Cyber-Sicherheit ohne Entschlüsselung des Internetverkehrs

Bei Cloudflare haben wir das Ziel, ein besseres Internet zu schaffen. Das bedeutet, Dienste zur Verbesserung der Sicherheit, Performance und Zuverlässigkeit von Websites, Internetanwendungen bereitzustellen und so dafür zu sorgen, dass sich mehr Menschen sicher, schnell und verlässlich mit dem Web verbinden können. Kunden sind unter Umständen dazu verpflichtet, dafür zu sorgen, dass personenbezogene Daten die Europäische Union nicht verlassen. Wir wollen sie dabei ebenso unterstützen wie bei der Einhaltung anderer einschlägiger Vorschriften zur Datenverarbeitung. Doch die einzuhaltenden Bestimmungen können von Kunde zu Kunde stark variieren. Deshalb möchten wir hier einige der Methoden vorstellen, mit denen wir unseren Kunden dabei helfen, ihre Vorgaben und Ziele in den Bereichen Sicherheit, Datenschutz und Compliance zu erreichen.

Aktuell umfasst das globale Netzwerk von Cloudflare mehr als 270 Städte in über 100 Ländern und Wirtschaftsräumen. Dank Direktverbindungen zu so gut wie jedem Service- und Cloud-Provider erreicht es 95 % der Weltbevölkerung innerhalb von 50 ms. Wie unsere Kunden wissen, fungiert Cloudflare als Reverse-Proxy: Endnutzer im Internet passieren erst das Cloudflare-Netzwerk, bevor sie die Website des Kunden erreichen.

Die Anwendungsdienste von Cloudflare

Die meisten Kunden nutzen unsere *Anwendungsdienste* für den Schutz ihrer Websites. Dazu zählen:

- Eine Web Application Firewall, mit der Traffic auf verbreitete Sicherheitsbedrohungen hin überprüft wird, die eine Website kompromittieren könnten;
- Ein Cache (CDN), in dem vorübergehend Kopien von öffentlich zugänglichen Inhalten gespeichert werden, um diese schneller bereitstellen zu können; und
- Bot-Management, um zu ermitteln, ob Traffic menschlichen Ursprungs ist oder von einer Maschine stammt.

Um diese Services anzubieten, müssen wir den Inhalt des Datenverkehrs in unseren Edge-Servern überprüfen, damit wir schädlichen Traffic aufspüren oder die Übermittlung beschleunigen können. Der Traffic wird auf dem Weg zu Cloudflare verschlüsselt, beim Erreichen unserer Edge-Server überprüft, anschließend erneut verschlüsselt und an die Ursprungsserver unserer Kunden weitergeleitet.

Bei der Bereitstellung von Anwendungsdiensten über Cloudflare die Rolle eines *HTTP-Reverse-Proxy*. Das bedeutet, dass Cloudflare das HTTP-Protokoll (das Protokoll des Webs) nutzt, um sowohl mit den Servern der Endnutzer als auch mit denen unserer Kunden zu kommunizieren. Um den Datenverkehr unter die Lupe zu nehmen, beenden wir

TLS-Verbindungen von Endnutzern.

Die Netzwerkdienste von Cloudflare

Cloudflare bietet auch eine Reihe von *Netzwerkdiensten*. Dazu zählen:

- Die Erkennung und Abwehr von Denial of Service (DoS)-Angriffen
- Eine IP-Firewall, die bestimmte IPs und Ports blockieren kann
- Die Lösung Argo Smart Routing, die Wege für eine effizientere und zuverlässigere Übermittlung des Datenverkehrs über das Internet findet.

Unsere Netzwerkdienste können zwar ebenfalls die Performance verbessern und vor Bedrohungen schützen, funktionieren aber ein wenig anders als unsere Anwendungsservices. Anstatt den Traffic-Inhalt zu inspizieren, prüfen sie nur Pakete oder Verbindungen. Man kann sich das vorstellen wie ein Spediteur, der Kartons überprüft, während sie von A nach B geliefert werden. Unsere Anwendungsdienste öffnen den Karton kurz (und versiegeln ihn dann wieder), um festzustellen, ob der Inhalt gefährlich ist. Demgegenüber befassen sich unsere Netzwerkdienste nur damit, ob ein Karton bestimmte Merkmale aufweist, die auf etwas Ungutes schließen lassen.

Zu unseren Netzwerkdiensten zählt Spectrum. Kunden setzen diese Lösung meistens ein, weil sie etwas anderes als Websites schützen wollen – beispielsweise einen E-Mail- oder einen VOIP-Server. Es gibt aber auch eine Konstellation, bei der Spectrum für die Sicherheit von Websites sorgt.

Genau genommen handelt es sich bei Spectrum um einen *TCP/UDP-Reverse-Proxy*, der auf Verbindungs- oder Sitzungsebene arbeitet. Weil TLS lediglich ein Protokoll ist, das über TCP läuft, müssen TLS-Verbindungen für die Bereitstellung dieser Services nicht beendet werden.

Die Lösung funktioniert insbesondere gut für Kunden, die ihre Websites besser schützen wollen, ohne dass jemand ihren Traffic überprüft. Manche Behörden könnten beispielsweise Richtlinien oder Vorschriften unterliegen, die das Inspizieren des Traffics durch Dritte untersagen, mag dies noch so sicher und datenschutzfreundlich durchgeführt werden. Solche Kunden können auf die Netzwerkdienste von Cloudflare – DoS-Schutz, Firewall und Traffic-Beschleunigung – zurückgreifen. Mit dieser Option werden Websites zwar nicht ganz so umfassend abgesichert, das ist aber immer noch besser, als über gar keinen Schutz zu verfügen.

Datenlokalisierung mithilfe von Anwendungs- und Netzwerkdiensten

Für Kunden, die unsere Anwendungsdienste nutzen und selbst darüber bestimmen möchten, wo ihre Daten überprüft und gespeichert werden, bietet Cloudflare die Data

Localisation Suite. Auch Kunden, die unsere Netzwerkdienste verwenden, können wir Kontrolle über den Speicherort ihrer Daten geben, in diesem Fall mittels unserer Customer Metadata Boundary. Diese Komponente unserer Data Localisation Suite wurde vergangenes Jahr eingeführt, um sicherzustellen, dass Traffic-bezogene *Metadaten* – Endnutzerprotokolle, die die Identität der Kunden verraten, und die Analysedaten, die wir in unserer Funktion als Auftragsverarbeiter für unsere Kunden verarbeiten – die EU nicht verlassen.

Customer Metadata Boundary wurde zwar mit Blick auf unsere Anwendungsdienste entwickelt, funktioniert aber ebenso gut in Verbindung mit Spectrum. Wie unsere Anwendungsdienste erzeugt Spectrum Nutzungsprotokolle. Ohne Customer Metadata Boundary würden diese Protokolle an unser zentrales Rechenzentrum in den Vereinigten Staaten übermittelt. Ist jedoch Customer Metadata Boundary aktiviert, sorgt Cloudflare dafür, dass diese Protokolle nicht an Orte außerhalb der EU übertragen werden.

Deshalb können wir mit unseren Netzwerkdiensten und Customer Metadata Boundary den Anforderungen an Datenlokalisierung von Kunden gerecht werden, die einerseits sichere und leistungsstarke Websites benötigen, andererseits aber verhindern müssen, dass der Internetverkehr von Dritten entschlüsselt wird.