

Case Study

Kwizda erhöht mit Gigamon die Sichtbarkeit des SSL-Verkehrs von 65% auf 90%



Vor Gigamon hatten wir überall Out-of-Band-SSLEntschlüsselung, und wir entschlüsselten im Durchschnitt etwa 65 Prozent des Datenverkehrs. Jetzt, mit der Giga-SMART SSLEntschlüsselungs-Engine, erhalten wir normalerweise weit über 90 Prozent Sichtbarkeit in den verschlüsselten Datenverkehr.

BRUNO LARCHER
IT-Manager Infrastructure

Herausforderungen

- Erhöhte Verfügbarkeit der Bestell-Webschnittstelle
- Überwachung und Erkennung versteckter Bedrohungen im verschlüsselten Datenverkehr.
- Entschlüsselung des Nord-Süd-Verkehrs, um ihn effektiv zu überwachen und zu untersuchen

Lösung

- GigaVUE® HC Series
- GigaSMART®
- GigaVUE V Series

Kundennutzen

- Erhöhung der Sichtbarkeit des SSLVerkehrs von 65 % auf 90 %.
- Verbesserung der Verfügbarkeit der Anwendung der Medikamentenbestellung
- Überwachung der Netzwerkaktivität bei gleichzeitiger Erfüllung der gesetzlichen Anforderungen an die Verschlüsselung des Nord-Süd-Verkehrs

Über Kwizda

Die Kwizda Holding GmbH, ein Unternehmen im Bereich Life Sciences, ist in der Herstellung, dem Vertrieb und der Vermarktung von Arzneimitteln, Generika, rezeptfreien Medikamenten und Krankenhausinfusionen tätig. Das Unternehmen wurde 1853 gegründet und hat seinen Sitz in Wien, Österreich.

Unternehmerische Herausforderung

Für die Kwizda Holding GmbH, war und ist es von größter Bedeutung, dass ihr Haupt-Web-Interface, über das die Kunden ihre Pharmabestellungen per XML aufgeben und verarbeiten, immer verfügbar, sowie reaktionsschnell und sicher ist.

Verschlüsselung ist das Mittel der Wahl, um die Sicherheit von Transaktionen zu gewährleisten, wenn Kundeninformationen über Netzwerke Dritter, oder das Internet laufen, um mit der Kwizda-Infrastruktur zu kommunizieren. Sie erschwert es der IT-Abteilung jedoch auch, versteckte Bedrohungen innerhalb des verschlüsselten Datenverkehrs zu überwachen und aufzudecken.

Gemäß gesetzlichen Vorgaben muss der gesamte Datenverkehr, der Kundeninformationen enthalten könnte, verschlüsselt werden, sobald Daten einen Server verlassen, oder über das Netzwerk übertragen werden. Kwizda setzt den Diffie-Hellman-Algorithmus mit Perfect Forward Secrecy zur Verschlüsselung ein, der dem aktuellen Stand der Technik entspricht.

Diese gesetzlichen Vorgaben gelten auch für die ERP-Daten, die innerhalb von SAP übertragen und gespeichert werden. Obwohl diese Implementierung vollständig innerhalb einer VMware-ESX-7.0-Umgebung erfolgt, muss der Verkehr laut Gesetz, zwischen virtuellen Servern, innerhalb von VMware, immer noch verschlüsselt werden. Somit muss die verwendete Überwachungslösung in der Lage sein, auch diesen Nord-Süd-Verkehr zu entschlüsseln, um ihn effektiv überwachen und untersuchen zu können.

Projektumsetzung

Mit der Gigamon Lösung wird der gewünschte, zentralisierte Überblick, sowohl über den existierenden Ost-West-, wie auch den in den VMware-Instanzen laufenden, Nord-Süd-Datenverkehr, geschaffen. Die GigaSMART Inline-SSL/TLS-Entschlüsselungsfunktionalität macht den mit Diffie-Hellman-Verschlüsselung abgesicherten Netzwerkverkehr, sichtbar. Dadurch wird ein sinnvoller Einsatz der Security Tools und eine Performance-Analyse, überhaupt erst möglich. Durch das implementierte Inline-Bypass-Modul, ist zudem die dauerhafte Verfügbarkeit des Haupt-Web-Interfaces von Kwizda, auch im Falle eines Stromausfalls, oder einer Fehlfunktion der Überwachungslösungen, garantiert. Die einfache Implementierung und die Leistungsfähigkeit der Lösung, haben den Kunden überzeugt. Gigamon wird laufend um weitere Tools wie SIEM und Intrusion Detection erweitert.

Benefit

Der Hauptvorteil ist die Erhöhung der Sichtbarkeit des SSL-Datenverkehrs von 65 % auf 90 %.

Dank der Gigamon-Lösung ist Kwizda nun in der Lage, Analysedaten an SIEM weiterzuleiten, das den gesamten Datenverkehr untersucht, um Malware und bösartige Software zu erkennen und abzuwehren, die sich auf verschlüsselten Datenverkehr stützen - ebenso wie andere Anomalien.

Dank dieser Lösung ist Kwizda weiterhin in der Lage, die Netzwerkaktivität zu überwachen und gleichzeitig die gesetzlichen Anforderungen zur Verschlüsselung des Nord-Süd-Verkehrs zwischen SAP-Servern innerhalb eines VMware-Clusters zu erfüllen.

Durch den Einsatz des Inline-Bypass-Moduls kann Kwizda die Verfügbarkeit der Medikamentenbestellanwendung sicherstellen.

Über Gigamon

Gigamon® bietet eine Pipeline für Deep Observability, die sofort verwertbare Informationen auf Netzwerkebene nutzt, um die Leistungsfähigkeit von Observability-Werkzeugen zu maximieren. Diese effektive Kombination ermöglicht es IT-Organisationen, Sicherheit und Compliance umfassend zu gewährleisten, die Ursachen von Leistungsengpässen schneller zu identifizieren und den Verwaltungsaufwand zu senken, der ansonsten durch das Management hybrider und Multi-Cloud-Infrastrukturen entsteht. Das Ergebnis: Moderne Unternehmen realisieren das volle Transformationspotenzial der Cloud. Gigamon unterstützt mehr als 4.000 Kunden weltweit, darunter über 80 Prozent der Fortune-100-Unternehmen, 9 der 10 größten Mobilfunkanbieter und Hunderte von Behörden und Bildungseinrichtungen weltweit. Um mehr zu erfahren, besuchen Sie bitte gigamon.com.

**Weltweiter Hauptsitz**

3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

© 2023 Gigamon. Alle Rechte vorbehalten. Gigamon und Gigamon-Logos sind Marken von Gigamon in den Vereinigten Staaten und/oder anderen Ländern. Gigamon-Marken finden Sie unter gigamon.com/legal-trademarks. Alle anderen Marken sind die Marken der jeweiligen Eigentümer. Gigamon behält sich das Recht vor, diese Veröffentlichung ohne vorherige Ankündigung zu ändern, zu modifizieren, zu übertragen oder anderweitig zu überarbeiten.