Die Aussichten von SSL Everywhere

SSL bildet im digitalen Zeitalter die letzte Verteidigungsfront für Kommunikation und Handel weltweit. Daher ist es für Unternehmen an der Zeit, zum Schutz von SSL ein höheres Sicherheitsniveau zu etablieren.

Whitepaper

Inhalt

Einführung

Bisher oblag allein dem Staat der Schutz der sicheren Datenübertragung. Doch durch die globale Ausweitung des World Wide Web ist die Kryptographie zum Anliegen für jedermann geworden. Aufgrund der Risiken durch Kriminalität und Ausspionieren werden heute fast alle wichtigen Sprach- und Handelsdaten mit einem einzigen kryptographischen Protokoll verschlüsselt: SSL.

SSL ist der Satz von kryptographischen Protokollen, der die Datenübertragung sichert. Heute ist SSL häufig das einzige Tool, das zwischen einem Lauscher und seinem Angriffsziel bzw. einem Dieb und einem Händler steht. Daher ist SSL so wichtig wie nie zuvor. Auch wenn es eine unbequeme Wahrheit ist – Unternehmen müssen ihr gesamtes Sicherheitsniveau erhöhen, um diese letzte Verteidigungsfront zu schützen.

Kryptographie für jedermann

Lange vor dem Anbruch des digitalen Zeitalters wurde die Kryptographie von mächtigen Menschen verwendet, um ihre Interessen zu schützen – oder ihren Feinden Schaden zuzufügen. Der römische Herrscher Julius Cäsar verwendete bekanntermaßen Geheimcode, um militärisch wichtige Nachrichten zu verschlüsseln. Seit Anbeginn unserer Zeitrechnung nutzen im Ausland stationierte Botschafter Geheimcode, um Mitteilungen an ihre Vorgesetzten im Heimatland zu schützen. Maria Stuart wurde aufgrund von Kryptoanalyse Hochverrat angelastet. Vom viktorianischen England wurde die Kryptoanalyse bis zu den Weltkriegen nur von Behörden betrieben. Diese setzten sie stets auf die gleiche Weise ein: für nachrichtendienstliche Zwecke, die dem Schutz von Kirche oder Staat galten.

Doch mit der globalen Ausweitung des World Wide Web ging eine unerwartete Entwicklung einher. Plötzlich konnten alle Menschen rund um den Globus frei miteinander kommunizieren. Die ersten Diskussionen konzentrierten sich auf technische, infrastrukturelle Konzepte – und später ging es dann vor allem um Kätzchenbilder. Doch inzwischen verwenden Menschen für jede Art von privater Kommunikation soziale Medien. Da soziale Medien öffentlich sind, können interessierte Behörden diese Kommunikation überwachen. Datenschützer versuchen, diesem Problem mittels Kryptographie beizukommen.

Daher wird nun zum ersten Mal in der Geschichte Kryptographie – in Form von SSL – nicht nur verwendet, um die Interessen von Machthabern zu schützen, sondern auch zum Schutz der Kommunikation von jedermann. Inzwischen erwartet jeder, dass SSL allerorts eingesetzt wird, und zwar nicht nur zum Schutz der Privatsphäre, sondern natürlich auch zur Verhinderung von Cyber-Diebstahl. Um diesen Ansprüchen gerecht zu werden, müssen globale Unternehmen ein breiter gefasstes, höheres Sicherheitsniveau zum Schutz von SSL aufbauen. Schließlich ist dies die letzte Verteidigungsfront für Kommunikation und Handel.

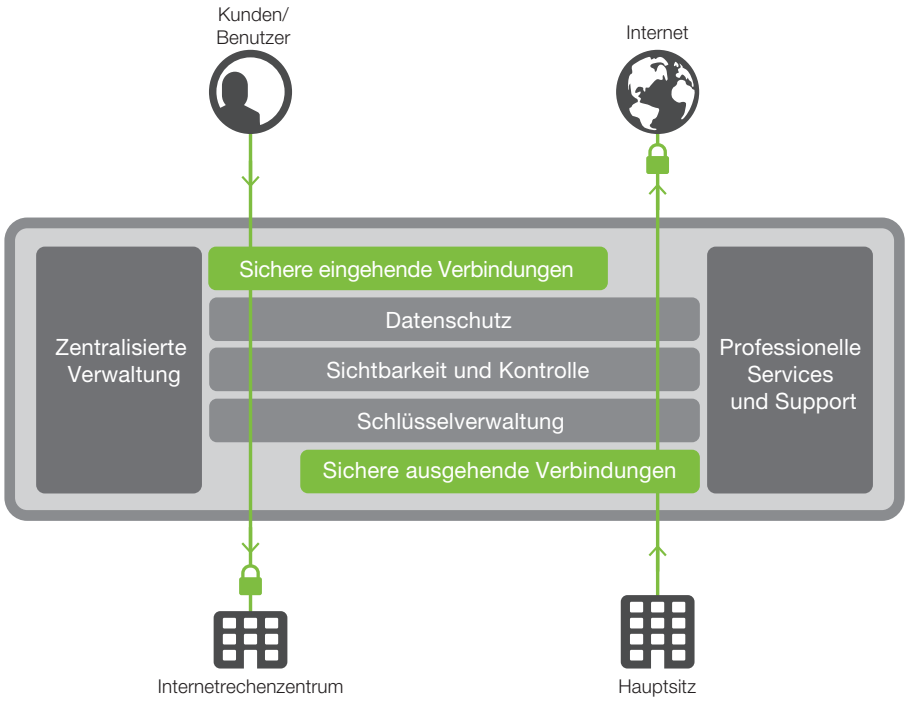

Abbildung 1: Die SSL Everywhere-Lösung von F5.

Die Erhöhung des Sicherheitsniveaus

Die ordnungsgemäße Bereitstellung von SSL kann sogar für erfahrene Administratoren eine abschreckende Aufgabe sein. Glücklicherweise werden von bestimmten Gruppen Richtlinien zur Verfügung gestellt (ergänzend zu den in diesem Whitepaper empfohlenen Richtlinien), um bei der Bereitstellung und Bewertung eines ordnungsgemäßen SSL-Sicherheitsniveaus zu helfen. Das Open Web Application Security Project (OWASP) pflegt einen Best-Practice-Leitfaden für SSL. Das SSL Labs-Projekt stellt ein umfassendes Prüftool bereit, das Administratoren dabei unterstützen kann, das Sicherheitsniveau ihrer Website zu bewerten. Zu den empfohlenen Vorgehensweisen gehören Methoden für die Zukunftssicherung von Geheimtext, für die optimale Schlüsselverwaltung und für Refactoring im Hinblick auf eine widerstandsfähige Sicherheitsarchitektur.

Verhinderung von passiver Überwachung mittels vorwärts gerichteter Geheimhaltung

Im Jahr 2013 wurden Vorwürfe gegen staatliche Nachrichtendienste bekannt, breitgefächerte Datenerfassung von Bürgern der Vereinigten Staaten, Europas und weltweit betrieben zu haben. Die betroffenen Daten umfassten angeblich Metadaten zu Mobilfunkanrufen, Texte von SMS-Mitteilungen und sogar verschlüsselte Daten (Geheimtext) aus E-Mails und anderer Kommunikation.

Selbst wenn sich ein Unternehmen außerhalb des Zuständigkeitsbereichs einer Regierungsbehörde befindet, kann die jeweilige Behörde ggf. den Geheimtext und die Metadaten des Unternehmens über Jahre hinweg abhören und aufzeichnen. Später könnte die Behörde Zugriff auf die entsprechenden Schlüsseldateien erhalten, was die Entschlüsselung von Millionen von zuvor gespeicherten Mitteilungen ermöglichen würde. Aufgrund der Gefährdung von Langzeitschlüsseln werden Mitteilungen, die heute noch sicher sind, dies in der Zukunft nicht zwangsläufig bleiben.

SSL verfügt über eine passive Überwachungs-Gegenmaßnahme namens Perfect Forward Secrecy (PFS), die das Schüsselgenerierungsprotokoll zwischen den beiden Seiten der SSL-Verbindung um einen zusätzlichen Austausch erweitert. Wenn PFS aktiviert ist, können Angreifer bzw. Lauscher nicht einfach einen einzelnen Schlüssel aufdecken, um Millionen von zuvor aufgezeichneten Kommunikationen zu entschlüsseln. PFS lässt sich ganz einfach einrichten, indem eine zusätzliche kryptographische Chiffre aktiviert wird (welche direkt in das Gerät für die SSL-Terminierung integriert ist). Daher übernehmen Anbieter sozialer Netzwerke und andere Unternehmen, für die Datenschutz einen hohen Stellenwert hat, diese Technik schnell weltweit.

Schutz von Schlüsseldateien mittels einer erweiterten Speicherungsarchitektur

Im Frühjahr 2014 löste folgende Meldung weltweit Entsetzen aus: Ein schädlicher Softwarefehler (der unter dem Namen Heartbleed bekannt wurde) in der weitverbreiteten OpenSSL-Bibliothek war bereits seit über zwei Jahren vorhanden und ermöglichte das Ausspionieren von Millionen von Websites. Heartbleed – so genannt, da sich der Code im „Heartbeat"-Code der Bibliothek befindet – hatte eine verheerende Auswirkung. Er führte dazu, dass die Inhalte eines Gerätespeichers unbemerkt von Angreifern aufgedeckt werden konnten. Jeder, der vor der offiziellen Entdeckung im Jahr 2014 von Heartbleed wusste, hätte die Möglichkeit gehabt, den größten Teil des Internets zu durchsuchen und die wertvollsten Daten (z. B. private Schlüssel und Passwörter von Serveradministratoren) zu sammeln, ohne Warnmeldungen auszulösen oder Spuren auf den Geräten zu hinterlassen. Heartbleed wird wohl als eine der gravierendsten Internetschwachstellen aller Zeiten in die Geschichte eingehen.

Nach dem Heartbleed-Vorfall konnte sich nur noch eine Klasse von SSL-Nutzern sicher fühlen: Nutzer der FIPS 140-2-Hardware-Sicherheitsmodule (HSM). Ein HSM ist eine separate Software- und Hardwaresicherheitsgrenze um einen kryptographischen Kern und einen Schlüsselspeicherort herum. Die Schlüssel werden in der Regel innerhalb des Speicherorts erstellt und verlassen diesen niemals. Da die Schlüssel nie in den Speicher des Netzwerk-Hosts übertragen werden, konnten sie durch Heartbleed auch nicht aufgedeckt werden.

HSM-Geräte befolgen die strengen FIPS 140-2-Richtlinien für kryptographisches Design und können kostspielig sein. Finanzielle Institutionen und Regierungsbehörden verwenden sie seit Jahren und haben Möglichkeiten gefunden, sowohl im Hinblick auf Verwaltung als auch Kosteneffizienz Mehrwert aus ihnen zu schöpfen. Unternehmen verwenden HSM-Geräte als zentralen Schlüsselspeicherort (z. B. ein Gerätepaar pro Datenzentrum), was bedeutet, dass auch der Schulungsaufwand für Bediener und die Betriebskosten zentralisiert werden. Services, die eine Entschlüsselung benötigen, können über das interne Netzwerk auf die zentralisierten HSMs zugreifen. So sparen Unternehmen Kapital und Betriebskosten.

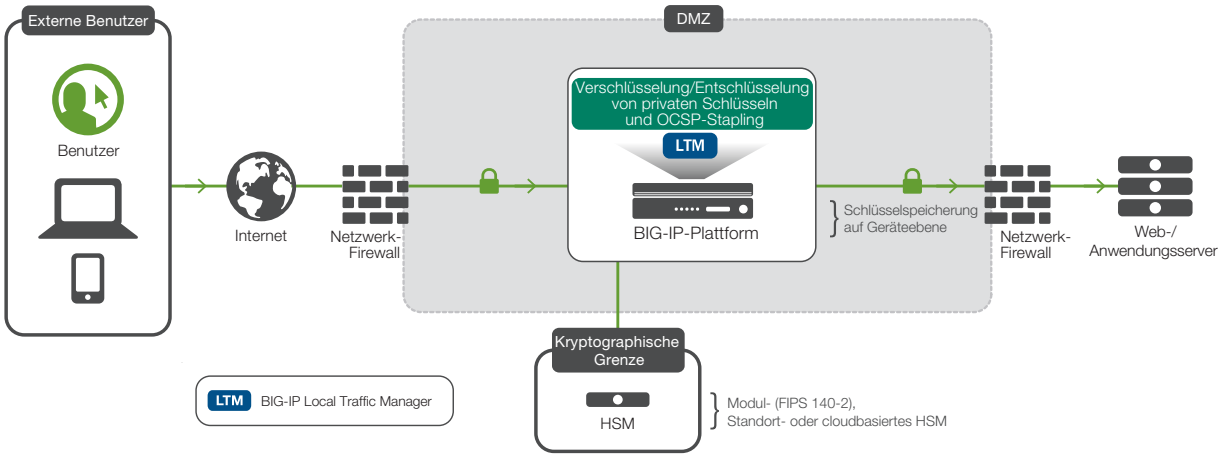

Abbildung 2: Die erweiterte Schlüsselspeicherung ermöglicht Sicherheit in der Cloud.

In das Netzwerk integrierte HSMs (netHSMs) werden in externen Datenzentren und Private Clouds eingesetzt. Sie ermöglichen Unternehmen, von einem Datenzentrum aus Entschlüsselungsdienste von einem externen Datenzentrum anzufordern. NetHSMs werden sogar in Public Clouds eingesetzt. Unternehmen verknüpfen diese öffentlichen netHSM- (sogenannte CloudHSM-) Geräte mit zugehörigen Geräten innerhalb des Unternehmensdatenzentrums und verwenden zentralisierte Sicherheitskontrollen, z. B. Application Delivery Controller, um die Anfragen zwischen ihnen zu überwachen. Die HSM-Geräte (in privater, Netzwerk- oder Cloud-Konfiguration) und die vorwärts gerichtete Geheimhaltung werden zum Bestandteil des neuen SSL-Sicherheitsniveaus.

Lückenloser Schutz mit „Always-On“-SSL Everywhere

Der Sicherheitsanalyst John Kindervag von Forrester Research beschreibt den Sicherheitsansatz des sogenannten „Zero Trust“-Modells (ZTM). ZTM arbeitet unter der Prämisse, dass die Architektur sehr viel sicherer wird, wenn jede Komponente im Netzwerk jeder anderen Komponente misstraut. Der Datenverkehr zwischen den Geräten wird dabei so behandelt, als hätte er bereits andere Sicherheitsmaßnahmen umgangen. Eine auf diesem Modell basierende Architektur wird in zahlreichen Netzwerken umgesetzt, insbesondere dort, wo die Sicherheitsperimeter besonders porös sind, wie z. B. bei Unternehmen-zu-Cloud sowie Unternehmen-zu-Unternehmen-zu-Cloud.

Die Einführung eines Modells, in dem Quellen stets als nicht vertrauenswürdig gehandhabt werden, bedeutet, dass sogar die unternehmensinterne Datenübertragung geschützt wird. Das Forrester-Modell konzentriert sich auf ein „Gateway für Netzwerksegmentierung“, das Sicherheit und Verfügbarkeitsservices über mehrere Hochgeschwindigkeitsverbindungen in jede Netzwerkzone bietet. Das betreffende Gerät benötigt sehr viel mehr Einblick in Paketdaten, unter anderem in die Anwendungsebene.

Um Daten auf Anwendungsebene zu verarbeiten, muss das Gerät diese zunächst entschlüsseln und nach der Verarbeitung gemäß den Grundsätzen von ZTM erneut verschlüsseln. Jahrelang war die Wiederverschlüsselung von SSL-Daten nach der Sicherheitsanalyse lediglich im Finanzsektor gängige Praxis, um den internen Sicherheitsvorschriften entsprechender Unternehmen gerecht zu werden. Inzwischen findet sie jedoch weitere Verbreitung.

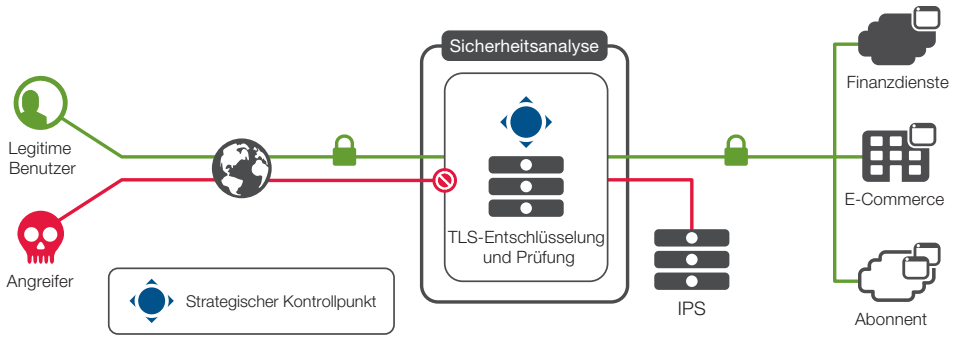

Abbildung 3: Das „Zero Trust"-Modell kann die Wiederverschlüsselung im Unternehmensdatenzentrum erfordern.

Die Wiederverschlüsselung von Daten ist ganz im Sinne des ZTM. Hierdurch werden Daten vor Hosts im Netzwerk geschützt, die durch Angreifer oder Überwachungsbehörden gefährdet sein könnten. Das Verfahren kann jedoch ebenso Daten vor Sicherheitsanalysegeräten verbergen, wie z. B. Intrusion Detection-Systemen, Durchflussmessgeräten und webbasierten Firewalls.

Zusammenfassung

Auch wenn es eine unbequeme Wahrheit ist: Die Internetsicherheit hat inzwischen einen vergleichbaren Stellenwert wie Menschenrechte, Meinungsfreiheit und das Recht auf freien Handel. Doch IT-Leiter sehen PFS, HSMs und ZTM mit erheblichen Investitionen verbunden, die einem Handelsunternehmen anscheinend keinen Mehrwert bringen. Wenn Daten innerhalb von SSL-Sitzungen nicht ordnungsgemäß geschützt werden, sind diese Daten ggf. nicht nur vor Ausspionieren sicher, sondern auch für das Unternehmen nicht einsehbar.

Doch glücklicherweise lassen sich diese Probleme überwinden. Es gibt Unternehmen, die diesen Sicherheitsherausforderungen heute mit innovativer Architektur gerecht werden. So erzielen sie das neue Sicherheitsniveau, das in der risikoreichen Welt, in der wir heute leben, erforderlich ist.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 (USA) 888-882-4447 www.f5.com

Nord-, Mittel- und Südamerika
info@f5.com

Asiatisch-pazifischer Raum
apacinfo@f5.com

Europa/Naher Osten/Afrika
emeainfo@f5.com

Japan
f5j-info@f5.com

Lösungen für eine Welt der Anwendungen