

# Zuverlässiger Schutz sensibler Informationen

## Sicherheit von Web-Anwendungen

Web-Anwendungen sind mittlerweile zum bevorzugten Ziel von Hackern und IT-Kriminellen geworden. Bei einer aktuellen Sicherheitsstudie des FBI<sup>1</sup> gaben 95 Prozent der befragten Unternehmen an, dass sie im vergangenen Jahr mehr als zehn ernste Sicherheitsvorfälle im Zusammenhang mit dem Web verzeichneten. Im Jahr 2004 traf dies lediglich auf fünf Prozent der Unternehmen zu.

Diese Entwicklung hat nach Ansicht von Sicherheitsexperten mehrere Ursachen. Eine mögliche Erklärung sind die geringen technischen Voraussetzungen für die Angreifer: Um Web-Anwendungen zu manipulieren, benötigen Hacker meist weder umfangreiche Programmierkenntnisse noch spezielle Hilfsmittel. In vielen Fällen genügen frei verfügbare Tools oder wenige Befehlszeilen, die über einen Standard-Webbrowser eingegeben werden. Dazu kommt, dass Web-Anwendungen oft ungenügend oder überhaupt nicht geschützt sind.

## Chancen und Risiken für Unternehmen im Internet

Unternehmen können in vielen Bereichen von Web-Anwendungen und Web Services profitieren. So lassen sich zum Beispiel via Internet Geschäftsprozesse beschleunigen und optimieren: Immer mehr Unternehmen binden Partner, Dienstleister und Lieferanten Web-basiert in ihre Infrastruktur ein, damit sie Informationen in Echtzeit austauschen können. Auch Geschäfte mit Endkunden werden heute immer häufiger online abgewickelt. Unternehmen, die E-Business betreiben, haben eine Verantwortung dafür, dass sensible Informationen jederzeit geschützt sind. In der Realität wird allerdings häufig zu wenig für die Sicherheit von Kundendaten getan.

Während Unternehmen also immer noch zu nachlässig mit sensiblen Daten umgehen, wächst gleichzeitig die Bedrohung durch gezielte Angriffe: Das US-Unternehmen SecureWorks registrierte im ersten Quartal 2006 täglich 100 bis 200 Web-Attacken auf die Datenbanken seiner Kunden. An der Art der Angriffe konnten die Experten des Unternehmens ablesen, dass die Eindringlinge nicht planlos Systeme sabotieren wollten, sondern gezielt vorhatten Daten zu manipulieren oder herunterzuladen. Dies zeigt, dass hinter Angriffen auf Web-Anwendungen heute immer häufiger auch konkrete wirtschaftliche Interessen stecken.

---

<sup>1</sup> CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 2005

## Traditionelle Sicherheitskonzepte oft nicht ausreichend

Web-Anwendungen müssen also sicherer werden – aus technischer Sicht sind dabei allerdings mehrere Herausforderungen zu bewältigen. Ein grundsätzliches Problem ist, dass Web-Anwendungen häufig unter großem Zeit- und Kostendruck entwickelt werden, ohne dass von Anfang an über das Thema Sicherheit nachgedacht wird. Oft versuchen die Programmierer erst nachträglich, Schwachstellen zu beseitigen und Sicherheitslücken durch Patches zu schließen. Währenddessen entstehen bereits neue Bedrohungen im Web, so dass laufend zusätzliche Schutzmaßnahmen benötigt werden.

Die größten Gefahren für Webapplikationen sind dabei Angriffe auf Anwendungsebene, wie zum Beispiel Buffer-Overflow-Exploits, SQL-Injection oder Cross-Site-Scripting. Diese Angriffe werden von traditionellen Sicherheitskomponenten wie Netzwerk-Firewalls und Intrusion-Detection-Systemen in der Regel überhaupt nicht erkannt. Der Grund ist, dass die traditionellen Sicherheitssysteme nicht in der Lage sind, den Application Traffic auf Session- oder User-Ebene zu „verstehen“ und böses von normalem User-Verhalten zu unterscheiden. Sicherheitslösungen, die Web-Anwendungen zuverlässig schützen sollen, müssen aber genau dazu in der Lage sein.

Die so genannten Zero-Day-Angriffe, also Angriffe für die noch keine Schutzmechanismen entwickelt wurden, sind für Sicherheitssysteme eine der schwierigsten Herausforderungen. Highlight "Document type" in the graphic header and replace it with a short but accurate description of the document type you are creating.

## Schutz von Web-Anwendungen durch die NetScaler Application Firewall

Die Citrix NetScaler Application Firewall schützt Web-Anwendungen vor den oben beschriebenen Bedrohungen. Die Sicherheitskomponente analysiert den gesamten bidirektionalen HTML-Datenverkehr von Web-Anwendungen, um Angriffe auf Applikationsebene zu identifizieren und zu blockieren. Dabei wird auch die SSL-verschlüsselte Kommunikation durchleuchtet, bevor sie an die Webanwendung weitergeleitet wird. Denn der Datenverkehr, der über eine SSL-Verbindung geschickt wird, ist nicht automatisch ungefährlich: Hacker versuchen häufig, Angriffe über geschützte SSL-Tunnel auszuführen, um sie so vor Netzwerk-Sicherheitskomponenten zu verbergen.

Eine der Besonderheiten ist ihr "positives Sicherheitsmodell": Die Lösung ist in der Lage, korrektes Anwendungsverhalten durch einen Abgleich mit einer "White List" zu erkennen. Erwünschte Zugriffe werden weitergeleitet, der gesamte übrige Webverkehr wird blockiert. Im Gegensatz zu Sicherheitslösungen, die bekannte Angriffstypen anhand einer "Black List" abwehren, schützt die Application Firewall so auch vor bisher unbekanntem Angriffen (Zero-Day-Protection).

Ergänzt wird das positive Sicherheitsmodell durch eine lernfähige Technologie – die Adaptive Learning Engine. Diese stellt sicher, dass die Application Firewall nicht versehentlich zulässiges Anwendungsverhalten blockiert. Insbesondere dynamisch generierte Anfragen durch Client-seitiges Javascript werden von manchen Sicherheitssystemen fälschlicherweise als feindliche Angriffe interpretiert. Die Adaptive Learning Engine sorgt dafür, dass dies nicht passiert: Die Technologie analysiert das Verhalten von Web-Anwendungen und schlägt dem Administrator selbstständig entsprechende Policies vor. So hilft sie ihm, Sicherheitsregeln zu optimieren und erlaubtes Anwendungsverhalten zu definieren.

Ein Ausspähen der internen IT-Infrastruktur wird durch Abschirmung von Informationen über die Applikationsumgebung (Serveradressen, Domain-Bezeichnungen, Verzeichnisstrukturen oder Angaben über Datenbank-Technologie und Betriebssysteme) verhindert. Angreifer können so nicht gezielt nach möglichen Schwachstellen suchen, um ihre Attacken an die individuelle Umgebung anzupassen. Die Sicherheitstechnologien der Citrix NetScaler Application Firewall schützen Web-Anwendungen, ohne dabei die Performance der Applikationen zu beeinträchtigen. Durch den Einsatz der Citrix Lösung verbessern sich teilweise sogar die Antwortzeiten, da rechen- und speicherintensive Aufgaben von den Web-Servern auf die Application Firewall verlagert werden. Die Citrix Komponente lässt sich auch in Hochverfügbarkeits-Szenarien einsetzen: Unternehmen können dazu mehrere Application Firewalls zu einem ausfallsicheren Cluster zusammenschließen.

Citrix NetScaler Application Firewall wird über eine einfach zu bedienende, browserbasierte Managementkonsole verwaltet. Diese zentrale Konsole kann für das Management aller Geräte in einem Cluster verwendet werden. Alle Änderungen an anwendungsspezifischen Sicherheitsrichtlinien werden automatisch an die Firewall-Geräte im Cluster weitergegeben. Damit ist höchste Effizienz beim Management gewährleistet. Anhand der Sicherheitsrichtlinien wird definiert, in welchem Maße eine bestimmte Anwendung geschützt werden soll. Zu den Schutzmaßnahmen zählen die Validierung von Eingaben in Formularfeldern, die Abwehr von SQL-Injection-Attacken, die Festlegung von zulässigen Start-URLs, die Erkennung von Cookie-Manipulationen, die Verhinderung von Buffer-Overflows und vieles mehr. Durch die Verwendung einer SSL-verschlüsselten Verbindung für die gesamte Management-Kommunikation ist dabei für ein Maximum an Sicherheit gesorgt.

## Umfassende Sicherheit für Web-Services

Web-Services bieten eine bisher nie da gewesene Interoperabilität und ermöglichen es Entwicklern, geschäftskritische Anwendungen direkt mit bestimmten Anwender- und Anwendungsgruppen zu verknüpfen. Der Mangel an wirkungsvollen Sicherheitslösungen für Web-Services hält die Unternehmen jedoch leider allzu oft davon ab, diese Technologie im vollen Umfang zu nutzen. Die Sicherheitsbedenken der Unternehmen sind durchaus begründet. Anwendungen mit Web-Service-Schnittstellen bieten Hackern einen Direktzugang zu kritischen Datenbank- und Netzwerkressourcen. Hinzu kommt, dass selbst Sicherheitssysteme auf Netzwerkebene, z.B. Firewalls, in diesem Fall keinen Schutz bieten – und zwar aus dem einfachen Grund, dass diese Systeme die XML-Kommunikation nicht prüfen können.

## PCI DSS

Die führenden Kreditkartenunternehmen American Express, Discover Financial Services, JCB, MasterCard Worldwide und Visa International haben sich in dem PCI SSC (Payment Card Industry Security Standards Council) zusammen geschlossen. Oberstes Ziel ist der Schutz der sensiblen Zahlungskartendaten und die Standardisierung und Verbesserung der Zahlungsabwicklung von Kredit-, Debit- und Geldautomatenkarten.

Alle Webshops, Finanzdienstleister, Service Provider und Unternehmen, die mit Kreditkarten-Transaktionen arbeiten, d.h. Karteninhaberdaten speichern, verarbeiten oder übermitteln sind aufgefordert, den PCI DSS (Data Security Standard) einzuhalten. Um die Einhaltung der in dem mit zwölf Sicherheitsvorgaben definierten PCI Regelwerk zu gewährleisten, ist eine Zertifizierung nötig, die von autorisierten Unternehmen durchgeführt wird. Die erste Regel des PCI Sicherheitsprogramms besagt, dass die Einrichtung und Betrieb einer Firewall zum Schutz der Daten von Kreditkarteninhabern nötig ist.

Händler sind – abhängig vom Transaktionsumfang – in unterschiedliche Kategorien unterteilt, die wiederum an Fristen zur Einhaltung des Standards gebunden sind.

- Kategorie 1: Händler mit mehr als sechs Millionen Kartentransaktionen pro Jahr
- Kategorie 2: Händler mit ein bis sechs Millionen Kartentransaktionen pro Jahr
- Kategorie 3: Händler mit 20.000 bis 1 Million Kartentransaktionen pro Jahr
- Kategorie 4: alle anderen Händler

Zu den wichtigsten durch den PCI SSC festgelegten Fristen zählen:

- 31. März 2007 – alle Händler der Kategorie 1 und 2 müssen belegen, dass sie die vollständige Kartennummer, Daten der Magnetstreifen Spuren, Kartenverifizierungscode (CVV2) und PIN-Nummer nicht speichern.
- 30. September 2007 – alle Händler der Kategorie 1 müssen den PCI DSS vollständig umgesetzt haben
- 31. Dezember 2007 – alle Händler der Kategorie 2 müssen den PCI DSS vollständig umgesetzt haben.
- 20. Juni 2008 – eine Application Firewall zur Absicherung der Daten ist Pflicht

Citrix NetScaler Application Firewall erfüllt die Anforderungen des Sicherheits-Standards PCI-DSS. Damit ist sichergestellt, dass Kreditkartennummern nicht versehentlich in die falschen Hände gelangen. Denn: der einfachste Weg zu einer großen Ansammlung von Kreditkartendaten zu kommen, führt über eine Web-Anwendung, die an eine Backend-Datenbank angebunden ist. Schwachstellen im Code von Web-Anwendungen können einen Missbrauch der Datenbank-Informationen zur Folge haben – und zum Verlust von mitunter Tausenden von Kreditkartennummern führen. Das Commerce Protection Module der NetScaler Application Firewall verhindert die nicht autorisierte Übermittlung von Kreditkartennummern durch Web-Anwendungen. Mit der „Deep Stream Inspection“-Technologie wird jede Instanz einer Kreditkartennummer in einer Web-Server-Antwort erkannt. Anschließend kann das SAFE Commerce-Modul entweder die Übertragung blockieren oder mehrere Ziffern der Kreditkartennummer unkenntlich machen, so dass sie für Hacker wertlos ist. SAFE Commerce kann quasi als letzte Verteidigungslinie gegen Hacker fungieren, die Kreditkartennummern stehlen wollen.

Die in Citrix NetScaler Application Firewall enthaltenen Schutzmodule für Geschäftsobjekte bieten vordefinierte Schutzroutinen für bestimmte Objekte (d.h. für US-Sozialversicherungsnummern oder Kreditkartennummern). Zudem ist es möglich, beliebige, vom Administrator definierte Datenobjekte zu schützen. Es kann sogar eine einzelne Instanz eines geschützten Datenobjekts innerhalb einer beliebigen Web-Server-Antwort erkannt, blockiert oder umgeschrieben werden – noch bevor das Objekt ungewollt preisgegeben wird. Die NetScaler Application Firewall erfüllt damit die wachsenden Datenschutzerfordernungen, die sich aus neuen gesetzlichen Bestimmungen ergeben (z.B. HIPAA, Gramm-Leach-Bliley Act usw.).

Citrix NetScaler Application Firewall ist als allein stehende Netzwerkkomponente oder als Modul der Citrix NetScaler Platinum Edition verfügbar (auch als FIPS 140-2 konforme Version).