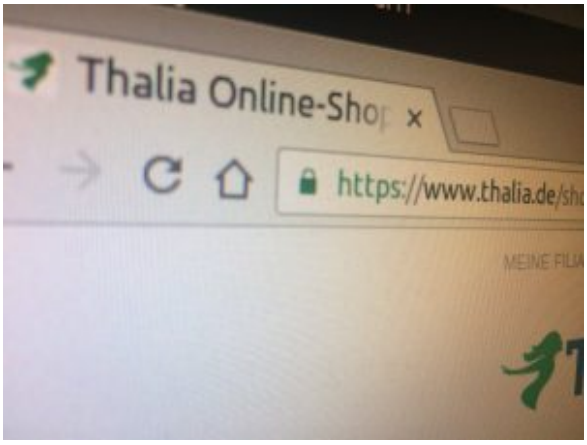
Alles auf „grün“ – Unser Weg hin zu „SSL für Alles“



Alles auf „grün“: hier ist die komplette Umstellung unserer Mandanten / Domain thalia.de gemeint

HTTPS ist nicht nur ein von Google bestätigter Rankingfaktor, auch einige Internet-Browser weisen inzwischen Webseiten, die noch nicht über HTTPS erreichbar sind, als unsicher aus. Aus Nutzersicht macht es also ganz klar Sinn Websites auf HTTPS umzustellen. Niemand möchte, dass sensible Daten von Dritten abgefangen werden können. Sieht ein Nutzer, dass eine Website vom Browser als unsicher eingestuft wird, überlegt er es sich zweimal, ob er einen Kauf abschließt oder seine Daten für einen Newsletter oder andere Dienste hinterlegt. Eine Einstufung als sicher kann ihn hingegen in seiner Kaufabsicht bestärken. Natürlich sind bei Thalia die Seiten, auf denen sensible Daten sind bzw. erhoben werden, schon immer verschlüsselt. Wir haben uns jedoch bewusst entschieden alle Seiten zu verschlüsseln was neben den erwähnten positiven Faktoren für den Kunden auch die Performance optimiert als auch die Administration der Seite vereinfacht.

Auch im Bezug auf die **Sichtbarkeit** in Suchmaschinen ist die Nutzung von

HTTPS anzuraten. Schon seit August 2014 ist HTTPS als Rankingfaktor bei Google etabliert. Seit Ende 2015 versuchen sämtliche Suchmaschinen automatisch Websites unter HTTPS aufzurufen. Ist eine Website unter HTTP und HTTPS aufrufbar, wird in der Regel die HTTPS-Version indexiert. Eine Studie des SEO-Tool-Anbieters Searchmetrics von 2015 bestätigt einen Zusammenhang zwischen der Nutzung von HTTPS und der Sichtbarkeit in Suchmaschinen einer Website. Laut der Studie haben Websites mit HTTPS tendenziell bessere Rankings.

Doch nicht nur die Sichtbarkeit und / oder Indexierung von Inhalten ist maßgeblich für eine erfolgreiche Umstellung auf HTTPS. Unsere gesamte eCommerce Platform unterliegt regelmäßigen PCI (Payment Card Industry Data Security Standard) Audits. Mithilfe dieser extern beauftragten Audits wird sichergestellt, dass sämtliche Zahlungsmodalitäten (Visa, Paypal, etc.), sowie Verfahren innerhalb unserer eCommerce Plattform, die Anforderungen und Regeln des PCI erfüllen. Einer der wichtigsten Punkte ist dabei die Absicherung sämtlicher Kommunikation zwischen Plattform, Endbenutzer sowie Drittanbieter. Dieses ist für uns ein Baustein um Kundendaten maximal zu schützen.

> ***Es ist ziemlich sinnvoll SSL auf allen Webseiten zu haben. Lasst es uns angehen! Aber nicht ohne die Fachabteilungen.***

Für die Umsetzung haben wir uns bewusst für den Wasserfall-Ansatz entschieden. Gestartet mit dem Thema „SSL für Alles“ sind wir im März 2016 mit einer großen Kickoff Veranstaltung, bei der alle Fachbereiche (insgesamt 12), die Berührung mit der eCommerce Plattform hatten, eingebunden waren. Auch wenn es schnell und einfach möglich gewesen wäre auf dem Apache ein HTTPS-Forwarding einzurichten, ohne die einzelnen Fachbereich wäre es auf keinen Fall gegangen. Der Shop wäre dann zwar technisch auf HTTPS gewesen, jedoch hätten sich die Kollegen gefragt, wo plötzlich die Umsätze hin sind.

Ausgehend von der großen Kickoff Veranstaltung begann anschließend die erste Planung der für die Umstellung notwendigen Ressourcen. Dabei kamen unglaubliche Zahlen zutage: 195 PT und 31.09.2016. So viel schon mal vorweg: das Datum konnten wir nicht halten

„Vorbereitung & Planung ist alles“…

…hat mal ein schlauer Mensch gesagt und lag damit verdammt richtig. Doch auch eine noch so genau Planung und Vorbereitung, in der man(n) denkt, auch wirklich an alles, absolut alles gedacht zu haben, relativiert sich, wenn die Umstellung naht und der „Schalter umgelegt“ wird.

Es versteht sich von selbst, dass eine solche Umstellung von HTTP auf HTTPS nicht auf den produktiven Systemen „per Hand“ durchgeführt werden kann und darf. Zur Absicherung der Plattform und aus Gründen der Stabilität sowie aus Sicherheitsgründen haben wir uns dafür entschieden die bisherige produktive Webstrecke bestehend aus diversen Webservern, Loadbalancern und Firewalls nicht zu verändern. Stattdessen haben wir parallel eine komplett neue Webstrecke mit den eben genannten Komponenten aufgesetzt. Mithilfe dieser sind wir in der Lage die Umstellung schnell, sicher und ohne Ausfall zu planen und im Vorfeld testen.

Mit der Bereitstellung einer dedizierten Webstrecke — bestehende aus neuen IP Adressen, frischen Webservern auf Basis von Apache — sowie einer Vielzahl von Erweiterung / Änderungen an Firewall sowie Loadbalancer haben wir die Möglichkeit geschaffen, diese neue Strecke mit Anbindung an das produktive Backend ausgiebig zu testen und weiter zu optimieren, ohne dabei den eigentlichen produktiven Traffic in irgendeiner Weise negativ zu beeinflussen. Eine gute Ausgangsbasis, wenn man bedenkt, dass wir durch den Aufbau einer dedizierten bzw parallelen Strecke jederzeit hin und her schalten könnten.

Unsere Domain thalia.de sowie die dazugehörigen (virtuellen) Webserver sind nicht nur der Endpunkt für den Einstieg in den bereits genannten Online-Shop. Vielmehr bietet thalia.de eine Vielzahl von Diensten für die unterschiedlichsten Geräte bzw. Konsumenten — wie bespielsweise OAuth, API, Partner-Integration, Mobile Apps (XCA), Hörbuch Downloads, etc… — und natürlich auch sämtliche Microservices, die in den letzten Monaten durch die einzelnen Teams bereitgestellt worden sind. Nicht zu vergessen sind hier auch die Abhängigkeiten zu externen Partnern, wie Paypal, Payback, Visa, usw., um nur einige zu nennen.

Die Umstellung ist nicht nur ein simples HTTPS-Forwarding auf dem Apache

Und spätestens an dieser Stelle dürfte jedem klar sein, dass eine scheinbar triviale Anforderung (HTTP zu HTTPS) weitreichende Auswirkungen haben kann. Daher ist es umso wichtiger das Gesamtbild aller Funktionalitäten und Abhängigkeiten vor Augen zu haben. Hand auf's Herz: Ist dazu wirklich irgendjemand in der Lage? Die Antwort darauf ist so nüchtern wie erschreckend: Nein. Aus der Theorie wissen wir, dass eine oder maximal eine handvoll Personen einen sehr guten Überblick haben. Der Rest *weiß* einfach, an wen man sich wenden kann und muss, wenn der Fall eintritt. Aus diesem Grund haben wir uns dafür entschieden alle wichtigen Vertreter der einzelnen Services (Shop-Management-System, App Services, IT Betrieb,) für den Tag der Tage in einem Raum zu vereinen. Die Umstellung ist ein Team-Erfolg.

SSL und SEO – so passt beides zusammen

Um eine möglichst Suchmaschinen-konforme Umstellung zu erreichen, mussten die folgenden Punkte zwingend eingehalten werden. Wie gut, dass wir dafür unseren Spezialisten am Tag der Umstellung an Board hatten. Eine zentrale Rolle spielt dabei die Google Search Console (ehemals Google Webmaster Tools). Hier ist es unbedingt notwendig, direkt nach der Umstellung auch die neue HTTPS-Version der Webseite einzurichten.

Umstellung auf HTTPS: Die wichtigsten Tipps

- Alle alten URLs sollten mit einem 301-Redirect auf die HTTPS-Variante weitergeleitet werden
- Auch Canonical Tags sollten in die SSL-Variante umgeschrieben werden
- Sofern bei den internen Links keine relativen Links verwendet wurden, sollten diese ebenfalls umgebaut werden, um unnötige Redirects zu vermeiden
- Die robots.txt Datei sollte auch via HTTPS erreicht werden
- Es sollte sichergestellt sein, dass alle internen und externen Ressourcen (Bilder, Scripte, CSS etc.) über HTTPS laden – ansonsten werden im Browser für den Nutzer abschreckende Warnungen angezeigt
- In der Google Search Console sollte eine neue Property für die HTTPS-Version der Seite angelegt sein
- Die Sitemap sollte neu erstellt und bei der Google Search Console eingereicht werden

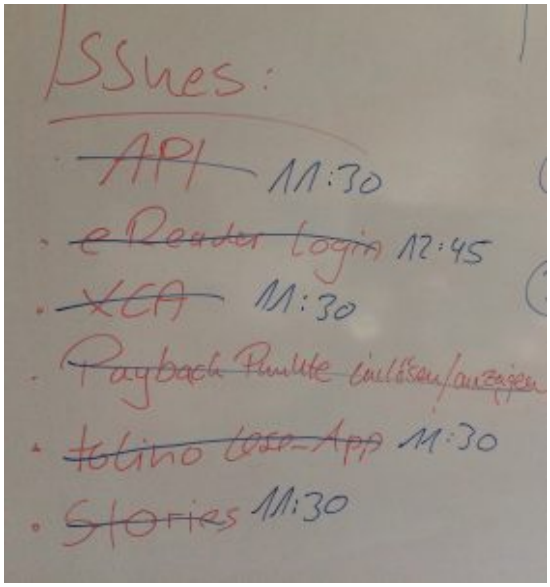
- HTTP Strict Transport Security (HSTS) sollte eingeführt werden: Dieser Sicherheitsmechanismus schützt HTTPS-Verbindungen vor der Aushebelung der Verbindungsverschlüsselung durch downgrade-Attacken

„Harry, leg den Schalter um !“

Eine Umstellung in der Nacht kam für uns nicht in Frage. Wir sind mutig und haben ein Top-Team welches am Morgen deutlich frischer ist. Ein beliebtestes Ritual darf an einem solchen Tag jedoch nicht fehlen: ausgiebig gemeinsam Frühstücken.

Käse, Wurst, Lachs, Mett und 40 Brötchen waren es zu Beginn :-)

Gut gestärkt geht es dann in die letzte Vorbereitungsphase, in der alle anwesenden Teilnehmer(/-innen) noch einmal alle notwendigen Punkte durchgehen. Für die vorliegende Umstellung von HTTP auf HTTPS haben wir uns für einen klassisch-moderaten Ansatz entschieden: Anstatt Änderungen im DNS zu einem gegebenen Zeitpunkt durchzuführen und darauf zu warten, dass diese Änderungen weltweit propagiert sind (Notiz am Rande: Ein TTL von 5 Minuten kann auch sehr sehr lang sein), entschieden wir uns für eine Anpassung bei unserem vorgeschalteten DDoS-Schutz. Mit Hilfe des dazugehörigen Webportals kann im Handumdrehen der Upstream (in diesem Fall unser Endpunkt) aktualisiert werden, ohne dabei auf TTL oder sonstiges warten zu müssen, denn diese Art von Änderungen werden sofort aktiv. Hinzu kommt der charmante Vorteil, dass wir jederzeit und auf direktem Wege wieder zur ursprünglichen Konfiguration hätten zurück kehren können. Das passt und befriedigt auch die verbleibenden kritischen Stimmen.



Auszug aus unserem Whiteboard vom Tag der Umstellung: Störungen sowie die Lösungszeit sind hier vermerkt.

Wer jetzt erwartet hat, dass diese Umstellung ohne irgendwelche „Ruckler“ oder sonstigen Seiteneffekte vollzogen worden ist, den müssen wir hier enttäuschen. Auch Thalia kennt Murphys-Law. Es gibt immer Punkte, die zuvor nicht berücksichtigt werden konnten oder schlichtweg auf der Strecke geblieben sind. Doch eine gute Vorbereitung heißt auch, genau diese Punkte in kürzester Zeit anzugehen sowie diese Probleme aus dem Weg zu räumen. Denn hey, dafür haben wir doch „alle Mann an Board bzw. in einem Raum eingesperrt“.

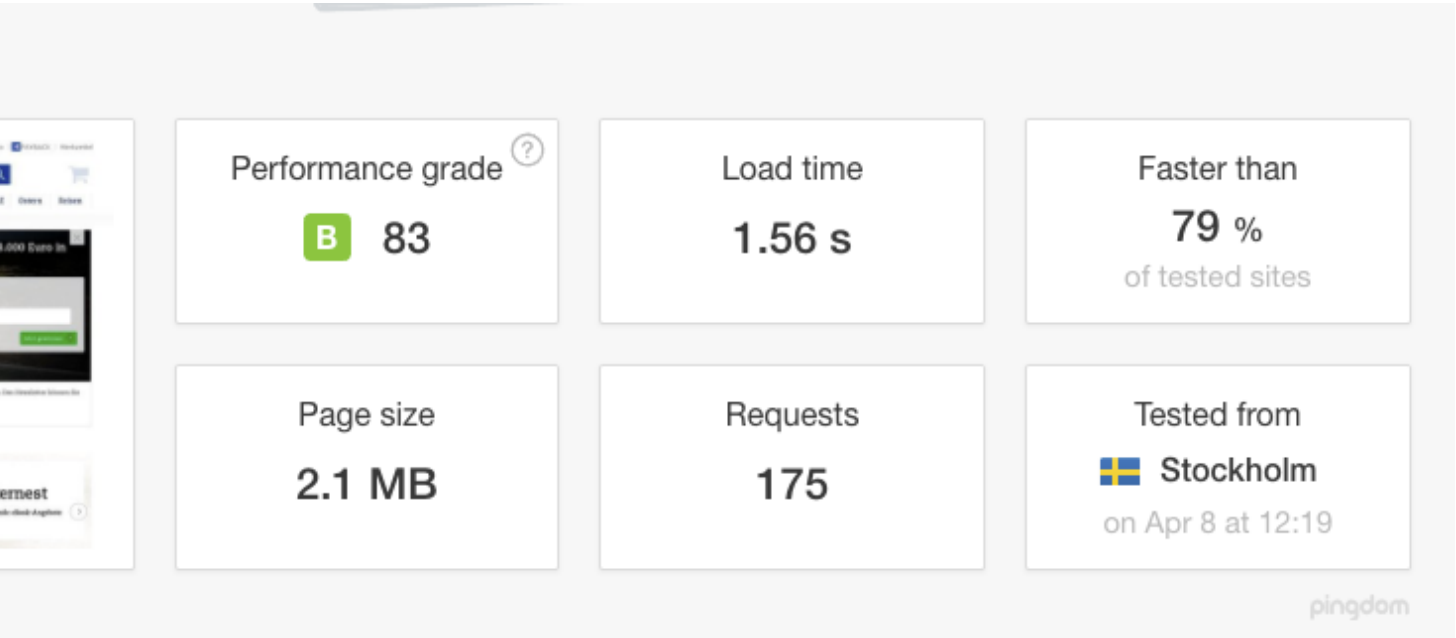
Bereits Wochen zuvor haben wir in (in teils penetranter Art & Weise) sämtliche Bereichen, Abteilungen sowie interne und externe Partner auf diese Umstellung sensibilisiert, wodurch genügend Raum und Zeit gegeben worden ist, sämtliche Probleme zu klassifizieren, zu adressieren und schnellstmöglichst lösen zu können.

Fazit & Lesson’s Learned

Unsere Vorgehensweise sämtliche Stakeholder und notwendigen Ressourcen an einem (physikalischen) Ort zu bündeln (bzw einzusperren) erwies sich wieder einmal als sehr nützliche Methode / Methodik, denn alle gemeldeten Problemchen konnten während des normalen Tagesbetriebs gelöst werden. Dank unserer ASB (=Automatische Service Bereitstellung) konnte ein Hotfix noch am gleichen Tag

erstellt, getestet und in Produktion ausgerollt werden.

Die Umstellung auf HTTPS (SSL/TLS) hat darüber hinaus noch weitere Vorteile: Wir sind ab sofort in der Lage HTTP/2 Verbindungen zu unterstützen, welches eine effizientere Nutzung der Netzwerk-Ressourcen und kürzere Latenzen verspricht (und auch einhält). Verbesserungen sollen aber auch eine Kompression der Header der IP-Pakete sowie Multiplex- und Push-Techniken bringen. Browser können mittels Multiplexing mehrere Messages gleichzeitig über eine Verbindung beziehen und Server können Elemente im voraus, also ohne Anfrage des Browsers pushen. Dies wird umso deutlicher, wenn wir uns vor Augen führen, wie viele Bilder beim Aufruf der sämtlicher Seiten geladen und übertragen werden müssen: HTTP/2 erweist sich hier als bemerkenswert effizient, da sämtliche Anfragen parallel und mit nur einer Verbindung übertragen werden. Dies wiederum hat zur Folge, dass die Ladezeit erheblich verbessert werden konnte.

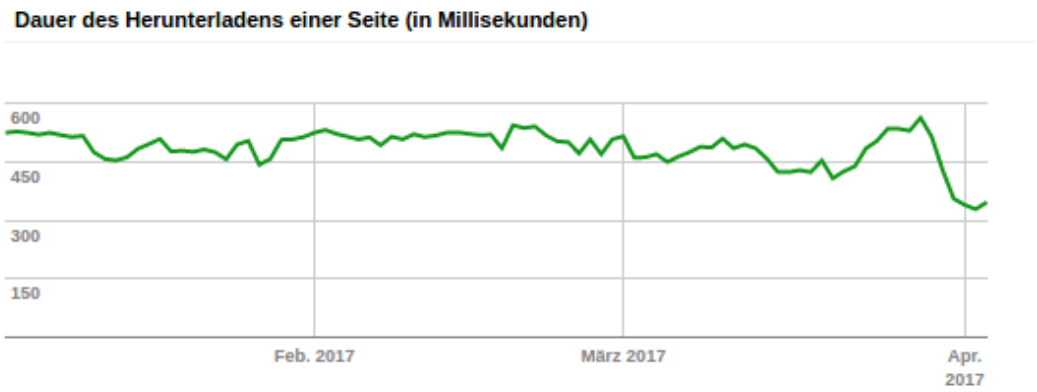


tellung auf HTTPS inkl HTTP/2 (Quelle: tools.pingdom.com)

Gut zu erkennen, wie mit nur einer Verbindung — Dank HTTP/2 — mehrere Bilder / Assets geladen und übertragen

Mittels HSTS (HTTP Strict Transport Security) wurde ein zusätzlicher HTTP-Header eingeführt, mit dem der Server dem Browser signalisiert, dass eine Seite künftig nur noch über HTTPS abgerufen werden soll. Der Browser speichert diese Information lokal für einen im Header festgelegten Zeitraum („Max. Age“), der im Prinzip wie ein Cache funktioniert. Ab diesem Moment wendet der Client sich direkt über HTTPS an den Host, auch wenn der Nutzer explizit „http://“ in der Adresszeile des Browsers eingibt oder einem „http“-Link dorthin folgt. Ein

weiterer Vorteil für den Client, über den Sicherheitsgewinn hinaus: Durch die entfallende Umleitung verkürzen sich die Antwortzeiten.



> Auch Google indiziert die Domain www.thalia.de nun deutlich schneller als zuvor (Unsere Änderung wurde Ende März in Produktion ausgerollt)

Ausblick

Der erste Schritt in die richtige Richtung ist vollbracht. In den kommenden Wochen werden wir das Verhalten sowie die Performance weiter im Auge behalten und ständig weiter optimieren, um unseren Kunden und Besuchern eine best mögliche User Experience zu präsentieren. In Sachen Performance und User Experience stehen unsere Edge-Provider (MyraCloud Security sowie Akamai) ganz oben auf der Liste der Agenda. Hier gilt es zu bewerten, inwiefern wir das Caching weiter verfeinern können.