OWASP Global AppSec:
Webseiten gekonnt schützen

Ständig gefordert

Benjamin Häublein

Das Absichern von Webseiten und Cloud-Daten ist nach wie vor ein aktuelles Thema. Diesmal standen neue Browsermechanismen und die Tücken von Sprachassistenten im Blickpunkt der Konferenz.

Eine der drei diesjährigen Global-AppSec-Veranstaltungen fand vom 26. bis 30. Mai in Tel Aviv statt. Bereits im letzten Jahr hätte die AppSec Europe zunächst in Tel Aviv stattfinden sollen. Aufgrund von Problemen in der Planung wurde sie jedoch Anfang des Jahres nach London verlegt. Veranstalter ist die OWASP Foundation, die der IT-Sicherheitscommunity hauptsächlich durch die Sicherheitsrisikenliste OWASP Top 10 bekannt ist. Die Organisation ist in vielen Ländern durch jeweilige „Chapters" vertreten, so auch in Israel. Die bei der AppSec sonst übliche strikte Trennung der Tracks zwischen „Breakers, Builders and Defenders" fiel in diesem Jahr weniger auf als sonst. Israel ist als Standort vieler Hersteller innovativer Sicherheitsprodukte bekannt. Entsprechend zahlreich waren sie auf der Konferenz in Tel Aviv präsent.

Auch große, internationale Unternehmen wie Google, Microsoft und Netflix waren durch Vorträge vertreten. Krzysztof Kotowicz, Mike Samuel und Lukas Weichselbaum von Google präsentierten eine Auswahl neuer Browsermechanismen, die vor einer Vielzahl von Angriffen schützen sollen. So lassen sich Übergriffe zwischen Webseiten verschiedenen Ursprungs durch den Einsatz des Cross-Origin Opener Policy Headers verhindern. Dieser weist moderne Browser an, die Webseite von anderen offenen Webseiten zu isolieren. Bisher war es in Spezialfällen erlaubt, unter anderem auf den Titel der Seite zuzugreifen. Dadurch lässt sich in manchen Fällen erkennen, ob der aktuelle Benutzer auf der Zielseite eingeloggt ist.

Die neuen Sec-Fetch-* Headers in HTTP-Anfragen erlauben es einer Webapplikation, auf Serverseite festzustellen, welche Interaktion den Request auslöst. Die Headers enthalten Informationen darüber, ob das Erstellen der Anfrage durch eine Seite derselben Domain erfolgte, ob eine bewusste Benutzernavigation vorliegt oder ob eine Webapplikation die Anfrage browserseitig ausgelöst hat. Die Überprüfung dieser Werte ermöglicht dem Server, Cross-Site-Request-Forgery-Angriffe zu erkennen.

Immer wieder Cross-Site Scripting

Um Cross-Site Scripting (webseitenübergreifendes Scripting, XSS) einzudämmen, hilft der Einsatz einer Content-Security-Policy, Version 3, mit sogenannten Nonces in Applikationen (Nonce steht für Number Used Once und bezeichnet eine für einen bestimmten Zweck einmalig verwendete Zahl). Nonces erlauben es dem Browser, zu erkennen, welche Skripte innerhalb von Webseiten die Applikation auf Serverseite gewollt gesetzt hat. Der Gebrauch älterer Content-Security-Policy-Versionen ist beim Einsatz umfangreicher Policies nicht mehr zu empfehlen, da sie sich leicht umgehen lassen.

In Zukunft sollen sogenannte „Trusted Types" DOM-XSS bekämpfen, das erst beim Ausgeben von Werten durch JavaScript im Browser selbst zur Auslösung kommt. Sie ermöglichen es, mit JavaScript eine Liste erlaubter Werte zur Ausgabe zu definieren. Bei der Übergabe eines nicht erlaubten Wertes kann dieser entweder verworfen werden oder eine Fallback Policy für diesen Fall greifen. Eine solche Policy kann zum Beispiel mit DOMPurify die Ausgabe bereinigen, um Angriffe durch bösartige Werte zu verhindern.

Amichai Shulman und Yuval Ron (Technion – Israel Institute of Technology) demonstrierten in ihrem Vortrag „Alexa and Cortana in Windowsland" verschiedene mittlerweile geschlossene Schwachstellen im Sprachassistenten Cortana unter Windows. Die Aufzeichnung der Sprachbefehle an Cortana erfolgt zwar auf dem Endgerät, die Verarbeitung und Interpretation jedoch in der Cloud. Daraus erhält Windows die Rückmeldung, welche Aktionen in der Folge durchzuführen sind. Alle vorgestellten Schwachstellen bezogen sich auf das Ausgangsszenario, dass der Bildschirm des Windows-Systems gesperrt, Cortana aber aktiv war.

Es war den beiden Sicherheitsforschern über mehrere Wege gelungen, Programme im Kontext des Benutzers, der den Bildschirm gesperrt hatte, auszuführen und so den Login zu umgehen. Dazu nutzten sie zum Beispiel die Möglichkeit, mittels Cortana einen Termin zu erstellen. Diese Termine konnten sie mit Fotos versehen. Zur Auswahl der Fotos startete das System einen Dateiauswahldialog im Kontext des Benutzers. In diesem Dialog erfolgte der Start von Programmen.

Lokale Lösungen noch nötig

Ähnliche Probleme brachte die Integration des Dienstes Alexa von Amazon in den Cortana-Dienst. Um Cortana zu aktivieren, wurde auch im Sperrbildschirm ein Anmeldedialog für Amazon angezeigt – ein eingeschränktes Browserfenster, dem beispielsweise die Adresszeile fehlte. Mit Mühen gelang es den Sprechern jedoch, dort gezielt Webseiten wie Facebook zu besuchen und die vom Benutzer im Browser gespeicherten Passwörter zu nutzen, um so unberechtigten Zugriff zu erlangen.

Besonders hoben beide Microsofts Vorgehen hervor, die Schwachstellen zu schließen. Zunächst soll Microsoft versucht haben, möglichst alle Fixes nicht auf den Systemen der Benutzer durch Windows-Updates, sondern durch Anpassung der Logik in der Cloud vorzunehmen. Erst nachdem es den beiden mehrfach gelungen war, über verschiedene Wege bestimmte Funktionen auszunutzen, habe Microsoft diese durch ein Windows-Update endgültig aus den Systemen entfernt. Aus der Cloud kommende Probleme erfordern teilweise noch eine lokale Lösung.

Wer in den nächsten Jahren die AppSec Europe besuchen möchte, darf sich nicht beirren lassen. Das Branding AppSec Europe wird wohl aufgegeben. Stattdessen sollen jährlich drei Veranstaltungen mit dem Namen Global AppSec stattfinden, eine davon in Europa.

(nb@ix.de)