Das Ende naht: Viele Browser entziehen SHA-1 SSL-Zertifikaten in Kürze ihr Vertrauen

Der Secure Hash Algorithm SHA-1, der dafür sorgt, die Integrität von SSL-Zertifikaten sicherzustellen, war einst eines der am weitesten verbreiteten SSL-Zertifikate. Er gilt allerdings schon seit längerem als veraltet und gilt als Ursache für mehrere prominente Websiten-Hacks, so dass seine Tage nun wohl tatsächlich gezählt sind. Apple, Microsoft, Google und Mozilla haben nähere Informationen dazu bekannt gegeben, wann ihre Browser Webseiten mit SHA-1 SSL-Zertifikaten nicht mehr als vertrauenswürdig einstufen.

- Google Chrome: Mit der neuen Version 56 wird Chrome SHA-1 SSL-Zertifikate ab Januar 2017 nicht mehr vertrauen und informiert die Anwender durch eine Sicherheitswarnung.
- Mozilla Firefox: Auch mit der neuen Version Firefox 51 im Januar 2017 zeigt der Browser bei jeder Seite, die immer noch SHA-1 verwendet, an: „Keine vertrauenswürdige Verbindung“.
- Apple Safari: Es liegt noch kein genaues Datum vor, wann Apple offiziell SHA-1-Zertifikaten nicht mehr vertraut. Die letzten Versionshinweise für MacOS empfehlen dringend, Webseiten mit SHA-1 so schnell wie möglich zu meiden. Die Sierra-Version des Browsers zeigt mittlerweile nicht mehr das grüne Vorhängeschloss, das auf eine vertrauenswürdige Webseite hinweist.
- Microsoft Internet Explorer and Edge: Webseiten, die zum Start des neuen Browser am 14. Februar 2017 immer noch SHA-1 verwenden, werden einfach nicht mehr geladen. Anwender können aber nach einer Warnung entscheiden, ob sie die Webseite aufrufen wollen

„In vielen dieser Fälle sollte allerdings beachtet werden, dass manuell installierte oder selbst signierte Zertifikate weiterhin unterstützt werden“, so Michael Veit, IT-Sicherheitsexperte bei Sophos.

Es hat lange gedauert, bis es zu der Ablehnung von SHA-1 kam. Fast alle Webseiten vertrauen seit langer Zeit auf SHA-1-Zertifikaten für ihre SSL-Verschlüsselung. Weil sie allerdings so weit verbreitet sind, können sie auch leicht gehackt werden und sind so ein beliebtes Ziel von Passwort-Hackern. Webseiten, die Passwörter der Anwender mit SHA-1 ausgeben, machen es Hackern besonders einfach: Wie kürzlich bei Naked Security berichtet, kann ein Password Cracking Server jede mögliche Passwort-Variante mit SHA-1 innerhalb einer Stunde ermitteln. SHA-1 stand in Verbindung mit vielen Sicherheitsvorfällen in der Vergangenheit, wie zum Beispiel bei LinkedIn oder LivingSocial.

Die Forderung, SHA-1 nicht mehr zu verwenden, geht bereits auf das Jahr 2005 zurück. 2012 hat das National Institute of Standards and Technology (NIST) seine Sicherheitsrichtlinien Special Publication 800-57 aktualisiert und empfahl die

Aufhebung von SHA-1 als Standard. Doch erst als Google 2014 mitteilte, Webseiten aktiv zu ahnden, die SHA-1 nach 2016 verwenden, bewegte sich etwas – auch bei den Leuten, bei denen die Botschaft bis dahin noch nicht durchgedrungen war.

Heute nehmen die meisten Webseiten die Warnungen ernst. Mozilla schätzt, dass nur noch weniger als ein Prozent aller Webseiten SHA-1 SSL nutzen, andere Zahlen sehen das bedeutend unentspannter und gehen von einem Drittel aller Webseiten aus. Wie auch immer, die Tage von SHA-1 sind gezählt und Betreiber sollten aktiv werden.

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
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de