LANCOM™ Techpaper
Zertifikatsmanagement im Public Spot

Einleitung

Sicherheit ist bei dem Einsatz eines Public Spots ein wichtiges Thema. Dabei liegt der Focus auf der Verschlüsselung der Benutzeranmeldung und nicht der des allgemeinen Datenverkehrs über das WLAN. Dies ist relevant, damit sowohl Betreiber, als auch Nutzer sicherstellen können, dass mit den Zugangsdaten, die zur Verfügung gestellt werden, kein Missbrauch getrieben wird. Dieses Techpaper geht darauf ein, wie Zertifikate für eine entsprechende Sicherheit sorgen.

HTTPS

Um die sichere Anmeldung zu gewährleisten, wird auf HTTPS, eine Kombination von HTTP und SSL (Secure Sockets Layer) zurückgegriffen, damit die Daten verschlüsselt zwischen Client und Server übertragen werden. Hierbei wird das Gerät, welches den Public Spot bereitstellt als Server betrachtet und das Gerät, welches ihn nutzt als Client.

HTTPS nutzt Zertifikate des Standards X.509 der International Telecommunication Union (ITU). Ein Zertifikat besteht immer aus zwei Bestandteilen, einem öffentlichen Schlüssel und einer Signatur, die mit Hilfe eines privaten Schlüssels erstellt wurde. Der private Schlüssel bleibt dabei immer im Besitz des Servers und wird nicht übertragen.

Öffentliche und „Self-Signed" Zertifikate

Grundsätzlich gibt es drei verschiedene Arten Zertifikate zu erstellen: „Self-Signed" Zertifikate, bei dem der Server seinen öffentlichen Schlüssel selbst signiert, öffentliche Zertifikate, die von einer vertrauenswürdigen Stammzertifizierungsstelle (Certificate Authority - kurz CA) signiert wurden, und als dritte Möglichkeit die Signierung des öffentlichen Schlüssels durch eine private CA.

Die Aufgabe einer vertrauenswürdigen CA ist es sicherzustellen, dass der Antragsteller des Zertifikats für eine bestimmte Domäne auch der tatsächliche Domänenbesitzer ist, um den Missbrauch mit öffentlichen Zertifikaten zu verhindern. Ist eine Stammzertifizierungsstelle (Root CA) im Webbrowser als vertrauenswürdig eingestuft, werden alle Zertifikate, welche von ihr signiert wurden, auch als vertrauenswürdig angesehen. Somit wird von einem Webbrowser die Anmeldeseite eines Public Spots dann als vertrauenswürdig behandelt, wenn ein entsprechendes, von einer öffentlichen Stammzertifizierungsstelle signiertes, Zertifikat verfügbar ist. Sicherheitswarnungen (Abb.1), die auf das Fehlen eines vertrauenswürdigen Zertifikats zurückzuführen sind, treten also nicht auf.

Ein solches Zertifikat ist allerdings kostenpflichtig und hat nur eine begrenzte Laufzeit und wird daher meist dann eingesetzt, wenn der Public Spot für geschäftliche Zwecke genutzt wird.

Sicherheitswarnungen des Browsers sind bei „Self-Signed" Zertifikaten nicht zu umgehen, da der Webserver zunächst nicht vom Browser als vertrauenswürdig eingestuft ist. Self-Signed Zertifikate haben aber auch Vorteile. Zum einen werden sie von dem Server bei Bedarf generiert und müssen nicht erst beantragt werden und zum anderen ist ein Self-Signed Zertifikat kostenlos, da keine externe Dienstleistung in Anspruch genommen werden muss.

Abb.1 Sicherheitswarnung des Internet Explorers

LANCOM Systems

LANCOM™ Techpaper
Zertifikatsmanagement im Public Spot

Der Anmeldevorgang

Bei einer Verbindung mit dem entsprechenden Webserver wird das Zertifikat an den Client übertragen und dieser prüft, ob die Signatur des Zertifikats vertrauenswürdig ist. Zertifikate einer Stammzertifizierungsstelle, bestehend aus ihrem öffentlichen Schlüssel und signiert mit ihrem privaten Schlüssel, sind in den Webbrowsern hinterlegt. Wird die Signatur als authentisch eingestuft, generiert der Client einen zufälligen Sitzungsschlüssel, der mit dem öffentlichen Schlüssel des Webservers verschlüsselt wird. Dieser Datensatz wird nun an den Webserver übermittelt, der ihn mit Hilfe seines privaten Schlüssels entschlüsseln kann.

Nun habe beide Parteien, Webserver und Client den Sitzungsschlüssel. Hiermit wird nun ein SSL-Tunnel mit einer 128 Bit Verschlüsselung zwischen Webserver und Client hergestellt, der genutzt wird um Daten zwischen den beiden Parteien zu übertragen. Somit sind die Anmeldedaten verschlüsselt und können nicht von dritten missbraucht werden.

Der Anmeldevorgang ist in Abb.2 schematisch dargestellt.

Zusätzliche Sicherheit

Für Public Spots bietet es sich an, mit einer Firewall spezifische Protokolle und Ports zu sperren, um Missbrauch weiter vorzubeugen.

Benutzerfreundlichkeit

In einem Public Spot ist die Benutzerfreundlichkeit sehr wichtig. Von daher sollte auf öffentliche Zertifikate zurückgegriffen werden, um Nutzer nicht den Sicherheitswarnungen des Webbrowsers auszusetzen und dadurch zu verunsichern.

Erwerb von Zertifikaten

Zertifikate, die durch eine vertrauenswürdige Stammzertifizierungsstelle signiert wurden, können bei den entsprechenden Unternehmen erworben werden. Einige Beispiele für Unternehmen, die einen entsprechenden Service anbieten, sind Deutsche Telekom (Telesec) und Verisign. Die Kosten für Standardzertifikate, die als vertrauenswürdig eingestuft werden, bewegen sich in einem Rahmen von niedrigen zweistelligen Beträgen pro Monat.

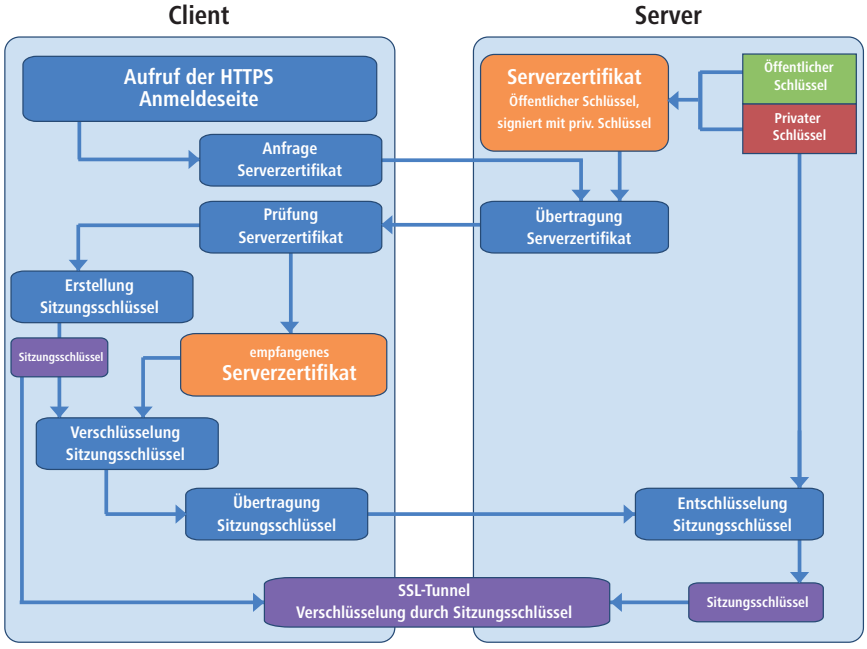

Abb.2 Schematische Darstellung eines HTTPS-Anmeldevorgangs

LANCOM Systems

LANCOM™ Techpaper
Zertifikatsmanagement im Public Spot

Implementierung

Sobald das Zertifikat vorhanden ist, muss es auf dem Gerät zur Verfügung gestellt werden. Bei einem LANCOM Gerät kann dies komfortabel mit Hilfe von LANconfig oder WEBconfig (Abb.3) geschehen. Zusätzlich muss noch über WEBconfig oder Kommandozeile im Feld *Geraete-Hostname* (Abb.4) der Name, auf den das Zertifikat verweist eingetragen werden. Die Auflösung des Names zur entsprechenden IP-Adresse des Gerätes muss natürlich gegeben sein.

Fazit

Bei geschäftlich genutzten Public Spots ist zu einem vertrauenswürdig eingestuftem Zertifikat zu raten, da es eine größere Sicherheit bietet und bei Gästen und Kunden kein Gefühl der Unsicherheit durch durch Sicherheitswarnmeldungen des Webbrowers hervorruft. Entsprechende Zertifikate sind einfach und kostengünstig zu beziehen, und die Integration in LANCOM Public Spot Lösungen kann einfach und schnell erfolgen.

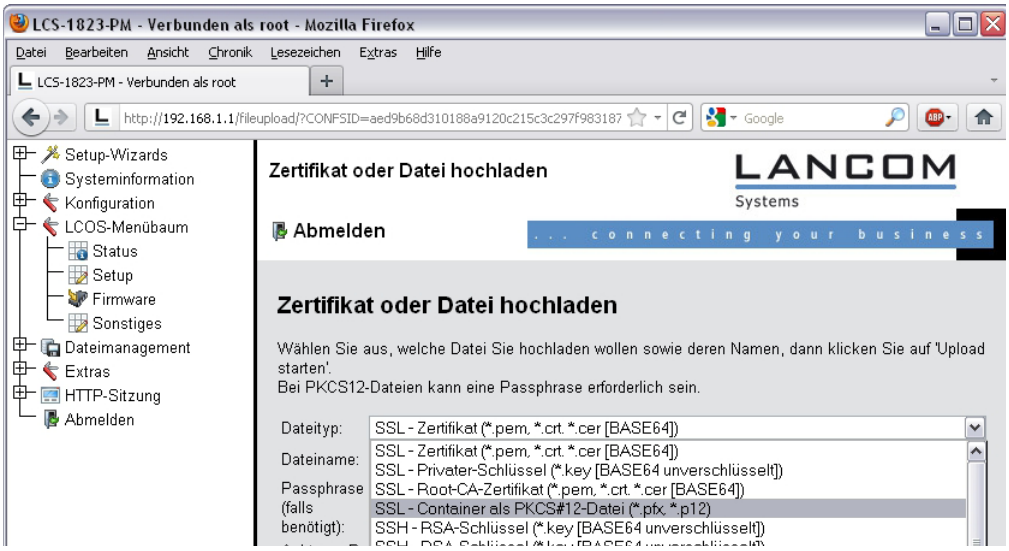

Abb.3 Einspielen eines Zertifikats über WEBconfig

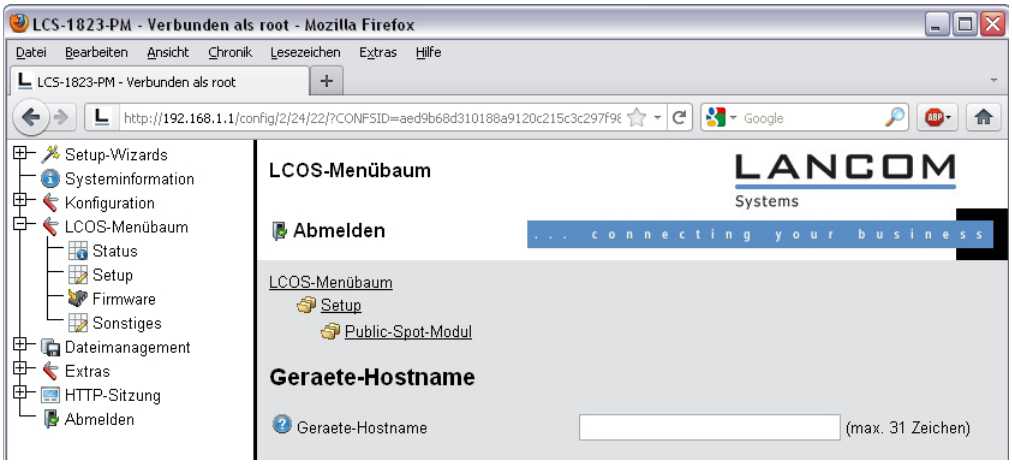

Abb.4 Eintrag des Gerätenamens über WEBconfig

LANCOM Systems GmbH I Adenauerstr. 20/B2 I 52146 Würselen I Deutschland I E-Mail info@lancom.de

LANCOM Systems