SONICWALL™

KURZDARSTELLUNG: DIE SCHATTENSEITE DER VERSCHLÜSSELUNG

Warum Ihre Netzwerksicherheitslösung in der Lage sein muss, den Datenverkehr zu entschlüsseln, um verborgene Bedrohungen zu stoppen

Zusammenfassung

Die Websitzungen Ihrer Benutzer sind heute wahrscheinlich zum Großteil über Secure Sockets Layer / Transport Layer Security (SSL/TLS) bzw. HTTPS verschlüsselt. Dafür sorgt ein starker Trend in der IT-Industrie zum komplett verschlüsselten Internet, deren Befürworter vor allem zwei Ziele verfolgen:

- Cyberkriminellen das Mitlesen des Datenverkehrs im Internet zu erschweren
- die Sicherheit und Vertraulichkeit persönlicher Daten zu gewährleisten

Während normale User ihre Kommunikation immer häufiger chiffrieren, hat sich die Verschlüsselung zu einem beliebten Bedrohungsvektor für Hacker entwickelt, mit der sie ihre Angriffe maskieren, Sicherheitsmechanismen umgehen und letzten Endes Hintertüren direkt ins Netzwerk eines Unternehmens finden. Schließlich kann Ihre Sicherheitslösung keine Bedrohungen aufhalten, die sie nicht sehen kann. Ohne eine angemessene Lösung haben alle Angriffe mittels SSL/TLS eine 100-prozentige Erfolgschance. Die Folgen sind der Verlust von geheimen Daten und geistigem Eigentum sowie eine Schädigung des Rufs.

Verschlüsselungsprotokolle kommen überall zum Einsatz

SSL/TLS wird in vielen Bereichen genutzt – angefangen beim E-Handel bis hin zum Onlinebanking. Der Datenverkehr in Unternehmen wird zunehmend mittels SSL/TLS geschützt. Einige Branchen nutzen dieses Verschlüsselungsprotokoll sogar für den Großteil des Netzwerkverkehrs. SSL schützt Daten während der Übertragung, indem ein verschlüsselter Kanal über das öffentliche Internet oder private Netzwerke hergestellt wird. Somit lassen sich die Daten weder abfangen noch infizieren.

Darüber hinaus stellt SSL sicher, dass die Daten nicht an einen vermeintlich vertrauenswürdigen Ort gelangen, der von einem Hacker kontrolliert wird. Wichtige und sensible Daten wie etwa Kreditkarteninformationen, Benutzernamen und Passwörter werden so übertragen, dass möglichst nur der gewünschte Empfänger auf die Daten zugreifen kann. Wurde SSL früher vor allem von Websites sowie FTP- und Telnet-Servern genutzt, so ist das Protokoll heute bei einer Vielzahl von Anwendungen im Einsatz, darunter Java-basierten Anwendungen, Application-Management-Services und Cloud-basierten Services. Zu den bekanntesten Anwendungen, die eine SSL-Verschlüsselung unterstützen, gehören Facebook und Twitter. Darüber hinaus sind

Veraltete Netzwerksicherheitslösungen sind gewöhnlich nicht in der Lage, SSL-/TLS-verschlüsselten Verkehr zu prüfen, oder haben eine so schwache Performance, dass sie bei einer Durchführung der Prüfung unbrauchbar werden.

auch Browser-Add-ons verfügbar, die eine Nutzung von SSL via HTTPS erzwingen können.[1]

Im vierten Quartal 2015 machten HTTPS-Verbindungen (SSL/TLS) durchschnittlich 64,6 Prozent aller Webverbindungen aus und wuchsen somit fast das gesamte Jahr über stärker als HTTP. Im Januar 2015 wurden 109 Prozent mehr HTTPS-Verbindungen verwendet als im Januar 2014. Außerdem stieg die Nutzung in jedem Monat des Jahres 2015 durchschnittlich um 53 Prozent im Vergleich zum entsprechenden Monat des Vorjahrs.

Viele Firewalls sind mit der Prüfung von verschlüsseltem Datenverkehr überfordert

Mithilfe von SSL/TLS können findige Angreifer Command-and-Control-Kommunikationen und bösartigen Code präparieren, um Intrusion-Prevention-Systeme (IPS) und Anti-Malware-Systeme zu umgehen. Diese Angriffe können einen großen Schaden anrichten, weil die meisten Organisationen einfach nicht über die richtige Infrastruktur verfügen, um sie aufzuspüren. Veraltete Netzwerksicherheitslösungen sind meist nicht in der Lage, SSL-/TLS-verschlüsselten Verkehr zu prüfen, oder haben so wenig Leistung, dass sie de facto unbrauchbar werden, wenn sie die Prüfung durchführen. Eine Prüfung des HTTPS-Verkehrs durch eine Next-Generation Firewall erfordert sechs zusätzliche Rechenprozesse im Vergleich zu einer Klartextprüfung.

Auf die Performance wirken sich dabei vor allem diese zwei Prozesse aus:

- die Einrichtung einer sicheren Verbindung
- die Entschlüsselung und Wiederverschlüsselung des Verkehrs für einen sicheren Datenaustausch

Die Performance-Einbußen können in einigen Fällen sehr hoch sein und bei Unternehmen, die noch veraltete Sicherheitssysteme nutzen, eine SSL-/TLS-Prüfung praktisch unmöglich machen.

Die meisten Cyberangriffe sind opportunistisch und finanziell motiviert. Das heißt: Jedes Unternehmen kann zur Zielscheibe von Attacken werden.

Was bedeutet das für Ihre Organisation?

In diesem Jahr haben Cyberkriminelle enorm von der Zunahme des HTTPS-Verkehrs sowie der mangelnden Visibilität profitiert. So konnte ein Angreifer mithilfe einer Werbeanzeige auf Yahoo bis zu 900 Millionen User mit Malware infizieren. Die Kampagne leitete Yahoo-Nutzer auf eine Site weiter, die mit dem Angler-Exploit-Kit infiziert war. In den Wochen davor waren womöglich weitere 10 Millionen Anwender betroffen. Grund waren Werbeanzeigen eines als „E-planning“ bekannten Marketingunternehmens.

Fazit

Verschlüsselungstechnologien kommen heute überall zum Einsatz und sind zu einem beliebten Bedrohungsvektor für Hacker geworden. Ihre Netzwerksicherheitslösung sollte daher in der Lage sein, den Datenverkehr zu entschlüsseln. Nur so können Sie sicher sein, dass verborgene Bedrohungen effektiv gestoppt werden.

Weitere Informationen erhalten Sie in unserer Lösungsübersicht Best Practices gegen verschlüsselte Bedrohungen.

[1] *UBM Tech-E-Paper: Next-Gen Security (Sicherheit der nächsten Generation)*

Über uns

Seit über 25 Jahren ist SonicWall als zuverlässiger Sicherheitspartner bekannt. Von Access Security über Netzwerksicherheit bis zu Email Security: Wir haben unser Produktportfolio kontinuierlich weiterentwickelt, damit unsere Kunden Innovationen realisieren, Prozesse beschleunigen und wachsen können. Mit über einer Million Sicherheitsgeräte in nahezu 200 Ländern und Regionen weltweit bietet SonicWall seinen Kunden alles, was sie brauchen, um für die Zukunft gerüstet zu sein.

Wenden Sie sich bei Fragen zu den Nutzungsmöglichkeiten dieses Materials an:

SonicWall Inc.
5455 Great America Parkway,
Santa Clara, Kalifornien (USA) 95054
Informationen zu regionalen und internationalen Niederlassungen finden Sie auf unserer Website.
www.sonicwall.com

SolutionBrief-DarkSideOfEncryption-EU-IMAG-22649