Web Application Firewall – ein notwendiger Schutz für moderne Unternehmen

Erfahren Sie, was traditionelle Sicherheitslösungen für Netzwerke nicht bewältigen können und warum Ihre Organisation eine Web Application Firewall als Grundpfeiler für die IT-Sicherheitsstrategie benötigt

CITRIX®

Um Webinhalte, die für moderne Organisationen allgegenwärtig sind, effizient zu schützen, müssen IT-Verantwortliche die Möglichkeiten und Einschränkungen der heute verfügbaren Sicherheitstechnologien kennen. Beispielsweise können traditionelle Netzwerk-Firewalls und Intrusion-Prevention-Systeme große Mengen an Bedrohungen auf niedrigeren Netzwerkschichten herausfiltern. Sie zeigen jedoch große Defizite, wenn es darum geht, Webinhalte vor den immer gezielteren, anwendungsspezifischen Bedrohungen zu schützen, denen Organisationen heute regelmäßig ausgesetzt sind. Firewalls der nächsten Generation bieten zwar eine merklich verbesserte Granularität bei der Überwachung des Zugriffs auf Netzwerkressourcen, jedoch zeigen auch sie Defizite beim wichtigen Schutz von Webinhalten.

In diesem Whitepaper werden die Herausforderungen eines angemessenen Schutzes moderner Webinhalte vor Bedrohungen aus dem Netz beschrieben. Zudem wird untersucht, welche Rollen verschiedene Sicherheitstechnologien übernehmen und – was vielleicht noch wichtiger ist – welche Rollen sie nicht übernehmen können. Das Whitepaper erklärt, warum eine Web Application Firewall für Organisationen eine notwendige strategische Komponente für den Schutz von Bedrohungen aus dem Netz ist. Exemplarisch stellen wir Ihnen dann die Einsatzmöglichkeiten der NetScaler AppFirewall vor. Mit ihrer einzigartigen Kombination aus Funktionen für die Anwendungssicherheit und die Optimierung von Anwendungs-Performance ist sie eine ideale Lösung, um die aktuellen Anforderungen von Unternehmen zu erfüllen.

Das Problem mit dem Schutz von Web-Anwendungen

Es gibt zahlreiche Gründe, warum Webinhalte ein erhebliches Risiko für Organisationen von heute darstellen. Die größten Probleme sind die Verbreitung von Webinhalten, die Tatsache, dass sie zum bevorzugten Ziel heutiger Hackergruppen geworden sind, und der unzureichende Schutz, der von sogenannten „Sicherheitslösungen für die Anwendungsschicht“ geboten wird.

Webinhalte sind allgegenwärtig

Organisationen entwickeln und erwerben heutzutage eine Vielzahl an Web-Anwendungen. Im Mittelpunkt stehen dabei Anwendungen für Kunden und Auftraggeber und immer häufiger auch mobile Apps sowie Anwendungen, die Back-Office-Services und -Funktionen ermöglichen. Obwohl umsatzgenerierenden Anwendungen immer noch die größte Aufmerksamkeit geschenkt wird, wäre es unklug, die Bedeutung anderer Anwendungsklassen für den alltäglichen Betrieb zu ignorieren – einschließlich von Anwendungen für die Bereiche Lieferkettenmanagement, Finanzen, Personalmanagement, Forschung und Produktentwicklung.

Was bedeutet das für die IT-Sicherheitsteams von heute? Da sich Web-Anwendungen in Organisationen verbreiten und zunehmend von externen sowie internen Anwendern genutzt werden, sind nicht nur an der Netzwerkgrenze entsprechende Schutzmaßnahmen notwendig.

Eine weitere Konsequenz ergibt sich aus der schieren Vielfalt an Web-Anwendungen, die in Unternehmen eingesetzt werden. Hier gibt es heute unzählige Kombinationen von kommerziell erhältlichen und individuell entwickelten Web-Anwendungen. Daher ist es unrealistisch zu erwarten, dass Sicherheitstechnologien, deren Regeln und Mechanismen für einen breitbandigen Einsatz ausgelegt sind – wie zum Beispiel die Erkennung von abweichendem Protokollverhalten auf der Vermittlungsschicht – alle Web-Anwendungen umfassend schützen können. Sicherheitsteams benötigen zudem Tools, die nicht nur eine größere Flexibilität und eine deutlich tiefgreifendere Granularität für die Überprüfung und Kontrolle bieten, sondern sich im Idealfall automatisch an neue Anwendungen anpassen.

Webinhalte sind das bevorzugte Ziel von Hackern

Als wenn ihre Verbreitung sie nicht schon attraktiv genug für Hacker machen würde, sind Webinhalte zudem bekanntermaßen anfällig für Angriffe. Mehrere Faktoren sind für diese riskante Situation verantwortlich:

- der hohe Grad an Komplexität vieler Webinhalte
- die häufige Einbettung von Programmbibliotheken von Drittanbietern
- die gängige Implementierung hochmoderner (sprich unerprobter) Protokolle, Technologien und Funktionen
- Entwickler und Unternehmensmanager, die mehr Wert auf Funktionalität und eine kurze Time-to-Market legen als auf Maßnahmen zur Verbesserung der Code-Qualität und zur Reduzierung von Schwachstellen

Und das ist noch nicht das Schlimmste: Viele Web-Anwendungen dienen zudem als direkte Verbindung zu wertvollen oder vertraulichen Informationen, darunter Zahlungs- und Bestelldaten von Kunden, urheberrechtlich geschützten Produktspezifikationen, Krankenakten sowie personenbezogenen Daten. Sobald sich ein Hacker einen Weg durch die benutzerfreundliche Vordertür einer normalerweise auswärtsgerichteten Web-Anwendung gebahnt hat, ist es nur noch eine Frage der Zeit, bis dieser einen oder mehrere der konfigurierten Pfade zu den Backend-Datenbanken nutzt.

Unter diesen Voraussetzungen ist es keine Überraschung, dass man häufig Nachrichten über gewaltige Sicherheitsverstöße hört, bei denen Millionen von Datensätzen gefährdet wurden. Aus dem 2014 veröffentlichten Verizon Data Breach Investigations Report geht hervor, dass 35 Prozent der bestätigten Datensicherheitsverstöße, die für 2013 analysiert wurden, auf Web-Anwendungen verübt wurden.
Es ist zudem wichtig, zu erkennen, dass die Angriffe aus dem Web, die es in die öffentlichen Schlagzeilen schaffen, nur die Spitze des Eisbergs sind. Die eigentliche Situation ist um einiges schlimmer, als es die meisten Unternehmensmanager wahrhaben wollen, da die überwiegende Mehrheit der Web-Attacken als zu unwichtig für die Nachrichten angesehen werden oder von den betroffenen Organisationen einfach nicht gemeldet werden.

Services auf der Anwendungsschicht zu schützen reicht nicht aus

Man darf nicht übersehen, dass traditionelle Netzwerk-Frameworks und die dazugehörige Terminologie möglicherweise für Missverständnisse sorgen. Insbesondere gilt dies für Schicht 7 des bekannten OSI-Referenzmodells. Obwohl diese „Anwendungsschicht" genannt wird, handelt es sich immer noch – wie bei allen anderen Schichten dieses Modells – um die Kommunikation im Netzwerk. Technisch gesehen bezieht sie sich auf die verschiedenen Protokolle und Services, die von Anwendungen verwendet werden, um Kommunikationspartner zu identifizieren, die Verfügbarkeit von Ressourcen zu bestimmen und die Kommunikation zwischen zwei Parteien, die dieselbe Anwendung verwenden, zu synchronisieren. Beispiele von Protokollen auf der Anwendungsschicht sind HTTP (für das Internet), FTP (für die Dateiübermittlung) und SMTP (für E-Mails).

Die Missverständnisse entstehen durch die zahlreichen Sicherheitstechnologien, die angeblich einen „Schutz auf der Anwendungsschicht" bieten. Solche Behauptungen mögen aus technischer Sicht stimmen – beispielsweise wenn ein Intrusion-Prevention-System RFCs für HTTP durchsetzt – sind leider aber dennoch in gewisser Weise irreführend. Das Problem ist, dass der Schutz, den diese Lösungen bieten, für einen umfassenden Schutz von „Anwendungen" völlig unzureichend ist. Dies liegt daran, dass sie nur indirekt dabei helfen, die Infrastruktur-Anwendungen auf der „höheren Schicht" (z. B. Web-Server und Datenbankmanagement-Systeme), Unternehmensanwendungen (z. B. Salesforce.com) und Daten, die zwangsläufig vorhanden sind, zu schützen (siehe Abbildung 1).

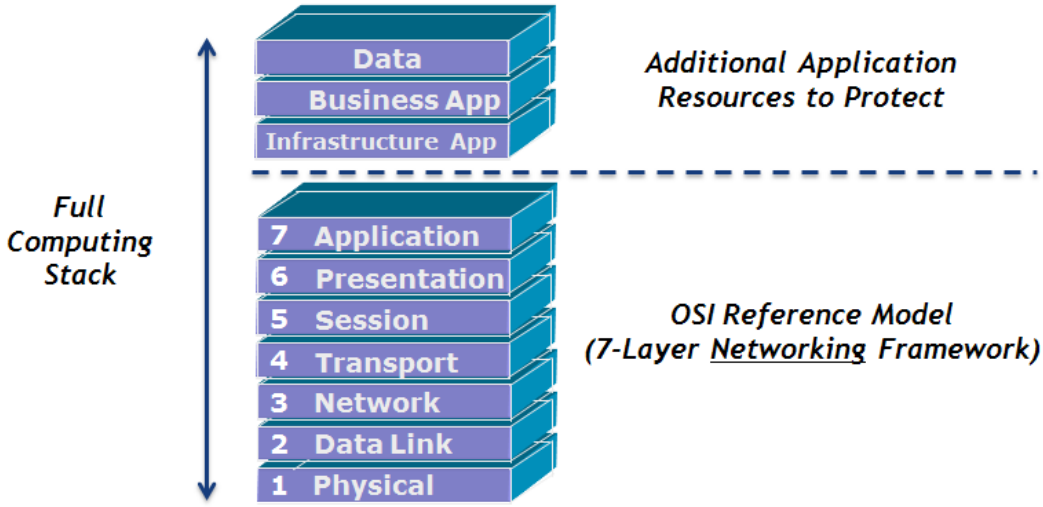

Abbildung 1: Das vollständige Schichtenmodell des Computernetzes

Um ihre wichtigen Webinhalte zu schützen, benötigen Organisationen Sicherheitstechnologien, die umfassenden Schutz auf folgenden Ebenen bieten:

- Physische Abdeckung – bietet Schutz für alle Nutzungsszenarien, sowohl an den Grenzen als auch intern
- Funktionelle Abdeckung – bietet nicht nur Richtliniendurchsetzung in der Form von granularer Zugriffskontrolle, sondern auch explizite Erkennung von/Schutz vor Bedrohungen
- Logische Abdeckung – bietet Schutz auf allen Schichten des Computernetzes, von Services/Protokollen auf Vermittlungs- und Anwendungsschicht bis hin zu Infrastruktur-Anwendungen, kundenspezifischen Unternehmensanwendungen und sogar Daten

Eine umfassende Abdeckung wie diese einzurichten, erfordert Investitionen in mehr als lediglich gewöhnliche Netzwerk-Firewalls und Intrusion-Prevention-Systeme (IPS).

Bestehende Technologien für die Netzwerksicherheit

Üblicherweise eingesetzte Technologien zur Netzwerksicherheit spielen eine wichtige Rolle beim Schutz unternehmenskritischer Webinhalte einer Organisation. Jedoch ist es wichtig zu verstehen, dass sie Einschränkungen haben und alleinstehend keinen ausreichenden Schutz bieten.

Netzwerk-Firewalls

Die Hauptfunktion einer üblichen Netzwerk-Firewall ist die Zugriffskontrolle – Richtlinien, die vorgeben, welcher Anwendungs-Traffic die Netzwerkgrenze, an der die Firewall implementiert ist, nach innen oder nach außen überschreiten darf. Zustandsbehaftung ist die Fähigkeit, zurückkehrenden Traffic, der zu autorisierten ausgehenden Sessions gehört (und umgekehrt), dynamisch zuzuordnen und zu genehmigen. Jedoch ist es so:

- Da die Zugriffskontrolle einer normalen Firewall nur auf Attributen der Vermittlungsschicht basiert (z. B. Port, Protokoll und Quell/Ziel-IP-Adresse), ist ihre Granularität eher gering. Daher kann die Firewall nicht immer die individuellen Anwendungen, die einen bestimmten Port/ein bestimmtes Protokoll nutzen – wie z. B. die zahlreichen HTTP-Web-Anwendungen, die den TCP-Port 80 verwenden – voneinander unterscheiden und somit kontrollieren.
- Gewöhnliche Netzwerk-Firewalls verfügen nicht über die Funktionen, Bedrohungen explizit aufzuspüren und zu verhindern. Den einzigen Schutz, den sie gegen Malware, Angriffe und andere unautorisierte Aktivitäten vorweisen, ist ein Nebenprodukt der Zugriffskontroll-Richtlinien, die sie durchsetzen sollen. Wenn eine Bedrohung beispielsweise von einem Kommunikationspfad abhängig ist, der nicht „offen" ist, wird diese standardmäßig blockiert (ohne jemals erkannt zu werden).

Im Endeffekt bietet die gewöhnliche Netzwerk-Firewall relativ wenig Schutz für Webinhalte einer Organisation.

Intrusion-Prevention-Systeme für Netzwerke

Netzwerk-IPS-Technologie bietet nur geringe Funktionalität hinsichtlich der Zugriffskontrolle und konzentriert sich stattdessen auf die Erkennung von Bedrohungen. Die umfassenden Mechanismen, auf denen diese Technologie beruht, sind unter anderem Signaturen bekannter Bedrohungen und Schwachstellen sowie die Erkennung von Protokoll- und Verhaltensanomalien, die auf schädliche Aktivitäten und unbekannte Bedrohungen hindeuten. Es wird üblicherweise Schutz bis zur Anwendungsservice-Schicht sowie für alle geläufigen Internetprotokolle geboten, einschließlich HTTP(s), DNS, SMTP, SSH, Telnet und FTP.

Es gibt auch einen sporadischen Schutz auf höheren Schichten des Computernetzes, da IPS-Technologie nicht selten Signaturen für bekannte Schwachstellen und Bedrohungen enthält, die mit den beliebtesten Infrastruktur- und Unternehmensanwendungen von heute in Verbindung stehen. Diese erweiterte Abdeckung geht zwar in die richtige Richtung, ist jedoch nicht ausreichend und lässt die IPS-Technologie in der Mitte feststecken, wodurch sie anfällig für die folgenden beiden Fälle ist:

- Falsch negative Treffer – aufgrund des Fehlens tiefgreifender Visibilität und des Verständnisses für Anwendungen werden die meisten Bedrohungen auf hohen Schichten nicht erkannt (wie z. B. solche, die die Anwendungslogik manipulieren) sowie
- Falsch positive Treffer – beim Versuch, weitläufig anwendbare Signaturen zu schreiben, die Standard- sowie kundenspezifische Web-Anwendungen vor einer großen Bandbreite von Bedrohungen auf hohen Schichten schützen sollen, werden stets zahlreiche Fehlalarme ausgelöst

Obwohl die explizite Erkennung/Bekämpfung von Bedrohungen die IPS-Technologie zu einer nützlichen Ergänzung normaler Netzwerk-Firewalls macht, bietet die lückenhafte Abdeckung der Anwendungsservice-Schicht nur wenig zusätzlichen Schutz für die Webinhalte einer Organisation.

Firewalls der nächsten Generation

Die Firewall der nächsten Generation (Next-Generation Firewall, NGFW) verbindet die Fähigkeiten von Netzwerk-Firewalls und IPS in einer einzelnen Lösung. Eine NGFW erweitert diese Funktionen üblicherweise mit Nutzer- und Anwendungsidentitäten als Attributen für einen kontrollierten Zugriff auf/von einem Netzwerk. Mit Ausnahme von Anwendungsfällen mit äußerst hohen Durchsatzanforderungen (d. h. mehrere Gbps) wird hier eine bequeme konsolidierte Lösung mit einigen zusätzlichen Extras geboten. Hinsichtlich des Schutzes von Web-Anwendungen bleibt jedoch ein Mangel bestehen: die Application-Awareness. Die Fähigkeit, Anwendungen unabhängig von dem verwendeten Port und Protokoll zu identifizieren, auch Application-Awareness genannt, unterscheidet sich von der Application-Fluency.

Technologien mit Application-Awareness, wie die Anwendungsprotokoll-Dekodierung und Anwendungssignaturen, identifizieren die spezifische Infrastruktur und Unternehmens-Anwendungen, die für jeglichen Netzwerk-Traffic verantwortlich sind. Daher ermöglicht Application-Awareness präzise Zugriffskontrolle. Es können jetzt separate Richtlinien aufgestellt werden, wenn mehrere Anwendungen und Services dieselben Protokolle und Ports verwenden. Beispielsweise kann der Großteil des Internet-Traffics aufgeteilt werden, sodass eine Handvoll hilfreicher und unternehmenskritischer Web-Anwendungen Zugriff erhalten, während weniger erwünschte Web-Anwendungen wie Web-Mail, Dateiaustauschdienste und Facebook-Spiele selektiv eingeschränkt oder vollständig blockiert werden können.

Als Voraussetzung für eine explizite Bedrohungserkennung auf höheren Schichten erfordert die Application-Fluency ein noch tieferes Verständnis der zu schützenden Anwendung, einschließlich der Feststellung, welche Eingaben und Navigationsabläufe gültig sind und wie die Anwendung sich im Normalfall verhält (bzw. wie nicht).

Unter dem Strich bieten NGFWs zwar verbesserte Zugriffskontrollfunktionen und eine Möglichkeit, zahlreiche Einzel-Appliances abzulösen, aber Organisationen verfügen damit weiterhin nur über die expliziten Erkennungs-/Schutzfunktionen geläufiger IPS. Der Umfang und die Tiefe der Abdeckung reichen nicht aus, um die meisten Webinhalte – besonders kundenspezifische – vor den zunehmend komplexen und gezielten Angriffen zu schützen, die jetzt einen erheblichen Teil der Bedrohungslandschaft ausmachen.

Die Web Application Firewall – Meister im Bereich der Anwendungen

Die Web Application Firewall (WAF) fängt dort an, wo andere Sicherheitstechnologien aufhören. Sie bietet Schutz vor Angriffen, die auf den höchsten Schichten des Computernetzes ausgeführt werden. Automatisierte Lernroutinen, die durch manuell konfigurierte Richtlinien ergänzt werden, sorgen für ein zuverlässiges „Verständnis“ darüber, wie jede Web-Anwendung sich verhält, einschließlich aller individueller Funktionen und der Geschäftslogik. Auf dieser Basis erkannte Abweichungen stehen für vermuteten schädlichen Traffic. Dieser wird automatisch gemäß den vom Administrator definierten Richtlinien behandelt – zum Beispiel blockiert, mit Einschränkungen zugelassen oder protokolliert.

Verglichen mit den Sicherheitstechnologien, die vorher in diesem Whitepaper besprochen wurden, sind WAFs einzigartig in ihrer Fähigkeit:

- Eingaben zu validieren und dadurch gefährliche SQL-Injection-, Cross-Site-Scripting- und Directory-Traversal-Angriffe zu verhindern
- Angriffe, bei denen Cookies, Sessions oder Parameter manipuliert werden, zu erkennen
- Angriffe zu blockieren, die Schwachstellen von kundenspezifischen Webinhalten ausnutzen
- das Auslesen von vertraulichen Daten durch Identifizierung und Blockierung auf Objektebene zu verhindern

- SSL-verschlüsselten Traffic für eingebettete Bedrohungen jeder Art zu inspizieren
- Bedrohungen, die Schlupflöcher in der Anwendungslogik von kundenspezifischen Unternehmens-Anwendungen ausnutzen, zu verhindern
- sich gegen Distributed-Denial-of-Service(DDoS)- und Angriffe auf der Anwendungsebene zu schützen
- Informationen in Serverantworten dynamisch zu verschleiern, da diese nützlich für Hacker sein könnten
- umfassenden XML-Schutz, einschließlich der Schemavalidierung von SOAP-Nachrichten, und XPath-Injection-Schutz zu bieten sowie XML-Anhänge, die schädliche Inhalte enthalten könnten, zu identifizieren/blockieren
- die Anforderung 6.6 der Datensicherheitsstandards der Kreditkartenindustrie (PCI DSS) zu ermöglichen

Branchenführende WAFs – wie die NetScaler AppFirewall – bieten all diese anwendungsorientierten Schutzfunktionen und zudem Support für Zugriffskontrollregeln auf der Vermittlungsschicht und eine signaturbasierte Komponente für die Erkennung bekannter Bedrohungen. Sicherheitsteams müssen jedoch wissen, dass WAF-Lösungen vom Design her schwerpunktmäßig Protokolle wie HTTP, HTTPS, XML und SOAP schützen.

Zusammenfassung der Sicherheitstechnologien

Tabelle 1 zeigt eine Gegenüberstellung der oben beschriebenen Sicherheitstechnologien. Zu den wichtigsten neuen Erkenntnissen gehören die folgenden:

- Obwohl sie für das Aufspüren zahlreicher Bedrohungen auf niedrigen Schichten nützlich sind, zeigen die meisten geläufigen Sicherheitstechnologien – Netzwerk-Firewalls und IPS – große Defizite beim Schutz von Web-Anwendungen
- Obwohl keine einzelne Sicherheitstechnologie einen umfassenden Schutz für Web-Anwendungen bietet, kommen WAFs diesem Ziel am nächsten
- Die Kombination von NGFWs und WAFs ist eine effiziente Art, einen leistungsstarken, umfassenden Schutz vor Bedrohungen für alle wichtigen Webinhalte von Organisationen zu ermöglichen

Vergleich von Sicherheitstechnologien für den Schutz von Webinhalten

	Netzwerk-Firewall	Intrusion-Prevention-System	Firewall der nächsten Generation	Web Application Firewall
Wirksam auf	Schichten 3–4	Schichten 3–7	Schichten 3–7	Schichten 3–7+
Implementierungs-architektur (typisch)	Layer-3-Gateway	Transparentmodus	Layer-3-Gateway	Reverse Proxy
Zugriffs-kontrollgranularität	Port, Protokoll, IP-Adresse	nicht zutreffend	Port, Protokoll, IP-Adresse, Nutzer, Anwendung	Port, Protokoll, IP-Adresse
Techniken zur Erkennung von / Schutz vor Bedrohungen	nicht zutreffend	Signaturen, Musterabgleich, Erkennung von abweichenden Protokollen und Verhalten	Signaturen, Musterabgleich, Erkennung von abweichenden Protokollen und Verhalten	Signaturen, Erkennung von abweichenden Protokollen, Erkennung von abweichendem Anwendungsverhalten
Protokollabdeckung	Jedes	Jedes	Jedes	Weborientiert: HTTP(s), XML, SOAP, SPDY
Inspektion von SSL-/ verschlüsseltem Traffic	nicht zutreffend	nicht zutreffend	Ja	Ja
DDoS-Schutz	Vermittlungsschicht (grundlegend)	Vermittlungsschicht	Vermittlungsschicht	Anwendungsschicht
Schutz von Web-Anwendungen	Minimal	Bekannte/unbekannte Schwachstellen/ Bedrohungen, hauptsächlich für Netzwerk- und Anwendungsservice-Schichten	Bekannte/unbekannte Schwachstellen/ Bedrohungen, hauptsächlich für Netzwerk- und Anwendungsservice-Schichten	Umfassende Abdeckung, einschließlich der kompletten Anwendungsschicht

NetScaler AppFirewall

Die einzigartigen Funktionen zum Schutz von Bedrohungen aus dem Netz machen die WAF zu einer notwendigen Komponente der Sicherheitsarchitektur eines Unternehmens. Umso wichtiger ist es, bei der Auswahl einer Lösung auf den vollen Funktionsumfang zu achten.

NetScaler AppFirewall ist eine umfassende, ICSA-zertifizierte Lösung für die Sicherheit von Web-Anwendungen, die bekannte und unbekannte Angriffe auf Web- und Web-Service-Anwendungen blockiert. Die NetScaler AppFirewall nutzt ein hybrides Sicherheitsmodell und analysiert jeglichen bidirektionalen Traffic, einschließlich SSL-verschlüsselter Kommunikation. Dadurch schützt sie vor unterschiedlichsten Sicherheitsbedrohungen, ohne dass dabei Anwendungen modifiziert werden müssen.

Nachfolgend werden die wichtigsten Schutzfunktionen der NetScaler AppFirewall genannt:

Hybrides Sicherheitsmodell. Um Angriffe auf bisher unbekannte Schwachstellen zu bekämpfen, wird eine Policy-Engine mit positiven Richtlinien benötigt, die Genehmigungen für legitime Interaktionen zwischen Nutzern und Anwendungen erteilt und automatisch andersartigen Datenverkehr blockiert. Zusätzlich identifiziert eine Engine mit einem negativen Richtlinien-Modell bekannte Angriffsmuster und schützt Anwendungen vor diesen.

XML-Schutz. NetScaler AppFirewall blockiert nicht nur geläufige Bedrohungen, die für den Angriff auf XML-basierte Anwendungen angepasst werden können (z. B. Cross-Site-Scripting, Command-Injection), sondern enthält auch zahlreiche XML-spezifische Schutzfunktionen, darunter eine umfassende Schema-Gültigkeitsprüfung und die Fähigkeit, verbundene DoS-Angriffe auf der Anwendungsschicht zu unterbinden (z. B. übermäßige Rekursionen).

Fortschrittlicher Schutz für dynamische Elemente. Verschiedene sitzungsrelevante Schutzmaßnahmen sichern dynamische Anwendungselemente wie Cookies, Formfelder und sitzungsspezifische URLs. Dadurch werden Angriffe verhindert, die das Vertrauensverhältnis zwischen Client und Server ausnutzen (z. B. Cross-Site-Request-Forgery).

Speziell angepasste Sicherheitsrichtlinien. Eine fortschrittliche Learning-Engine ermittelt automatisch das erwartete Verhalten von Web-Anwendungen für Unternehmen und generiert für Menschen lesbare Richtlinien-Empfehlungen. Administratoren können dann die Sicherheitsrichtlinie den individuellen Anforderungen jeder Anwendung anpassen und somit mögliche falsch positive Treffer verhindern.

Garantierte Compliance. NetScaler AppFirewall ermöglicht es Unternehmen, Datensicherheits-Anforderungen wie den PCI DSS einzuhalten. Dieser empfiehlt ausdrücklich den Gebrauch von WAFs für auswärtsgerichtete Anwendungen, die Kreditkartendaten verarbeiten. Es können detaillierte Berichte generiert werden, um alle für die PCI-Anforderungen relevanten Schutzmaßnahmen zu dokumentieren, die in der Firewall-Richtlinie definiert sind.

Kompromisslose Performance. Die Web-Anwendungs-Sicherheitslösung mit der besten Performance auf dem Markt bietet einen umfassenden Schutz mit über 12 Gbps, ohne die Antwortzeiten von Anwendungen zu verschlechtern.

Weiterhin zeichnet sich NetScaler AppFirewall durch die einzigartige Möglichkeit aus, als Komponente der vollständigen NetScaler-Anwendungsbereitstellungsplattform implementiert zu werden. Die Vorteile dieses Ansatzes umfassen erhebliche Verbesserungen der Performance von Web-Anwendungen (aufgrund der fortschrittlicheren Beschleunigungs- und Server-Offload-Funktionen) sowie der Zuverlässigkeit (aufgrund von Server Load Balancing, Server Health Monitoring und Failover-Funktionen auf Seitenebene). Das Ergebnis ist eine Lösung, die Organisationen beispiellosen Schutz vor Bedrohungen aus dem Web und gleichzeitig den anspruchsvollen Anwendern von heute einen Benutzerkomfort mit maximaler Performance bietet.

Fazit

In der Vergangenheit war es vielleicht möglich, mit gewöhnlichen Netzwerk-Firewalls und Intrusion-Prevention-Systemen die wenigen Web-Anwendungen, die für die durchschnittliche Organisation von Bedeutung waren, ausreichend zu schützen. Da die Abhängigkeit von Webinhalten deutlich größer geworden ist und Hacker viel häufiger gezielte, anwendungsspezifische Angriffe durchführen, ist dies heutzutage nicht mehr der Fall. Sogar Firewalls der nächsten Generation weisen Mängel auf, da ihre Vorteile hauptsächlich eine konsolidierte Infrastruktur und eine gesteigerte Granularität für das Erstellen und Durchsetzen von Zugriffskontrollrichtlinien umfassen.

Um die zahlreichen nach außen und nach innen gerichteten Webinhalte ihrer Organisation zu schützen, müssen Sicherheitsteams diese anderen Schutzfunktionen – die immer noch sehr nützlich für die Filterung großer Mengen an Bedrohungen auf niedrigeren Schichten sind – mit einer Web Application Firewall ergänzen. Funktionsreiche WAFs wie die NetScaler AppFirewall verfügen über ein tiefes Verständnis darüber, wie sich jede Anwendung im Normalfall verhält, und können abweichendes Verhalten und abweichende Informationen über die Anwendungsservice-/Protokollebene hinaus erkennen. Sie bieten zudem einen Schutz vor Bedrohungen, den andere gängige Sicherheitstechnologien – ob alt oder neu – nicht erreichen können.

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Schweiz

India Development Center
Bangalore, Indien

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hongkong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, Großbritannien

CITRIX®

Über Citrix
Citrix (NASDAQ:CTXS) führt die Umstellung auf Software-definierte Arbeitsplätze an und unterstützt neue Formen der effizienten Zusammenarbeit – mit Lösungen in den Bereichen Virtualisierung, Mobility Management, Netzwerk und SaaS. Citrix-Lösungen ermöglichen sichere, mobile Arbeitsumgebungen und erlauben Mitarbeitern, mit jedem Endgerät, über jedes Netzwerk und aus der Cloud direkt auf ihre Anwendungen, Desktops, Daten und Kommunikationsdienste zuzugreifen. Mehr als 400.000 Unternehmen und über 100 Millionen Anwender setzen weltweit auf Technologien von Citrix. Im Jahr 2015 erwirtschaftete das Unternehmen einen Umsatz von 3.28 Milliarden US-Dollar. Weitere Informationen sind zu finden unter http://www.citrix.de