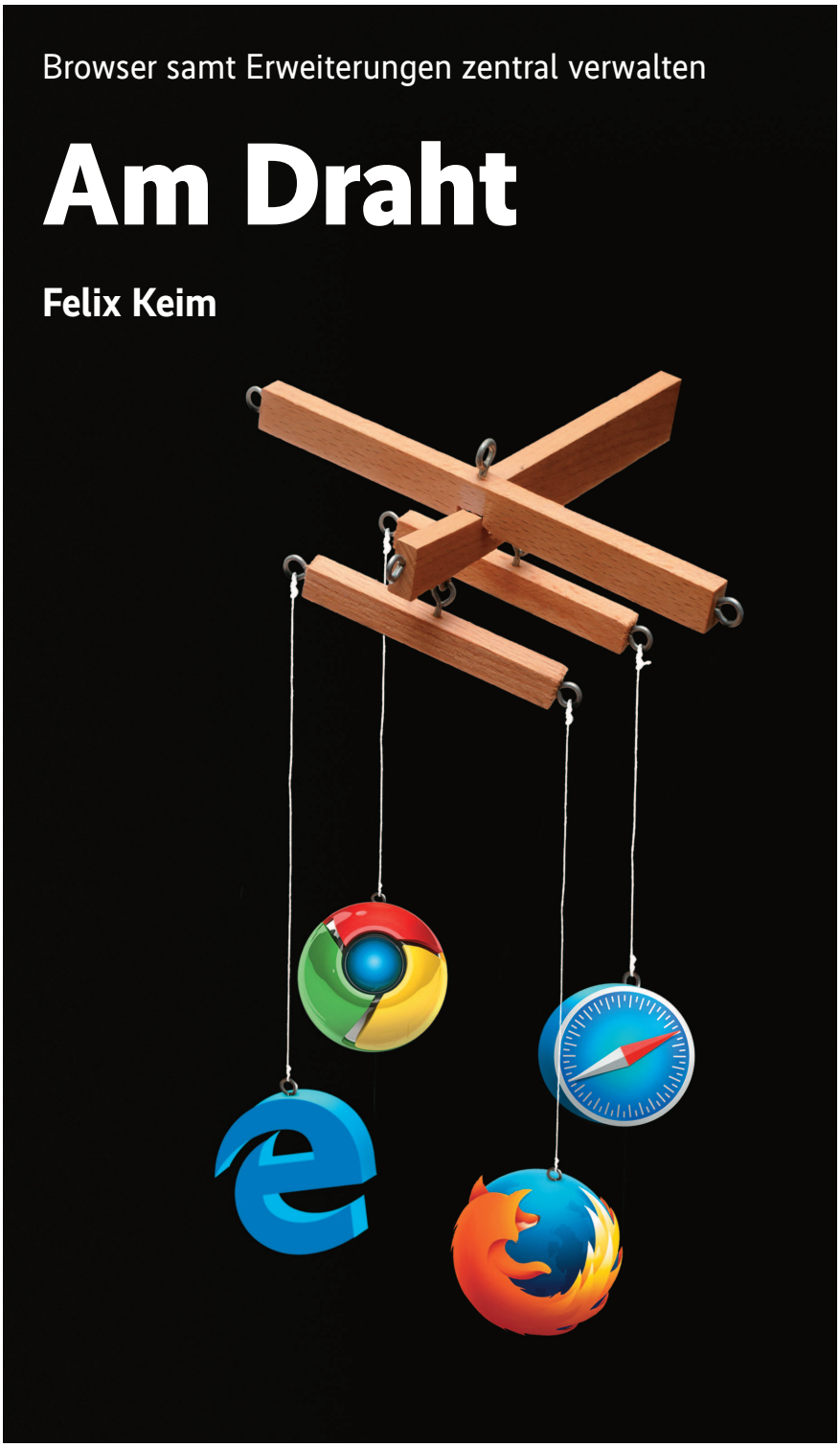
Browser samt Erweiterungen zentral verwalten

Am Draht

Felix Keim



Webbrowser sind nicht nur Einfallstore für schädliche Software und Angriffe aller Art, in jüngster Zeit stellten sie sich überdies als äußerst „geschwätzig“ in Sachen Datenübertragung heraus. Zum Schutz der Firmendaten sollten Unternehmen diese Programme unter die Lupe nehmen und die mit ihnen verbundenen Risiken minimieren.

Webbrowser sind die in einem Unternehmen gegenüber Angriffen mit Abstand am stärksten exponierten Anwendungen. Jeden Tag verarbeiten sie und ihre Plug-ins sowie Erweiterungen Unmengen fremden Codes in Form komplexer Websites. Die zentrale Verwaltung ist in vielen Unternehmen aber lediglich für Microsofts Internet Explorer und gegebenenfalls seinen Nachfolger Edge umgesetzt – obwohl auch andere Browser zur Nutzung freigegeben sind oder zumindest deren Nutzung geduldet wird. Das ist fahrlässig und vor allem unnötig, denn Möglichkeiten hierzu bieten auch Firefox und Chrome.

Im vergangenen Jahr wurden laut der Schwachstellen-Website „CVE Details“ im Internet Explorer insgesamt 27 Sicherheitslücken gefunden, die gemäß CVSS-Standard als kritisch gelten. Sein Nachfolger Edge brachte es auf 20, Chrome kommt auf 24, Firefox auf 13 kritische Schwachstellen. Das reine Zahlenmaterial sagt zunächst wenig über die absolute Sicherheit eines Browsers aus oder darüber, wie viel sicherer der eine gegenüber dem anderen sein mag. Aufschlussreich ist jedoch der Vergleich mit anderer browsernaher Software.

Beispielsweise fanden Sicherheitsexperten für das weitverbreitete Flash-Plug-in im gleichen Zeitraum 224 kritische Schwachstellen. Der PDF-Betrachter Adobe Acrobat DC, der sich per Plug-in ebenfalls in den Browser integriert, hatte immerhin 192 kritische bekannt gewordene Sicherheitslücken. Ein Angreifer muss also nicht notwendigerweise eine Schwachstelle im Browser selbst ausnutzen, sondern wird vermutlich eher versuchen, Sicherheitslücken in beliebten Plug-ins für seinen Angriff zu nutzen.

Angriff via Add-on

Anders als Plug-ins, die im Browser meist zur Darstellung bestimmter Inhalte wie Flash-Animationen oder PDF-Dateien genutzt werden, erweitern Add-ons die Funktionen eines Browsers. Auch sie sind angreifbar – prominenteste Vertreter waren jüngst die Erweiterungen, die sich bei der Installation von Adobe Reader DC oder Cisco WebEx in den Browser integrierten. Lücken im erstgenannten Add-on ermöglichten es einem Angreifer, per Cross-Site Scripting JavaScript-Code im Browser des Opfers auszuführen. Das WebEx-Add-on konnte gar dazu missbraucht werden, auf dem Gerät des Betroffenen beliebigen Code zur Ausführung zu bringen, beispielsweise in

Form eines nachgeladenen Spionage-Programms.

Doch Verwundbarkeiten sind nicht das einzige Problem der Erweiterungen. So deckten Reporter des NDR Ende des letzten Jahres auf, dass der Anbieter des Webservice WOT (Web of Trust) die mittels des zugehörigen Browser-Add-on gesammelten Informationen über das Surfverhalten der Nutzer ohne ausreichende Anonymisierung an Dritte weitergab. Den Reportern war es anhand eines erlangten Datensatzes möglich, einzelne Personen zu identifizieren und ihre detaillierte Surfhistorie einzusehen und auszuwerten.

Den technisch wohl meist weniger versierten Nutzern der Erweiterung nun Vorwürfe zu machen, wäre nicht angebracht, denn ihre Absicht dürfte es vermutlich gewesen sein, sicherer zu surfen. Überhaupt ist es ohne die genaue Untersuchung eines Add-on kaum möglich vorherzusagen, was es im Hintergrund genau tut. So installiert Firefox jede Erweiterung, die man über die eingebaute Add-on-Suchfunktion finden kann, ohne weitere Rückfrage. Chrome hingegen zeigt vor dem Installieren aus dem Chrome Web Store immerhin die benötigten Rechte an und fordert eine Bestätigung durch den Anwender.

Da technisch bedingt die meisten Add-ons die potenziell zum Missbrauch geeignete Funktion „Alle Ihre Daten auf von Ihnen besuchten Websites lesen und ändern“ fordern (Abbildung 1), macht dies in der Praxis jedoch kaum einen Unterschied. Beispiele für solche Add-ons sind Passwort-Manager wie LastPass, Werbeblocker wie uBlock Origin, Proxy-Umschalter wie ProxySwitch Omega und die genannten Adobe Reader, Cisco WebEx und WOT.

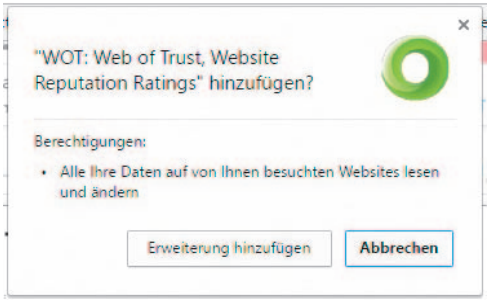
Um Missbrauch zu verhindern, erscheint in der Unternehmens-IT die zentrale Verwaltung von Browser-Plug-ins und -Add-ons zweckmäßig. Der Artikel zeigt, wie sie sich für unternehmensrelevante Browser umsetzen lässt.

Microsofts Internet Explorer und Edge

Der Internet Explorer ist seit jeher über Gruppenrichtlinien konfigurierbar. Die entsprechenden Vorlagen bieten Hunderte Richtlinien, um ihn detailliert an die Vorgaben und Bedürfnisse eines Unternehmens und die seiner Anwender anzupassen. Sinnvoll ist lediglich, dass möglichst aktuelle Gruppenrichtlinienvorlagen verwendet werden, in denen auch die neuesten Richtlinien für Microsofts Edge enthalten sind.

Falls der Zuständige nicht weiß, wann die Vorlagen das letzte Mal aktualisiert wurden, kann er sie auf der Microsoft-Webseite herunterladen (zu finden über „Alle Links“ im blauen Kästchen), installieren und dann an den Ort kopieren, an dem sie in der Active-Directory-Domäne bereitgestellt werden: in der Regel also entweder im Verzeichnis *%windir%\PolicyDefinitions* auf einem Domänen-Controller oder – falls die Vorlagen zentral gespeichert sind – unter der Netzwerkadresse *\\FQDN\SYSVOL\FQDN\policies\PolicyDefinitions* (FQDN ist durch den Namen der Domäne zu ersetzen). Über die Gruppenrichtlinienverwaltung findet man die entsprechenden Richtlinien dann sowohl unter *Computerkonfiguration* als auch unter *Benutzerkonfiguration*, jeweils in */Richtlinien/Administrative Vorlagen/Windows-Komponenten/* unter *Internet Explorer* beziehungsweise *Microsoft Edge*.

Microsoft verwendet für ActiveX-Steuerelemente, zum Beispiel das Adobe-Flash-Plug-in, Browser-Hilfsobjekte und -erweiterungen sowie Symbolleisten, beim Internet Explorer den Überbegriff „Add-ons“. Einen Marktplatz für Erweiterungen, wie man ihn von Firefox und Chrome kennt, gibt es hier nicht. Über die Internet-Explorer-Galerie („Alle Links“) lässt sich der Browser lediglich um zusätzliche Suchanbieter und Tracking-Schutz-Listen erweitern. Beim Edge-Browser spricht Microsoft nicht mehr von Add-ons, sondern von „Extensions“ und meint damit Erweiterungen, wie man sie von Chrome und Firefox kennt. Im Microsoft Store befinden sich derzeit circa 20 solcher Extensions.



Mit Erteilen dieser Berechtigung erlaubt der Benutzer indirekt auch, dass er ausspioniert wird (Abb. 1).

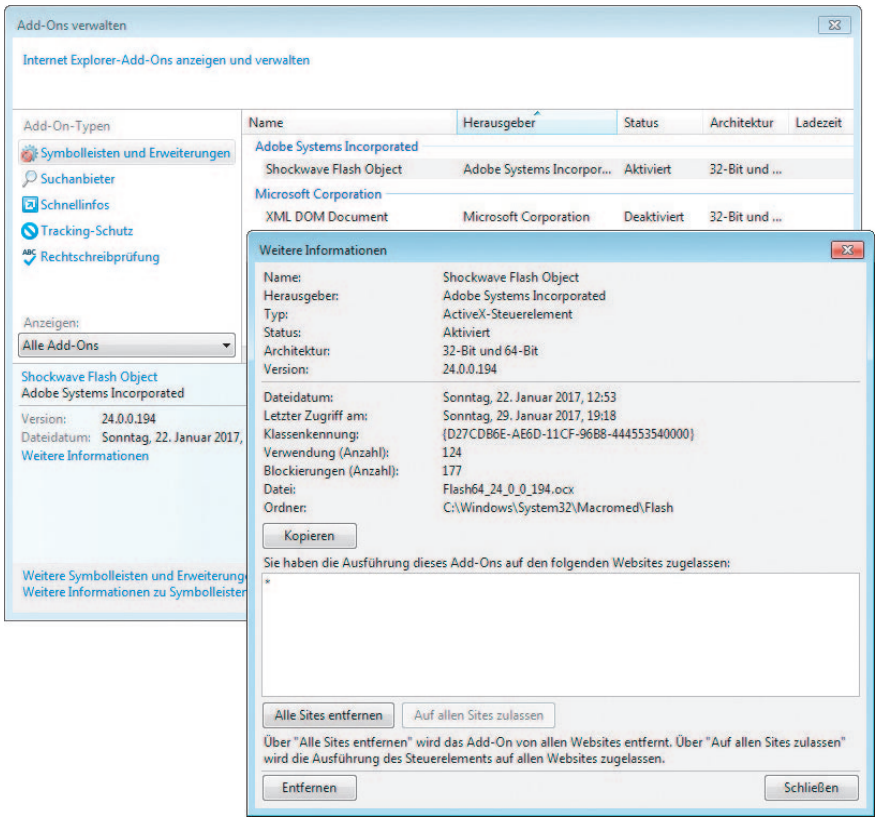
Nutzen, was explizit erlaubt ist

Über die Gruppenrichtlinien lassen sich die Add-ons für den Internet Explorer unter */Sicherheitsfunktionen/Add-on-Verwaltung* konfigurieren. Zunächst ist die Richtlinie „Alle Add-ons sperren, soweit diese nicht explizit in der Add-on-Liste aufgeführt sind“ zu aktivieren. Anschließend legt man die erlaubten Add-ons in der Add-on-Liste fest. Hierzu muss man die Class-ID des Add-on in Verbindung mit dem Wert „1“ definieren, der festlegt, dass das Add-on zugelassen werden soll. Die Class-ID eines Add-on lässt sich über den Internet Explorer auslesen, indem man dort die Add-on-Verwaltung unter „Extras“ aufruft und anschließend „Symbolleisten und Erweiterungen“, gefolgt von „Anzeigen: Alle Add-ons“. Nach einem Doppelklick auf das Add-on wird die Class-ID bei „Klassenkennung“ angezeigt. Für Adobe Flash lautet sie etwa *{D27CDB6E-AE6D-11CF-96B8-444553540000}* (Abbildung 2).

Der Internet Explorer unterstützt kein natives „Click to Play“, das in anderen Browsern bewirkt, dass zum Anzeigen bestimmter Inhalte erforderliche Plug-ins nur nach Zustimmung des Anwenders ausgeführt werden. Websites werden mit Click to Play schneller dargestellt, weil beispielsweise Flash-Animationen erst nach

X-TRACT

- Browser-Erweiterungen – sogenannte Plug-ins oder Add-ons – bergen das Risiko der Angreifbarkeit in sich und können überdies unbemerkt Daten über den Benutzer an Dritte weitergeben.
- Unternehmen sollten daher nichts dem Zufall überlassen und die Browser-Programme zentral verwalten. Mit diversen Richtlinien lässt sich das Installieren unerwünschter Erweiterungen zumindest teilweise steuern – die Rechte der Nutzer variieren bei den verschiedenen Browsern.
- Über das zentrale Konfigurieren von Browser-Programmen hinaus ist es sinnvoll, weitere Härtungsmaßnahmen zu ergreifen. Beispielsweise sollten sicherheitsbewusste Unternehmen Synchronisierungsfunktionen, die vertrauliche Daten in der Cloud vorhalten, deaktivieren.



Nur wenn die ausgelesene Class-ID eines Add-on auf die Liste der erlaubten Erweiterungen gesetzt wird, darf man es nutzen (Abb. 2).

Bestätigung starten. Die Funktion hat aber auch einen Sicherheitsaspekt: Bindet eine Website zum Beispiel einen versteckten Flash-Exploit ein, so wird dessen Ausführung verhindert, da der Nutzer nur das bestätigt, was er sehen möchte.

Um das Click-to-Play-Verhalten im Internet Explorer nachzuahmen – also zu verhindern, dass erlaubte Add-ons ohne Weiteres auf jeder Website ausgeführt werden können –, kann man die Richtlinie „ActiveX-Filterung einschalten“ aktivieren. Diese Einstellung blockiert zunächst sämtliche ActiveX-Steuerelemente für die ganze Website, worauf ein blaues Icon in der Adresszeile des Internet Explorer hinweist (Abbildung 3). Ein Anwender kann die ActiveX-Filterung durch einen Klick auf das Icon und die darauf erscheinende Schaltfläche „ActiveX-Filterung ausschalten“ deaktivieren. Anders als bei Click to Play, das die einmalige Ausführung eines bestimmten Plug-in erlaubt, gilt das Abschalten der ActiveX-Filterung zum einen dauerhaft und zum anderen für alle etwaig von der Website geladenen Plug-ins.

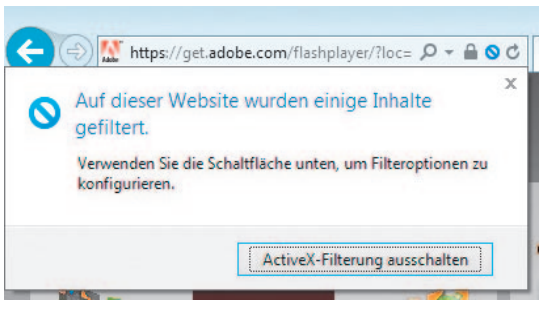
Sicherheit via Gruppenrichtlinien

Um das Installieren von ActiveX-Steuerelementen durch Benutzer zu verbieten, Aufforderungen zum Installieren solcher Steuerelemente zu unterbinden sowie weiterhin die Ausführung veralteter und somit potenziell verwundbarer Plug-ins auszuschalten, aktiviert man die Richtlinien
– „Benutzerbezogene Installation von ActiveX-Steuerelementen verhindern“;
– „/Sicherheitsfunktionen/ActiveX-Installation einschränken/Internet Explorer-Prozesse“;
– „/Sicherheitsfunktionen/Add-on-Verwaltung/Schaltfläche ‚Einmal ausführen‘ für veraltete ActiveX-Steuerelemente aus Internet Explorer entfernen“.

Nebenbei verfügt der Internet Explorer ohne zusätzliche Erweiterungen über einen eingebauten Werbeblocker – er heißt bei Microsoft „Tracking-Schutz“, kann mittels der populären Filterliste „EasyList Germany“ aber auch Werbung entfernen. Die Konfiguration ist nicht direkt über Gruppenrichtlinieneinstellungen vorgesehen, jedoch können die benötigten Einstellungen als Registrierungsschlüssel im Gruppenrichtlinieneditor unter *Benutzerkonfiguration/Einstellungen/Windows-Einstellungen/Registrierung* an die Anwender verteilt werden (Listing 1). Das Deaktivieren des Filters ist dann ebenso wie bei der ActiveX-Filterung pro Website dauerhaft möglich (Abbildung 4).

Für den Edge-Browser sind bisher lediglich rund 20 Gruppenrichtlinieneinstellungen verfügbar. Erweiterungen kann man durch Deaktivieren der Richtlinie „Erweiterungen zulassen“ ausschließlich global abschalten. Flash kann über einen Registrierungsschlüssel deaktiviert werden (Listing 2) – allerdings wird die Konfiguration dabei nicht gesperrt. Damit ist es dem Anwender möglich, Flash jederzeit wieder zu aktivieren.

Übrigens: Flash ist seit Windows 8 im Betriebssystem enthalten und wird per Windows-Update aktualisiert. Im Internet Explorer und in Edge funktioniert Flash seitdem auch ohne zusätzliche Plug-in-Installation. Diese ist nur noch unter Windows 7 notwendig.



Das Deaktivieren der ActiveX-Filterung beim Internet Explorer erlaubt das Ausführen von Steuerelementen für die gesamte Webseite (Abb. 3).

Googles Chrome

Sowohl Chrome als auch die Open-Source-Variante Chromium erkennt Gruppenrichtlinieneinstellungen standardmäßig an. Für Chrome ist es dabei unerheblich, ob der Browser vom Anwender per One-Click-Installer oder beispielsweise per Softwareverteilung als MSI-Paket (Microsoft Software Installation) installiert wurde. Voraussetzung für das zentrale Verwalten ist lediglich das Bereitstellen der Gruppenrichtlinienvorlagen, die man auf der Chromium-Webseite herunterladen kann („Alle Links“).

Diese werden wie Chrome häufig aktualisiert, regelmäßige Updates lohnen sich hier. Zu beachten ist jedoch, dass für die Verwaltung von Chrome und Google-Updates zwei separate Vorlagenpakete

Den Tracking- und Werbeschutz zu deaktivieren, ist manchmal erforderlich, um die Inhalte einer Webseite zu sehen – wie hier bei bild.de (Abb. 4)

Listing 1: Tracking-Schutz

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Safety\PrivacIE]
"FilteringMode"=dword:00000000
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Safety\PrivacIE\
                                                    Lists\{31AEECFF-0FC9-4BCD-9537-E98962F90AF7}]
"Name"="EasyList Germany   EasyList"
"Url"=http://easylist-msie.adblockplus.org/easylistgermany+easylist.tpl
"Enabled"=dword:00000001
```

Für den Internet Explorer lässt sich die Tracking-Schutz-Liste „EasyList Germany" per Registry konfigurieren.

Listing 2: Flash deaktivieren

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\SOFTWARE\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\
                                microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\Addons]
"FlashPlayerEnabled"=dword:00000000
```

Flash in Microsofts Edge-Browser lässt sich in der Registry deaktivieren.

existieren und beide bereitzustellen sind. Ist dies geschehen, so findet man die entsprechenden Richtlinien in der Gruppenrichtlinienverwaltung unter „Computerkonfiguration" und „Benutzerkonfiguration", jeweils in */Richtlinien/Administrative Vorlagen/Google/* unter „Google Chrome" beziehungsweise „Google Update".

Um Plug-ins zu verwalten, sind diese zunächst einmal alle zu sperren. Dazu aktiviert man die Richtlinie „Liste der deaktivierten Plug-ins angeben" und trägt den Wert „*" ein. Anschließend definiert man per „Liste der aktivierten Plug-ins angeben" die tatsächlich erforderlichen Plug-ins. Standardmäßig mitgeliefert und als Ausgangskonfiguration empfohlen sind: Adobe Flash Player, Chrome PDF Viewer, Widevine Content Decryption Module und Native Client.

Damit Chrome die konfigurierten Plug-ins regelmäßig aktualisiert, wählt man die Einstellung „Dadurch werden Komponentenupdates in Google Chrome aktiviert". Ein Nachinstallieren spezieller Plug-ins für das Anzeigen von Inhalten verhindert die Richtlinie „Angeben, ob Plug-in-Suchfunktion deaktiviert werden soll".

Deaktivieren sollte man außerdem die Richtlinien „Ausführung veralteter Plug-ins zulassen" und „Führt Plug-ins, die eine Autorisierung erfordern, immer aus". Da Chrome für Plug-ins Click to Play unterstützt, sollte man dies unter */Inhaltseinstellungen/* mit der Richtlinie „Standardeinstellung für Plug-ins" konfigurieren. Anwender können dann erlaubte Plug-ins auf Wunsch mit nur zwei Klicks aktivieren und gezielt entscheiden, dass bestimmte Flash-Objekte ausgeführt werden sollen.

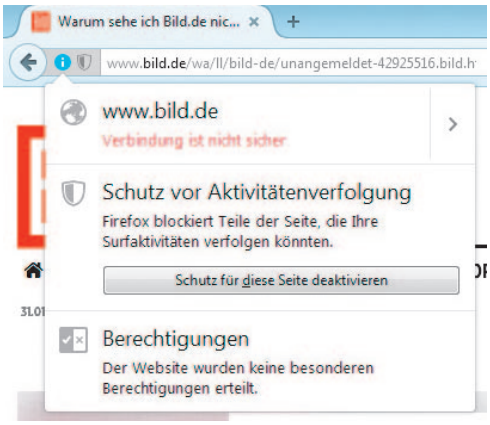
Unter dem Begriff „Extensions" fasst Google Erweiterungen, Designs und Apps zusammen. Sie lassen sich unter */Erweiterungen/* verwalten. Auch hier werden zunächst alle Erweiterungen mit „*" in der Richtlinie „Schwarze Liste für Installation von Erweiterungen konfigurieren" verboten und anschließend per „Weiße Liste für Installation von Erweiterungen konfigurieren" die erlaubten definiert. Dies muss über 32-stellige Erweiterungs-IDs erfolgen, die man etwas umständlich, aber dennoch am einfachsten aus der Chrome-Web-Store-URL der Erweiterung extrahiert. Die URL für den Werbeblocker uBlock Origin ist beispielsweise https://chrome.google.com/

webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm, die ID lautet entsprechend cjpalhdlnbpafiamejdnhcphjbkeiagm.

Möchte man Anwendern nicht nur erlauben, bestimmte Erweiterungen zu installieren, sondern sie gleich selbst verteilen, ist das über die Richtlinie „Liste der Apps und Erweiterungen konfigurieren, deren Installation erzwungen wurde“ möglich. Jeder Eintrag besteht zum einen aus der ID der zu installierenden Erweiterung und zum anderen aus der Chrome-Web-Store-Update-URL, die immer gleich lautet. Da Google Chrome – was wenig überrascht – keinen Werbeblocker enthält, lässt sich als Ersatz zum Beispiel uBlock Origin installieren. Dazu muss man lediglich cjpalhdlnbpafiamejdnhcphjbkeiagm;https://clients2.google.com/service/update2/crx eintragen.

Automatische Updates nimmt unter Windows der Google-Update-Dienst vor. Ist eine zentrale Softwareverteilung vorhanden, über die Chrome regelmäßig aktualisiert wird, sollte man ihn deaktivieren. Anderenfalls sollte man sicherstellen, dass der Dienst für das regelmäßige Suchen und Installieren von Updates konfiguriert ist. Unter */Google Update/Preferences/* regelt die Richtlinie „Auto-update check period override“ genau das – der Wert „0“ schaltet die Update-Prüfung ab und „480“ legt beispielsweise fest, dass alle acht Stunden nach Updates gesucht wird.

Ist im Unternehmen ein Web-Proxy vorhanden und soll Google Update regelmäßig Updates suchen und installieren, lohnt sich die Aktivierung von „Download URL class override“, denn dadurch lassen sich Download-URLs verwenden, die man zwischenspeichern kann (Cache). Unter */Google Update/Preferences/* lässt sich mittels „Update policy override default“ die Standardrichtlinie für Software-Updates von Google festlegen. Will man Updates per Softwareverteilung installieren, so empfiehlt sich die Einstellung „Updates disabled“, anderenfalls wählt man „Always allow updates“. Darüber hinaus legt die Richtlinie „Allow installation default“ fest, ob Google-Software per Google Update beziehungsweise Installer installiert werden darf – dann sollte sie aktiviert sein.



Der Schutz vor Aktivitätenverfolgung – also der Werbeblocker – lässt sich bei Bedarf seitenweise abschalten (Abb. 5).

Mozillas Firefox

Leider bieten weder Firefox noch die für die Verwendung in Organisationen gedachte Variante Firefox ESR (Extended Support Release) die Möglichkeit der zentralen Verwaltung per Gruppenrichtlinien. Stattdessen lassen sich Konfigurationsvorgaben mithilfe zweier Dateien umsetzen. Die Datei *mozilla.cfg* enthält die eigentliche Konfiguration und wird direkt im Installationsverzeichnis des Firefox abgelegt. Eine weitere Datei *autoconfig.js* verweist mittels

```
pref("general.config.filename", "mozilla.cfg");
pref("general.config.obscure_value", 0);
```

lediglich auf die Konfigurationsdatei und stellt sicher, dass diese geladen wird – man legt sie im Unterverzeichnis *\defaults\pref* des Installationsverzeichnisses ab. Ist eine Softwareverteilung vorhanden, kann man die beiden Dateien gemeinsam mit dem Firefox-Setup paketieren und ausrollen. Wenn nicht, bietet sich die Verteilung per Gruppenrichtlinie an. Dazu muss man die beiden Dateien zunächst an einen Netzwerkort kopieren, auf den die Computerkonten der Domäne Zugriffsrechte besitzen, zum Beispiel *\\FQDN\SYSVOL\FQDN\Firefox*. Anschließend muss eine neue Gruppenrichtlinie erstellt und die Verteilung der Dateien unter *Computerkonfiguration/Einstellungen/Windows-Einstellungen/Dateien* konfiguriert werden. Das geschieht per „Ersetzen“ unter Angabe der kompletten Pfade sowohl der Quell- als auch der Zieldatei, wobei Platzhalter wie %programfiles% oder %programfiles(x86)% verwendet werden können. Die Option „Nur einmalig anwenden“ stellt sicher, dass die Dateien nicht bei jeder Gruppenrichtlinienaktualisierung, sondern lediglich einmal kopiert werden.

Im folgenden Beispiel werden die Einstellungen in der Konfigurationsdatei *mozilla.cfg* per Funktion *lockPref()* gesetzt, um eine Änderung durch Anwender zu verhindern. Die nachfolgenden Zeilen bewirken, dass Firefox nicht nur sich selbst, sondern auch Suchmaschinen und Erweiterungen ohne Zutun des Anwenders aktuell hält:

```
lockPref("app.update.enabled", true);
lockPref("app.update.auto", true);
lockPref("app.update.mode", 0);
lockPref("app.update.silent", true);
lockPref("app.update.service.enabled", true);
lockPref("app.update.staging.enabled", true);
lockPref("browser.search.update", true);
lockPref("extensions.update.enabled", true);
lockPref("extensions.update.autoUpdateDefault",
true);
```

Die in Firefox für das private Browsen bereits standardmäßig aktivierte Tracking-Protection (deutsch „Aktivitätenverfolgung“) lässt sich für den regulären Browsing-Modus aktivieren – und bei Bedarf wieder abstellen (Abbildung 5). Das blockiert den größten Teil der Werbung ohne zusätzliche Erweiterung. Der Parameter zur Aktivierung der Aktivitätenverfolgung lautet:

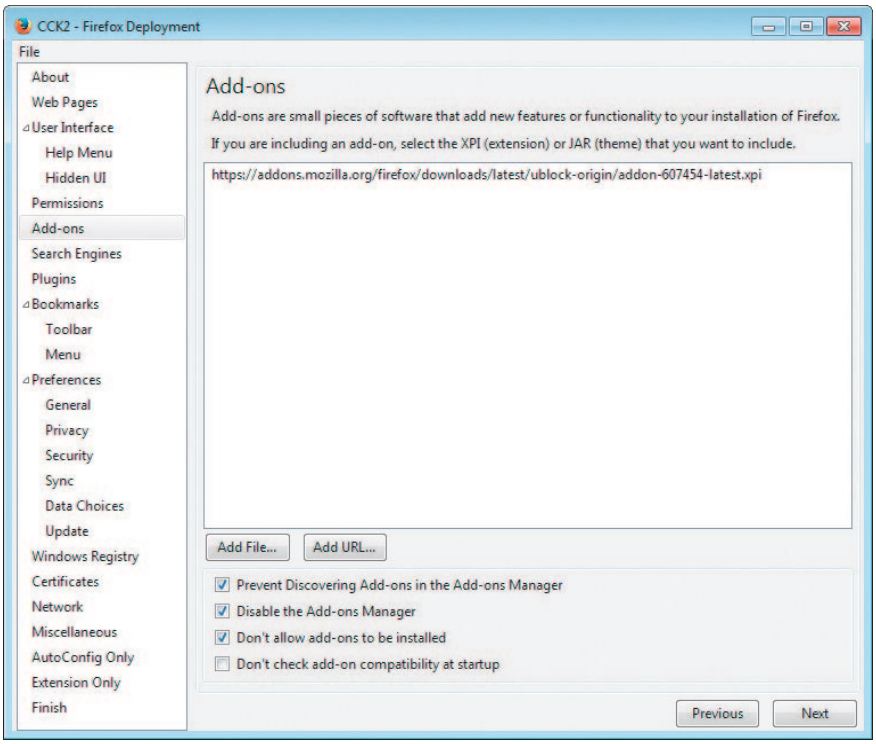
```
lockPref("privacy.trackingprotection.enabled",
true);
```

Firefox unterstützt für Plug-ins Click to Play, das Flash-Plug-in muss man dafür jedoch explizit konfigurieren:

```
lockPref("plugins.click_to_play", true);
lockPref("plugin.default.state", 1);
lockPref("plugin.state.flash", 1);
```

Mit der genannten Methode per „Preferences“ lässt sich eine minimalistische Konfiguration erreichen. Das Installieren von Erweiterungen durch den Anwender lässt sich so aber nicht verhindern, geschweige denn Add-ons gezielt verteilen. Für solche Zwecke hat der Mozilla-Enthusiast – und mittlerweile auch -Mitarbeiter – Michael Kaply die Firefox-Erweiterung „CCK2“ geschrieben, die über eine grafische Oberfläche umfangreiche und komplexe Anpassungen des Firefox ermöglicht (Abbildung 6). Die nötigen Konfigurationsdateien werden dann von CCK2 kompiliert und als ZIP-Archiv zur Verfügung gestellt. Lediglich um die Verteilung der Konfiguration muss man sich noch kümmern. Kaply stellt CCK2 auf seiner Website kostenlos zur Verfügung („Alle Links“), bietet Unternehmen aber auch kostenpflichtige Support-Services an.

Die Firma FrontMotion hingegen stellt auf ihrer Webseite zwei verschiedene Arten von MSI-Paketen zur einfacheren Verteilung von Firefox zur Verfügung, die, anders als das offizielle Firefox-Setup, beide bereits das Flash-Plug-in enthalten. Die Variante „MSI for Firefox“ enthält den Browser im unveränderten Original, die „FrontMotion Firefox Community Edition“ hingegen ist dahingehend angepasst, dass sie sich per ebenfalls zum Download verfügbarer Gruppenrichtlinienvorlagen zentral verwalten lässt.



Über die grafische Oberfläche der Firefox-Erweiterung CCK2 kann man den Browser an eigene Bedürfnisse anpassen (Abb. 6).

Der Nutzen ist in der Praxis jedoch begrenzt, da nicht alle Konfigurationsparameter in den Vorlagen enthalten sind und sich komplexe Szenarien nicht allein mittels sogenannter „Preferences“ umsetzen lassen. Dies erfordert umfangreiches Scripting oder eben den Einsatz des genannten CCK2. Als kostenpflichtige Alternative bietet FrontMotion mit dem „Firefox Packager“ einen Dienst zum Erstellen angepasster Firefox-MSI-Pakete an. Diese können neben Konfigurationsvorgaben auch Icons, Erweiterungen und Unternehmenszertifikate enthalten.

Ergänzende Maßnahmen

Die vorgestellten Konfigurationsmöglichkeiten beziehen sich lediglich auf das Management von Browser-Plug-ins und -Add-ons und bilden nur einen Bruchteil der möglichen und sinnvollen Maßnahmen, die sich zur Absicherung der genannten Browser empfehlen. So ist etwa das Härten des Internet Explorer sowohl allgemein als auch in Bezug auf die Sicherheitskonfiguration der verschiedenen Zonen sinnvoll.

Abhängig von den Vorgaben des Unternehmens kann das Deaktivieren weiterer Funktionen notwendig oder zumindest sinnvoll sein. Bei Chrome gehören dazu „Cast“, „Cloud Print“ und die Cloud-Synchronisierung von Lesezeichen, Chroniken, Kennwörtern und anderen vertraulichen Daten. Eine solche Sync-Funktion existiert ebenfalls im Firefox und sie lässt sich auch dort konfigurieren. Bei Bedarf können außerdem „Heartbeat“, die Einbindung des Dienstes „Pocket“ und die Funktion „Seite teilen“ deaktiviert werden. Für alle genannten Browser ist es darüber hinaus möglich, das Übermitteln von Nutzungs- und Absturzdaten sowie solchen zur Verbesserung der Benutzerfreundlichkeit abzuschalten.

Des Weiteren bieten Internet Explorer und Edge mit „SmartScreen“ und Chrome sowie Firefox mit „Safe Browsing“ Filter an, die den Anwender beim Aufruf von Malware- oder Phishing-Seiten warnen. Diese können aktiviert und ein Ignorieren der Warnungen verhindert werden. Unter Datenschutzaspekten sind solche Dienste jedoch fragwürdig. Weitere Empfehlungen zur Härtung und sicheren Konfiguration der genannten Webbrowser bietet das „Center for Internet Security“ (CIS) auf seiner Website zum kostenfreien Download an („Alle Links“). (ur)

Felix Keim

arbeitet als IT-Sicherheitsberater und Trainer bei der cirosec GmbH in Heilbronn.

Alle Links: www.ix.de/ix1703034