Always On SSL:
Schutz für Ihre Website

Entwickeln und Fördern von Best Practices zum Schutz vor Gefahren hinsichtlich Datenschutz, Identität und Sicherheit für Online-Dienste, Behörden, Unternehmen und Kunden sowie zur Stärkung des Online-Vertrauens

Stand: 29. Juni 2012

Inhaltsverzeichnis

Executive Summary

Das Internet in seiner heutigen Form konnte nur auf der Grundlage von Vertrauen der Nutzer in die Seriosität der Website-Anbieter entstehen. Schon seit Langem verwenden die führenden Online-Händler und -Geldinstitute SSL (Secure Socket Layer) und TLS (Transport Layer Security), um den Datenaustausch und die Transaktionen ihrer Kunden zu schützen. Diese Verfahren ermöglichen seit über zehn Jahren die vertrauensvolle Nutzung von Webbrowsern, Mobilgeräten, E-Mail-Clients und anderen Online-Anwendungen und sind nach wie vor grundsätzlich sicher. Websites und die beteiligten Nutzer verwenden SSL und TLS in der Regel zum Schutz vertraulicher Daten wie Kennwörter und Kreditkartennummern. Seit 2005 hat sich die Anzahl der Websites, die SSL/TLS einsetzen, mehr als verdoppelt und heute wird die Zahl der Sites mit SSL-Zertifikaten von Zertifizierungsstellen auf über 4,5 Millionen geschätzt.[1].

Aber die Online-Welt hat sich durch Web 2.0 und soziale Netzwerke verändert: Viele Menschen bleiben länger online oder sind sogar permanent bei Diensten wie Facebook, Google Mail oder Twitter angemeldet. Solche Dienste sind für viele zu einem unverzichtbaren alltäglichen Kommunikationsmedium geworden. Hier geht es um den Schutz von weit mehr Daten als nur Kreditkartennummern. Auch die Bedrohungslage hat sich geändert – allerorten drohen Botnets, Malware, Datenabschöpfung, gefälschte E-Mails, Online-Betrug und andere Gefahren für Sicherheit und Datenschutz. Leider hat die Handhabung der Online-Sicherheit nicht immer mit diesen Bedrohungen Schritt gehalten. So verschlüsseln zwar viele Unternehmen die Authentifizierung bei der Anmeldung eines Benutzers mit dem SSL/TLS-Protokoll, die im weiteren Verlauf der Sitzung aufgerufenen Seiten aber nicht mehr. Diese Praxis ist riskant, denn so sind Website-Besucher nicht ausreichend vor Online-Angriffen geschützt. Millionen Benutzer können dadurch sogar beim Besuch einer seriösen Website Gefahren ausgesetzt sein, ohne dies zu ahnen.

Die Online Trust Alliance (OTA) als Zusammenschluss von Unternehmen, für die Online-Sicherheit eine große Rolle spielt, appelliert an alle, die mit Sicherheit, Handel und interaktiver Werbung im Internet zu tun haben, zum Schutz der Kunden an einem Strang zu ziehen und geeignete Maßnahmen zu ergreifen, um das Vertrauen der Nutzer zu bewahren. Benötigt werden sicherheitsfördernde Best Practices, die herstellerunabhängig, einfach zu implementieren und global verfügbar sind. Eine dieser Maßnahmen ist dauerhaft aktiviertes SSL (Always On SSL, AOSSL): Dabei wird SSL/TLS auf der gesamten Website eingesetzt, um die Nutzer vom ersten Aufrufen der Site bis zum Abmelden durchgängig zu schützen. AOSSL ist gut umsetzbar, hat sich bewährt und sollte auf allen Websites, auf denen die Besucher vertrauliche Daten eingeben oder angezeigt bekommen, implementiert werden.

Dieses Whitepaper stellt dar, warum Always On SSL unverzichtbar ist und wie Sie vorgehen können, um für Ihre Kunden einen lückenlosen Schutz einzurichten. Ausführliche Fallberichte illustrieren, was Facebook, Google, PayPal und Twitter als AOSSL-Vorreiter unternommen haben, um gemeinsam das Internet sicherer zu machen.

Die OTA bedankt sich an dieser Stelle für die Mitarbeit des OTA Steering Committee und seiner Mitglieder, darunter AllClear, DigiCert, Epsilon, IID, Intersections, LashBack, MarkMonitor, Message Systems, Microsoft, PayPal, Pitney Bowes, Publishers Clearing House, Return Path, Secunia, Star Marketing Group, Symantec, TrustSphere und VeriSign, Inc.

[1] Netcraft-Umfrage zu SSL, Februar 2012

Besonderer Dank gebührt Alex Rice von Facebook, Adam Langley von Google, Andy Steingruebl von PayPal, John Scarrow von Microsoft, Quentin Lui und Rick Andrews von Symantec, Bob Lord von Twitter und Craig Spiezle von der OTA für ihre Beiträge und ihre Mitarbeit an diesem Whitepaper.

Aktualisierte Versionen dieses Dokuments finden Sie unter https://otalliance.org/aossl.htm. Kommentare dazu können Sie uns unter staff@otalliance.org zusenden.

Warum online ein durchgängiger Schutz notwendig ist

Internetnutzern stehen zum Suchen, Einkaufen und Austauschen von Informationen immer mehr multimediale, interaktive und individualisierte Dienste zur Verfügung – Stichwort Web 2.0. Um ihren Benutzern die gewünschten Inhalte liefern zu können, verwenden viele dieser Dienste Browser-Cookies, die zustandsbehaftete, dauerhafte Sitzungen einrichten. Bei der Anmeldung an einer Website muss der Benutzer zur Authentifizierung normalerweise seinen Benutzernamen und sein Kennwort eingeben. Der Webserver generiert dann eine für diesen Benutzer eindeutige Sitzungs-token-ID und sendet diese an den Browser, der sie in seinem Cache als Cookie ablegt. Bei jeder Interaktion des Benutzers mit der Website sendet der Browser den im Cookie gespeicherten Inhalt wieder an den Webserver. Der Cookie bleibt so lange gültig, bis er abläuft oder gelöscht wird.

HTTP und unsichere Cookies als Einfallstore für Angreifer

Viele Websites übertragen die Anmeldedaten mit dem HTTPS-Protokoll über eine verschlüsselte SSL-Verbindung, stufen die Sitzung nach Generierung des Sitzungs-Cookies aber wieder auf HTTP-Niveau zurück. Damit bleibt zwar das Benutzerkennwort geschützt, aber der Cookie, und mit ihm die Sitzungs-ID, wird bei jedem Datenabruf vom Server als Klartext übertragen. Dadurch besteht die Gefahr von Session-Hijacking. Diese Vorgehensweise gaukelt den Benutzern außerdem eine trügerische Sicherheit vor, denn sie erhalten den Eindruck, die gesamte Sitzung sei verschlüsselt, tatsächlich gilt das aber nur für den Anmeldevorgang.

Andere Unternehmen verwenden zwar auf der gesamten Website HTTPS, kennzeichnen die Sitzungscookies aber nicht als sicher. Auch dieses Vorgehen birgt Risiken: Nutzer geben häufig nur einen Teil der URL in die Adresszeile ein, ohne „https://“ davor. Vor der Umleitung auf die entsprechende HTTPS-Seite sind die Cookies während dieser ersten Anfrage ungeschützt. Ein Angreifer, der ein offenes Netzwerk überwacht, muss nur eine einzige unverschlüsselte HTTP-Anfrage abfangen, um den Cookie eines Opfers zu stehlen und Zugang zu seinem Konto zu erlangen.

Diese Probleme sind nicht neu und können bei jeder Website auftreten, die Sitzungscookies verwendet. Selbst Suchmaschinen, die Suchanfragen speichern, können Opfer eines solchen Angriffs werden. Unternehmen können es sich nicht mehr leisten, dem tatenlos zuzusehen, und alleine die Aufklärung der Benutzer reicht nicht aus. Die allgemeine Online-Sicherheit steht derzeit auf der Kippe, daher sind an Websites Änderungen erforderlich, die die lückenlose Sicherheit und damit das Vertrauen der Kunden weiterhin gewährleisten.

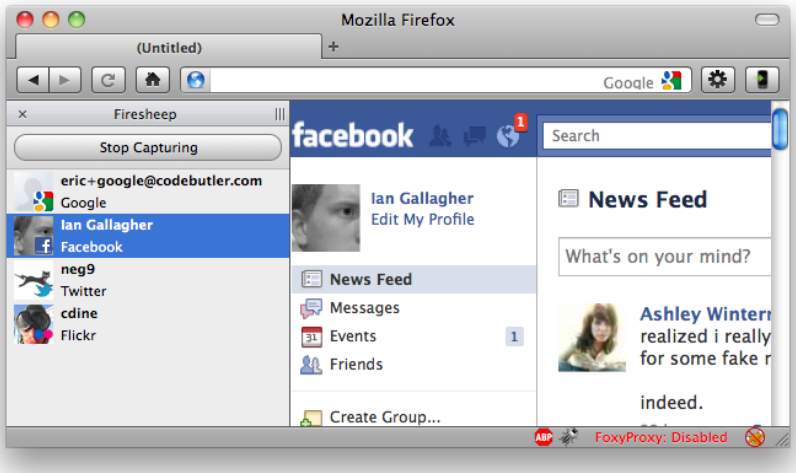
Session-Hijacking ist beängstigend einfach

Zwar ist Session-Hijacking kein neues Problem, aber in den Blickpunkt sowohl von Benutzern als auch von Angreifern rückte die grundsätzliche Unsicherheit ungesicherter HTTP-Verbindungen (und offener Wi-Fi-Netze) 2010 mit der Veröffentlichung des Plugins „Firesheep“ für den Browser Firefox. Firesheep, geschrieben von Eric Butler und Ian Gallagher, macht es selbst Angreifern ohne Programmierkenntnisse „unglaublich einfach“, in fremde Benutzerkonten bei zahlreichen beliebten Diensten einzudringen – man nennt das Sidejacking. Firesheep sucht offene Netzwerke, beispielsweise eine unverschlüsselte Wi-Fi-Verbindung in einem Café oder einer Bücherei, und verbindet sich damit. Ein Sniffer sucht und übernimmt dann ungesicherte Cookies. Sobald jemand aus dem Netzwerk eine unsichere und Firesheep bekannte Website aufruft, zeigt Firesheep dessen Benutzernamen und die

damit verbundenen Dienste an. Der Angreifer braucht jetzt nur noch den Namen des Opfers doppelt anzuklicken und erhält umgehend Zugang zu dessen Benutzerkonto.

In puncto Leistungsfähigkeit und Benutzerfreundlichkeit ist Firesheep zweifellos sehr innovativ. Butler und Gallagher wollten damit allerdings auf die Bedeutung und das Ausmaß einer Schwachstelle hinweisen, vor der Sicherheitsexperten bereits jahrelang gewarnt hatten. Schon etliche Jahre vor Firesheep konnten Angreifer mit Tools wie „Hamster“, „Ferret“ oder „CookieMonster“ relativ einfach offene Netzwerke abhören, Cookies stehlen und HTTP-Sitzungen kapern.

Abbildung 1: Screenshot von Firesheep im Einsatz



Mithilfe solcher Tools kann ein Angreifer diese Schwachstelle ausnutzen und sich teilweisen oder sogar vollständigen Zugang zum Konto des Opfers verschaffen. Einige Dienste schützen sich vor Sidejacking, indem sie beispielsweise nach dem alten Kennwort fragen, wenn ein Benutzer sein Kennwort ändern möchte. In vielen Fällen kann ein Angreifer das Benutzerkonto seines Opfers jedoch vollständig übernehmen, das Kennwort ändern und sogar weitere mit diesem Konto verbundene Dienste kapern.

Gefährdet sind nicht nur Nutzer in Cafés

Vielfach wird angenommen, dass sich die Gefahr von Session-Hijacking auf Cafés beschränkt und man sich als Benutzer lediglich vor unverschlüsselten Wi-Fi-Netzen schützen muss. Diese Ansicht entspricht jedoch nicht der Realität, denn Tools wie Firesheep können in *allen* Netzwerken eingesetzt werden, ob kabellos oder kabelgebunden, bei denen Cookies über unverschlüsselte HTTP-Sitzungen übertragen werden. Das Risiko für Unternehmen und Behörden, die soziale Netzwerke, Webmail oder Web-2.0-Anwendungen benutzen, wird ebenfalls oft übersehen. Wenn ein Mitarbeiter eine unsichere Website besucht und diese Sitzung von einem Angreifer gekapert wird, kann der Angreifer von diesem Konto aus Malware verbreiten und eventuell sogar Zugriff auf vertrauliche Daten erlangen – der Datenschutz ist dann nicht mehr gewährleistet. Die möglichen Konsequenzen einer solchen Datenschutzverletzung wird jeder Website-Betreiber unbedingt vermeiden wollen.

Mit der Aufklärung der Benutzer ist es nicht getan

Um die Benutzer stärker für diese Problematik zu sensibilisieren und der Gefahr von Sidejacking vorzubeugen, hat die Electronic Frontier Foundation (EFF) eine eigene Firefox-Erweiterung geschrieben: HTTPS Everywhere. Diese erzwingt die Nutzung von HTTPS-Verbindungen bei bestimmten Websites. Weiterhin haben die EFF und Access, ein Zusammenschluss von Aktivisten für Freiheit im Internet, gemeinsam HTTPS Now aus der Taufe gehoben: Diese Aufklärungskampagne soll das

Thema international bekannter machen und Always On SSL als Mindeststandard bei der Online-Sicherheit etablieren. Zur Kampagne gehört eine Website, auf der Benutzer Informationen über die Nutzung von HTTPS auf Websites recherchieren und einbringen können.[2] HTTPS Everywhere funktioniert zwar gut auf bestimmten Websites, schützt seine Benutzer aber nicht beim Besuch von Websites, die diese Funktion nicht unterstützen. Außerdem wird HTTPS Everywhere nicht von Chrome, Safari und Internet Explorer unterstützt. Daher ist diese Erweiterung nur von begrenztem Nutzen, solange nicht alle gängigen Browser diese Funktion standardmäßig unterstützen oder enthalten.

Der Einsatz der EFF ist hervorragend, aber durch Benutzeraufklärung und Tools auf Client-Seite alleine sind die bekannten Schwachstellen in der Verwaltung von Online-Sitzungen nicht aus der Welt zu schaffen. Zudem ist es äußerst unwahrscheinlich, dass Benutzer in Zukunft auf den Internetzugang über offene Netzwerke in Cafés, Bibliotheken, Flughäfen und an anderen öffentlichen Orten verzichten werden. Website-Betreiber sollten die Daten ihrer Benutzer unbedingt schützen, und zwar unabhängig davon, welchen Browser diese verwenden oder wie sie ins Internet gehen. Indem Unternehmen Sidejacking-Angriffe bereits im Vorfeld durch gezielte Schutzmaßnahmen verhindern, beugen sie nicht nur der Abwanderung ihrer Kunden vor, sondern auch den horrenden Kosten, die Schadensersatzforderungen und negative Berichterstattung nach sich ziehen können.

Always On SSL ermöglicht die sorglose Internetnutzung

Always On SSL ist ein kostengünstiges Sicherheitsprinzip, das Website-Besucher lückenlos schützt. Es ist kein Produkt, kein Dienst und kein Ersatz für vorhandene SSL-Zertifikate, sondern vielmehr eine Herangehensweise an das Thema Sicherheit, die anerkennt, dass nicht nur die Benutzeranmeldung, sondern der gesamte Besuch auf einer Website geschützt werden muss. Zu Always On SSL gehört zunächst einmal der Einsatz von HTTPS auf der gesamten Website, weiterhin aber auch die Kennzeichnung von Sitzungscookies als sicher, damit der Cookie-Inhalt nicht über unverschlüsselte HTTP-Verbindungen gesendet wird. Zusätzliche Maßnahmen wie SSL-Zertifikate mit Extended Validation (EV) und HSTS (HTTP Strict Transport Security) können die Infrastruktur noch besser gegen Man-in-the-Middle-Angriffe absichern.

> *„Wir bei Symantec betrachten Always On SSL als eine relativ einfache und ausgesprochen kostengünstige Methode, viele gängige Bedrohungen der Datenübertragung über das Netzwerk auszuschalten. Die in diesem Dokument beschriebenen Erfahrungen führender Internet-Unternehmen zeigen, dass dies eine praktikable und lohnende Möglichkeit ist. Wir können allen Website-Betreibern nur eindringlich empfehlen, Always On SSL so bald wie möglich zu implementieren.“*
>
> *– Quentin Liu, Symantec*

Folgen Sie vielen guten Vorbildern

Da Online-Angriffe immer häufiger und einfacher werden, sind Unternehmen in aller Welt zunehmend auf dem Prüfstand und müssen zeigen, dass alle Online-Transaktionen mit vertraulichen Daten sicher sind. Behörden und Datenschutz-Aktivisten drängen Unternehmen, Always ON SSL einzusetzen.

[2] https://www.eff.org/press/archives/2011/04/19-0

Nach Berichten über gehackte SSL-Verbindungen bat Charles Schumer, US-Senator der demokratischen Partei, im Januar 2011 Yahoo!, Twitter und Amazon schriftlich[3], das Einfallstor HTTP zu schließen, und forderte sie auf, Always On SSL zügiger zu implementieren.

Heute haben sich einige der größten und renommiertesten Online-Dienste, darunter Facebook, Google, PayPal und Twitter, für Always On SSL entschieden und implementieren HTTPS zur Verschlüsselung aller ein- und ausgehenden Datenübertragungen, sogar bei Werbung und nicht vertraulichen Daten. Diese Unternehmen haben erkannt, dass ein durchgängiger Schutz immer wichtiger wird, und tun das Ihre, um das Internet für alle Benutzer sicherer zu machen.

Facebook

Ende Dezember 2011 war Facebook mit 483 Millionen aktiven Benutzern im Tagesdurchschnitt und monatlich 845 Millionen Benutzern[4] die am häufigsten besuchte[5] Website im Internet. Facebook legt größten Wert auf Datenschutz und die Sicherheitsexperten des Unternehmens haben ausgeklügelte Systeme entwickelt, um den Dienst vor Spam, Phishing, Malware und anderen Bedrohungen zu schützen.[6] Im Januar 2011 hat Facebook im Rahmen einer Initiative zur Verbesserung der Sicherheit mit der Implementierung von Always On SSL begonnen. Dazu erhielten die Benutzer die Möglichkeit, Facebook über HTTPS-Verbindungen zu nutzen. Diese Änderung wurde von den Benutzern sehr positiv aufgenommen: mehr als 19 Prozent der aktiven Facebook-Nutzer entschieden sich für das sichere Surfen.

Millionen Apps müssen mitziehen

Deutlich schwieriger war die Umstellung der mehr als eine Million Facebook-Entwickler auf HTTPS und OAuth 2.0[7], einen offenen Standard, der gemeinsam von Yahoo!, Twitter, Google und anderen entwickelt wurde. Die Umstellung war unumgänglich, da viele Apps externer Anbieter blockiert werden, wenn Benutzer HTTPS verwenden, die App dies aber nicht unterstützt. Der Browser gibt in diesem Fall Sicherheitswarnungen wegen teilweise unsicherer Inhalte aus. Um die Entwickler zu unterstützen, gab Facebook einen auf sechs Monate angelegten Plan für die Umstellung von Websites und Apps auf HTTPS vor.[8]

Für Entwickler, die ihre Apps von vornherein auf die Unterstützung sicherer Verbindungen ausgelegt hatten, verlief diese Umstellung problemlos. Einige größere Anbieter mit zahlreichen Anwendungen mussten allerdings mehr Zeit und Ressourcen aufwenden, um die betreffenden Stellen im Code zu finden, zu ändern und die Infrastruktur entsprechend umzustellen.

> *„Wir sind jetzt viel überzeugter, einen sicheren und vertrauenswürdigen Dienst über Netzwerke bereitstellen zu können, in denen die Daten unserer Nutzer zuvor eventuell nicht vollständig geschützt waren.“*
>
> *– Alex Rice, Facebook*

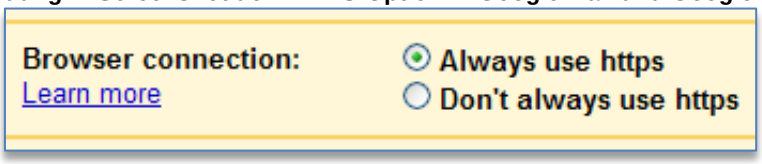
Für Facebook hat sich die Umstellung auf Always On SSL definitiv gelohnt. Für die Authentifizierung und für Apps, die über HTTPS bereitgestellt werden, gilt jetzt ein einheitlicher Standard, wodurch die Plattform einfacher, sicherer und zuverlässiger wird. Dieser erste Schritt ist jetzt abgeschlossen und Facebook arbeitet nun am nächsten Projekt: Die internationale Infrastruktur soll erweitert werden, um die Wartezeiten auf ein akzeptables Maß zu verkürzen. Dies ist ein äußerst wichtiger Aspekt für Facebook, da sich rund 80 Prozent seiner aktiven Nutzer außerhalb Nordamerikas befinden.

[3] http://www.infosecurity-magazine.com/view/16328/senator-schumer-current-internet-security-welcome-mat-for-wouldbe-hackers/
[4] http://newsroom.fb.com/content/default.aspx?NewsAreaId=22
[5] http://www.google.com/adplanner/static/top1000/
[6] https://www.facebook.com/blog/blog.php?post=486790652130
[7] http://oauth.net/2/
[8] https://developers.facebook.com/blog/post/497/

Google

Angefangen hat Google als Suchmaschine, die vorwiegend öffentlich zugängliche Daten nutzte. Inzwischen sind auch immer stärker individualisierte Dienste im Angebot und Google hat längst erkannt, wie wichtig es ist, vertrauliche Daten zu schützen. Google Mail und Google Apps wurden als Spitzenprodukte konzipiert, die solide genug sein sollten, um als Grundlage für den Geschäftsablauf bei Google selbst dienen zu können. Deshalb war HTTPS-Unterstützung von Anfang an dabei. Zuerst wurde HTTPS verpflichtend zum Schutz der Anmeldedaten eingesetzt. Im Juli 2008 führte Google dann für Benutzer von Google Mail und Google Apps die Möglichkeit ein, *immer HTTPS zu verwenden*.

Abbildung 2: Screenshot der HTTPS-Option in Google Mail und Google Apps



Im Januar 2010 machte Google schließlich HTTPS zur Standardeinstellung für Google Mail und Google Apps[9], so dass es für die Benutzer noch bequemer wurde, den E-Mail-Verkehr zwischen Browser und Google jederzeit zu verschlüsseln. Für diese Umstellung waren keine zusätzlichen Rechner und keine zusätzliche Hardware erforderlich und die Auswirkungen auf die Leistung erwiesen sich als vernachlässigbar. Von Google durchgeführte Studien ergaben, dass SSL/TLS weniger als ein Prozent der Prozessorleistung auf den eingesetzten Rechnern beanspruchte – weniger als 10 KB Arbeitsspeicher pro Verbindung und weniger als zwei Prozent des Netzwerkverkehrs.

Sicheres Suchen

Die Suchvorgänge ebenfalls sicher zu gestalten, war eine anspruchsvollere Aufgabe. Im Mai 2010 führte Google die Möglichkeit verschlüsselter Suchvorgänge ein, die besser gegen das Ausspähen durch Dritte geschützt sind. Kürzlich hat Google HTTPS für angemeldete Benutzer als Standardeinstellung für die Suche eingeführt. Hier werden sowohl die Suchanfragen als auch die Seiten mit den Suchergebnissen verschlüsselt.[10] Der Vorteil liegt auf der Hand: Die Benutzer sind bei der Suche durch den lückenlos verschlüsselten Datenaustausch zwischen ihrem Computer und Google sicherer und haben die Gewissheit, dass ihre Daten nicht mitgelesen werden können. Eine komplexere Herausforderung stellten allerdings die gesamten Strukturen im Zusammenhang mit der Suche dar, insbesondere Webanalyse und Suchmaschinenoptimierung (SEO).

Klickt ein Benutzer auf ein Ergebnis seiner Google-Suche, um die entsprechende Website aufzurufen, gibt der Browser im Kennzeichen *Referrer* an, dass der Besucher durch einen Google-Link auf die Website gelangt ist. Viele SEO-Spezialisten und Experten für Webanalyse verwenden diese Angabe für Nutzungsstatistiken oder um den Erfolg ihrer Maßnahmen für Online-Marketing auszuwerten. Verwendet ein Benutzer jedoch die sichere Suche, sind die Suchbegriffe geschützt. Websites, die über die Google-Ergebnisse aufgerufen werden, wissen dann zwar, dass ein Besucher von Google kam, erfahren aber nicht, über welche Suchbegriffe.

Allerdings bietet Google zu diesem Zweck in seinen „Webmaster Tools“ eine Zusammenstellung der 1000 häufigsten Suchanfragen an, über die Besucher in den letzten 30 Tagen auf die Website gelangt sind. Anhand dieser Daten können Webmaster genauere Statistiken über die Besucher ihrer Website erstellen, während die Suchanfragen derjenigen Nutzer, die HTTPS aktiviert haben, vertraulich bleiben. Und wenn jemand auf eine Anzeige auf den Seiten mit den Google-Suchergebnissen

[9] http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html
[10] http://googleblog.blogspot.com/2011/10/making-search-more-secure.html

klickt, sendet der Browser die betreffende Suchanfrage weiterhin über das Netzwerk, so dass die Anbieter die Wirkung ihrer Kampagnen feststellen und ihre Anzeigen und Angebote verbessern können.

Google will in seinen Produkten in Zukunft noch stärker auf Always On SSL setzen und die Experten des Unternehmens werden weiterhin Informationen und Ratschläge zu SSL/TLS veröffentlichen. Außerdem engagiert sich Google für einen breiteren und wirkungsvolleren Einsatz von SSL in der gesamten Online-Branche. Wunschziel ist es, alle legalen Online-Inhalte zu schützen, so dass sich alle Nutzer sicher im gesamten Internet bewegen können.[11]

PayPal

PayPal wurde 1998 gegründet und ist heute der weltweit führende Online-Zahlungsdienstleister. Das Unternehmen setzte schon früh auf SSL/TLS: Seit 2000 werden alle Seiten nach dem Anmeldebildschirm über HTTPS ausgeliefert, die Anmeldung selbst ist seit 2006 ebenfalls durch HTTPS geschützt. PayPal war außerdem eines der ersten Unternehmen, das SSL-Zertifikate mit Extended Validation (EV) einsetzte, und begann schon 2007 damit, EV-SSL auf allen Anmeldeseiten zu implementieren.[12]

Da Transaktionen das Kernstück des PayPal-Dienstes sind, ist die Systemleistung ein besonders wichtiger Aspekt für das Unternehmen. Im Gegensatz zu vielen anderen Websites, bei denen Sitzungen relativ lange dauern, liegt der Anteil kurzer Sitzungen bei PayPal deutlich höher. Da der SSL/TLS-Handshake der zeitaufwendigste Abschnitt im gesamten Ablauf ist, war den IT-Spezialisten bei PayPal klar, dass mögliche Auswirkungen auf die Leistung besonders sorgfältig überwacht und gehandhabt werden mussten. In manchen Fällen führte die Umstellung auf HTTPS aber auch zu einer Beschleunigung, da nun alle Inhalte von denselben Servern über die Browserverbindungen ausgeliefert werden konnten.

Da PayPal ein besonders begehrtes Angriffsziel von Phishern, Hackern und anderen Online-Betrügern ist, entschieden sich die Sicherheitsexperten des Unternehmens für aufwendige Maßnahmen zum Schutz ihrer Kunden und ihres guten Rufs. Das Ziel bestand darin, Phishing-Versuche ins Leere laufen zu lassen und Angriffe von aktiven Tools wie SSLStrip zu unterbinden. (Im Gegensatz zu passiven Tools wie Firesheep, die den Netzwerkverkehr lediglich abhören, leiten aktive Tools ihn um oder verändern ihn.)[13]

Am Ende dieser Bestrebungen stand die Veröffentlichung der Spezifikation „HTTP Strict Transport Security“ (HSTS), an deren Entwicklung Jeff Hodges, Sicherheitsspezialist bei PayPal, beteiligt war.[14] Diese Spezifikation definiert Methoden, mit denen festgelegt werden kann, dass eine Website nur über sichere Verbindungen aufgerufen werden kann bzw. Benutzer mit bestimmten Websites nur über sichere Verbindungen kommunizieren können. HSTS wird derzeit von den Browsern Chrome und Firefox unterstützt. Websites wie die von PayPal, die HSTS verwenden, signalisieren den Browsern eindeutig, dass sie Inhalte nur über verschlüsselte Verbindungen ausliefern. Dadurch verhindern sie, dass die Benutzer versehentlich eine unverschlüsselte HTTP-Seite nutzen oder im Zuge eines Phishing- oder SSLStrip-Angriffs auf eine HTTP-Seite umgeleitet werden.

Twitter

Auf der Kommunikationsplattform Twitter finden sich praktisch in Echtzeit Meldungen über viele aktuelle Ereignisse. Von besonderer Bedeutung ist dies in Ländern mit eingeschränkter Meinungsfrei-

[11] http://googleblog.blogspot.com/2011/10/making-search-more-secure.html
[12] https://otalliance.org/resources/EV/index.html
[13] http://www.thoughtcrime.org/software/sslstrip/
[14] http://tools.ietf.org/html/draft-hodges-strict-transport-sec-02

heit. Einige von der Öffentlichkeit beachtete Sicherheitsprobleme gab es auch bei Twitter, aber das Unternehmen hat rasch reagiert und die Sicherheit seiner Benutzer deutlich verbessert.

Zwar unterstützte Twitter HTTPS bereits für seine Web-Schnittstelle, Smartphone-Clients und die Website für Mobilgeräte, beispielsweise zum Absenden der einzelnen Beiträge, aber mit dem ambitionierten Vorhaben der Implementierung von Always On SSL ging das Unternehmen noch einen Schritt weiter.[15] Im Mai 2011 kündigte Twitter an, seinen Benutzern über die Benutzereinstellungen die Möglichkeit zu geben, immer HTTPS zu nutzen. Die überaus positive Resonanz war Anlass für Twitter, die Umstellung zu beschleunigen, so dass HTTPS im Januar 2012 zum Standardmodus für alle Benutzer gemacht wurde.

Bei der Umstellung auf Always On SSL stand Twitter vor einigen speziellen Herausforderungen. Da ein Teil des Datenverkehrs über externe Content Delivery Networks (CDN) abgewickelt wird, musste unbedingt gewährleistet sein, dass diese CDN ausreichende Kapazität zur Verarbeitung des durch SSL erhöhten Datenvolumens hatten. Für Twitter und seine Partner war es ebenfalls wichtig, Verweise rückverfolgen und Analysen durchführen zu können, weshalb die Programmierer des Unternehmens Teile des Codes umschrieben, um bestimmte Probleme aufgrund von Inhalten aus unterschiedlichen Quellen zu vermeiden.

Erkenntnisse

Bei ihren Aktivitäten haben die Sicherheitsexperten von Facebook, Google, PayPal und Twitter wertvolle Erkenntnisse gewonnen, die sie zum Wohle der Allgemeinheit der OTA zugänglich gemacht haben. So soll es Website-Betreibern erleichtert werden, sich selbst und die Besucher ihrer Websites vor Sidejacking und anderen Online-Angriffen zu schützen. Bevor auch Sie Always On SSL für Ihre Website implementieren, sollten Sie diese wichtigen Aspekte berücksichtigen.

SSL erfordert keine teuren Rechenkapazitäten

Manche Firmen scheuen vor Always On SSL zurück, weil sie fürchten, dadurch könnten Verwaltungsaufwand und Kosten für die Website steigen. SSL/TLS-Zertifikate, die von einer Zertifizierungsstelle ausgestellt werden, sind zwar nicht kostenlos, aber sie haben einen festen Preis und es ist nicht erforderlich, vorhandene SSL-Zertifikate zu ersetzen. Wenn Sie mehrere sichere Domänennamen benötigen, können Sie diese beim Kauf der Zertifikate als „Subject Alternative Name“ (SAN) angeben.

Neben den Kosten eines SSL-Zertifikats müssen natürlich die Anforderungen an die Rechenleistung berücksichtigt werden, ebenso die eventuell erforderliche Anschaffung weiterer Hardware, um die zusätzliche Prozessorbelastung bewältigen zu können.

Bei großen und stark besuchten Websites könnte man annehmen, dass der zusätzliche Rechenaufwand zur Ver- und Entschlüsselung der Datenpakete erheblich höhere Anforderungen an die Hardware stellt. Tatsächlich aber haben viele Unternehmen andere Erfahrungen gemacht.

So haben beispielsweise die Forscher bei Google genauestens untersucht, wie viel Rechenleistung für Always On SSL erforderlich ist. Dabei stellten sie fest, dass in ihrer IT-Umgebung keine zusätzliche Hardware notwendig war. Die Beobachtungen deuten insgesamt darauf hin, dass die Mehrbelastung durch SSL/TLS dank technischer Fortschritte inzwischen minimal ist. Dennoch empfiehlt es sich, die Leistung des Webservers genau zu beobachten, um

> *„Wenn Sie ab hier nicht mehr weiterlesen, merken Sie sich eine Sache: SSL/TLS ist von der Rechenleistung her nicht mehr teuer. Das war vielleicht vor zehn Jahren der Fall, heute aber nicht mehr. Auch Sie können es sich leisten, Ihren Nutzern HTTPS zu bieten.“*
>
> *– Adam Langley, Google*

[15] https://dev.twitter.com/docs/tweet-button/faq

festzustellen, ob in Ihrer Umgebung Leistungseinbußen auftreten.[16]

Die Netzwerk-Reaktionszeit beeinflusst die Leistung

Der lückenlose Einsatz der HTTPS-Verschlüsselung führt zu etwas mehr Datenverkehr und damit längeren Reaktionszeiten im Netzwerk, vor allem wegen des umfangreicheren Datenaustausches zwischen Client und Server beim SSL/TLS-Handshake.[17] Besondere Bedeutung gewinnt dieses Problem beim Datenaustausch über große Entfernungen und speziell für Benutzer, denen nur eine begrenzte Bandbreite zur Verfügung steht. Websites, bei denen in vielen eher kurzen Sitzungen ein großes Datenvolumen anfällt, sind ebenfalls betroffen. Das Problem der Reaktionszeiten ist nicht trivial. Mit guter Planung lassen sich die Leistungseinbußen aber in den Griff bekommen. Wie das Beispiel einiger Finanzdienstleister zeigt, ist es möglich, standardmäßig mit starker Verschlüsselung zu arbeiten und dennoch anspruchsvolle Inhalte zügig bereitzustellen.[18] Darüber hinaus sind bei Google erste Versuche mit neuen Verfahren wie etwa „False Start“ im Gange, mit denen sich die Verzögerung durch den SSL/TLS-Handshake um 30 Prozent reduzieren ließ.[19]

Sicherheitsbewusste Webentwicklung erleichtert den Umstieg

Wenn bei der Webentwicklung von Anfang an auf Sicherheit geachtet wird, entstehen sichere Websites und Webanwendungen, die in der Entwicklung unwesentlich mehr kosten, sich aber langfristig auszahlen.[20] Das Auffinden und Umschreiben einzelner Code-Abschnitte kann sich als kosten- und zeitaufwendig erweisen, insbesondere für größere Unternehmen mit vielen Produkten. Alle heute entwickelten Websites sollten HTTPS als Standard verwenden und HTTP-Anfragen sofort auf HTTPS umleiten, insbesondere bei Webformularen. Es gibt noch viele weitere Aspekte zu berücksichtigen. Bei MozillaWiki und Gruppen wie dem Open Web Application Security Project (OWASP) finden sich umfassende Richtlinien zur Erstellung sicherer Webanwendungen und -dienste.[21]

Quellenvielfalt bedeutet größere Komplexität

Bei den meisten Websites werden durch Hyperlinks Inhalte aus unterschiedlichen, oft externen Quellen zusammengeführt, wodurch die Situation komplexer wird. Jeder Verweis mit einem HTTP-Link stellt ein Risiko für eine ansonsten sichere Website dar, denn ein aktiver Angreifer könnte das Laden eines CSS oder von JavaScript-Code ausnutzen.[22] Auch wenn eine HTTPS-Seite ein Bild, ein iframe-Fenster oder eine Schriftart über einen HTTP-Link lädt, kann sich ein Man-in-the-Middle-Angreifer dazwischenschalten. Websites wie etwa Facebook gehen inzwischen zunehmend dazu über, diesem Risiko durch die obligatorische Verwendung von SSL/TLS entgegenzutreten: Anwendungen und Inhalte, die sich nicht über HTTPS einbinden lassen, werden blockiert.[23] Dies gilt insbesondere für die folgenden Elemente:

- Bilddateien und Links zu Bilddateien im <img>-Tag
- externe Stylesheets im CSS-Format (.css)
- JavaScript-Dateien (.js)
- eingebettete Medien und Inhalte von iframe-Fenstern (Flash usw.)
- URLs in der DOCTYPE-Angabe oder in <html>-Tags
- Aufrufe externer APIs und SDKs (z. B. Facebook-SDK)

[16] http://www.imperialviolet.org/2010/06/25/overclocking-ssl.html
[17] http://www.semicomplete.com/blog/geekery/ssl-latency.html
[18] http://www.wired.com/images_blogs/threatlevel/2009/06/google-letter-final2.pdf
[19] http://googleonlinesecurity.blogspot.com/2010/05/extending-ssl-to-google-search.html
[20] https://www.owasp.org/index.php/OWASP_Guide_Project
[21] https://wiki.mozilla.org/WebAppSec/Secure_Coding_Guidelines
[22] https://www.eff.org/https-everywhere/deploying-https
[23] http://googleonlinesecurity.blogspot.com/2011/06/trying-to-end-mixed-scripting.html

Relative Links sind eine Möglichkeit, das Problem der Vermischung sicherer und nicht sicherer Inhalte zu vermeiden, da sie weder HTTP noch HTTPS angeben. Relative Links können allerdings wiederum für Suchmaschinen-Spamming oder URL-Hijacking ausgenutzt werden, vor ihrer Verwendung sollten Vor- und Nachteile daher sorgfältig für den Einzelfall abgewogen werden.[24]

Always On SSL für Ihre Website

Unternehmen, denen es mit dem langfristigen Schutz ihrer Kunden und ihres guten Rufs ernst ist, werden sich für Always On SSL entscheiden. Die OTA hat die Vorgehensweise zur Implementierung von Always On SSL in einzelne Schritte unterteilt. Wie Tabelle 1 zeigt, steigt mit der Anzahl der implementierten Sicherheitsfunktionen auch die Sicherheit Ihrer Website.

Tabelle 1: Sicherheitsfunktionen von Always On SSL im Überblick

Sicherheitsfunktion	Gut	Besser	Am besten
Permanentes HTTPS	✓	✓	✓
***Sichere* Cookies**	✓	✓	✓
Permanentes HTTPS mit Extended Validation		✓	✓
HTTP Strict Transport Security (HSTS)			✓

Dauerhaftes HTTPS auf jeder Webseite erzwingen

Der größte Vorteil von Always On SSL ist sicherlich, dass es für Besucher nicht einfacher sein könnte, auf allen Seiten Ihrer Website HTTPS zu verwenden. HTTPS ist dasselbe textbasierte Protokoll wie HTTP, läuft aber über eine verschlüsselte SSL/TLS-Sitzung. Um HTTPS zu erzwingen, sind lediglich die folgenden Schritte erforderlich:

- Installieren Sie ein SSL/TLS-Zertifikat von einer anerkannten Zertifizierungsstelle.
- Leiten Sie alle Verbindungen zum Webserver über Port 443 statt Port 80.
- Geben Sie die Verschlüsselungsstärke vor (z. B. 128-Bit).

Zum Einstieg können Sie Ihren Benutzern HTTPS zunächst als Option anbieten. Langfristig sollten Sie aber zu HTTPS als Standardprotokoll wechseln und den Besuchern die Möglichkeit geben, es bei Bedarf zu deaktivieren. Durch die Verwendung von HTTPS auf der ganzen Website schaffen Sie das erforderliche Mindestmaß an Sicherheit für den sinnvollen Schutz der Benutzer und von deren Daten.

Korrekte Implementierung von SSL-Zertifikaten

Um HTTPS zu aktivieren, sollten Sie ein gültiges SSL/TLS-Zertifikat von einer anerkannten Zertifizierungsstelle verwenden. Zwar verschlüsselt auch ein selbstsigniertes Zertifikat den Datenaustausch zwischen Besucher und Website, aber nur ein von einer Zertifizierungsstelle ausgegebenes Zertifikat garantiert den Besuchern, dass die Identität der Website-Inhaber von einer vertrauenswürdigen Organisation überprüft wurde. Mit einem selbstsignierten Zertifikat wird die Verbindung vom Browser unter Umständen als potenziell gefährlich eingestuft und der Benutzer erhält eine Warnung, dass diese Website möglicherweise nicht sicher ist. Die Auswahl der richtigen Zertifizierungsstelle ist daher von entscheidender Bedeutung.

[24] http://www.dummies.com/how-to/content/prevent-someone-from-hijacking-your-web-sites-sear.html

Vergewissern Sie sich, dass die gewählte Zertifizierungsstelle kompromissloser Sicherheit verpflichtet ist und eine robuste Infrastruktur mit gutem Kundendienst hat. Berücksichtigt werden sollten ebenfalls die Arbeitsweise der Zertifizierungsstelle bei der Identitätsüberprüfung und der Ausstellung von Zertifikaten, die Zuverlässigkeit und die Geschwindigkeit der Genehmigung von Zertifikaten, der jährliche Prüfbericht einer unabhängigen und anerkannten Audit-Gesellschaft sowie die Garantie, dass die Zertifizierungsstelle ihre Zusagen erfüllt.

Das SSL-Zertifikat sollte für die Vertrauenskette außerdem alle Zwischenzertifikate enthalten. Bei Problemen mit einem Zertifikat blockieren viele Browser den Zugriff auf die betreffende Website oder geben eine Sicherheitswarnung aus. Anbieter wie Facebook, die auf SSL-Verschlüsselung bestehen, sperren ihren Benutzern möglicherweise sogar den Zugriff auf Ihre Inhalte, falls in der Zertifikatskette Probleme auftreten. Es gibt etliche Tools unabhängiger Anbieter zur SSL-Analyse, mit denen Sie Ihre SSL/TLS-Implementierung überprüfen können, um etwaige Fehler oder Probleme zu beheben.

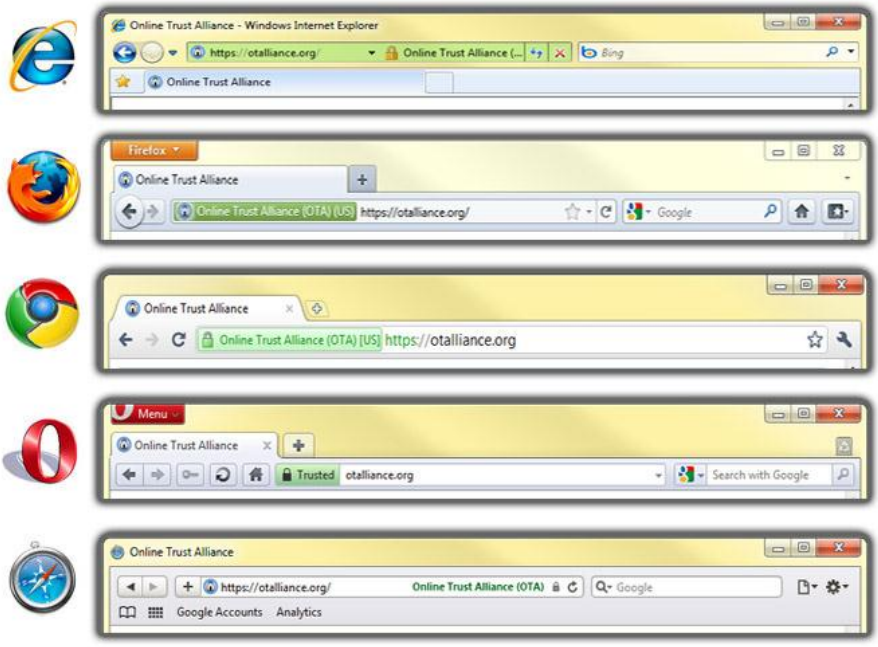
Verwendung des Attributs „sicher“ für alle Sitzungscookies

Optional kann ein Sitzungscookie das Attribut „sicher“ („secure“) erhalten, das dafür sorgt, dass der Browser diesen Cookie nur über eine HTTPS-Verbindung an den Webserver zurücksendet. Mit diesem Attribut signalisiert der Webserver dem Browser, dass es einer sicheren Verbindung dient, den Inhalt des Cookies zu schützen. So wird verhindert, dass Cookies über HTTP übertragen werden, selbst wenn der Browser versehentlich – oder weil er getäuscht wurde – versucht, eine HTTP-Verbindung zum Webserver aufzubauen.

Zertifikate mit Extended Validation stärken Sicherheit und Vertrauen

Um Websites noch stärker gegen Angriffsformen wie z. B. SSLStrip zu schützen, empfiehlt die OTA SSL-Zertifikate mit Extended Validation (EV). Die Antragsteller werden vor der Ausstellung eines EV-Zertifikats einer strengen Identitätsprüfung entsprechend den Regeln des CA/Browser-Forums unterzogen, eines Zusammenschlusses von über 30 renommierten Zertifizierungsstellen und Browserherstellern.

Abbildung 3: Die Darstellung von EV SSL-Zertifikaten in verschiedenen Browsern



Dabei werden die Identität und die Existenz der Website-Betreiber anhand zuverlässiger unabhängiger Quellen überprüft. Beim Aufrufen einer mit EV SSL-Zertifikaten geschützten Website wird die

Adressleiste grün hinterlegt und der Name des Website-Betreibers wird angezeigt. So haben Benutzer die Identität des Betreibers jederzeit vor Augen.

Die OTA empfiehlt verantwortungsbewussten Unternehmen, jede Website, für die eine sichere Verbindung erforderlich ist, mit einem EV-Zertifikat zu sichern. Die IT-Abteilungen sollten die Unternehmensleitung und die Benutzer darüber informieren, dass EV-Zertifikate die Sicherheit der Benutzer schützen und das Unternehmen gegen Angriffe sichern. Es sollten nur noch Browser eingesetzt werden, die EV-Zertifikate unterstützen, und jede Website, über die Online-Transaktionen abgewickelt werden, sollte ihre Strategie für Sicherheit und Markenschutz um die Prüfung auf EV-Zertifikate erweitern.

HSTS schützt vor aktiven Angriffen

HTTPS-Verbindungen werden oft dann aufgebaut, wenn Besucher durch eine Anmeldeschaltfläche oder von einer HTTP-Seite zu einer HTTPS-Website umgeleitet werden. Es ist allerdings auch möglich, bei diesem Übergang von einer ungesicherten Verbindung zu einer gesicherten einen Man-in-the-Middle-Angriff zu starten, und zwar entweder passiv oder indem das Opfer (z. B. durch eine Phishing-E-Mail) dazu gebracht wird, auf einen HTTP-Link zu einer seriösen Website zu klicken.

Der beste Schutz vor solchen Angriffen ist die Implementierung von HSTS für Ihre Website. Diese Spezifikation beschreibt Methoden, mit denen festlegt werden kann, dass bestimmte Websites nur über sichere Verbindungen aufgerufen werden können bzw. Benutzer mit bestimmten Websites nur über sichere Verbindungen kommunizieren können. HSTS wird von Google Chrome und Mozilla Firefox unterstützt und Websites wie PayPal.com, die HSTS einsetzen, signalisieren dem Browser ausdrücklich, dass sie Daten nur über verschlüsselte Verbindungen entgegennehmen oder ausliefern.[25] HSTS verhindert, dass Angreifer Sitzungscookies stehlen, wenn Website-Besucher von einer HTTP- auf eine HTTPS-Verbindung umgeleitet werden. Es ist derzeit die stärkste Waffe gegen Phishing und Man-in-the-Middle-Angriffe.

Fazit

Schon lange empfehlen viele Fachleute Website-Entwicklern und -Betreibern den Einsatz von SSL/TLS zur Sicherung der Benutzeranmeldung, von Finanztransaktionen und anderen wichtigen Aktivitäten. Bislang haben viele Unternehmen jedoch ihre Sites aufgrund von Vorbehalten wegen Kosten, Leistung und anderen Aspekten nur zögerlich auf verschlüsselte Verbindungen umgestellt. Die Online-Welt ist allerdings an einem Punkt angelangt, an dem klar ist, dass der Einsatz von HTTPS auf ausgewählten Seiten nicht mehr ausreichend ist, um moderne Benutzer, die immer und überall online sind, zu schützen. SSL/TLS selbst ist zwar weiterhin grundsätzlich sicher, doch die Entwicklung von Firesheep hat gezeigt, dass Websites umfassend geschützt werden müssen, nicht nur die Anmeldeseite oder der Warenkorb. Vereinfacht gesagt ist SSL mit dem Sicherheitsgurt im Auto vergleichbar, der während der gesamten Fahrt angelegt sein muss.

Always On SSL ist kein Allheilmittel gegen Hijacker und muss Teil einer groß angelegten Sicherheitsstrategie sein, mit der Kunden beim Besuch Ihrer Website geschützt werden sollen. Dennoch hat es sich als Schutz vor Sidejacking und anderen Man-in-the-Middle-Angriffen bewährt und ist unter dem Aspekt der Rechenleistung für die meisten Unternehmen mittlerweile erschwinglich. Facebook, Google, PayPal, Twitter und andere haben gezeigt, dass es selbst für sehr große und komplexe Websites möglich ist, vielfältigste Inhalte über HTTPS auszuliefern. Reaktionszeiten und heterogene Quellen können zwar problematisch sein, aber die in diesem Whitepaper vorgestellten Richtlinien und

[25] http://hacks.mozilla.org/2010/08/firefox-4-http-strict-transport-security-force-https/

Best Practices werden Ihnen helfen, auch damit umzugehen und Ihren Kunden optimale Leistung bereitzustellen.

Darüber hinaus trägt Always On SSL natürlich auch dazu bei, das Vertrauen der Besucher in Ihre Website zu bewahren. Der Schutz dieses Vertrauens ist eine ausgesprochen diffizile Aufgabe, die mit technischen Mitteln allein nicht zu lösen ist. Irgendwann kommt der Punkt, an dem man dem System einfach vertrauen muss – wie Ken Thompson, einer der Hauptautoren von UNIX, einmal schrieb, ist es vermutlich noch wichtiger, den Menschen zu vertrauen, die die Software geschrieben haben.[26] Mit Always On SSL als Maßstab für die Sicherheit signalisieren Sie den Besuchern Ihrer Website, dass Sie Benutzersicherheit und Datenschutz ernst nehmen und deshalb angemessene Schutzmaßnahmen ergreifen.

Über die Online Trust Alliance (OTA)

Die OTA ist eine unabhängige nichtkommerzielle Organisation zur Entwicklung und Förderung von Best Practices und allgemein anerkannten Richtlinien zum Schutz vor Gefahren für Datenschutz, Identität und Sicherheit von Online-Diensten, Unternehmen und Kunden. Damit soll das Online-Vertrauen gestärkt werden. Die OTA fördert einen offenen Dialog und die Zusammenarbeit von IT-Herstellern, Unternehmen und Behörden und verzeichnet bereits Erfolge bei der Bekämpfung verschiedener Formen von Online-Betrug, -Gefahren und -Vorgehensweisen, die das Vertrauen in Online-Angebote untergraben und die Rufe nach offiziellen Regelungen lauter werden lassen.

https://www.otalliance.org/

[26] http://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf

