SURFEN ODER NOCH WAS?

Sicherheitsrisiko Webbrowser

Webbrowser speichern heutzutage allerhand Daten der Benutzer. Der Surf-Verlauf, Passwörter, Kreditkartendaten, Cookies und viele weitere sensible Informationen sind im Browser gespeichert, damit das Surfen schnell und bequem vor sich geht. Auch die Entwickler von Webseiten und die Werbebranche haben ein starkes Interesse daran, daß der Nutzer nicht komplett anonym ist – und verlassen sich z.B. auf Cookies, die ihrerseits zahlreiche Informationen besuchter Webseiten speichern ... *von Egon Kando*

All diese im Browser gespeicherten Informationen, wie besuchte Webseiten inklusive URL, Seitentitel und Zeitstempel, HTTP-Cookies, LocalStorage, Daten des Passwortmanagers, Browser-Cache und Daten, die automatisch ausgefüllt werden, stellen ein großes Risiko dar, sollten sie in die falschen Hände geraten. Nutzer wähnen sich größtenteils sicher, sind ihre Daten doch im Browser verborgen und darüber hinaus verschlüsselt. Doch an diese Browser-Daten zu gelangen, ist gar nicht so schwierig, wie man es vermuten möchte.

So können Hacker an die im Browser gespeicherten Nutzerdaten gelangen

Für Cyberkriminelle reicht einfach zu handhabende und leicht verfügbare Malware aus, um auf die in Webbrowsern gespeicherten Daten zuzugreifen. Bei einem Test von tausend der beliebtesten Websites, darunter Facebook, Google Mail, Amazon, Instagram und PayPal, fanden sich die persönlichen Daten der Benutzer, die lokal und im Webbrowser des Computers in den oben genannten Formaten gespeichert wurden. Durch die Überprüfung der gespeicherten Anmeldeinformationen sind Kriminelle in der Lage, gespeicherte Passwörter für alle getesteten Websites zu extrahieren. Dies ist keine Schwäche der Websites selbst, sondern der Standard-Passwortmanager von Webbrowsern. Wie kann man sich nur davor schützen?

Balance zwischen sicherem und bequemem Surfen

Überhaupt keine Daten abzuspeichern, indem man alle bestehenden Daten löscht und fortan im Incognito-Modus surft, böte die höchstmögliche Sicherheit. Das Surfen wäre damit zwar sicher, allerdings alles andere als bequem. Mit einigen Maßnahmen kann man jedoch die Sicherheit erhöhen, ohne die Bequemlichkeit zu opfern. Da die größte Bedrohung von Malware ausgeht, sollte eine Antivirensoftware ausgeführt werden. Dies sollte den Großteil aller Malware stoppen, inklusive der, die auf die Erfassung von Webbrowser-Daten abzielt. Auch die Verwendung eines Passwortmanagers von einem Drittanbieter ist in der Regel für Angreifer schwieriger zugänglich als die integrierten Browser-Passwortmanager. Ebenso läßt das Deaktivieren von HTTP-Cookies weniger Spielraum für Datenmißbrauch durch Angreifer, verursacht jedoch auf vielen Webseiten Probleme, insbesondere wenn diese eine Anmeldung erfordern. Eine effektive Methode ist es, regelmäßig entweder alle oder ausgewählte Browserverläufe zu löschen.

Egon Kando ist Regional Sales Director Central & Eastern Europe bei Exabeam. Der diplomierte Ingenieur ist seit über 18 Jahren im IT-Security Markt tätig.

Großes Risiko für Verbraucher und Unternehmen

Die Gefahr, daß im Browser gespeicherte Nutzerdaten gehackt und genutzt werden, ist nicht nur für Verbraucher groß, sondern auch für Unternehmen. So können Firmenkundendaten abgegriffen und in einigen Fällen Bankkontonummern wiederhergestellt werden. Darüber hinaus können Kriminelle feststellen, wann ein Mitarbeiter in der Regel am Arbeitsplatz und wann er zu Hause ist. Der Zugriff auf den Browser-Verlauf des Mitarbeiters zeigt Angreifern auch dessen persönliche Interessen oder Details aus dem Privatleben und kann so helfen, Passwörter zu erraten. Um das Risiko von gespeicherten Unternehmensdaten in von Mitarbeitern genutzten Browsern zu minimieren, gelten prinzipiell die gleichen Maßnahmen wie für Verbraucher. Ein weiteres wichtiges Werkzeug im Kampf gegen Angreifer sind gezielte Schulungen von Mitarbeitern, um deren Bewußtsein für die möglichen Gefahren zu sensibilisieren. Der Schutz durch wachsame Mitarbeiter ist seit jeher einer der Grundpfeiler der IT-Sicherheit jedes Unternehmens.

FAZIT

Auch Unternehmen müssen sich der Gefahr von in Browsern gespeicherten Daten bewußt sein. Um die Sicherheit zu erhöhen, ohne die Bequemlichkeit beim Surfen zu opfern, können zahlreiche Maßnahmen ergriffen werden, die es Cyberkriminellen erschweren, an die wertvollen Daten zu gelangen. <<

Bild: Exabeam