung

Viele der hier genannten Empfehlungen beziehen sich auf bestimmte Richtlinieneinstellungen. Die vollständige Dokumentation finden Sie unter https://chromeenterprise.google/policies.

Schutz vor Bedrohungen

Mit den folgenden Funktionen wird das Sicherheitsrisiko durch schädliche Websites bei Chrome minimiert:

- Dank der Website-Isolierung erhält jede Website einen unabhängigen Speicherplatz im Arbeitsspeicher (Betriebssystemprozess). In diesem Hilfeartikel finden Sie weitere Informationen.
- Sandbox-Technologien verringern dabei das Risiko, dass der Rest des Computers durch eine Schwachstelle beeinträchtigt wird.
- Die Funktion „Safe Browsing“ erkennt schädliche und betrügerische Inhalte/Software, indem sie das Web durchgehend scannt und Gefahren klassifiziert. Nutzer werden gewarnt, bevor sie eine Seite aufrufen, die als potenziell schädlich gekennzeichnet ist.

Chrome ist von Grund auf sicher konzipiert, sodass Nutzer durch die Standardeinstellungen im Internet besser geschützt sind. Darüber hinaus können Sie den Browser mithilfe der folgenden beiden Ansätze so konfigurieren, dass er zusätzlichen Schutz vor Bedrohungen bietet:

- Die Standardeinstellung von Chrome erzwingen, damit Nutzer sie nicht überschreiben können
- Durch Kompromisse bei der Nutzerfreundlichkeit für noch mehr Sicherheit sorgen

Die folgenden beiden Unterabschnitte beschreiben mögliche Konfigurationen innerhalb dieser Bereiche.

Bestehende Chrome-Standardeinstellungen erzwingen

Bei den Standardeinstellungen von Chrome hat die Sicherheit der Nutzer höchste Priorität. Einige dieser Einstellungen lassen sich bei Bedarf vom Nutzer ändern, was jedoch die Sicherheit beeinträchtigen kann. Daher können Administratoren diese Einstellungen durch eine entsprechende Richtlinie erzwingen.

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen

Ich möchte sicherstellen, dass bisherige Administratoren in unserer Organisation keine unsicheren Richtlinien aktiviert haben.	● –	● –	Um von den Vorteilen der (optimalen) Standardkonfiguration zu profitieren, stellen Sie sicher, dass die folgenden Richtlinien deaktiviert sind:
			
			`EnableDeprecatedWebPlatformFeatures`
			`RunAllFlashInAllowMode`
			`SuppressUnsupportedOSWarning`
			`EnableOnlineRevocationChecks`
			`OverrideSecurityRestrictionsOnInsecureOrigin`
			`CertificateTransparencyEnforcementDisabledForCas`
			`CertificateTransparencyEnforcementDisabledForLegacyCas`
			`LegacySameSiteCookieBehaviorEnabled`
			`LegacySameSiteCookieBehaviorEnabledForDomainList`
			`ChromeVariations`
			`DnsOverHttpsMode`
			`LookalikeWarningAllowlistDomains`
			`SafeBrowsingAllowlistDomains`
			`RemoteAccessHostAllowRemoteAccessConnections`
			
			Hierbei handelt es sich nicht um eine vollständige Liste aller Sicherheitsrichtlinien, sondern lediglich um solche, die von zahlreichen Unternehmen verwendet werden. Weitere Richtlinien finden Sie in der Liste der Chrome Enterprise-Richtlinien.

Ich möchte sicherstellen, dass Nutzer keine fundamentalen Sicherheitsfunktionen deaktivieren können.	● –	● –	Aktivieren Sie die folgenden Richtlinien: `AllowOutdatedPlugins`, `SafeBrowsingProtectionLevel` und `ThirdPartyBlockingEnabled`. Für die Nutzer wird sich hierdurch nichts ändern; sie können lediglich keine Änderungen an diesen Einstellungen mehr vornehmen.

Bestehende Chrome-Standardeinstellungen erzwingen (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich möchte Nutzer vor Malware-Downloads und Phishing schützen und sicherstellen, dass sie diese Sicherheitseinstellungen nicht überschreiben können.	Gering	–	Die Chrome-Funktion „Safe Browsing“ bietet Schutz vor Malware-Downloads und Phishing. Unter Safe Browsing in Chrome verwenden finden Sie weitere Informationen. Einige Unternehmen neigen dazu, diese Funktion zu deaktivieren, da sie ihre bestehenden Sicherheitsprodukte (Antivirenprogramm, Firewall) als ausreichend einstufen. Doch Safe Browsing lässt sich mit Ihrer Lösung kombinieren. So prüfen Antivirenprogramme vor allem den Inhalt von Downloads, während Safe Browsing vielmehr den Kontext in den Fokus rückt – d. h. die Kette an Verknüpfungen, die den Nutzer zum betreffenden Link geführt hat. Wenn Sie diese Funktion deaktivieren, können Sie nicht länger von diesem Wissen profitieren. Das Chrome-Team empfiehlt Ihnen daher, Safe Browsing aktiviert zu lassen. Indem Sie die Richtlinie `SafeBrowsingProtectionLevel` auf „1“ setzen, können Sie Nutzer davon abhalten, sie zu deaktivieren. Sie ist in den Standardeinstellungen aktiviert. Dadurch sollten keine sichtbaren Auswirkungen auf den Nutzer entstehen. In M79 haben wir das erweiterte Safe Browsing in den Chrome-Einstellungen angekündigt – eine neue Option für Nutzer, die eine zusätzliche Sicherheitsebene beim Surfen im Web benötigen bzw. möchten. Das Aktivieren dieser Funktion erhöht den Schutz vor schädlichen Websites und Downloads beträchtlich. Indem Daten in Echtzeit über das erweiterte Google Safe Browsing geteilt werden, profitieren Chrome-Nutzer von einem proaktiven Schutz vor schädlichen Seiten. Sie können das erweiterte Safe Browsing aktivieren, indem Sie `SafeBrowsingProtectionLevel` auf „2“ setzen.

Bestehende Chrome-Standardeinstellungen erzwingen (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich möchte Nutzer vor Malware-Downloads und Phishing schützen und sicherstellen, dass sie diese Sicherheitseinstellungen nicht überschreiben können.	Gering	–	Sie können das erweiterte Safe Browsing auch mit der folgenden Einstellung bedingungslos erzwingen: `DisableSafeBrowsingProceedAnyway` Dies wirkt sich insofern auf Nutzer aus, als dass sie davon abgehalten werden, weitere Seiten aufzurufen, wenn die Safe Browsing-Funktion eine Website fälschlicherweise als Phishingversuch eingestuft hat. Wenn Sie möchten, können Sie zusätzlich die Richtlinie `DownloadRestrictions` auf „2“ setzen, um Safe Browsing etwas strenger zu erzwingen. Weitere Informationen finden Sie unter Download schädlicher Dateien verhindern. Einige Unternehmen haben sogar die Druckfunktion deaktiviert, da sie gespeicherte PDFs als potenzielle Träger von Malware einstufen. Das Chrome-Sicherheitsteam hält dies nicht für sinnvoll. In nahezu allen Fällen zerstört die Konvertierung einer Website in ein PDF jegliche schädliche Inhalte, wobei wir die Nutzung eines sicheren PDF-Viewers für solche Dateien empfehlen (z. B. Chrome selbst).
Ich möchte eine Drittanbieter-Software verwenden, bei der Code in Chrome eingeschleust werden muss.	Hoch	Hoch	Chrome hält Drittanbieter-Software auf dem PC davon ab, ihren eigenen Code in Chrome einzuschleusen. Solche Drittanbieter-Einschleusungen haben sich als wesentliche Quelle von Abstürzen und Programmfehlern erwiesen, die (theoretisch) von Betreibern schädlicher Websites ausgenutzt werden können. Wir empfehlen daher die Standardeinstellung (`ThirdPartyBlockingEnabled` True). Andere Sicherheitsprogramme empfehlen Ihnen möglicherweise, die Blockierung ihres Codes aufzuheben, um Chrome steuern oder die Einstellungen beeinflussen zu können. Tun Sie dies, können Sie zwar von deren Funktionalität profitieren; gleichzeitig steigt jedoch auch die Absturzrate und das Risiko ausnutzbarer Schwachstellen. Wenn Sie ein Sicherheitsprogramm verwenden, bei dem ausführbarer Code in Chrome eingeschleust wird, wenden Sie sich bitte an Ihren Anbieter. Dieser kann prüfen, ob die gewünschte Funktionalität stattdessen über eine Chrome-Erweiterung bereitgestellt werden kann.

Nutzerfunktionalität beschränken, um die Angriffsfläche zu reduzieren

Sie können die Funktionalität von Chrome ändern, um die Angriffsfläche für schädliche Websites zu verringern. Jedes blockierte Element bedeutet dabei eine funktionale Beeinträchtigung für die Nutzer.

Viele dieser Änderungen haben zur Folge, dass Chrome-Funktionen deaktiviert werden. Wir möchten betonen, dass alle Funktionen so entwickelt wurden, dass sie sofortigen Schutz bieten – weshalb es nicht nötig sein sollte, sie zu deaktivieren. Dennoch sind wir uns dessen bewusst, dass zahlreiche Unternehmen bestimmte Änderungen vornehmen möchten bzw. müssen. Daher finden Sie im Folgenden einige Hinweise, um Ihnen diesbezügliche Entscheidungen zu erleichtern.

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Meine Organisation verfügt über eigene vertrauenswürdige Root-Zertifikate auf Endpunkten, um auf Unternehmensserver zuzugreifen. Falls Angreifer den privaten Schlüssel für diese vertrauenswürdigen Zertifikate stehen sollten, möchte ich in der Lage sein, diese zu sperren.	Gering	–	Sperrüberprüfungen für solche Zertifikate können Sie wie folgt aktivieren: `RequireOnlineRevocationChecksForLocalAnchors` Chrome kann nicht dafür garantieren, dass Zertifikate auf Grundlage lokaler Anchors erkannt werden können – dies hängt von der Einrichtung des Betriebssystems ab und funktioniert anders je nach Plattform und Version. Sollte die Sperrung nicht zugänglich sein, können die Zertifikate nicht verwendet („hard-fail“) und Websites möglicherweise nicht aufgerufen werden.
Ältere Versionen von Chrome, die in meiner Umgebung laufen, könnten von schädlichen Websites angegriffen werden.	Gering	–	Mit den folgenden Richtlinien können Sie einen Neustart von Chrome erzwingen, um für schnellere Updates zu sorgen: `RelaunchNotification` und `RelaunchNotificationPeriod`. Diese sind im Rahmen einer Unternehmensumgebung dringend zu empfehlen – nur so können Sie sicher sein, dass Ihre Nutzer immer die aktuelle Chrome-Version mit den neuesten Sicherheitsupdates verwenden.
Ich möchte unbedingt vermeiden, dass die Passwörter von Nutzern im Internet aufgrund älterer Authentifizierungsprotokolle („Digest“, „Basic Auth“) abgefangen werden könnten.	Gering	–	Sie können diese alten Schemas mit `AuthSchemes` deaktivieren. Nur wenige moderne Websites nutzen sie, sodass es in einer Unternehmensumgebung Sinn ergibt, diese zu deaktivieren. Ab Chrome 75 empfehlen wir „NTLM“ und „Negotiate“. Stellen Sie außerdem sicher, dass die Dienste in Ihrem Unternehmen moderne Authentifizierungsmechanismen verwenden.

Nutzerfunktionalität beschränken, um Angriffsfläche zu reduzieren (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich möchte verhindern, dass Dokumente aus der Cloud die Sicherheitslücken von Druckern ausnutzen können.	Gering	–	Mit der folgenden Richtlinie können Sie dafür sorgen, dass Ihre Unternehmensdrucker keine Dokumente von Google Cloud Print empfangen können: `CloudPrintProxyEnabled`.
Ich habe Bedenken, dass Angreifer, die bereits im Netzwerk sind, das WPAD-Protokoll gefährden und sich lateral ausbreiten könnten.	Gering	–	Sie können `ProxyMode` nutzen, um Proxy Auto-Discovery zu deaktivieren.
Ich habe Bedenken, dass das automatische Herunterladen von Dateien eine Gelegenheit für Angreifer darstellen könnte, unvorhergesehene DLL-Angriffe durchzuführen oder Passwort-Hashes an schädliche SMB-Server weiterzugeben. Ich möchte die automatischen Downloads deaktivieren.	Mittel	–	Um Nutzer zu jedem Download explizit aufzufordern, verwenden Sie `PromptForDownloadLocation`.
Ich möchte 3D-Grafiken deaktivieren, da sie meiner Meinung nach die Angriffsfläche vergrößern. Außerdem werden sie nur von wenigen Websites benötigt, die unsere Nutzer verwenden.	Mittel	–	Sie können 3D-Grafiken mithilfe der Richtlinie `Disable3DAPIs` deaktivieren. Chrome bietet bereits signifikante Risikominderungen gegen 3D-Grafik-Angriffe, darunter eine Ebene namens „ANGLE“. Ihre Aufgabe ist es, 3D-Eingaben zu säubern und jeglichen GPU-bezogenen Code in einem Sandbox-Prozess zu isolieren. Die Deaktivierung von WebGL beeinträchtigt virtuelle Globus- und Kartenprodukte.
Ich möchte das Risiko verringern, dass Daten einer Website durch Seitenkanalangriffe über eine andere Website abgegriffen werden können.	Mittel	–	Mit `IsolateOrigins` können Sie die Website-Isolierung noch genauer einstellen. Weitere Informationen erhalten Sie unter Daten mit Website-Isolierung schützen. Hinweis: Bei dieser Einstellung wird mehr Arbeitsspeicher verbraucht.

Nutzerfunktionalität beschränken, um Angriffsfläche zu reduzieren (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich möchte vermeiden, dass externe Nutzer über Chrome Remote Desktop die Möglichkeit haben, Computer in unserem Netzwerk zu steuern.	Mittel	–	Die Chrome Remote Desktop-App kann auf dieselbe Weise blockiert werden wie jede andere App oder Erweiterung. Weitere Informationen finden Sie unter Verwendung von Chrome Remote Desktop regeln.
Ich möchte Erweiterungen und Apps deaktivieren, da sie meiner Meinung nach die Angriffsfläche vergrößern. Außerdem macht es mir nichts aus, in die Workflows der Nutzer einzugreifen.	Hoch	Gering	Die Produktivität der Nutzer wird durch das Blockieren aller Erweiterungen erheblich beeinflusst. Darüber hinaus erhöhen einige Erweiterungen tatsächlich die Sicherheit der Nutzer, beispielsweise ein Drittanbieter-Passwortmanager für persönliche Passwörter. Wir empfehlen Ihnen, Erweiterungen nach Berechtigung zu verwalten: 1. Blockieren Sie ausschließlich solche Erweiterungen, deren geforderte Berechtigungen Sie für riskant halten. 2. Für alle anderen Erweiterungen blockieren Sie lediglich den Zugriff auf vertrauliche Hosts. So können Sie beispielsweise alle Erweiterungen zulassen, die weder die Webcam nutzen noch den Bildschirm aufnehmen. Zusätzlich können Sie andere Erweiterungen daran hindern, auf Ihre wichtigsten Unternehmensseiten zuzugreifen. Weitere Informationen finden Sie unter Berechtigungen für Chrome-Apps und Erweiterungen und Erweiterungen im Unternehmen verwalten. Außerdem können Sie Ihren Chrome Enterprise-Experten kontaktieren, wenn Sie eingehender darüber informiert werden möchten, weshalb dieser Ansatz für Unternehmen sinnvoll ist. Wenn Sie keine spezifischen Berechtigungen ausfindig machen können, die Sie beunruhigen, können Sie mit der Richtlinie `ExtensionInstallBlacklist` auch direkt bestimmte Erweiterungen blockieren. Der Wert „*“ in der Sperrliste gibt an, dass alle Erweiterungen ausgeschlossen sind, sofern sie nicht ausdrücklich auf die Zulassungsliste gesetzt wurden. Ziehen Sie in Betracht, einen Genehmigungsprozess für zusätzliche Erweiterungen einzurichten. Das Blockieren/Genehmigen bestimmter Erweiterungen ist aufgrund der unzureichenden Skalierung nicht zu empfehlen. Alle Chrome-Erweiterungen müssen entweder direkt aus dem Chrome Web Store oder auf Grundlage der unten beschriebenen Mechanismen bereitgestellt werden. Hier finden Sie weitere Informationen zu externen Erweiterungen. Über `BlockExternalExtensions` können Sie die Installation externer Erweiterungen verhindern.

Nutzerfunktionalität beschränken, um Angriffsfläche zu reduzieren (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich möchte Nutzer davon abhalten, Ausnahmen hinzuzufügen, um gemischte Inhalte für bestimmte Seiten zuzulassen.	Hoch	Gering	Über „DefaultInsecureContentSetting" können Sie die Verwendung von Ausnahmen bei unsicheren Inhalten regeln. Ist diese Richtlinie nicht konfiguriert, dürfen Nutzer Ausnahmen hinzufügen, um blockierbare gemischte Inhalte zuzulassen und das automatische Upgrade auf HTTPS von optional blockierbaren gemischten Inhalten zu deaktivieren.
Ich möchte Probleme, die womöglich aufgrund der Cookies oder des Cache auf dem Nutzergerät entstanden sind, per Fernzugriff beheben.	Hoch	–	Über die Admin-Konsole können Sie Remote-Befehle senden, um Cookies oder den Cache zu löschen.

Datenschutz

Datenschutz steht bei Chrome an erster Stelle. Viele Unternehmen möchten so wenig personenidentifizierbare Informationen oder personenbezogene Daten (zusammenfassend als „personenidentifizierbare Informationen“ bezeichnet) wie möglich auf PCs speichern. Sie wissen häufig nicht, dass Chrome diese Daten schützt.

Einige der stärksten Sicherheitsfunktionen von Chrome, z. B. „Safe Browsing“ und Passwortmanager, müssen Informationen mit Google-Diensten austauschen. Das Chrome-Sicherheitsteam empfiehlt Ihnen daher dringend, diese Funktionen zu aktivieren. Wenn Sie in Bezug auf die Verwendung der übermittelten Daten Bedenken haben, lassen Sie sich von Ihrem Chrome Enterprise-Experten hierzu beraten.

Die benötigten Informationen teilen sich in drei Kategorien:

- Auf Unternehmensgeräten gespeicherte personenidentifizierbare Informationen
- Daten, die ins Internet gesendet werden
- Daten, die an Google gesendet werden

Einstellungen zu personenidentifizierbaren Informationen, die auf Unternehmensgeräten gespeichert sind

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich fürchte, dass andere Nutzer (**keine Administratoren**) auf sensible Daten wie auf dem Laufwerk gespeicherte Passwörter einer Person zugreifen können, wenn sie (entweder später oder gleichzeitig per VDI) auf demselben Computer angemeldet sind wie die betroffene Person. Ich fürchte, dass Computer gestohlen und auf der Festplatte befindliche Passwörter ausgelesen werden.	–	–	Alle personenbezogenen Daten (Browserverlauf, Cache, Passwörter, Autofill-Daten) werden gebündelt im sogenannten „Profil“ des Nutzers gespeichert. Solche Profile werden durch Standard-Berechtigungsmodelle des Betriebssystems geschützt, sodass andere Nutzerkonten normalerweise nicht darauf zugreifen können. Falls ein anderer Nutzer oder ein Dieb uneingeschränkten Zugriff auf den Computer hat, könnte diese Person solche Dateien möglicherweise lesen. Doch die empfindlichsten Teile des Chrome-Profils – darunter Passwörter und Kreditkartendetails – sind mit der Data Protection API (DPAPI) von Microsoft verschlüsselt, die speziell auf Datenschutz ausgelegt ist. Daten können daher von Administratoren oder anderen Personen, die vollen Zugriff auf das Laufwerk haben, nicht eingesehen zu werden. Außerdem wird das Anmeldepasswort des Nutzers für die Verschlüsselung der Daten verwendet. Detaillierte Informationen dazu finden Sie in der DPAPI-Dokumentation von Microsoft. Nur wenn Administratoren Zugriff auf die privaten Schlüssel auf einem Domaincontroller haben, sind sie theoretisch in der Lage, diese Daten zu entschlüsseln. Besondere Schritte wären demnach nur erforderlich, wenn Sie sich über Folgendes Gedanken machen: • Administratoren oder solche Personen, die physischen Zugriff auf das Laufwerk haben • Zugriff auf Daten wie den Browser-Cache oder andere Teile des Chrome-Profils, die nicht verschlüsselt sind Weitere Informationen im Fall diesbezüglicher Bedenken finden Sie in der nächsten Zeile.

Einstellungen zu personenidentifizierbaren Informationen, die auf Unternehmensgeräten gespeichert sind (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich fürchte, dass **Administratoren**, die sich auf demselben Computer anmelden (entweder später oder gleichzeitig per VDI), Zugriff auf sensible Daten wie den Browser-Cache anderer Nutzer auf dem Laufwerk dieses Computers haben.	Hoch	–	Dies ist ein sehr spezieller Fall, gegen den sich die meisten Unternehmen nicht schützen. Hinweis: Die meisten sensiblen Daten wie Passwörter und Kreditkartennummern unterliegen nicht dieser Art von Zugriff – siehe vorherige Zeile. Sollten Sie weiterhin Bedenken haben, die den Administratorzugriff auf sensible Profilbereiche wie den Browser-Cache betreffen, nutzen Sie die Richtlinie `ForceEphemeralProfiles` und erzwingen Sie gleichzeitig die Anmeldung des Nutzers in Chrome (`ForceBrowserSignin`), sodass seine wichtigen Lesezeichen und sonstigen Einstellungen jedes Mal heruntergeladen werden. Außerdem können Sie `BackgroundModeEnabled` deaktivieren, falls Sie die einzelnen Sitzungen zeitlich begrenzen möchten. Die Auswirkungen auf den Nutzer sind hoch, da er sich stets aufs Neue anmelden muss, um Chrome zu verwenden. Außerdem beeinträchtigt es die Leistung, da Profilinformationen und Cache bei jeder Nutzung neu heruntergeladen bzw. aufgebaut werden müssen. Hier finden Sie weitere Informationen zum flüchtigen Modus. Um weitere Informationen zu erhalten, kontaktieren Sie bitte Ihren Chrome Enterprise-Experten. Einige Unternehmenskunden entscheiden sich dafür, keine Cookies dauerhaft zu behalten, und ändern daher die Einstellung der Richtlinie `DefaultCookiesSetting`. Dies können wir nicht empfehlen, da es die normalen Abläufe im Internet enorm beeinträchtigt. Außerdem kann es schwerwiegende Sicherheitsprobleme nach sich ziehen, da Nutzer ihre Passwörter öfter als nötig eingeben müssen, wodurch sich das Phishingrisiko erhöht. Ein Administrator mit bösartigen Absichten oder jemand mit physischem Zugriff auf den Computer könnte Keylogger, anderweitige Spyware oder sogar ein falsches Chrome-Binärprogramm installieren. Diese Antwort bezieht sich vor allem auf den Zugriff auf Profildaten auf dem Laufwerk und stellt keine vollständige Lösung von Problemen mit Administratoren dar, die bösartige Absichten hegen. Eine umfassendere Lösung, die über Chrome hinausgeht, sind verschlüsselte Nutzer-Basisverzeichnisse.

Einstellungen zu personenidentifizierbaren Informationen, die auf Unternehmensgeräten gespeichert sind (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich fürchte, dass jemand beim physischen Zugriff auf einen entsperrten Computer die Passwörter eines anderen Nutzers sehen kann.	● Hoch	● Hoch	Einige Unternehmen deaktivieren den Passwortmanager in Chrome, indem sie die Richtlinie `PasswordManagerEnabled` auf inaktiv setzen. Wir empfehlen, den Passwortmanager aktiviert zu lassen. Damit erleichtern Sie es Ihren Nutzern, starke Passwörter auf verschiedenen Websites zu verwenden – und dies ist einer der wichtigsten Beiträge, die Sie für die Sicherheit Ihrer Nutzer leisten können. Unter Einstellungen zu Daten, die an Google gesendet werden finden Sie weitere Informationen zu Verwaltungsoptionen für Passwörter. Stattdessen empfehlen wir Ihnen, Richtlinien zu Displaysperren auf dem Betriebssystem einzurichten und sicherzustellen, dass das System über starke Passwörter verfügt.

Einstellungen zu Daten, die ins Internet gesendet werden (Datenverlust)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich möchte Uploads verhindern.	–	–	Derzeit bietet Chrome keine Richtlinienoptionen an, mit denen sich der Upload von Dateien verhindern lässt. Beachten Sie insbesondere, dass `AllowFileSelectionDialogs` in diesem Fall nicht zum gewünschten Ziel führt, da Uploads immer noch über Drag-and-drop oder andere Mechanismen durchgeführt werden können.

Einstellungen zu Daten, die ins Internet gesendet werden (Datenverlust) (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich möchte die Aktivitäten meiner Nutzer im Blick behalten, um verdächtiges Verhalten frühzeitig zu erkennen.	–	–	Sie können den Ressourcenverbrauch des Chrome-Browsers, den Anmeldestatus, Verbindungen, Nutzungsmuster und das Surfverhalten erfassen. Weitere Informationen finden Sie unter Verwendung des Chrome-Browsers unter Windows erfassen.
Ich möchte Chromecast deaktivieren, um sicherzustellen, dass vertrauliche Daten ausschließlich auf dem Hauptbildschirm des Computer angezeigt werden können.	Mittel	–	Passen Sie die Richtlinie `EnableMediaRouter` an.
Ich möchte Websites daran hindern, Video- oder Audioaufnahmen zu machen (beispielsweise über WebRTC).	Mittel	–	`VideoCaptureAllowed` und `AudioCaptureAllowed` sollten in diesem Fall deaktiviert werden. In Kombination mit den Richtlinien „AllowedUrls“ können Sie zusätzlich eine Zulassungsliste erstellen. Unternehmen wird gelegentlich empfohlen „WebRTC zu deaktivieren“. Man kann das WebRTC-Stack nicht vollständig deaktivieren. Es ist deshalb vorteilhafter, die spezifischen Sensoren zu deaktivieren, die in Ihrem Unternehmen als Risiko gelten. Wir gehen davon aus, dass in Zukunft weitere Tools für Videokonferenzen und Telefonie ins Internet verlagert werden, weshalb Sie damit rechnen sollten, dass die Auswirkungen auf Ihre Nutzer mit der Zeit ein immer größeres Ausmaß annehmen werden. Aus diesem Grund empfiehlt es sich, diese Entscheidung in einem Jahr noch einmal zu überdenken.
Ich möchte Websites daran hindern, eine Aufnahme vom Bildschirm zu machen.	Mittel	–	Aktuelle Chrome-Versionen stellen ohne eine Erweiterung keine APIs für die Bildschirmfreigabe bereit. Diese APIs werden voraussichtlich in Zukunft für Websites verfügbar sein, unterliegen dabei jedoch der in der vorherigen Empfehlung genannten Richtlinie `VideoCaptureAllowed`. Um in diesem Punkt auf den neuesten Stand zu bleiben, kontaktieren Sie bitte Ihren Chrome Enterprise-Experten.

Einstellungen zu Daten, die ins Internet gesendet werden (Datenverlust) (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich möchte schädliche Websites davon abhalten, den Lesezugriff anzufragen, um auf serielle Ports zuzugreifen – auch dann, wenn dies den Zugriff für legitime Websites sperrt.	Mittel	–	Über `DefaultSerialGuardSetting` können Sie die Nutzung der File System API für den Lesezugriff regeln. Wenn die Richtlinie auf „3“ gesetzt ist, dürfen Websites über die File System API den Lesezugriff auf Dateien und Verzeichnisse im Dateisystem des Host-Betriebssystems anfragen. Ist sie auf „2“ gesetzt, wird der Zugriff verweigert. Wenn sie nicht konfiguriert ist, können Websites den Zugriff anfragen, aber Nutzer können diese Einstellung ändern.
Ich möchte schädliche Websites davon abhalten, über die File System API den Lesezugriff auf Dateien und Verzeichnisse im Dateisystem des Host-Betriebssystems anzufragen – auch dann, wenn dies den Zugriff für legitime Websites sperrt.	Mittel	–	Über `DefaultFileSystemReadGuardSetting` können Sie die Nutzung der File System API für den Lesezugriff regeln. Wenn die Richtlinie auf „3“ gesetzt ist, dürfen Websites über die File System API den Lesezugriff auf Dateien und Verzeichnisse im Dateisystem des Host-Betriebssystems anfragen. Ist sie auf „2“ gesetzt, wird der Zugriff verweigert. Wenn sie nicht konfiguriert ist, können Websites den Zugriff anfragen, aber Nutzer können diese Einstellung ändern.
Ich möchte schädliche Websites davon abhalten, den Zugriff auf und die Nutzung von Bewegungs- und Lichtsensoren anzufragen – auch dann, wenn dies den Zugriff für legitime Websites sperrt.	Mittel	–	Über `DefaultSensorsSetting` können Sie die Nutzung der Standard-Sensoreinstellungen regeln. Wenn die Richtlinie auf „1“ gesetzt ist, dürfen Websites auf Sensoren wie Bewegungs- und Lichtsensoren zugreifen und diese nutzen. Ist sie auf „2“ gesetzt, wird der Zugriff auf alle Sensoren verweigert. Wenn sie nicht konfiguriert ist, gilt die Richtlinie „AllowSensors“, aber Nutzer können diese Einstellung ändern.

Ich möchte schädliche Websites davon abhalten, auf USB- oder Bluetooth-Geräte zuzugreifen – auch dann, wenn dies den Zugriff für legitime Websites sperrt.	Mittel	Mittel	`DefaultWebUsbGuardSetting`
			`DefaultWebBluetoothGuardSetting`
			
			Möglicherweise benötigen einige Websites für die Multi-Faktor-Authentifizierung den Zugriff auf Hardware-Tokens über USB oder Bluetooth. Wenn Sie USB oder Bluetooth deaktivieren, beeinträchtigen Sie unter Umständen die Sicherheit solcher Websites.

Einstellungen zu Daten, die ins Internet gesendet werden (Datenverlust) (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich möchte schädliche Websites davon abhalten, auf Informationen zum Standort zuzugreifen – auch dann, wenn dies den Zugriff für legitime Websites sperrt.	Hoch	Gering	Sie deaktivieren den Standortzugriff über die Richtlinie: `DefaultGeolocationSetting` Dies beeinträchtigt die Nutzererfahrung enorm. Außerdem ist denkbar, dass der Standort für bestimmte Websites als Sicherheitsfaktor gilt, weshalb eine Deaktivierung auch die Sicherheit beeinträchtigen könnte.
Ich möchte Drittanbieter-Websites davon abhalten, unsere Nutzer im Web per Tracking zu verfolgen.	Hoch	Gering	Einige Unternehmen deaktivieren Drittanbieter-Cookies über die Richtlinie `BlockThirdPartyCookies`. Dies kann zur Beeinträchtigung einiger Websites führen, darunter auch Webdienste zur Authentifizierung, weshalb die Richtlinie sich unter Umständen negativ auf die Sicherheit auswirken könnte.

Einstellungen zu Daten, die an Google gesendet werden

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich möchte Chrome davon abhalten, Informationen an die DNS-Server von Google weiterzugeben.	–	–	Es herrscht die Annahme, dass die Richtlinie `BuiltInDnsClientEnabled` deaktiviert werden müsste, um die Nutzung der DNS-Server von Google durch Chrome zu verhindern. Das ist falsch – diese Option bezieht sich ausschließlich auf den clientseitigen Software-Stack am Endpunkt und hat keine Auswirkungen darauf, welche Server verwendet werden. Unter keinen Umständen wird der Google-DNS-Stack mit Google-Servern kommunizieren – es sei denn, der Endpunkt wurde entsprechend konfiguriert. In Bezug auf den Datenschutz gibt es für Unternehmen keinen Grund, diese Option zu ändern.
Ich möchte verhindern, dass vertrauliche Informationen über Abstürze und Nutzungsaktivitäten an Google gesendet werden.	Gering	–	Sie können das anonyme Crash Reporting mit der Richtlinie `MetricsReportingEnabled` deaktivieren. Die erfassten Messwerte sind jedoch anonym. Indem Sie die Berichterstellung zulassen, kann Google Ihre Anforderungen und Stabilitätsprobleme besser verstehen, wodurch Ihr Unternehmen entsprechend profitiert.
Ich möchte nicht, dass Google auf den PCs in meiner Organisation nach Malware sucht.	Gering	Gering	`ChromeCleanupReportingEnabled` ist für die Steuerung der Berichterstellung und die Übermittlung der entsprechenden Informationen an Google zuständig. Die separate Richtlinie `ChromeCleanupEnabled` regelt, ob Chrome nach Malware sucht, und fordert den Nutzer im Bedarfsfall auf, diese zu entfernen. Mit diesen beiden Richtlinien können Sie separat darüber entscheiden, ob Sie den integrierten Malware-Entfernungsdienst von Chrome nutzen und die Erkennungsdaten an Google senden möchten.
Ich möchte nicht, dass vertrauliche Dokumente über Google an Cloud-Drucker gesendet werden.	Mittel	–	Passen Sie die Richtlinie `CloudPrintSubmitEnabled` an. Weitere Informationen finden Sie in diesem Hilfeartikel.
Ich möchte nicht, dass Benachrichtigungstexte über Google-Dienste gesendet werden.	Mittel	–	Einige Unternehmen deaktivieren Benachrichtigungen mit der Richtlinie `DefaultNotificationsSetting`, damit der Benachrichtigungstext nicht über die Back-End-Dienste von Google gesendet werden muss. Weitere Informationen finden Sie in diesem Whitepaper.

Einstellungen zu Daten, die an Google gesendet werden (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich möchte nicht, dass Google unsere Passwörter kennt.	● Mittel	● Mittel	Wir empfehlen Ihnen dringend, den Passwortmanager für Ihre Nutzer zu aktivieren. Nutzer können damit leichter starke Passwörter verwenden, wodurch Ihre Sicherheit im Ganzen profitiert. Weitere Informationen finden Sie im NCSC-Beitrag zu Passwortmanagern. Wenn die Synchronisierung in Chrome ausgeschaltet ist, werden Passwörter nicht an Google gesendet. Sie werden lediglich auf dem Endpunkt gespeichert und per Anmeldepasswort des Nutzers verschlüsselt, sodass sie auch von Personen mit physischem Zugriff auf das Laufwerk nicht gelesen werden können (siehe vorherige Antworten zu personenidentifizierbaren Informationen auf dem Endpunkt). Wenn die Synchronisierung in Chrome eingeschaltet ist, werden diese Passwörter standardmäßig in der Google-Infrastruktur gespeichert. Dabei nehmen wir die Sicherheit dieser Informationen sehr ernst. Lediglich in bestimmten Situationen – wie z. B. aus rechtlichen Gründen – kann es notwendig sein, diese weiterzugeben. Weitere Information dazu, wie Sie ganz einfach verhindern können, dass Google auf diese Daten zugreifen kann, finden Sie im nächsten Abschnitt weiter unten. Generell möchten wir Unternehmensnutzern mit dem Passwortmanager die Möglichkeit bieten, sich bestmöglich zu schützen. Falls Sie weitere Funktionen oder Einstellungen wünschen, die für Sie ausschlaggebend wären, um den Passwortmanager zu aktivieren, lassen Sie sich von Ihrem Google Chrome Enterprise-Experten hierzu beraten. Einige Unternehmen entscheiden sich dafür, die Option zum Importieren von Passwörtern aus anderen Browsern zu deaktivieren (`ImportSavedPasswords`). Wie bei Passwortmanagern im Allgemeinen halten wir es für wichtig, dass die Verwendung starker Passwörter für die Nutzer so einfach wie möglich gemacht wird. Daher empfehlen wir, die Importfunktion beizubehalten.

Einstellungen zu Daten, die an Google gesendet werden (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich möchte nicht, dass Google die Profildaten unserer Nutzer kennt – einschließlich Passphrasen und Lesezeichen.	Mittel	Mittel	Ihre Nutzer können eine Passphrase für die Synchronisierung festlegen, über die ihr Profil (Passwörter, Lesezeichen usw.) verschlüsselt wird. So werden diese Informationen nicht in Klartextform hochgeladen. Hier erhalten Sie weitere Informationen. Wenn Ihre Nutzer eine Passphrase festlegen, können sie ihre Chrome-Daten in der Google-Cloud speichern und darüber synchronisieren, ohne dass Google sie lesen kann. Neue Geräte erfordern die Eingabe dieser Passphrase durch den Nutzer. Außerdem hat dies Auswirkungen auf den synchronisierten Verlauf und beeinträchtigt daher den Workflow. Derzeit bietet Chrome keine Richtlinien an, um solch eine Passphrase zu erzwingen. Wenn Sie weitere Fragen haben, lassen Sie sich von Ihrem Chrome Enterprise-Experten hierzu beraten.
Aus Gründen der Compliance möchte ich keinerlei Daten an Google senden.	Hoch	Hoch	Wir empfehlen Ihnen dringend, Safe Browsing beizubehalten, um Ihre Nutzer vor Malware und Phishing zu schützen. Diese Funktion nutzt Kontextinformationen zum Nutzerzugriff auf eine Seite und kann so in vielen Fällen Bedrohungen effizienter erkennen als andere Sicherheitsprodukte für Unternehmen. Hier finden Sie weitere Informationen zu den Sicherheits- und Datenschutzrichtlinien von Chrome. Zusätzlich können Sie die Synchronisation von Lesezeichen, Verläufen und Passwörtern mit der Richtlinie `SyncDisabled` verhindern. Wir empfehlen jedoch dringend, die Funktionalität des Passwortmanagers aufrechtzuerhalten. In den vorherigen zwei Zeilen dieser Tabelle finden Sie die Optionen, die Ihnen hierbei zur Verfügung stehen. Sie entscheiden, welche Optionen für Ihr Unternehmen am besten geeignet sind. Die meisten Unternehmen möchten Funktionen beibehalten, die einen klaren Sicherheitsvorteil bieten und die von bestimmten Nutzeraktionen (z. B. Google Übersetzer) ausgelöst werden. Um mehr Informationen über den Datenaustausch bei unterschiedlichen Diensten zu erhalten und die passenden Richtlinien für Sie zu finden, lassen Sie sich von Ihrem Chrome Enterprise-Experten hierzu beraten.

Verwaltung und Leistung

In diesem Abschnitt werden die Anforderungen beschrieben, die Unternehmen für die Verwaltung und Leistung von Chrome benötigen. Einige dieser Anforderungen beziehen sich dabei unter anderem auf Sicherheit und Datenschutz.

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich fürchte, dass der Passwortmanager in Chrome Support-Eskalationen verursacht, wenn die Passwörter der Nutzer nicht korrekt synchronisiert werden.	–	–	Das Chrome-Sicherheitsteam empfiehlt ausdrücklich die Verwendung des Passwortmanagers, weil es damit für Nutzer leichter ist, starke Passwörter einzusetzen. Wir möchten den Vorgang dabei so nahtlos und einfach wie möglich gestalten. Falls Sie diesbezügliche Bedenken haben, kontaktieren Sie bitte Ihren Chrome Enterprise-Experten.
Ich möchte sicherstellen, dass die Google Workspace-Passwörter meiner Nutzer nicht durch Phishingangriffe in die falschen Hände geraten.	● –	● –	Aktivieren Sie die Passwort-Warnung, wie unter Wiederverwendung von Passwörtern überwachen und verhindern beschrieben.
Die Testanforderungen meiner Organisation machen es schwierig, Chrome immer auf dem neuesten Stand zu halten.	● –	● –	Chrome hat mehrere Release-Versionen, die Ihrem Unternehmen einen Vorabzugriff auf neue Funktionen, Fehlerkorrekturen und Sicherheitsverbesserungen ermöglichen. Wir empfehlen, dass einige Ihrer Mitarbeiter die Beta- oder Entwicklerversionen abonnieren, um neue Funktionen zu testen und Ihnen die entsprechende Zeit zu verschaffen, die Unternehmensanwendungen zu aktualisieren. Dadurch haben Sie außerdem die Möglichkeit, eventuelle Bedenken mit Ihrem Chrome Enterprise-Experten zu besprechen, bevor eine funktionsgefährdende Änderung die stabile Version beeinträchtigt. Wir empfehlen dringend, auf diese Weise vorzugehen, anstatt Aktualisierungen zu verschieben. Andernfalls könnten bekannte Sicherheitslücken in Ihrer Organisation ausgenutzt werden. Dabei ist unbedingt zu beachten, dass die Entwicklung von Chrome größtenteils auf offener Basis erfolgt. Sobald ein Sicherheitsupdate auf der stabilen Version veröffentlicht wurde, werden die Fehlerdetails öffentlich einsehbar. Es ist enorm wichtig, dass Ihre Nutzer die aktuelle Version von Chrome verwenden.

Verwaltung und Leistung (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich fürchte, dass das Chrome Cleanup Tool die Leistung beeinträchtigt und aufgrund unseres bestehenden Virenscanners sowieso überflüssig ist. Meine Organisation möchte anstelle von Chrome ihren eigenen Virenscanner nutzen, um Probleme zu erkennen und an uns zu melden.	–	Mittel	Einige Unternehmen möchten das Chrome Cleanup Tool deaktivieren, da sie Leistungseinbußen befürchten (insbesondere in VDI-Umgebungen). Oder sie ziehen es vor, dass Malware von der Antivirensoftware des Unternehmens erkannt wird, damit der entsprechende Benachrichtigungsfluss über ihre Tools für Sicherheitsinformationen und Ereignisverwaltung und andere Prozesse erfolgt. Beachten Sie bitte, dass sich dies auf die Sicherheit auswirkt. Das Chrome Cleanup Tool konzentriert sich mehr auf unerwünschte Software als auf Viren, sodass es unterschiedliche Softwareprogramme erkennen und entfernen kann. Wenn Sie es dennoch deaktivieren wollen, passen Sie die Richtlinie `ChromeCleanupEnabled` entsprechend an. Hinweis: Wenn Sie verhindern möchten, dass das Chrome Cleanup Tool seine Ergebnisse an Google sendet, haben Sie hierfür bessere Möglichkeiten – siehe die vorherige Antwort zu „Ich möchte nicht, dass Google auf den PCs in meiner Organisation nach Malware sucht“.
Das Intranet meiner Organisation ist noch nicht auf HTTPS umgestellt und die entsprechenden Sicherheitswarnungen beunruhigen die Nutzer.	–	Mittel	Sie können diese Warnungen mit der Richtlinie `OverrideSecurityRestrictionsOnInsecureOrigin` vermeiden. Da diese Richtlinie höchstwahrscheinlich eingestellt wird, empfehlen wir Ihnen, so schnell wie möglich auf HTTPS umzustellen.
Ich möchte sicherstellen, dass ein vollständiges Aktivitätsprotokoll verfügbar ist, damit ich Bedrohungen auch rückwirkend untersuchen kann.	Gering	–	Normalerweise können Nutzer das Speichern des Browserverlaufs deaktivieren. Mit der Richtlinie `SavingBrowserHistoryDisabled` lässt sich das verhindern. Außerdem können Sie mit der Richtlinie `IncognitoModeAvailability` den Inkognitomodus deaktivieren.
Ich möchte, dass Nutzer den von unserem Unternehmen genehmigten Passwortmanager verwenden anstatt den, der in Chrome integriert ist.	Gering	Gering	Es ist eine gute Entscheidung, Ihren Nutzern einen Passwortmanager zur Verfügung zu stellen. Den integrierten Passwortmanager können Sie über die Richtlinie `PasswordManagerEnabled` deaktivieren. Wenden Sie diese Richtlinie ausschließlich für Ihr Unternehmensprofil an. So können Nutzer auch weiterhin den integrierten Passwortmanager in Chrome nutzen, sobald sie sich in ihrem privaten Profil anmelden.

Verwaltung und Leistung (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich möchte Nutzer davon abhalten, bestimmte Seiten aufzurufen, die gegen die Unternehmensrichtlinien verstoßen.	Mittel	–	Dies kann mithilfe von Zulassungs- und Sperrlisten festgelegt werden. Weitere Informationen finden Sie in diesem Hilfeartikel.
Das Verhalten von Chrome soll vorhersehbar sein, damit Änderungen nur nach einem Versionsupgrade erfolgen.	Mittel	–	Mit Variationen sind kleine Konfigurationsänderungen an Google Chrome möglich, ohne dass eine neue Version veröffentlicht werden muss. Dazu werden bestehende Funktionen aktiviert oder deaktiviert. Wenn Sie `ChromeVariations` auf `VariationsEnabled (value 0)` setzen oder diese Richtlinie erst gar nicht festlegen, können alle Variationen am Browser durchgeführt werden. Wir raten jedoch davon ab, das Framework für Chrome-Varianten zu deaktivieren. Dadurch wird unter Umständen verhindert, dass Google schnell kritische Sicherheitsupdates bereitstellt. Außerdem erhöht sich dadurch erheblich das Risiko von Sicherheits- und Kompatibilitätsproblemen in Ihrer Organisation.
Ich möchte sicherstellen, dass bei jedem Start des Browsers eine zentrale Anmeldeseite oder andere Unternehmensseite angezeigt wird, auf der die Nutzer Richtlinien zustimmen oder anderweitige Informationen sehen können, die meine Organisation als wichtig einstuft.	Mittel	–	Prüfen Sie bitte die Richtlinien `„RestoreOnStartupURLs“`, `„HomepageIsNewTabPage“`, `„NewTabPageLocation“` und `„HomepageLocation“`.
Ich möchte nicht, dass meine Nutzer den Inkognitomodus verwenden, da sie andernfalls dazu verleitet werden können, für die Arbeit unangemessene Seiten aufzurufen.	Mittel	–	Passen Sie die Richtlinie `IncognitoModeAvailability` an.

Verwaltung und Leistung (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich habe Endpunktsoftware, die nicht mit dem DNS-Stack von Chrome kompatibel ist.	Mittel	Mittel	Chrome verfügt über einen integrierten DNS-Stack, welcher mit der Richtlinie `BuiltInDnsClientEnabled` deaktiviert werden kann. Diese Einstellung wirkt sich lediglich auf den verwendeten DNS-Software-Stack aus und beeinflusst nicht, welche DNS-Server zum Einsatz kommen. Wenn Sie auf Ihrem Endpunkt Software haben, die das normale Verhalten von DNS-APIs modifiziert, müssen Sie Chrome möglicherweise so einstellen, dass der DNS-Stack des Systems verwendet wird. Dies kann die Geschwindigkeit und Reaktionsfähigkeit von Webseiten beeinflussen und die Sicherheit beeinträchtigen, da Chrome zukünftige Verbindungen nicht auf DNS-over-TLS oder andere sichere Protokolle aktualisieren kann.
Ich muss den Internettraffic mit Middleboxes überprüfen.	Mittel	Mittel	Dazu müssen Sie auf jedem Endpunkt ein Root-Zertifikat installieren. Google greift zu starken Mitteln, um die Sicherheit von verwendeten Zertifikaten im Internet zu überprüfen (beispielsweise mithilfe von Certificate Transparency). Es ist uns jedoch nicht möglich, die korrekte Nutzung Ihrer Unternehmenszertifikate zu verifizieren. Weitere Informationen zur Risikominderung finden Sie in der vorherigen Antwort zu „Meine Organisation verfügt über eigene vertrauenswürdige Root-Zertifikate auf Endpunkten, um auf Unternehmensserver zuzugreifen. Falls Angreifer den privaten Schlüssel für diese vertrauenswürdigen Zertifikate stehlen sollten, möchte ich in der Lage sein, diese zu sperren." Wir raten davon ab, ein Downgrade von TLS-Versionen aus Gründen der Kompatibilität mit früheren Middleboxes durchzuführen. Ältere Versionen als TLS 1.2 haben bekannte Schwachstellen, während die Architektur von TLS 1.3 gegen eine Reihe unbekannter Schwachstellen schützen soll.

Verwaltung und Leistung (Fortsetzung)

Unternehmensanforderung	Auswirkungen auf den Nutzer	Mögliche Nachteile in puncto Sicherheit	Optionen und Anmerkungen
Ich muss das Verhalten meiner Chrome-Nutzer mithilfe eines Drittanbieterprodukts überprüfen.	Mittel	–	Sie können die Installation von Drittanbieter-Sicherheitserweiterungen mit der Richtlinie `ExtensionInstallForcelist` erzwingen. Beachten Sie dabei, dass den Erweiterungen dadurch Zugriff auf Browserverlauf, Nutzerdaten und Seitenaufbau ermöglicht wird. Diese Methode ist empfehlenswerter als das Anpassen der Richtlinie `ThirdPartyBlockingEnabled`, mit der Drittanbietercode in den Browser eingeschleust werden kann. Das Chrome-Team hat die Erfahrung gemacht, dass Unternehmen mit eingeschleustem Drittanbietercode einem höheren Risiko ausgesetzt sind, da einige der in Chrome integrierten Schutzmaßnahmen außer Kraft gesetzt werden.
Meine Organisation wendet Richtlinien über die Google Cloud-Konfiguration je Nutzer an. Ich möchte sicherstellen, dass diese Richtlinien für die Nutzer ständig gelten, weshalb Chrome jederzeit in unserem Unternehmensprofil angemeldet sein soll.	Hoch	–	Mit einem Arbeitsprofil können Sie die Nutzeranmeldung in Chrome erzwingen. In diesem Hilfeartikel erhalten Sie weitere Informationen. Auf diese Weise werden Nutzer davon abgehalten, sich mit ihren privaten Chrome-Profilen anzumelden und dadurch ihre persönlichen Lesezeichen und Passwörter zu synchronisieren. Sie können diese Einstellung mithilfe der Chrome-Verwaltung über die Cloud oder der Windows-Gruppenrichtlinie auch auf Geräteebene anwenden.

Chrome verwalten

Als IT-Administrator können Sie Chrome Nutzern verschiedener Plattformen bereitstellen. Dabei stehen Ihnen Hunderte von Richtlinien zur Verfügung, mit denen Sie die Verwendung von Chrome regeln können.

Mit der Chrome-Verwaltung beginnen

BeyondCorp Enterprise

BeyondCorp ist ein Zero-Trust-Sicherheitsframework von Google. Damit erfolgt die Zugriffssteuerung nicht über Netzwerkperimeter, sondern über einzelne Nutzer und Geräte. Dadurch können Mitarbeiter von jedem Standort aus sicher arbeiten – ohne dass dafür ein traditionelles VPN benötigt wird. Mit BeyondCorp Enterprise können Nutzer einen Zero-Trust-Ansatz auf Grundlage derselben Richtlinien implementieren, die wir bei Google verwenden. Außerdem lässt sich der Zugriff auf SaaS-Anwendungen verwalten, die auf Google Cloud, anderen Clouds oder lokal laufen. BeyondCorp Enterprise umfasst neue Funktionen für den Datenschutz und den Schutz gegen Bedrohungen, die direkt in Chrome integriert sind.

Unser neues Whitepaper zum Thema sicherer Zugriff auf SaaS-Anwendungen mit BeyondCorp Enterprise führt gängige Szenarien auf und enthält eine Anleitung, wie IT-Führungskräfte mit diesen umgehen können. Wie bei jeder neuen Bereitstellung gibt es einige Sicherheitsfaktoren, die Organisationen in Betracht ziehen sollten, darunter:

- Den Zero-Trust-Zugriff auf genehmigte SaaS-Anwendungen regeln
- Schutz vor Datenpannen bei SaaS-Anwendungen
- Malware-Übertragungen und laterale Ausbreitung über genehmigte Anwendungen verhindern
- Den Aufruf von Phishing-URLs verhindern, die in Anwendungen eingebettet sind

Im Whitepaper werden all diese Punkte sowie weitere Szenarien konkret beschrieben. Hier können Sie es lesen. Weitere Informationen zu BeyondCorp Enterprise finden Sie außerdem in unserem On-Demand-Webinar oder auf unserer Produktseite.

Weitere Ressourcen

Hier finden Sie weitere Ressourcen mit nützlichen Informationen zur Chrome-Verwaltung in Ihrem Unternehmen:

Bereitstellungshandbuch für Chrome (Windows)
Liste der Chrome Enterprise-Richtlinien
Versionshinweise für Chrome Enterprise und Education
Chrome Enterprise und Education-Hilfe
Erweiterungen im Unternehmen verwalten