

Mehr Sicherheit für den Internetbenutzer

Ein kleines Vorhängeschloss symbolisiert dem Internetbenutzer, dass er sich angeblich auf einer sicheren Webseite befindet – doch welcher Anwender achtet darauf? Dies machen sich kriminelle Organisationen zunutze, indem sie dem Website-Besucher vorgaukeln auf einer vermeintlich sicheren Webseite zu sein, auf der er gar nicht ist. Nichtsahnend gibt der Benutzer seine Identifikation und sein Passwort preis.

Mit der Erweiterung des Online-Business wuchs die Sorge um die Zunahme von «Phishing» und anderen Internetbetrügereien, welche nebst finanziellen Folgen auch das Vertrauen in die elektronische Kommunikation schwächen. Der ursprünglich 1993 erstellte SSL-Standard erforderte von den Zertifikatsherausgebern keine weitergehenden Prüfungen betreffend Identität des Antragsstellers und dessen Berechtigung als Domäneninhaber. Die meist automatisch durchgeführte Prüfung ermöglicht damit technisch versierten

Hackern, mit gefälschter Identität, ein SSL-Zertifikat im Namen einer bekannten Firma oder Marke zu erwerben, um es für kriminelle Handlungen wie Identitätsdiebstahl (Phishing) einzusetzen. Dies hatte in den letzten Jahren zur Folge, dass das Vertrauen in SSL-Zertifikate geschwächt wurde. Kunden konnten nicht absolut sicher sein, ob sie sich auf der richtigen Webseite befinden oder gerade Opfer einer Phishing-Attacke waren.

Vom internationalen Industriekonsortium CA/Browser Forum (www.cabforum.org) wurde deshalb der neue SSL-Zertifikats-Standard ins

WEITERE INFORMATIONEN ZUM THEMA EV SSL

- CA/Browsers Forum: www.cabforum.org
- Authentication and Online Trust Alliance (AOTA): www.aotalliance.org
- QuoVadis Trustlink Schweiz AG: www.quovadis.ch

Leben gerufen. Teilnehmer am CA/Browser Forum waren führende internationale Certificate Authorities, die bekanntesten Browser-Anbieter (inkl. Microsoft, Mozilla, Opera und Konqueror), das «American Bar Association Information Security Committee» und WebTrust für Certification Authorities.

Einheitlicher Standard

Ziel war es, einen neuen, einheitlichen Prüfungsstandard für alle Zertifikatsherausgeber (Certificate Autho-

rities) zu setzen, unabhängig vom Standort des Unternehmens und der geschützten Webseite. Zusätzliche Identitätsinformationen sollen klar in den Browsern der neuen Generation automatisch angezeigt werden. Das existierende Vorhängeschloss-Symbol (yellow padlock) soll durch einen auffälligen Balken ergänzt werden, sodass die Besucher sich einfach versichern können, dass sie sich auf der richtigen und nicht auf einer gefälschten Website befinden. Der Webseitenbesucher soll die Identität



Quelle: iStockphoto

und Legitimität des Unternehmens besser überprüfen können, und das Vertrauen in das Unternehmen und die Kommunikationsbereitschaft zwischen dem Besucher und der angezeigten Webseite sollen erheblich gesteigert werden.

Die Mitte 2007 angekündigten neuen EV SSL-Zertifikate (erkennbar am grünen Balken im Internet Browser) haben sich innert weniger Monate durchgesetzt und erfreuen sich immer grösserer Beliebtheit. Die aktuelle von der Allianz für Authentisierung und Vertrauen im Internet AOTA (www.aotaalliance.org) publizierte Liste zeigt, dass die Webseiten von bereits über 3000 Firmen durch den Einsatz dieser neuen EV SSL-Zertifikate mehr Vertrauen und Sicherheit ausstrahlen und den Besuchern der Webseiten mehr Sicherheit geben.

Daran erkennt man's

Stösst ein Browser auf eine Webseite mit einem EV SSL-Zertifikat, so färbt sich der Adressbalken grün. Der Name des Zertifikatsinhabers und des vertrauenswürdigen Zertifikatsausstellers werden angezeigt. Das Wissen, auf der authentischen Webseite zu sein und dies auch über-



Grün bedeutet vertrauenswürdig und unbedenklich.

prüfen zu können, erhöht somit das Vertrauen des Benutzers zum Zertifikatsinhaber.

Beim Vorfinden des grünen Balkens hat der Besucher die Gewähr, dass eine rigorose Überprüfung der

Firma und der Domäne durch den autorisierten Zertifikatsaussteller im Vorfeld erfolgte. Dabei wird auch überprüft, ob das Unternehmen physisch, rechtlich und operativ existiert sowie ob die angegebene Domäne dem Unternehmen wirklich gehört. Die Prüfungen umfassen zusätzlich eine schriftliche Bestätigung durch eine dritte Partei (z.B. einen Notar oder die eingetragene Revisionsstelle gemäss Handelsregister-eintrag).

Der praktische Nutzen liegt auf der Hand: Einer der grössten Stolpersteine für die Kommunikation und den Online-Handel ist die Eingabe von persönlichen Daten und Kreditkarteninformationen. Die Bedenken bezüglich der Sicherheit der persönlichen Daten können den Kaufimpuls hemmen oder den Benutzer von einer elektronischen Transaktion abhalten. Färbt sich aber die Adressleiste des Browsers grün, so kann sich der Kunde auf die Sicherheit der Daten verlassen. Dies steigert das Sicherheitsgefühl beim Kunden und führt schlussendlich zu einem ungetrübten Einkaufsvergnügen. Die Zertifikatsausstellung erfolgt durch speziell geprüfte und anerkannte Zertifikatsanbieter gemäss den erhöhten Sorgfaltspflicht-Standards des CA/Browser Forums. In der Schweiz ist dies QuoVadis.



QuoVadis ist ein in der Schweiz und international akkreditierter Zertifizierungsdiensteanbieter (CSP Certification Service Provider) mit weltweiter Anerkennung (WebTrust). Angeboten werden elektronische Zertifikate nach Schweizerischer (ZertES) und europäischer Gesetzgebung (ETSI). Mit diesen Zertifikaten sind die Benutzer in der Lage, digitale Signaturen rund um den Globus anzuwenden.

Daneben bietet QuoVadis ihren Kunden und Geschäftspartnern Dienstleistungen und Lösungen an, mit deren Hilfe Geschäfte auf elektronischem Weg gesetzeskonform, sicher und vor allem vertrauenswürdig abgewickelt werden können.

QuoVadis bietet auch schlüsselfertige PKI-Lösungen als Managed Service im Outsourcing oder Root-Signing für bestehende Corporate CAs an.

Kontakt:
QuoVadis Trustlink Schweiz AG
 Teufenerstrasse 11
 9000 St.Gallen
 Tel. +41 71 272 60 60
 info.ch@quovadisglobal.com
 www.quovadis.ch

WEITERE ANWENDUNGSBEREICHE

Document Signing

Das Schweizerische Obligationenrecht (Art. 14 Abs 2bis OR) stellt die elektronische Signatur der Handunterschrift gleich. Mit dem qualifizierten elektronischen Zertifikat können verbindliche Signaturen im Sinne der Willensäusserung erstellt werden.

Secure E-Mail Communication

Mit der digitalen Signierung des E-Mails auf Basis eines anerkannten elektronischen Zertifikates wird die Datenintegrität und damit die Unanfechtbarkeit des E-Mails sichergestellt. Das E-Mail inkl. der beigefügten Anhänge (wie Word, Excel, PDF usw.) wird sicher und beweisfähig. Optional kann das E-Mail auch gleichzeitig mit Hilfe des Zertifikates verschlüsselt werden.

Document Archiving und Workflow

Für die gesetzeskonforme Ablage und Archivierung von elektronischen Dokumenten ist die elektronische

Signatur oder der elektronische Zeitstempel von grosser Bedeutung. Die elektronische Signatur stellt die Datenintegrität (Unverfälschbarkeit), Authentizität (Urheberschaft) und die Unanfechtbarkeit des Dokumentes sicher, gemäss den Vorgaben der Geschäftsbücherverordnung (GeBüV).

E-Commerce & e-Invoicing

Elektronische Rechnung, der damit verbundene elektronische Versand der Rechnungen sowie die unternehmensübergreifenden Geschäftsprozesse werden dank dem Einsatz des EIDI-V-konformen Zertifikates markant unterstützt.

Secure Login Procedures

Sicher und einfach ist das Login in Firmennetzen, basierend auf einem elektronischen Zertifikat. Der Benutzer setzt den USB-Token oder die Smartcard ein und hat lediglich noch den PIN einzugeben.