chrome enterprise

Aan de slag: gids voor het beheren van zakelijke extensies voor de Chrome-browser

Inleiding

Er zijn duizenden Chrome-browserextensies beschikbaar. Veel van deze extensies presteren uitstekend en besparen mensen een hoop tijd doordat ze de bedrijfsworkflows verbeteren of de efficiëntie optimaliseren. Of het nu gaat om optimalisatie van het RAM-gebruik, hogere browsersnelheden of verbetering van je grammatica, extensies zijn bedoeld om je productiviteit op het werk te vergroten. Je moet echter niet vergeten dat als extensies niet goed worden beheerd, ze ook risico's en kwetsbaarheden introduceren binnen de omgeving van een bedrijf. IT-teams van bedrijven moeten daarom een balans zien te vinden tussen de productiviteit van gebruikers en de beveiligingsbehoeften van het bedrijf.

Wat betreft extensiebeheer hebben IT-teams van bedrijven 3 belangrijke prioriteiten:

1. Gebruikers- en bedrijfsgegevens beschermen.
2. De installatie van schadelijke extensies voorkomen.
3. Zorgen dat gebruikers toegang hebben tot de extensies die nodig zijn om de productiviteit en efficiëntie te verbeteren.

Met zoveel nieuwe en bestaande extensies die ook nog eens doorlopend worden geüpdatet, is het cruciaal dat beheerders praktische tips volgen om de Chrome-extensies van hun gebruikers te controleren, beheren en beveiligen.

Deze technische paper bevat informatie over de verschillende opties die je hebt om extensies te beheren, zodat je een methode kunt kiezen die het best bij je behoeften past.

Criteria om rekening mee te houden

Voordat je met het beheren van extensies begint, moet je eerst bepalen welke parameters je organisatie gaat gebruiken om ze te beoordelen en goed te keuren Je kunt hiervoor de volgende vragen beantwoorden:

- Wat zijn de beveiligingsvoorschriften en nalevingsmaatregelen waaraan onze organisatie zich moet houden?
- Welke gebruikers- en bedrijfsgegevens worden er op apparaten van gebruikers bewaard?
- Welke rechten die extensies willen, zouden ons gegevensbeveiligingsbeleid kunnen schenden?

Als je dat eenmaal duidelijk hebt, kun je kijken welke opties je hebt om je extensies te beheren.

De traditionele benadering:

Je kon browserextensies eerst alleen beheren door elke extensie handmatig te beoordelen en daarna een lijst met toegestane en geblokkeerde extensies te maken om te bepalen welke extensies wel en niet op apparaten van gebruikers mochten worden geïnstalleerd. Sommige organisaties gebruiken deze benadering nog steeds.

In de Google Beheerdersconsole kun je kiezen uit de volgende mogelijkheden:

- Alle extensies toestaan behalve de extensies die je wilt blokkeren.
- Alle extensies blokkeren behalve de extensies die je wilt toestaan.
- Alle afzonderlijke extensies blokkeren of toestaan.
- Een of meer extensies afgedwongen installeren

In Microsoft[1] Groepsbeleid kun je templates gebruiken voor een beveiliging die vergelijkbaar is met de beveiliging die wordt toegepast voor bepaalde groepen of een hele organisatie, waaronder:

- Alle extensies toestaan behalve de extensies die je wilt blokkeren.
- Eén extensie blokkeren of toestaan.
- Een extensie afgedwongen installeren.

Beide benaderingen werken tot op zekere hoogte. Ze hebben wel hun beperkingen en vragen behoorlijk veel handmatig beheer.

De tijd die nodig is om ze te beoordelen, kan ten koste gaan van de productiviteit van zowel de gebruiker als de beheerder. En wat met het oog op de beveiliging misschien nog wel het belangrijkst is, is dat de extensies die al zijn toegestaan, kunnen worden verkocht aan en/of geüpdatet door entiteiten die niet door jou zijn goedgekeurd.

[1] Microsoft®, Windows® en Internet Explorer® zijn gedeponeerde handelsmerken van Microsoft Corporation in de Verenigde Staten en/of andere landen.

Een moderne benadering: extensies beheren op basis van rechten

Voor efficiënter, beter schaalbaar en beter beveiligd beheer van zakelijke extensies kun je met Chrome ook aangevraagde extensies beheren op basis van rechten. Met extensiebeheer op basis van rechten kunnen IT-teams gebruikers de gewenste extensies leveren zonder bedrijfsgegevens in gevaar te brengen. Dit is de methode die het IT-team van Google zelf gebruikt en ook andere bedrijven aanraadt.

Op basis van rechten kunnen extensies wijzigingen in een website of apparaat aanbrengen. Voor de goede werking van een extensie zijn er vaak specifieke rechten nodig.

Er zijn 2 belangrijke categorieën extensierechten: siterechten en apparaatrechten. Veel extensies gebruiken beide.

Met siterechten kun je bijvoorbeeld een extensie toestaan om afbeeldingen te blokkeren of om te bepalen hoever je kunt in- of uitzoomen op een site. Bij apparaatrechten kan het bijvoorbeeld gaan om de toegang tot USB-poorten, de zichtbaarheid van het scherm en de communicatie met programma's.

Als je het risico verder wilt verminderen, kun je overwegen om extensies te beheren met de volgende beleidsregels:

- **Geblokkeerde/toegestane rechten:** hiermee kun je voorkomen dat al toegestane extensies worden geüpdatet met nieuwe rechten en kun je eerder geïnstalleerde extensies uitschakelen als ze niet meer aan je vereisten voldoen.
- **Runtimeblokkering hosts:** geeft aan op welke sites extensies kunnen worden uitgevoerd.
- **Extensies afgedwongen installeren:** extensies worden universeel op de computers van je gebruikers geïnstalleerd, zodat ze over de tools beschikken om productief te kunnen werken.
- **Lijst met toegestane/geblokkeerde extensies:** indien nodig.

Deze methode om Chrome-extensies te beheren is beter beveiligd, makkelijker te beheren en is voor grote organisaties goed schaalbaar. De methode beschermt gebruikers tegen schadelijke extensies en bespaart de IT-afdeling een hoop tijd, omdat ze geen extreem lange lijsten met toegestane en geblokkeerde extensies meer hoeven te beheren, geen updates hoeven te beoordelen en niet elke extensie afzonderlijk hoeven goed te keuren. Het is een win-winsituatie.

chrome enterprise

Aan de slag: extensies beheren op basis van rechten

Ga als volgt te werk om je zakelijke extensies op basis van rechten te beheren:

1. Maak een lijst met extensies die je gebruikers al hebben geïnstalleerd (gebruik de rapportage van Cloudbeheer voor de Chrome-browser of houd een enquête onder je eindgebruikers).

2. Stel vast welke websites/hosts moeten worden beveiligd. Bepaal welke rechten een potentieel risico vormen en moeten worden beperkt.

3. Stel een hoofdlijst samen met alle gegevens die je hebt verzameld en deel deze met essentiële belanghebbenden zodat iedereen op één lijn zit.

4. Test je nieuwe beleidsregels in een testomgeving of met een kleine testgroep en rol de nieuwe beleidsregels vervolgens gefaseerd uit naar werknemers.

5. Evalueer de feedback van gebruikers.

6. Herhaal en verfijn het proces elke maand, elk kwartaal of elk jaar (wat voor jouw organisatie het best werkt).

Je hoeft de beleidsregels maar één keer in te stellen om een basislijn met toegestane rechten af te dwingen en gevoelige bedrijfssites te beschermen. Je bedrijf is niet alleen automatisch beter beveiligd, je biedt je gebruikers ook betere functionaliteit.

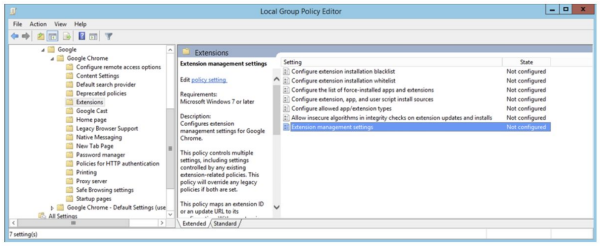
Het is zelfs mogelijk dat werknemers bepaalde extensies kunnen installeren die ze eerder niet konden installeren. Ze kunnen deze extensies alleen niet uitvoeren op gevoelige bedrijfssites.

Rechten instellen

Je kunt makkelijk bepalen welke extensies je gebruikers mogen installeren. Je kunt de rechten die acceptabel zijn, gewoon toewijzen en de rechten die niet acceptabel zijn, markeren.

Google Beheerdersconsole

In een Windows-, Chrome OS-, Mac[2]- en Linux-omgeving kun de Google Beheerdersconsole gebruiken om deze opties in te stellen. Als een extensie toegangsniveaus of rechten vereist die je beveiligingsbeleid schenden, wordt de extensie niet geïnstalleerd. Je kunt bijvoorbeeld een extensie blokkeren die verbinding maakt met de USB-apparaten van je gebruikers of geen toegang biedt om cookies te lezen. Als een geïnstalleerde extensie rechten nodig heeft die zijn geblokkeerd, wordt de extensie niet uitgevoerd. De extensie wordt



Groepsbeleid

Een andere veelgebruikte manier om extensies in Windows te beheren, is het gebruik van instelbeleid voor extensies. Met de editor voor groepsbeleidsbeheer kun je via een json-tekenreeks of in het Windows-register meerdere beleidsregels op één plek instellen. Met het beleid voor extensie-instellingen kun je bijvoorbeeld de installatiemodus

[2] Mac en macOS zijn handelsmerken van Apple Inc., gedeponeerd in de Verenigde Staten en andere landen.

bepalen, URL's updaten, geblokkeerde rechten beheren, bronnen installeren, bepalen welke typen zijn toegestaan, geblokkeerde installaties beheren en beheren voor welke host runtime wordt geblokkeerd of toegestaan. Je kunt ervoor kiezen om hier alle instellingen voor extensiebeheer in te stellen, maar je kunt deze opties ook instellen via andere afzonderlijke beleidsregels. Je bepaalt de instelling via het Windows-register of een json-tekenreeks in de Windows-editor voor groepsbeleid.

Aanvullende overwegingen

Sommige grote organisaties willen liever een eigen site voor extensiedownloads. Google raadt deze benadering niet aan, omdat de eigen website mogelijk minder goed beveiligd is dan de Chrome Web Store, die gebruikmaakt van geautomatiseerde en handmatige codescans om te voorkomen dat er schadelijke code naar gebruikers wordt gestuurd.

Cloudbeheer voor de Chrome-browser is een nieuwe console waarmee je op één centrale plek je Chrome-browserinstellingen voor je Windows-, Mac- en Linux-computers kunt instellen. De console geeft een gedetailleerd beeld van de status van de Chrome-browser in je omgeving en biedt direct inzicht in het volgende:

- Huidige versies van de Chrome-browser die naar de desktops en laptops van het bedrijf zijn geïmplementeerd, ongeacht het type desktop of laptop.
- De extensies die voor elke browser zijn geïnstalleerd.
- De beleidsregels die op elke browser worden toegepast.

De console biedt je ook de mogelijkheid om een verdachte extensie met één klik op de knop voor al je computers te blokkeren.

Chrome-extensies beheren zoals we dat bij Google doen

Nadat jarenlang de traditionele extensiebeheermethode met lijsten van geblokkeerde en toegestane extensies werd gebruikt voor de ruim 300.000 eindpunten, wilde het interne IT-team van Google een minder omslachtige benadering met een goede balans tussen de beveiliging en behoeften op het gebied van zakelijke IT en de productiviteit van werknemers. Hun oplossing om extensies te beheren op basis van rechten, is een schaalbare en beveiligde oplossing die de overhead aanzienlijk heeft verlaagd.

Net als Google kun jij ook overstappen van lijsten met toegestane en geblokkeerde extensies naar de beter beveiligde methode die we in deze technische paper beschrijven. Je beschikt over de beveiliging die je bedrijf nodig heeft en biedt je werknemers tegelijkertijd de mogelijkheid om veilige, productiviteitsverhogende extensies te installeren.

Ga aan de slag met extensiebeheer op basis

Bekijk de volgende informatiebronnen voor meer inzicht in de Chrome-browserextensie:

Lees de gids Extensies beheren in je bedrijf
Bekijk de video Google Cloud Next '19 Breakout Session: How Google Cloud IT Manages Enterprise Extensions
Verken de opties van Cloudbeheer voor de Chrome-browser
Bekijk de downloads in de Chrome-browser voor jouw bedrijf
Meer informatie over Enterprise Support voor de Chrome-browser
Bekijk de lijst met beleidsregels voor de Chrome-browser
Bezoek het Helpcentrum voor zakelijke Chrome-browsers en het Helpforum voor de Chrome-browser