Ein gigantisches Auge schaut uns beim Websurfen über die Schulter

Gierig, lautlos, unberechenbar – JavaScript ist der neue Stern am Cyberschurken-Himmel und vermiest einem gehörig das Surfen oder virtuelle Shoppen.

Wiesbaden, 5. Dezember 2017. Das nächste Mal, wenn man eine Webseite öffnet, stelle man sich vor, dass gleichzeitig eine Filmcrew eintrifft. Ein Kameramann platziert seine Kameralinse direkt über der eigenen Schulter und zwar so blitzartig schnell, dass die Webseite, die man gerade aufruft, noch nicht einmal vollständig geladen ist. Da hat die mitschauende Kameralinse bereits alles auf dem Bildschirm gierig erfasst. Jeder Mausklick, Scroll und Tastenschlag wird registriert. Unrealistisch? Mit Nichten, denn man vergisst allzu gerne, dass die virtuelle Linse existiert, alles sieht und speichert. So bewegt man sich beispielsweise durch den Checkout-Prozess und wird nach Namen, Adresse und Bezahlmodalitäten gefragt. Solange die Daten noch unversendet auf dem Bildschirm stehen, klebt der Kameramann die Kreditkartennummer mit einem Klebesteifen ab und filmt dann alles. Clever, denkt man noch, dass er die Kreditkartennummer abgedeckt hat, doch Name, Adresse, Email, Kartenfälligkeit wurde vom Tape nicht verdeckt. Prompt fällt einem ein, dass der Kameramann beim Log-in das Passwort ebenfalls nicht abgedeckt hat – Ungemach macht sich breit. Natürlich ist diese Geschichte nicht wahr. Das alles passiert nämlich ohne Kameramann.

Das allwissende, gierige Auge Saurons

JavaScript ist für dieses Szenario verantwortlich. Eine Programmiersprache, die in Webseiten eingebettet wird und die – mehr als jede andere Technologie – das WWW von einer Sammlung an Dokumenten zu einer Kollektion von interaktiven Apps verwandelt. Die betagte, funktionsreiche und etablierte Werkzeugtasche beult sich mit so nützlichen Sachen, wie: clientX und clientY Tools, die die exakte Lokalisierung des Cursors erfassen. Das onkeypress-Ereignis, das jeden Tastendruck verfolgt. Die value-Eigenschaft, die den Inhalt von Formularfeldern festhält. Und darüber hinaus unzählige Objekte, Eigenschaften und Ereignisse, die Webseiten Zugang zu allem möglichen geben, vom aktuellen Aufenthaltsort bis zum Akkustatus des Laptops.

JacaScript Funktionen lassen sich verbinden, so dass sich jede winzige Aktion, die man auf der Webseite macht, aufgenommen wird. Das Skript, dass die Session wiedergibt, operiert wie ein stiller Kameramann. Diese Skripte sind nicht sinnfrei. Sie existieren, um den Webseiten-Betreibern bei der Verbesserung ihrer Seite zu helfen, indem sie das User-Verhalten beobachten. Aber: wie viele Webseiten-Nutzer realisieren, dass da gerade gigantische Mengen an Daten gesammelt werden und dass ihre Entscheidung, die Ware im virtuellen Einkaufskorb nun zur Kasse zu bringen oder die Seite zu verlassen, völlig egal ist, und sämtliche geernteten Daten unter den Fittichen von ausgelagerten Tracking-Firmen sind?

Abhilfe schaffen

Eine aktuelle Studie von Wissenschaftlern der Princeton Universität zur Exfiltration von persönlichen Daten durch Session-Replay Skripte zeigte, in welchem Ausmaß dieser Code auf ganz normalen Webseiten eingesetzt wird, darunter bei hp.com, intel.com, costco.com und gap.com. Zwar sollte jeder Webseitenbetreiber darauf achten, dass die persönlichen Daten der Besucher nicht vom alles verschluckenden Auge Saurons gesehen werden. Bislang kann man sich darauf jedoch nicht verlassen. Aber Nutzer des Internets haben

Möglichkeiten, sich vor solchen Machenschaften zu schützen und es kommt vielleicht sogar Hilfe von offizieller Seite:

- Vor Session-Aufnahmen kann man sich auf die gleiche Art verabschieden, wie man das auch mit anderen Formen unerwünschten Trackings macht: indem man Browser Plugins verwendet, wie Ghostery oder Privacy Badger. Diese Tools können das Abgreifen von Informationen verhindern.

- Die Datenschutz-Grundverordnung regelt ab Mai 2018, wie Daten gesammelt, gelagert, zugänglich und genutzt werden dürfen. Auch wie Nutzer darüber informiert werden müssen und was bei Zuwiderhandlungen droht. Zwar kann die falsche Datenlagerung sehr teuer werden aber in Anbetracht einer weltweiten Vernetzung, ist diese europäische Regelung vielleicht nicht durchgängig wirkungsvoll.

Michael Veit, IT-Sicherheitsexperte bei Sophos, prognostiziert: „Im Sinne der Datenschutz Grundverordnung sollten Unternehmen im eigenen Interesse sehr vorsichtig sein, welche Daten sie sammeln und speichern. Es ist zu erwarten, dass verantwortungsvolle Unternehmen einen gewissen Teil an Datensätzen sogar löschen werden, um nicht Gefahr zu laufen, mit den neuen Gesetzen in Konflikt zu kommen – je weniger man aufbewahrt, desto weniger kann man verlieren. Allerdings ist dies noch keine Garantie für den Nutzer im Unternehmen oder zuhause. Hier gelten zwei grundsätzliche Regeln. Erstens kritischer im Surfverhalten zu sein und Daten nur dann anzugeben, wenn unbedingt nötig. Zweitens sollten die entsprechenden Security-Mechanismen installiert sein und dazu gehören neben dem wirksamen Security Tools auch Privacy Plugins für den bevorzugten Browser."

Mehr Details dazu steht auf Naked Security unter:
https://nakedsecurity.sophos.com/2017/11/24/a-gargantuan-all-seeing-eye-is-watching-you-on-popular-websites/

Über Sophos
Sophos ist führender Anbieter von Endpoint- und Network-Security-Lösungen der nächsten Generation. Als Pionier der Synchronized Security entwickelt Sophos sein innovatives Portfolio an Endpoint-, Netzwerk-, Verschlüsselungs-, Web-, E-Mail- und mobilen Security-Lösungen, die miteinander kommunizieren. Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Lösungen von Sophos mit hervorragendem Schutz vor anspruchsvollen Bedrohungen und Datenverlust. Sophos Produkte sind exklusiv über den weltweiten Channel mit mehr als 26.000 registrierten Partnern erhältlich. Sophos hat seinen Hauptsitz in Oxford, Großbritannien, und wird an der Londoner Börse unter dem Symbol "SOPH" öffentlich gehandelt. Weitere Informationen unter www.sophos.de

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +172 4536839
sophos@tc-communications.de