Pressemitteilung

Von Vorhängeschlössern und grünen Unternehmensnamen: So sichern Zertifikate Webseiten

- Zertifikatstyp und Aussteller bestimmen Sicherheitslevel
- Hohes Vertrauen nur bei Identitätsprüfung der Organisation
- Google-Zertifikatspläne: Rückschlag für Souveränität europäischer Internet-Nutzer
- IT-Sicherheitsmesse it-sa: Bundesdruckerei berät Organisationen bei Zertifikatsauswahl

Berlin, 8. Oktober 2018 – Google und andere Anbieter von Internetbrowsern forcieren aktuell den Einsatz sogenannter SSL-Zertifikate. Diese ermöglichen einen verschlüsselten Datentransfer zwischen dem Computer des Internet-Nutzers und Webseiten. So warnt der Google-Browser Chrome vor unverschlüsselten Seiten mit dem Hinweis „Nicht sicher". Umso wichtiger wird es für Unternehmen und Behörden, die eigenen Webseiten mit SSL-Zertifikaten zu schützen oder bestehende Zertifikate zu aktualisieren. Zahlreiche Zertifizierungsstellen (Certification Authorities, abgekürzt: CA) bieten Varianten von SSL-Zertifikaten an. Im behördlichen und geschäftlichen Umfeld empfehlen die IT-Sicherheitsexperten der Bundesdruckerei Zertifikatstypen mit Identitätsnachweis. „Eine Webseite ist erst dann vertrauenswürdig und sicher, wenn die Identität des Inhabers geprüft und bestätigt wurde", sagt Dr. Kim Nguyen, Geschäftsführer der Bundesdruckerei-Tochter D-TRUST, einem der größten Zertifikatsanbieter im EU-Raum.

SSL-Zertifikate werden von externen Zertifizierungsstellen verschiedener EU-Staaten ausgegeben. Dazu zählt auch die Zertifizierungsstelle „Let's Encrypt", deren Geschäftsmodell auf der Ausgabe kostenloser Zertifikate basiert. Bei diesen Zertifikaten wird jedoch die Identität des Seiteninhabers nicht überprüft. Somit können auch Cyberkriminelle leicht an Zertifikate kommen und mit gefälschten Webseiten Datenmissbrauch betreiben. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt seit Jahren vor solchen „gefälschten Zertifikaten".

Vertrauenswürdigkeit der Zertifizierungsstelle wichtig

Die europäische „Verordnung über elektronische Identifizierung und Vertrauensdienste" (eIDAS) bezeichnet besonders vertrauenswürdige Zertifizierungsstellen als qualifizierte Vertrauensdiensteanbieter. Für diesen

Status müssen Vertrauensdiensteanbieter die verschärften EU-Vorgaben umsetzen und werden regelmäßig von den nationalen Aufsichtsbehörden kontrolliert. Nguyen: „Qualifizierte Vertrauensdiensteanbieter sind die europäische Antwort auf die Frage: Wie lässt sich Vertrauen und Sicherheit in unsicheren Netzen herstellen?"

Zertifikat ist nicht gleich Zertifikat

SSL-Zertifikate lassen sich in die folgenden Typen und Sicherheitsniveaus unterteilen (siehe auch Grafik).

1. Domainvalidierte Zertifikate

Am weitesten verbreitet ist die Domain-Validierung (Domain Validation, abgekürzt: DV). Sie bietet die niedrigste Sicherheitsstufe. Die Zertifizierungsstelle prüft bei diesem Zertifikatstyp per E-Mail, ob der Auftraggeber auch Inhaber der Domain ist. Die Identität des Antragstellers wird nicht überprüft. Cyberkriminelle können also leicht DV-Zertifikate für ihre gefälschten Webseiten erhalten. DV-Zertifikate gibt es kostenlos oder zu günstigen Preisen bei Zertifizierungsstellen und Webhostern.

2. Organisationsvalidierte Zertifikate

Bei organisationsvalidierten SSL-Zertifikaten (Organization Validation, abgekürzt: OV) findet zusätzlich zum Domaincheck eine Identitätsprüfung der Organisation statt. Der Inhaber der Domain weist sich durch Dokumente wie einen Handelsregisterauszug aus. So wird ein Missbrauch weitgehend ausgeschlossen. OV-Zertifikate erfüllen hohe Sicherheitsanforderungen und sind daher für Webseiten von Unternehmen und Behörden erste Wahl. Sie werden von kostenpflichtigen Zertifizierungsstellen und Webhostern vergeben.

3. Erweitert validierte Zertifikate

Das höchste Sicherheitsniveau bieten sogenannte erweitert validierte Zertifikate (Extended Validation, abgekürzt: EV). Zusätzlich zum Domaincheck und zur Organisationsvalidierung erfordern sie einen individuellen Identitätsnachweis des Antragstellers. Dabei wird geprüft, ob diese Person tatsächlich bei der Organisation angestellt ist und ein EV-Zertifikat erwerben darf. Diese Zertifikate sorgen für Sicherheit auf Online-Banking-Niveau. Zum Einsatz kommen sie entsprechend vor allem bei Banken und Versicherungen sowie einigen Online-Shops. Wie OV-Zertifikate werden sie von kostenpflichtigen Zertifizierungsstellen und Webhostern vergeben.

4. QWACS

Eine besondere Form der EV-Zertifikate sind die qualifizierten Webseitenzertifikate (Qualified Website Authentication Certificates, abgekürzt: QWACS). Technisch entsprechen sie den EV-Zertifikaten, hinzu

kommt eine besonders hohe Rechtsverbindlichkeit im gesamten EU-Raum. Diese basiert auf der eIDAS-Verordnung. „Qualifizierte Webseitenzertifikate sind für Anwendungen mit den höchsten Sicherheitsanforderungen interessant. Dazu gehört Banking gemäß der neuen EU-Zahlungsrichtlinie PSD2, aber auch die digitale Vernetzung von Registern bei Behörden", erläutert Nguyen. QWACS dürfen nur von qualifizierten Vertrauensdiensteanbietern mit Sitz in der EU herausgegeben werden. In Europa ist D-TRUST aktuell einer der wenigen Anbieter von QWACS.

Google-Pläne beschränken digitale Souveränität europäischer User

Gemeinsam mit anderen Browser-Anbietern plant Google, die visuellen Hinweise, an denen der User den Zertifikatstyp und damit das Sicherheitsniveau erkennt, weitestgehend zu entfernen. Das sind zum Beispiel ein grünes Vorhängeschloss oder der Organisationsname in grüner Schrift. Sollten zukünftig nur noch Warnhinweise vor unverschlüsselten SSL-Verbindungen im Browser sichtbar sein, bedeutet dies für Nguyen einen Eingriff in die digitale Souveränität in Europa: „Europäischen Internet-Nutzern wird die Möglichkeit genommen, auf den ersten Blick in der Adresszeile zu erkennen, wer hinter einer Webseite steht", so Nguyen. „Sollte Google sein Interesse durchsetzen, wird der Anreiz für Webseitenbetreiber sinken, solche sicheren OV-Zertifikate einzusetzen. Dem Verbraucher würden somit zusätzliche Informationen über die Organisation im Zertifikat vorenthalten."

Auf der IT-Sicherheitsmesse it-sa vom 9. bis 11. Oktober in Nürnberg berät die Bundesdruckerei auf ihrem Stand (Halle 10) Organisationen bei der Zertifikatsauswahl. Weitere Infos gibt es hier.

Über die Bundesdruckerei

Die Bundesdruckerei GmbH unterstützt Staaten, Organisationen und Unternehmen mit Lösungen und Produkten für sichere Identitäten und sichere Daten. Die Technologien und Dienste zum Schutz sensibler Daten, Kommunikation und Infrastrukturen sind „Made in Germany". Sie basieren auf der zuverlässigen Identifikation von Personen und Objekten in der analogen und digitalen Welt. Die Bundesdruckerei erfasst, verwaltet und verschlüsselt Daten, produziert ID- und Wertdokumente sowie Prüfgeräte, entwickelt Software für hochsichere Infrastrukturen und bietet Pass- und Ausweissysteme sowie automatische Grenzkontrolllösungen an. Zur Bundesdruckerei-Gruppe gehören die Konzerngesellschaften D-TRUST GmbH, genua GmbH, Maurer Electronics GmbH und iNCO Sp. z o.o. Die Unternehmensgruppe beschäftigt über 2.500 Mitarbeiter und erzielte 2017 einen Umsatz von 520 Millionen Euro. Die Bundesdruckerei hält zudem Anteile an der Veridos GmbH, DERMALOG Identification Systems GmbH, cv

cryptovision GmbH und verimi GmbH. Weitere Infos unter www.bundesdruckerei.de.

Kontakt Bundesdruckerei:
Marc Thylmann
Pressesprecher
Bundesdruckerei GmbH
Tel.: +49 (0)30 2598 2810
Fax: +49 (0)30 2598 2808
E-Mail: marc.thylmann@bdr.de