# Verschlüsselung im Web

Chrome, Firefox & Co. verabschieden sich von TLS 1.0/1.1

Ab 2020 sollen die großen Webbrowser die als unsicher geltenden TLS-Versionen 1.0 und 1.1 nicht mehr unterstützen.

Verschlüsselung im Web: Chrome, Firefox & Co. verabschieden sich von TLS 1.0/1.1

Das Ende des Verschlüsselungsprotokolls Transport Layer Security (TLS) in den Ausgaben 1.0 und 1.1 rückt näher: Die Browser Chrome, Edge, Firefox, Internet Explorer 11 und Safari sollen die als veraltetet und unsicher geltenden TLS-Versionen ab 2020 nicht mehr unterstützen.

Der TLS-Standard sorgt im Internet in Form von HTTPS für einen verschlüsselten Seitenabruf. Außerdem ist TLS der wichtigste Standard für Authentifizierung im Internet. TLS 1.0 ist seit 19 Jahren im Einsatz. Die veralteten Versionen setzen unter anderem auf die schon lange als unsicher geltenden Hash-Verfahren MD5 und SHA-1.

Stellt ein Admin 2020 seinen Webserver nicht auf mindestens TLS 1.2 um, könnten Websites mit den Browsern nicht mehr abrufbar sein. Web-Admins sollten aber nicht nur Umstellen, sondern TLS 1.0 und 1.1 aus Sicherheitsgründen komplett deaktivieren. Ansonsten könnten Angreifer gegebenenfalls Websites mit Downgrade-Attacken wie Freak ins Visier nehmen.

Wann geht es los?

Microsoft hat bekanntgegeben, dass die Browser Edge und Internet Explorer 11 ab der ersten Hälfte 2020 die veralteten TLS-Versionen nicht mehr unterstützen. Google schreibt in seinem Security-Blog, dass Chrome derzeit noch 0,5 Prozent der HTTPS-Verbindungen via TLS 1.0 und 1.1 aufbaut. Damit soll in Testversionen des Browsers ab Anfang 2020 Schluss sein. In der finalen Ausgabe Chrome 81 sollen die Versionen dann endgültig deaktiviert sein.

Mozilla verkündet in seinem Blog, dass Firefox noch 0,1 Prozent alle Websites mit TLS 1.1 abruft. Im März 2020 wollen sie die Unterstützung streichen. Apple schreibt im WebKit-Blog, dass Safari noch rund 0,36 Prozent aller HTTPS-Verbindungen mit TLS 1.0 und 1.1 aufbaut. Apple will die Unterstützung ebenfalls im März 2020 fallen lassen.

Aussichten

Die Internet Engineering Task Force (IETF) arbeitet derzeit an einem Internet-Draft, den Einsatz von TLS 1.0 und 1.1 zu "verbieten". Wann es zu einer Finalisierung kommt, ist bislang unbekannt. Bereits erfolgreich als Standard verabschiedet ist indes TLS 1.3. Die aktuelle Version setzt unter anderem auf moderne Krypto-Algorithmen für die Transportverschlüsselung. Zudem ist beispielsweise der Einsatz von SHA-1 verboten. (des)