KOSTENGÜNSTIGE HANDHABUNG VON VERSCHLÜSSELTEM DATENVERKEHR IN DER GESAMTEN IT-INFRASTRUKTUR

Da bei immer mehr Websites, Unternehmensanwendungen und Webservices eine Verschlüsselung des Datenverkehrs notwendig ist, wächst die Last der Verarbeitung von verschlüsselten Daten in den verschiedenen Bereichen der IT-Infrastruktur exponentiell an. Das Jahr 2016 war ein wichtiger Meilenstein für die Traffic-Verschlüsselung: Mehr als 50 Prozent des gesamten Internet-Datenverkehrs wurden verschlüsselt, nachdem der verschlüsselte Datenverkehr in den vorherigen zwölf Monaten um mehr als 10 Prozent zugenommen hatte. Um neu entdeckte Sicherheitslücken in verschlüsselten Kommunikationsprotokollen zu schließen, wurden zudem neue Chiffren und Schlüsselaustauschverfahren eingeführt, die ein höheres Sicherheitsniveau bieten.

Durch diesen Trend profitieren Endanwender und Unternehmen von besserem Datenschutz, doch er bringt auch einige neue Herausforderungen. Ein Beispiel sind die notwendigen Aktualisierungen bei vorhandenen Infrastrukturen, die neue Verschlüsselungsstandards nicht unterstützen; ein anderes Beispiel ist der wachsende Prozentsatz von Cyberangriffen, die verschlüsselte Tunnel nutzen, um schädliche Aktivitäten zu verbergen.

Unpraktikabilität der Verarbeitung von verschlüsseltem Datenverkehr auf dem Server
Anwendungsserver waren ursprünglich nicht dafür vorgesehen, die Kommunikationsverschlüsselung und -entschlüsselung zu übernehmen. Die Architektur der Anwendungsinfrastruktur enthält deshalb in vielen Fällen (insbesondere bei einem hohen Aufkommen an verschlüsseltem Datenverkehr) einen Application Delivery Controller (ADC) mit dedizierter Hardware für die Verarbeitung von verschlüsseltem Traffic, sodass ein Offloading von den Servern erfolgt.

Angesichts der jetzt erforderlichen Unterstützung für neue Chiffren und eine schnell wachsende Kapazität von verschlüsseltem Datenverkehr müssen die meisten Unternehmen allerdings nach einer ADC-Lösung suchen, die aktuelle und zukünftige Anforderungen erfüllt.

Die neue Alteon D Line von Radware ist eine branchenführende Lösung, die allen oben genannten Herausforderungen beim Offloading der Verarbeitung des verschlüsselten Datenverkehrs von den Servern gerecht wird. Die zugehörige Software ist optimiert für den Umgang mit den neuesten Verschlüsselungsprotokollen und Chiffren. Die eingebettete dedizierte Hardware basiert auf dem neuesten Chipsatz, der in der Branche für die Verarbeitung von Traffic-Verschlüsselung und -Entschlüsselung verfügbar ist, und bietet ein unübertroffenes Preis-Leistungs-Verhältnis für Anwendungen jeder Art.

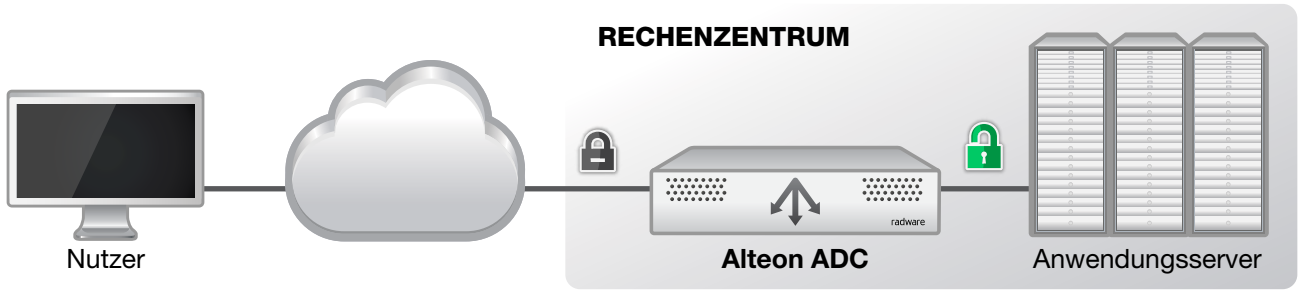

Abbildung 1: Offloading der Verarbeitung von verschlüsseltem Datenverkehr – Netzwerkdiagramm

Ganz gleich, ob die Architektur der Anwendungsinfrastruktur physische ADC-Appliances oder virtuelle Appliances in der Cloud enthält, die Alteon D Line sorgt mit fortschrittlichen ADC-Funktionen für die Einhaltung des Service-Levels und ein angemessenes Nutzungserlebnis bei der Anwendung. Dazu kommen eine starke Performance und eine kostengünstige Engine zur Verarbeitung von verschlüsseltem Datenverkehr.

Unternehmen haben damit jetzt die Möglichkeit, die Gesamtbetriebskosten ihrer Anwendungen zu verringern: In Kombination mit der neuen Alteon D Line können dieselben Anwendungsserver eingesetzt werden, um mehr Nutzer und erheblich größere Mengen von verschlüsseltem Traffic mit den neuesten Chiffren zu bewältigen.

Veränderung des Geschäftsszenarios zum Entfernen der Schwachstelle bei Geräten für Perimetersicherheit

Ein weiterer Bereich im Rechenzentrum, für den die zunehmende Nutzung von verschlüsseltem Datenverkehr Bedeutung hat, sind die Perimetersicherheitsgeräte. Derzeit sind diese Geräte überwiegend blind für Cyberbedrohungen, die in verschlüsselter Form durch sie hindurchlaufen. Der Hauptgrund dafür, dass viele Unternehmen den verschlüsselten Datenverkehr nicht inspizieren (laut Gartner galt das Ende 2016 für 80 Prozent der Unternehmen): Bei den Geräten kommt es zu Leistungseinbußen, wenn sie die übertragenen Daten entschlüsseln und wieder verschlüsseln (in den meisten Fällen wird die Performance um rund 80 Prozent reduziert).

In Unternehmen, die versuchten, dieses Problem direkt bei den Perimetersicherheitsgeräten anzugehen, erwies sich das Vorhaben letztlich als sehr kostspielig: Zum einen war eine Überprovisionierung erforderlich, weil Geräte für die Endsicherheit, beispielsweise Server, klassischerweise nicht für die SSL-Verarbeitung optimiert sind. Zum anderen musste die Überprovisionierung bei jedem Sicherheitsgerät erfolgen, für das die besagte Transparenz benötigt wurde, beispielsweise bei Firewall, IPS, WAF sowie bei Elementen für den DDoS- und Datenverlustschutz. Ein weiteres großes Problem war die nicht akzeptable Einführung von Latenz, da der permanente Prozess des Entschlüsselns und Verschlüsselns Zeit in Anspruch nimmt.

Die Radware-Lösung zur SSL-Inspektion ermöglicht Transparenz in Bezug auf den eingehenden verschlüsselten Datenverkehr (initiiert durch einen Client im Internet für einen Server innerhalb des Unternehmens) und auch in Bezug auf den ausgehenden verschlüsselten Datenverkehr (initiiert durch einen Client innerhalb des Unternehmens für einen Server in der Cloud bzw. im Internet).

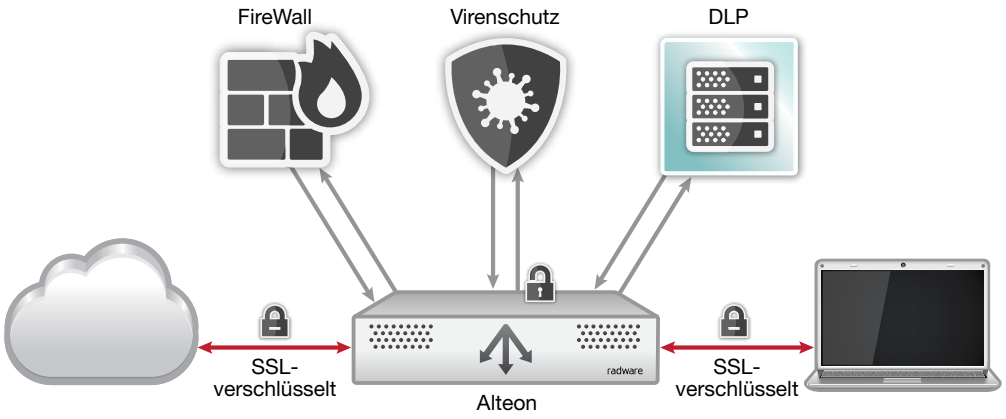

Abbildung 2: Lösung SSL Inspect zur SSL-Inspektion (Beispiel für ausgehenden Datenverkehr)

Basierend auf der Alteon D Line mit ihrer fortschrittlichen und äußerst effizienten SSL-Verarbeitungsengine bietet die Radware-Lösung zur SSL-Inspektion eine hohe Kapazität. Es handelt sich um eine kostengünstige Alternative zur Verarbeitung von verschlüsseltem Datenverkehr auf Perimetersicherheitsgeräten wie Firewalls, DLP-Servern zur Datenleckprävention, Anti-Malware, IDS/IPS und anderen Geräten. Durch Offloading der Verarbeitung des verschlüsselten Datenverkehrs von diesen Geräten vereinfacht die Lösung zur SSL-Inspektion die Implementierung. Zudem verringert sie die Latenz beim Datenverkehr auf ein Mindestmaß und sichert so ein äußerst schnelles und sicheres Nutzungserlebnis.

Die Nutzung der SSL-Inspektionsfunktion der Alteon D Line ermöglicht es Unternehmen, die bei den meisten aktuellen Perimetersicherheitsgeräten vorhandene Schwachstelle zu beheben. Der Kosten- und Arbeitsaufwand entspricht dabei einem Bruchteil dessen, was bei Verwendung der vorhandenen Sicherheitsgeräte anfallen würde (die Einsparung beträgt bis zu 60 Prozent). Das Geschäftsszenario zur Sicherung der Internetkommunikation wird damit erheblich attraktiver und vertretbarer.

Mehr Transparenz bei verschlüsseltem Datenverkehr im Zusammenhang mit DDoS-Schutzlösungen

Ein Verfahren, mit dem Cyberangreifer DDoS-Abwehrlösungen überwinden, ist die Ersetzung der HTTP-Flood-Angriffe durch HTTPS-Angriffe (also die Verschlüsselung der HTTP-Flood-Sitzungen). Deshalb haben die meisten Anbieter ihre

DDoS-Abwehrlösung um einen SSL-Proxy ergänzt, damit die DDoS-Abwehrgeräte bei den HTTPS-verschlüsselten Sitzungen Angriffe erkennen und blockieren können. Problem bei diesem Ansatz: Das Proxy-Gerät, das die verschlüsselten Sitzungen für die Überprüfung öffnet, wird selbst zur Schwachstelle, da es sich um ein statusbehaftetes Gerät mit Sitzungstabellen handelt. Eine Überlastung mit Sitzungen (das Wesen eines DDoS-Angriffs) ist leicht möglich.

Die SSL-Verteidigungslösung von Radware, die auf derselben Verarbeitungsengine für verschlüsselten Datenverkehr basiert wie die Alteon D Line, bietet einerseits eine statuslose Lösung für die Handhabung von SSL-Traffic, andererseits eine Engine mit hoher Kapazität, die alle neuen Chiffren unterstützt.

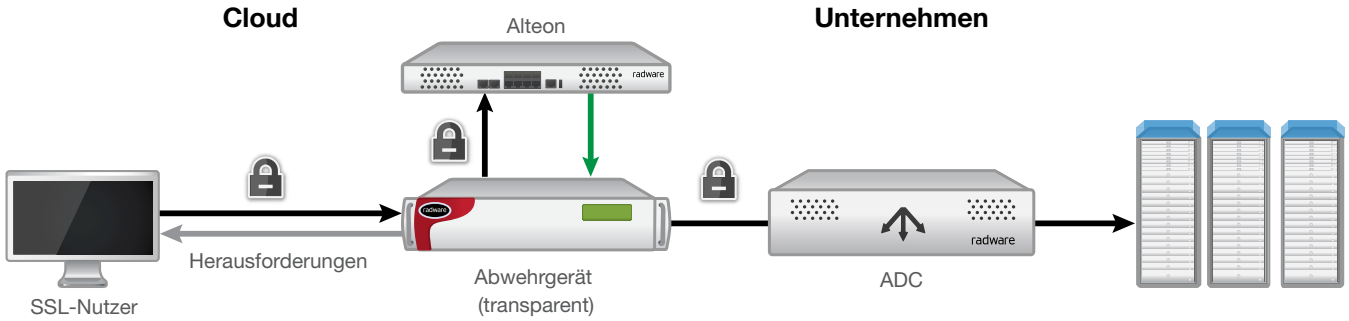

Abbildung 3: Architektur der SSL-Verteidigungslösung Defense SSL

Die spezielle Architektur der SSL-Verteidigungslösung, bei der sich der SSL-Proxy hinter dem DDoS-Abwehrgerät DefensePro verbirgt, sorgt in Kombination mit der leistungsstarken Verarbeitungsengine der Alteon D Line für verschlüsselten Datenverkehr dafür, dass Kunden eine hohe Kapazität erhalten. Auf verschlüsselte Angriffe kann damit auf äußerst kostengünstige Weise auch dann reagiert werden, wenn diese dasselbe Volumen haben wie unverschlüsselte Angriffe. Gleichzeitig werden die neuesten Chiffren unterstützt, und mögliche Überlastungsstellen werden eliminiert.

Über Radware

Radware® (NASDAQ: RDWR) ist ein weltweit führender Anbieter von Lösungen im Bereich Anwendungsbereitstellung und Cybersicherheit für virtuelle, cloud- und softwarebasierte Rechenzentren. Das vielfach ausgezeichnete Portfolio von Radware sorgt für eine optimale Quality of Service bei geschäftskritischen Anwendungen und gleichzeitig für eine maximale IT-Effizienz. Mehr als 10.000 Enterprise- und Carrier-Kunden weltweit profitieren von den Lösungen von Radware – zur schnellen Anpassung an Marktentwicklungen, Aufrechterhaltung der Business Continuity und Maximierung der Produktivität bei geringen Kosten. Weitere Informationen finden Sie auf der Website www.radware.com.

Schließen Sie sich der Radware-Community an und folgen Sie uns bei Facebook, Google+, LinkedIn, über das Radware-Blog, per SlideShare, Twitter, YouTube und Radware Connect (App für iPhone®) sowie über unser Sicherheitscenter DDoSWarriors.com, das umfassende Analysen zu Strategien, Trends und Bedrohungen bei DDoS-Angriffen bereitstellt.

Certainty-Support-Programm

Im Rahmen des Certainty-Support-Programms bietet Radware technischen Support für alle Produkte von Radware. Das Certainty-Support-Programm besteht auf jeder Stufe aus vier Elementen: telefonische Beratung, Software-Updates, Hardware-Wartung und Vor-Ort-Unterstützung. Bei besonders anspruchsvollen Implementierungen unterstützt ein spezialisiertes Technikerteam von Radware die Kunden zudem im Rahmen der Professional Services.

Weitere Informationen

Erfahren Sie mehr darüber, wie Sie Ihre Geschäfts- und IT-Investitionen mit den integrierten Anwendungsbereitstellungs- und Sicherheitslösungen von Radware optimal nutzen können. Senden Sie eine E-Mail an info@radware.com, oder besuchen Sie die Website www.radware.com.