LANCOM SYSTEMS

Whitepaper

Netzwerktransparenz durch DPI und Verschlüsselungsproxys

Die Rolle der Verschlüsselung

Da das öffentliche Internet heutzutage ohne eine angemessene Verschlüsselung nicht mehr vorstellbar ist (98 % des Webverkehrs ist verschlüsselt und die verschlüsselte Kommunikation ist in modernen Browsern Standard), ist es für jede Anwendung unerlässlich, angemessene Verschlüsselungstechnologien bereitzustellen und einzusetzen. Die Verschlüsselung ist notwendig, um die Daten der Anwendung und ihre Benutzer zu schützen.

Dies erklärt auch die lange Erfolgsgeschichte der modernen Verschlüsselung, die auf die Einführung von SSL 1.0 im Jahr 1994 vor fast 30 Jahren zurückgeht. Vor etwa 20 Jahren wurde AES in den Standard aufgenommen, was die Leistung und Anwendbarkeit der Protokolle drastisch erhöhte. Der heutige Standard ist bereits die sechste Iteration des Standards, der nach der Hälfte der Zeit von SSL in TLS umbenannt wurde.

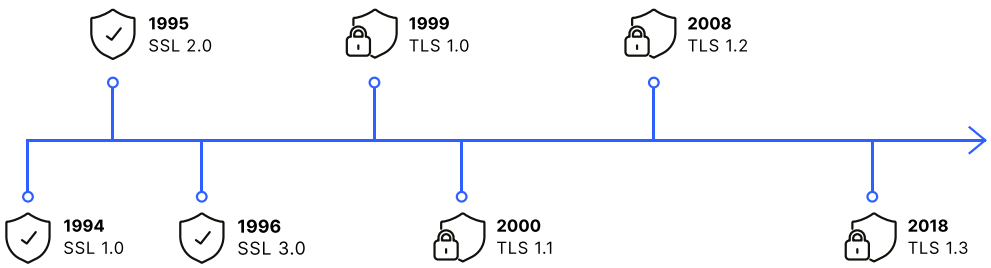

Abbildung 1:
Entwicklung SSL / TLS

Aktueller Trend

Bei der Verschlüsselung gibt es heute im Wesentlichen zwei Trends: Zum einen nimmt die Menge der zu verschlüsselnden Daten ständig zu. Traditionell waren die eigentlichen Nutzdaten das Hauptziel der Verschlüsselung, da sie naturgemäß die sensiblen Daten enthielten. Nun hat sich die Definition sensibler Daten erweitert und umfasst nun auch Dinge wie die Metadaten der verschlüsselten Nutzdaten. Folglich müssen auch die Metadaten verschlüsselt werden, was neue Technologien und Protokolle zur Unterstützung dieser Verschlüsselung wie TLS 1.3 oder DoH hervorgebracht hat.

Dies zeigt deutlich, dass wir uns auf eine Gesellschaft zubewegen, in der alles verschlüsselt ist.

Ein weiterer Trend ist das Aufkommen von Quantencomputern und deren Auswirkungen auf die aktuellen Verschlüsselungsmethoden und -algorithmen. Dies gefährdet den derzeitigen Anspruch auf Vertraulichkeit, den die Verschlüsselung bietet, zumal sich kryptografische Systeme im Allgemeinen nur ungern ändern und niemand die Entwicklungsgeschwindigkeit von Quantencomputersystemen wirklich vorhersagen kann. Die derzeitigen Verschlüsselungsalgorithmen sind anfällig für Quanten-entschlüsselungstechniken wie den Shor-Algorithmus, da der Quantenansatz die

Problemlösungsdomäne von der mathematischen Domäne der Primfaktorzerlegung auf die physikalische Domäne der Erzeugung von qbits verlagert und somit in der Lage ist, alle möglichen Zustände gleichzeitig statt sequentiell zu verarbeiten.

Es ist jedoch nicht alles verloren, denn es gibt neue oder angepasste traditionelle Algorithmen, die durch Quantenansätze nicht gebrochen werden können und daher als Post-Quanten- oder quantensichere Verschlüsselung bezeichnet werden.

Die positiven Aspekte

Die Verschlüsselung ist ein wesentlicher Bestandteil der heutigen Anwendungen. Jede Art von moderner Kommunikation hängt von einer zuverlässigen und starken Verschlüsselung ab, um die Integrität und Vertraulichkeit der übertragenen Informationen zu gewährleisten. Die Verschlüsselung bietet hierfür den sicheren Rahmen und sollte als Standardverfahren betrachtet werden. Sie würden die fraglichen Informationen ja auch nicht per Postkarte verschicken, oder?

Das Negative

In der Vergangenheit haben sich Middleboxen und Technologien wie Deep Packet Inspection (DPI) und Anwendungsanalyse stark auf die Metadaten der in SSL /TLS-verschlüsselten Verbindungen verwendeten Zertifikate verlassen. Mit der Einführung von TLS 1.3 sind diese Informationen nicht mehr ohne Weiteres verfügbar, da sie zusammen mit den regulären Nutzdaten, z. B. dem SNI-Teil (Server Name Identifier) des Handshakes, verschlüsselt werden. Daher sind andere Technologien erforderlich, um weiterhin die für die Anwendungskontrolle und -Verwaltung erforderlichen Informationen zu erhalten. Zu diesen Technologien gehört z. B. die Verhaltensanalyse des Pakettransports wie Größe, Häufigkeit und Timing-Eigenschaften.

Auswirkungen auf die Sichtbarkeit

Die Netzwerktransparenz ist für die Gewährleistung und Optimierung der Funktionalität und des Betriebs eines jeden Netzes unerlässlich.

Dies gilt insbesondere für Finanzinstitute und andere Einrichtungen, die erhöhte Anforderungen hinsichtlich der Einhaltung von Vorschriften und ähnlichen Themen haben. Die Verwendung von Verschlüsselung hat all dies unsichtbar und unzugänglich gemacht.

Daher ist der Einsatz von Anwendungs- und Netzwerk-Proxys sehr viel wichtiger geworden. Die notwendigen Daten zur Lösung der oben genannten Aufgaben können nur durch Entschlüsselung der Pakete gewonnen werden. Dies muss natürlich auf

sehr sichere und zuverlässige Weise geschehen und erfordert fundiertes Fachwissen sowie Änderungen an der Netzarchitektur, z. B. die Verteilung interner Zertifikate und Vertrauensketten, um die Ent- und Verschlüsselung auf Proxy-Ebene zu ermöglichen.

Auswirkungen auf Routing, Switching, Lastausgleich, Netzaufteilung usw.?

Grundlegende Netzfunktionen wie Routing und Switching dürften kaum betroffen sein. Natürlich leiden übergeordnete Funktionen, die von zusätzlichen Informationen abhängen, wie z. B. anwendungsbasiertes Routing, unter denselben Nachteilen in Bezug auf die Sichtbarkeit. In Folge muss die Technologie weiterentwickelt werden, um z. B. Verhaltensanalysen zu ermöglichen.

Die Auswirkungen auf andere Funktionen müssen von Fall zu Fall geprüft werden. Beispielsweise hängen die Auswirkungen auf den Lastausgleich stark von der Technologie ab, die für den eigentlichen Ausgleich verwendet wird. Round-Robin-Methoden sollten überhaupt nicht beeinträchtigt werden, während Methoden, die sich auf zusätzliche Daten stützen, wiederum unter denselben Folgen leiden.

Sicherheitsprobleme

Auch hier ist die Situation zweigeteilt. Einerseits erhöht die Verschlüsselung die Sicherheit erheblich, da sie Informationen verbirgt, die von Angreifern genutzt werden können, um Schwachstellen in der Organisation zu finden und diese auszunutzen. Zusätzlich ist es mit geeigneten Verschlüsselungstechniken fast unmöglich, bösartige Daten in vertrauenswürdige Informationsströme einzuschleusen.

Andererseits kann dieselbe Technologie von Angreifern genutzt werden, um Malware und bösartige Kommunikation vor Scan- und Erkennungssystemen zu verbergen. So kann beispielsweise ein Virus, der über einen kompromittierten Server heruntergeladen wird, von einer Scan-Engine nicht erkannt werden, wenn die Verbindung verschlüsselt ist.

Um dem entgegenzuwirken, müssen Unternehmen spezielle Maßnahmen für ihre Netzwerkinfrastruktur ergreifen um ihre verschiedenen Sicherheitssysteme wie Malware-Scanner, IDS / IPS-Engine usw. betriebsbereit zu halten.

Was können die größten netzwerkbezogenen Probleme von Unternehmen bei verschlüsseltem Datenverkehr sein?

Der oben beschriebene Verlust der Sichtbarkeit erfordert grundlegende Änderungen an der Netzwerkinfrastruktur, um die Dienste betriebsbereit zu halten und die Kontrolle über das Netzwerk zu behalten.

Um die Sichtbarkeit und das volle Scanning-Potenzial wiederzuerlangen, müssen verschlüsselte Verbindungen an dedizierten, vertrauenswürdigen Endpunkten terminiert werden, an denen der Datenverkehr entschlüsselt, gescannt und erneut verschlüsselt werden kann, bevor er an sein endgültiges Ziel weitergeleitet wird.

Dies stellt eine Herausforderung für die Handhabung und Verteilung der erforderlichen Zertifikate dar, insbesondere in BYOD-Szenarien. Einige Anwendungen schützen sich sogar ausdrücklich gegen diese Techniken, da sie aus ihrer Sicht nicht von Angriffen zu unterscheiden sind. In diesen Situationen stehen CISOs und Organisationen vor der schwierigen Entscheidung, entweder die gesamte Anwendung zu sperren oder die Gefahren der Blackbox-Kommunikation zu akzeptieren. Wenn die Wahl auf das Blockieren der Anwendung fällt, sind Anwendungsmanagement-Lösungen, die mit verschlüsseltem Datenverkehr arbeiten, z. B. DPI unter Berücksichtigung von Verhaltensanalysen, natürlich die bevorzugte Lösung.

Die Lösung

Die Anbieter von Sicherheitslösungen sind sich der Probleme und Herausforderungen, mit denen Unternehmen heute konfrontiert sind, natürlich sehr wohl bewusst. Sie bemühen sich, maßgeschneiderte Lösungen für die verschiedenen Verschlüsselungsszenarien anzubieten.

Eine gültige Lösung ist die Verwendung einer hochmodernen UTM-Firewall der nächsten Generation, die über verhaltensbasierte DPI und die erforderlichen Forward- und Reverse Proxys verfügt, um eine Überprüfung zu ermöglichen. Einen umfassenden Überblick über die verschiedenen Funktionen und ihre Auswirkungen finden Sie hier: www. lancom-systems.de/produkte/security

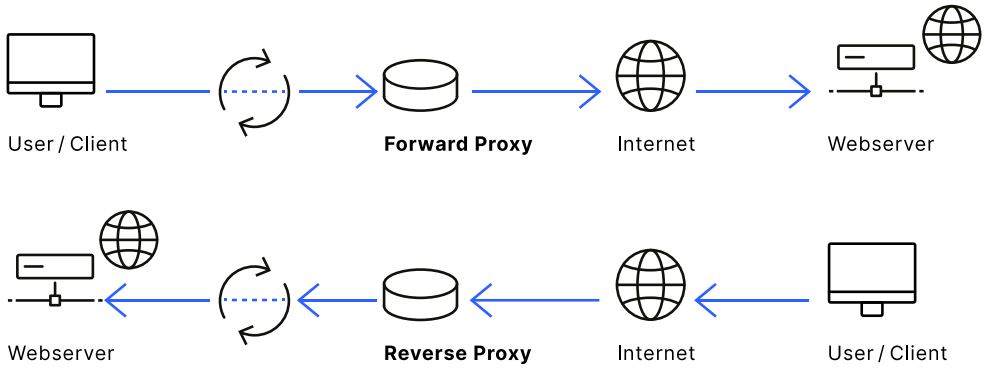

Abbildung 2:
Forward Proxy vs. Reverse Proxy

Fazit

Um die vorherigen Punkte zusammenzufassen:

→ Behavioral DPI zur Wiederherstellung der Anwendungssichtbarkeit
→ Entschlüsselung und Wiederverschlüsselung mittels Proxys zur Erkennung von Bedrohungen, die in verschlüsselter Kommunikation versteckt sind
→ Asset-Management-Infrastruktur zur Verwaltung und Überwachung von Zertifikatsinfrastrukturen
→ Die Erkennung von Netzwerkanomalien kann bei der Erkennung von Angriffen und Verstößen helfen.
→ Sensibilisierung der Mitarbeiter

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de
www.lancom-systems.de