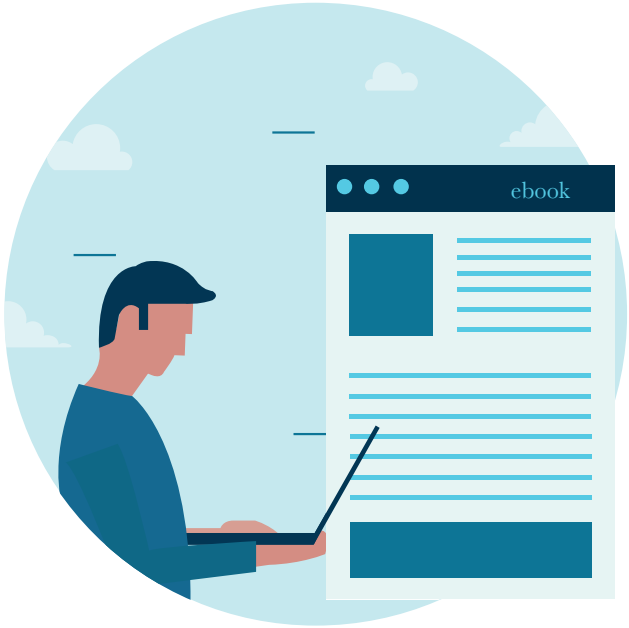
Warum die **Browser-Sicherheit** zur **Sicherheitsstrategie** jedes Unternehmens gehören sollte

Einleitung



Browser sind webbasierte Anwendungen, die Informationen aus dem Internet übertragen, darstellen und abrufen. In den 1980er Jahren erfüllten verlinkte Anwendungen die Aufgaben von Browsern. 1990 wurden der erste Webserver und das WorldWideWeb (der erste Webbrowser) entwickelt.

1994 kam dann der Durchbruch: Der von Marc Andreessen entwickelte Browser Netscape wurde zum ersten weit verbreiteten Browser; er setzte auf eine Strategie der „Coopetition“, die für Interoperabilität und Portabilität mit Partnern sorgte. Heute, mehr als zwanzig Jahre später, nutzen wir viele verschiedene Arten von Browsern mit modernen Funktionen.

Aktuell sind Browser die am häufigsten verwendeten Anwendungen auf jedem Gerät. Während es Ende 1998 nach Angaben von **Internet World Stats** weltweit etwa 147 Millionen Internet-User gab, waren es Mitte 2019 bereits 4,4 Milliarden. Neben der Anzahl der Anwender ist auch deren durchschnittliche Browser-Nutzungsdauer gestiegen: So verbrachte der durchschnittliche Amerikaner 2016 laut **USC Annenberg** 23,6 Stunden pro Woche im Internet, verglichen mit 9,4 Stunden im Jahr 2000. Die gleiche Studie ergab auch, dass mit dem Aufkommen der Smartphones 2010 der Internetzugang zu 23 Prozent über mobile Geräte erfolgte, während dieser Anteil 2016 auf 84 Prozent angestiegen war.

Diese Statistiken zeigen, welche Bedeutung Browser inzwischen gewonnen haben. Bevor wir auf die Schwachpunkte von Browsern, die damit verbundenen Sicherheitsrisiken und möglichen gravierenden Schäden eingehen werden und erläutern, wie Unternehmen diesen Problemen begegnen können, möchten wir noch einen kurzen Blick auf die Entwicklung von Browsern werfen.

Die Entwicklung der Browser

Browser haben sich seit 1990 enorm weiterentwickelt: Inzwischen unterstützen sie u. a. HTML5, JavaScript, CSS und MultiMedia und können damit eine Vielzahl interaktiver Medieninhalte anzeigen. Ermöglicht wurde die Darstellung datenintensiver Inhalte wie Videos, Bilder und Grafiken durch die Ablösung von Einwahlmodems durch Breitbandverbindungen.

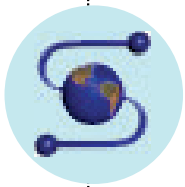
Nur wenige Jahrzehnte nach der Entwicklung des ersten Browsers kann heute jeder innerhalb von Sekunden mit einem Smartphone, Tablet oder auch einem Wearable auf jede beliebige Website zugreifen. Die digitale Transformation hat die Reichweite der Informationstechnologie erweitert, und Browser sind zu einem wichtigen Katalysator für diesen Wandel geworden. Lassen Sie uns einen Blick auf die wichtigsten Meilensteine der Browser-Entwicklung werfen:

1990

Mit WorldWideWeb wird der erste Browser veröffentlicht.

1992

Einführung von Lynx, ein reiner Text-Browser



1993

Mit Mosaic können erstmals grafische Inhalte dargestellt werden.

1994

Netscape Navigator wird zu einer wichtigen Erweiterung von Mosaic.

1995

Microsoft führt den Internet Explorer ein.
Auch Opera wird in Betrieb genommen.

2007

Safari für Mobilgeräte wird eingeführt.

2004

Mozilla lanciert Firefox.

2003

Apple führt Safari für den Mac ein.

1996

Beginn des „Browser-Kriegs“ zwischen Navigator und Internet Explorer.

2009

Google steigt mit Chrome in den Markt ein.

2011

Opera Mini für den mobilen Browser-Markt wird veröffentlicht.

2015

Microsoft führte Edge ein.

2018

Chrome wird der führende Browser und deckt rund 60 Prozent des Marktes ab.

Browser-basierte Cyber-Angriffe

Cyber-Angriffe entwickeln sich jeden Tag weiter – von Malware-basierten Takedowns bis hin zu Social Engineering („sozialer Manipulation“) – und haben bereits katastrophale Auswirkungen gehabt.

Lassen Sie uns einige gängige Angriffstaktiken erläutern, die auf Browser abzielen oder von Browsern ermöglicht werden:

Phishing und Spear-Phishing

Dabei handelt es sich um die häufigste Quelle von Browser-spezifischen Cyber-Attacken. Beim Phishing versenden Hacker bösartige E-Mails mit einer – angeblich – vertrauenswürdigen Absenderangabe, was User glauben lässt, es sei sicher, den Inhalt anzusehen. Die E-Mail enthält entweder einen bösartigen Link oder Anhang. Ein Klick darauf löst oftmals ein Skript aus, das dem Hacker den vollständigen Zugriff auf das System des Users ermöglicht – und damit Zugriff auf persönliche Informationen wie Sozialversicherungsnummern, Kredit-/Debitkartendaten, Bankkontoinformationen und Passwörtern sowie geschäftskritische Informationen. Gleichzeitig kann der Hacker zusätzliche Malware einspielen, die sich in andere Systeme des Netzwerks ausbreitet oder Daten löscht.

Einige Cyber-Kriminelle verwenden zudem sogenanntes Cloning, um ihre Phishing-Versuche zu unterstützen. Dabei werden gefälschte Profile, Seiten oder Websites erstellt, um auf die Anmeldeinformationen von Usern zuzugreifen und Kredit- oder Debitkartendetails abzugreifen.

Eine gezieltere Variante des Phishings ist das Spear-Phishing, bei dem ein spezifisches hochwertiges Ziel angegriffen wird. Spear-Phishing ist schwer zu erkennen oder abzuwehren, da die Inhalte sehr sorgfältig und individuell auf die Zielperson zugeschnitten werden, wodurch sie sehr glaubwürdig wirken. Der Angreifer gibt sich zudem meist als vertrauenswürdiger Absender, z. B. als Freund, Geschäftspartner oder Chef aus.

Man-in-the-Browser

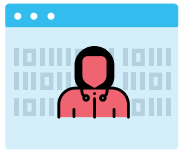
Bei dieser Angriffsart installiert ein Hacker einen einfachen Trojaner im Browser unter Ausnutzung vorhandener Schwachstellen im Browser selbst oder in Erweiterungen und Plug-ins. Durch die Installation einer bösartigen Erweiterung im Browser eines Users können sensible Informationen wie Passwörter, Kredit- oder Debitkartendaten, Sozialversicherungsnummern und vertrauliche Geschäftsdokumente ausfindig gemacht werden, um die Daten anschließend entweder zu stehlen oder sie über diese Erweiterung und die Funktionalität des Trojaners aus der Ferne aufzurufen.

Man-in-the-Browser(MITB)-Angriffe sind kompliziert, schwer zu identifizieren und zeigen, wie wichtig die Browser-Sicherheit für den Schutz der Daten ist. Browser, die von MITB-Angriffen infiziert wurden, können zum Einfallstor für noch gefährlichere Trojaner wie Zeus, Shamoon, Zberp, KinS und Triton werden.

Drive-by

Cyber-Kriminelle suchen nach angreifbaren Websites und versuchen, dort bösartige Skripte zu implementieren. Je nach Angriffstyp lösen Besucher einer infizierten Website entweder direkt die Malware aus oder werden zu einer anderen, noch bösartigeren Webseite weitergeleitet, die dann in der Lage ist, den Rechner des Besuchers zu durchsuchen.

Drive-by-Downloads sind schwer zu identifizieren, da sie keine Aktionen des Internet-Users erfordern, wie z. B. das Öffnen eines Anhangs. Drive-by-Angriffe können durch die Ausnutzung von Betriebssystem- oder Browser-Schwachstellen sowie veralteter Erweiterungen auftreten. Eine erhöhte Browser-Sicherheit ist der Schlüssel zur Bekämpfung von Drive-by-Angriffen.



Cross-Site-Scripting (XSS)

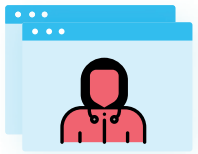
Diese Attacken ähneln Drive-by-Angriffen, hierbei laden Hacker jedoch sogenannte Payloads („Schadensroutinen“) auf eine wegen der Verwendung von JavaScript verwundbare Website hoch. Die Payload ändert oder ersetzt das vorhandene JavaScript durch ein bösartiges Skript, das Browser-Cookies stehlen kann. Besucht ein Anwender diese Website, löst er die Payload aus, die die Cookies an den Hacker versendet. Mit den Cookies kann der Hacker auf die sensiblen Informationen des Benutzers zugreifen und sogar eine gesamte Browser-Sitzung übernehmen (Session-Hijacking).

Adware

Adware ist eine Art von Malware, die in Browsern zu Marketingzwecken erscheint. Adware ersetzt typischerweise Anzeigen, die ein Benutzer normalerweise sehen würde, sowie die Standardsuchmaschine des Benutzers durch eine von dem Angreifer gewählte. Hacker profitieren von Adware, da sie Traffic für Websites generiert, die normalerweise nicht besucht werden. Fireball, eine Adware, die 2017 für Chaos in vielen Unternehmen sorgte, ist ein gutes Beispiel für diese Art von Bedrohung. Erweiterungen aus nicht vertrauenswürdigen Quellen sind oftmals ein Einfallstor für Adware. Durch genaue Überprüfungen, welche Erweiterungen installiert sind, können Sie Adware verhindern.

Cryptojacking

Beim Cryptojacking wird die Rechnerleistung eines Computers genutzt, um im Hintergrund eine Kryptowährung zu schürfen („Mining“). Dieser Vorgang erzeugt für den Hacker passive Einnahmen, in der Regel, ohne dass das Opfer überhaupt merkt, dass es infiziert ist. So wurden beispielsweise britische und kanadische Regierungsbehörden Opfer von Cryptojacking, als Hacker die in den offiziellen Websites integrierte Text-to-Speech-Software ausnutzten. Dabei schleusten die Angreifer ein Skript ein, um über die Browser der Besucher die Kryptowährung Monero zu „minen“. Manchmal wird die mit Cryptojacking-Malware gestohlene Rechenleistung auch für andere Zwecke als das Mining von Kryptowährungen weitergeleitet und genutzt.



Steganographic Payloads

Bei diesem Angriffstyp werden Dateien oder Nachrichten in einer Datei versteckt, die normalerweise keine Nachricht enthalten würde. So kann beispielsweise ein harmloses Bild als Tarn-Datei für eine ZIP-Datei dienen, die sich beim Klick auf das Bild automatisch extrahiert. Digitale Steganographie verbirgt die Tatsache, dass eine Nachricht übermittelt wird, was das Aufspüren bösartiger stenographischer Dateien nicht einfach macht. Im obigen Beispiel würde es nicht ausreichen, die Dateieigenschaften des Bildes zu überprüfen, um festzustellen, dass es eine ZIP-Datei enthält.

Der berüchtigte Banking-Trojaner Zeus, der auf Bank- und Finanzorganisationen abzielte, wurde mit steganographischen Embedding-Methoden aufgebaut, um seine Payload zu verbreiten. Der Trojaner Zeus lässt sich selbst mit aktueller Antiviren-Software kaum aufspüren und konnte so das bisher größte Botnetz im Internet schaffen. Das „Highlight“ des Zeus-Trojaners war, dass er mit Hilfe eines MITB-Angriffs auf den Weg gebracht wurde.

Warum Browser zu einem attraktiven Ziel für Cyber-Kriminelle geworden sind

Aufgrund ihrer Allgegenwärtigkeit sind Browser zu einem attraktiven Ziel für Cyber-Kriminelle geworden. Laut Internet World Stats nutzten 2018 95 Prozent der in Nordamerika lebenden Menschen das Internet. In Europa waren es 82, in Asien immerhin noch 49 Prozent. Dies zeigt deutlich, dass die Nutzungsrate des Internets in den westlichen Ländern besonders hoch ist und ganz allgemein auch in Zukunft weltweit weiter anwachsen wird.

Je nachdem, wo und wann ein Browser verwendet wird, können die abgerufenen und dargestellten Daten für einen geschäftlichen oder persönlichen Gebrauch bestimmt sein. Bei ausreichender Zeit oder den richtigen Ressourcen können bösartige Agenten diese Informationen identifizieren, indem sie die im Browser gespiegelten täglichen Routinen und Verhaltensweisen analysieren.

Sobald ein Cyber-Krimineller Zugriff auf sensible Browser-Daten hat, ist er seinem Opfer gegenüber im Vorteil und kann davon meist finanziell profitieren.

Für Cyber-Kriminelle gibt es unendlich viele Möglichkeiten wie Phishing, MITBs und Drive-by, um sensible Informationen und Anmeldeinformationen zu stehlen. Was alle diese Angriffsvektoren miteinander verbindet, sind die Browser. Sie sind zu allgegenwärtigen Plattformen für die Erledigung beruflicher und privater Aufgaben geworden, was sie zu einem attraktiven Ziel für Cyber-Kriminelle macht.

Viele Unternehmen haben ihre on-premise gehosteten, traditionellen Anwendungen aufgegeben und sind auf Cloud-basierte SaaS-Anwendungen umgestiegen, auf die nur über Browser zugegriffen werden kann. Das hat zur Folge, dass immer häufiger sensibelste Informationen in SaaS-Datenbanken gespeichert werden – im Vertrauen darauf, dass der SaaS-Anbieter die Unternehmensinformationen ordnungsgemäß schützt. Dieser Wechsel zum Cloud-Computing hat Cyber-Kriminellen ungeahnte neue Möglichkeiten des Datendiebstahls eröffnet.

In Anbetracht dessen, wie häufig nicht verifizierte Erweiterungen und veraltete Plug-ins in Browsern sind, ist die Wahrscheinlichkeit für Anwender hoch, Opfer von Trojanern, Crypto-Mining oder anderen bösartigen Browser-basierten Bedrohungen zu werden. Aufgrund der Allgegenwärtigigkeit von Browsern und den darin enthaltenen sensiblen Informationen, werden diese auch in Zukunft bevorzugter Ansatzpunkt für Cyber-Spionage bleiben.

Stellen Sie sich folgendes Szenario vor: Ein Hacker identifiziert eine Zielperson und manipuliert sie dann mit Phishing so, dass sie ihre Anmeldeinformationen für Facebook aushändigt. Anschließend kann der Hacker in den Facebook-Nachrichten der Zielperson potenziell für Erpressungen geeignetes Material identifizieren und die Zielperson so dazu bringen, die Login-Daten für ihr Firmenkonto auszuhändigen. Mit einem einzigen anonymen Takedown auf nur einer Angriffsebene hat sich der Hacker nun Zugang zu Unternehmensinformationen beschafft.

In echten Fällen können Angriffe auf Einzelpersonen und bösartige Aktivitäten auch von drei oder vier Ebenen aus gestartet werden. Das erschwert es, den Ursprung einer Attacke zu identifizieren. So könnte beispielsweise ein Hacker einen Regierungsmitarbeiter ins Visier nehmen und sich dann dessen private Anmeldeinformationen beschaffen. Er könnte auch einen Bekannten des Regierungsmitarbeiters hacken, um eine Phishing-E-Mail zu versenden.

Im nächsten Abschnitt zeigen wir, wie Browser geschützt werden können, um die Angriffsoptionen von Cyber-Kriminellen einzuschränken. Zudem erläutern wir, wie proaktive Sicherheitsrichtlinien für Browser eingesetzt werden können, um neue Cyber-Bedrohungen zu bekämpfen.

Browser-basierten Bedrohungen die Stirn bieten

Neben den bekannten Attacken – die eine permanente Bedrohung darstellen – sollten Sie stets Ausschau nach neuen Angriffsvarianten halten, die wahrscheinlich immer komplexer und schwerwiegender werden. Sorgen Sie für Visibilität, Kontrolle und regelmäßige Audits, um Browser-basierte Bedrohungen effektiv bekämpfen zu können.

Visibilität

Im Gegensatz zu anderer Software sind Browser keine eigenständigen Elemente, die alle ihre Funktionalitäten selbst erzeugen können: Sie sind dazu oft auf verschiedene andere Elemente wie Plug-ins und Erweiterungen angewiesen. Mit anderen Worten gleichen Browser eher einem Ökosystem, in dem mehrere Komponenten koexistieren, um auf ein gemeinsames Ziel hinzuarbeiten. Und hier beginnt die Komplexität.

Auch wenn es mehr als 500 Browser auf dem Markt gibt, hat Chrome mit rund 60 Prozent des weltweiten Marktanteils eine klare Vormachtstellung. Andere beliebte Browser sind Safari und Firefox, die auf Marktanteile von fünfzehn bzw. fünf Prozent kommen.

Jeder dieser Browser hat ein eigenes Ökosystem und bedient unterschiedliche Nutzungsanforderungen. Gerade die große Varianz an Funktionalitäten und Add-ons der jeweiligen Browser macht es oft schwierig, herauszufinden, welche Browser-Komponente ausgenutzt wurde, um ein Unternehmen zu infiltrieren. Um den Ursprung einer Bedrohung sicher identifizieren zu können, benötigen IT-Abteilungen einen Einblick in die verschiedenen Ökosysteme, die im Unternehmen vorhanden sind.

Es muss deutlich erkennbar sein, welche Websites, Erweiterungen und Plug-ins erforderlich sind, damit die User ihre Aufgaben im Unternehmen erledigen können. So sollte zum Beispiel bekannt sein, welche Anwendungen nicht geschäftskritisch sind und vor allem für die Vereinfachung oder Verbesserung von Arbeitsprozessen benötigt werden. Wenn die für die Arbeit benötigten Websites und Add-ons nicht ausreichend identifiziert werden können, laufen Sie Gefahr, dass sich in Ihrem Unternehmen eine Schatten-IT breitmacht. Eine Schatten-IT – also Anwendungen, Erweiterungen oder Funktionalitäten, die Mitarbeiter nutzen, obwohl sie nicht von einem IT-Administrator genehmigt wurden – stellt für Unternehmen eine große Bedrohung dar, da sie oftmals unbeabsichtigte Sicherheitslücken erzeugt.

IT-Teams verfügen über sorgfältige Prozesse zum Prüfen und Genehmigen von Anwendungen, um sicherzustellen, dass diese mit dem Unternehmen kompatibel sind. Schatten-IT-Anwendungen umgehen diese Sicherheitskontrollen, was Sicherheitsverletzungen und explodierende IT-Ausgaben nach sich ziehen kann. Für IT-Administratoren ist es daher essentiell, den Überblick über die von den Usern verwendeten Websites, Cloud-Anwendungen, Erweiterungen und Plug-ins zu behalten. Nur so können sie entscheiden, welche Anwendungen zur Genehmigung gelistet werden sollten und welche auf eine schwarze Liste gesetzt werden müssen.

Kontrolle

Um die Qualität der Inhalte zu optimieren, auf die Anwender zugreifen können, sollten IT-Abteilungen Kontrollen durchsetzen. Diese legen fest, welche Websites angezeigt und welche Plug-ins oder Erweiterungen sicher verwendet werden dürfen und genehmigt werden müssen. Das hilft, Angriffe zu reduzieren und die IT-Kosten in Schach zu halten. Auch hier profitieren Sie von Visibilität, da Sie die Sicherheitskontrollen für alle verwendeten Cloud-Anwendungen und -Erweiterungen so besser durchsetzen können. Setzen Sie Anwendungen, die für Ihr Unternehmen potenziell schädlich sind, auf die Blacklist oder schränken Sie den Zugriff ein. Alternativ können Sie auch nur die Anwendungen auf die Whitelist setzen, die User verwenden dürfen. Dadurch wird sichergestellt, dass User nicht versehentlich auf bösartigen Websites landen und dort Malware oder anderen Browser-basierten Angriffen ausgesetzt sind.

Audits

Schlussendlich sollten Sie sicherstellen, dass Plug-ins und Erweiterungen mit den sich ändernden Anforderungen der User Schritt halten. Sie müssen den Überblick über neue Releases und Updates behalten, und herausfinden, ob sie für den Einsatz in Ihrem Unternehmen notwendig und sicher sind. Wenn sie es nicht sind, sollten Sie sich nach geeigneten Alternativen umsehen. So stellen Sie sicher, dass die Mitarbeiterproduktivität nicht durch die Sicherheitsvorgaben des Unternehmens beeinträchtigt wird. Indem Sie diese drei Ansätze kombinieren, können Sie Ihr Unternehmen mit wirkungsvollen Maßnahmen gegen die meisten webbasierten Angriffe schützen.

Erfolgsmodelle zur Gewährleistung der Browser-Sicherheit

Zusätzlich zu den oben genannten obligatorischen Sicherheitsmaßnahmen sollten Sie als Präventivmaßnahme bestimmte Regeln in Ihrem Unternehmen einführen, die das Ausmaß webbasierter Cyber-Angriffe weiter reduzieren können.

Stellen Sie sicher, dass für die gesamte Kommunikation HTTPS und nicht HTTP verwendet wird

Da HTTP-Verbindungen ungesichert sind, können die mit HTTP übertragenen Daten von Dritten abgefangen und manipuliert werden. Wenn eine Website HTTPS verwendet, wird die Kommunikation verschlüsselt und die in die Website eingegebenen Daten können nicht von Dritten gehackt werden. Diese einfache Vorkehrung schützt Ihre Daten gegen Man-in-the-Browser-Attacken und ist eine wichtige Grundlage für die Datensicherheit im Internet.

Halten Sie Browser und Add-ons auf dem neuesten Stand

In Browsern und Add-ons werden immer wieder Schwachstellen entdeckt, für die Anbieter Updates zur Behebung veröffentlichen. Wenn ein Browser oder Add-on nicht aktualisiert wird, steigt die Wahrscheinlichkeit, dass diese Schwachstellen von Cyber-Kriminellen ausgenutzt werden. Einige Plug-ins und Browser interagieren auch direkt mit dem Betriebssystem, wodurch Browser-basierte Angriffe erhebliche Konsequenzen haben können, weshalb das Einspielen von Patches auf Ihrer Checkliste ganz oben stehen sollte.

Deaktivieren Sie unnötige Browser-Add-ons

Die meisten Browser-basierten Angriffe erfolgen über unzuverlässige Erweiterungen und Plug-ins, die von Usern im Unternehmen installiert werden. Diese Angriffe lassen sich exponentiell reduzieren, wenn Add-on-Installationen genau überwacht werden und nur zuverlässige Add-ons im Unternehmen aktiv sind. Bösartigen Erweiterungen sollten Sie proaktiv entgegenwirken, indem Sie sie frühzeitig erkennen und auf eine Blacklist setzen, bevor User dazu verleitet werden, diese zu installieren.

Deaktivieren der Google-Sync-Funktion in Chrome-Browsern

Google Sync ist eine Funktion, mit der User Daten mit der Google Cloud synchronisieren können, wodurch diese Daten von jedem Browser aus zugänglich sind, der mit dem betreffenden Chrome-Konto verbunden ist. Diese Funktion ist für den durchschnittlichen User praktisch, da damit über jedes Gerät des Users auf Passwörter, Lesezeichen usw. zugegriffen werden kann. Für Unternehmen bringt Google Sync jedoch die erhöhte Wahrscheinlichkeit mit sich, dass geschäftskritische Daten missbraucht oder gestohlen werden.

Die Deaktivierung von Google Sync stellt sicher, dass User nicht auf Lesezeichen und Browser-Verläufe zugreifen können, die auf vertrauliches Unternehmensmaterial verweisen. In den meisten Fällen stellen diese Informationen kein Risiko dar, da die Links außerhalb des Unternehmensnetzwerks normalerweise nicht zugänglich sind; Spoofing und andere Hacking-Techniken könnten die Informationen allerdings preisgeben. Daher sollten Sie es sich gut überlegen, Google Sync zu deaktivieren, um zu vermeiden, dass Passwörter außerhalb von Unternehmensgeräten zugänglich sind. Ebenso birgt Google Sync das Risiko des Missbrauchs von Berechtigungen auf gemeinsamen Unternehmensgeräten.

Darüber hinaus sollten Sie beachten, dass die von Google Sync gespeicherten Daten nur so lange sicher sind, wie die Google-Cloud-Server sicher sind. Werden diese gehackt, sind auch Ihre Daten gefährdet. Die einfachste Strategie, alle Probleme zu vermeiden, ist die Deaktivierung von Google Sync für Firmenkonten und auf Firmengeräten.

Stellen Sie sicher, dass Website-Blocker in Browsern aktiviert sind

Die Zahl der Websites, die Malware hosten, nimmt von Tag zu Tag zu. Dies hat dazu geführt, dass Browser-Anbieter eigene Datenbanken erstellen und pflegen, in denen bösartige Websites gelistet sind. Die Safe-Browsing-Funktion von Chrome, der SmartScreen-Filter von Edge und die Phishing-Protection-Funktion von Firefox erkennen und blockieren jeweils Webseiten, die in diesen Datenbanken erfasst sind, sobald der User versucht, diese anzusteuern. Aktivieren Sie diese Einstellungen, um zu verhindern, dass User auf Websites landen, die bereits als bösartig erkannt wurden.

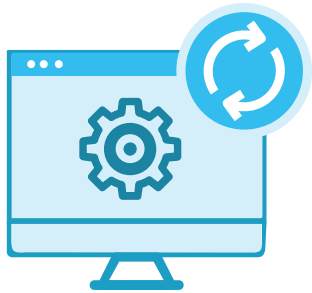
Was ist Browser Security Plus?

Derzeit setzen IT-Administratoren vor allem auf Endpoint-Security- und -Management-Tools, um ihr Netzwerk vor Cyber-Angriffen zu schützen. Da diese herkömmlichen Angriffsflächen nun in den meisten Unternehmen gut gesichert sind, haben sich viele Cyber-Kriminelle neuen Zielen zugewandt. Laut **Statista** erfolgte im ersten Quartal 2018 die zweithöchste Zahl der Exploit-Angriffe über Browser.

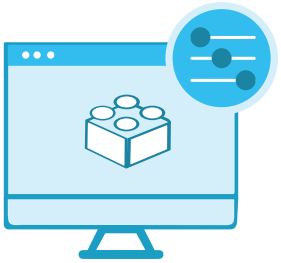
Vor diesem Hintergrund ist Browser-Sicherheit zu einem wichtigen Schlüssel für die Unternehmenssicherheit geworden, da sie die herkömmliche Sicherheits-Software für Endgeräte ergänzt. Um die notwendigen Sicherheitsmaßnahmen für Browser bereitzustellen, die herkömmliche Sicherheits-Tools für Endgeräte nicht enthalten, hat ManageEngine 2018 Browser Security Plus auf den Markt gebracht.

Die wichtigsten Features:

Konfigurationen und Deployment von Browser-Einstellungen:



Passen Sie die Browser-Einstellungen an die Bedürfnisse Ihres Unternehmens an und richten Sie diese Konfigurationen dann auf den gewünschten Computern ein. Browser-Konfigurationen können intelligent in Richtlinien gruppiert werden, die spezifische Anforderungen wie Bedrohungsabwehr und Data Leakage Prevention erfüllen.



Kontrolle und Verwaltung von Add-ons

Erlauben oder widerrufen Sie den Zugriff auf Browser-Add-ons wie Erweiterungen und Plug-ins basierend auf ihrer Zuverlässigkeit, und übertragen Sie unternehmenskritische Erweiterungen von einem zentralen Repository auf ausgewählte Computer.

Browser isolieren

Isolieren Sie vertrauenswürdige Websites und Geschäftsanwendungen von ihren nicht vertrauenswürdigen Gegenstücken. Nicht vertrauenswürdige Websites werden in einem virtuellen Browser dargestellt, um die Sicherheit der Unternehmensdaten zu gewährleisten.

Einhaltung von Vorschriften

Legen Sie die von Ihrer Organisation benötigten Regeln fest und überwachen Sie die Einhaltung der vom Center for Internet Security (CIS) vorgegebenen Security Technical Implementation Guidelines (STIG) und Branchensicherheitsstandards.

Anwendungen umleiten

Erzwingen Sie, dass bestimmte Anwendungen an bestimmte Browser umgeleitet werden. Denn Legacy-Anwendungen werden automatisch im Internet Explorer geöffnet, einem älteren Browser, auch wenn sie zuvor in Edge, Firefox oder Chrome aufgerufen wurden.

Browser Security Plus kostet ca. 7 US-Dollar pro Computer und Monat. Die kostenlose Version bietet ebenfalls alle Funktionen und eignet sich perfekt für kleine Unternehmen mit bis zu 25 Computern.

Weitere Informationen zu Browser Security Plus finden Sie unter **www.manageengine.de/browsersecurityplus.**

Jetzt kostenlos testen

Ihr ManageEngine-Partner:
MicroNova AG | Unterfeldring 6 | D-85256 Vierkirchen
Tel.: +49 8139 9300-456 | E-Mail: **sales-ManageEngine@micronova.de**
Web: **www.ManageEngine.de**