

ABSICHERUNG VON WEB-ANWENDUNGEN
SCHUTZ VON PORTALEN,
SHOPS & CO.



Web-Applikationen – allgegenwärtig in der Welt des Internets

Web-Anwendungen nutzt nahezu jeder wie selbstverständlich – und es ist ebenso selbstverständlich, dass sie auch funktionieren. War in der Vergangenheit oft nur die Rede von reinen Business-Anwendungen für Mitarbeiter wie zum Beispiel E-Mail-Portalen, bei denen die Mitarbeiter von außen Zugriff auf ihre elektronischen Nachrichten bekamen, oder CRM-Portalen, in denen die Kundendaten hinterlegt waren, so ist das Thema inzwischen in vielen Lebensbereichen mehr oder minder für jeden Internetnutzer relevant.

Sogenannte Provisioning-Portale unterstützen zum Beispiel das Einrichten und Verwalten von Mobilfunk- oder Festnetz-Konten. Sie ermöglichen den Nutzern die Einsicht in die Abrechnungen, das Kontrollieren des Einzelverbindungs nachweises, das Ändern von Konten- oder Adressdaten und vieles mehr. Das Gleiche gilt für private E-Mail-Konten, die Verwaltung des eigenen Nutzerprofils beim Online-Shopping, behördliche Formulare oder Universitäts- und Schüler-Portale.

Kurz: Fast jeder nutzt auf irgendeine Weise Web-Anwendungen – und glaubt (oder eher hofft!), dass seine - oft sehr sensiblen - Daten dort auch sicher sind.

B2B – Web-Anwendungen nicht wegzudenken

Innerhalb von Unternehmen kommunizieren inzwischen ebenfalls nahezu alle Applikationen auf Basis von XML, einer Markup-Sprache, die den einheitlichen Austausch von Daten zwischen völlig unterschiedlichen Anwendungen ermöglicht. Mithilfe XML-basierender Webservices können so auf einfache Weise Daten zwischen ERP-, CRM-, Office-, CMS- oder Produktionssystemen ausgetauscht werden. Die Manipulation eines solchen Dienstes hätte für ein Unternehmen unter Umständen fatale Folgen.

Sicherheitslücken vorprogrammiert

Natürlich bemühen sich Online-Portale, -Shops und sonstige Unternehmen mit Online-Diensten und -Zugängen um Sicherheit. Doch diverse Faktoren beeinflussen entweder die Sicherheit der Benutzerdaten selbst oder aber die Funktionsfähigkeit der jeweiligen Web-Applikationen.

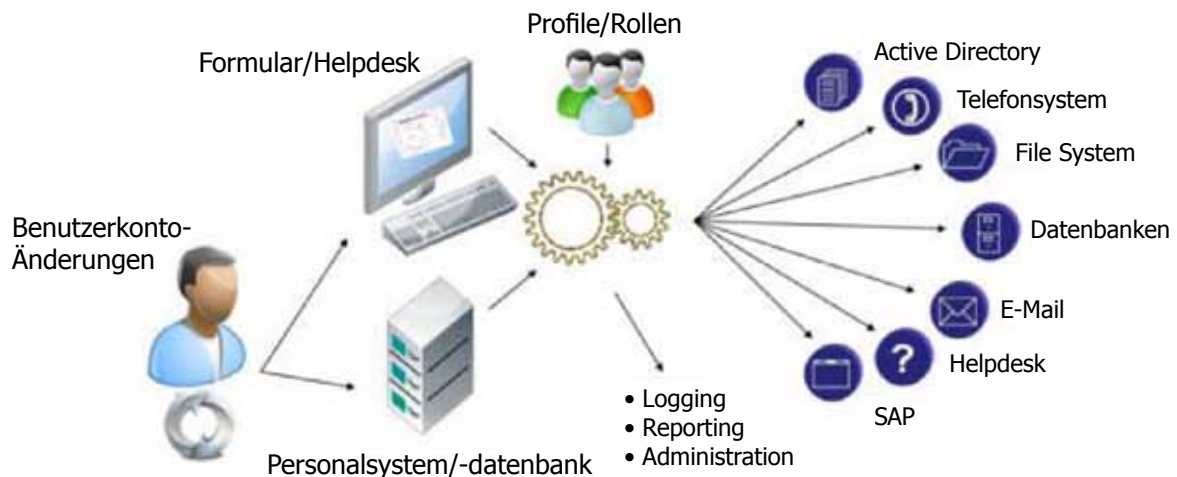
Zahllose Online-Shops sind immer noch mit einfachen Mitteln manipulierbar und so können (auch große) Online-Portale leicht gestört werden. Für die Betreiber sind diese Störungen oft mit hohen Kosten, Umsatzausfällen und einem nicht bezifferbaren Imageverlust verbunden – wie die jüngsten Vorfälle um einen japanischen Konzern der Unterhaltungselektronik beweisen.

Die Ursache für die Schwachstellen liegt in der Programmierung von Web-Anwendungen, die in der Regel auf eine bestimmte Funktionalität und auf eine möglichst schnelle Verfügbarkeit bei geringen Kosten abzielt. Das Einbinden der notwendigen Sicherheits-Algorithmen erfordert jedoch einen - mit zunehmender Komplexität der Anwendung - immens steigenden Programmieraufwand, was wiederum die Kosten erhöht und die Auslieferung verzögert. Gleiches gilt für die ständigen Updates der Anwendung, die nur noch selten statisch und unverändert bleibt.

Security in eine Web-Applikation einzubinden, stellt somit eine große Herausforderung dar und wird daher in den meisten Fällen schlicht vernachlässigt oder nur oberflächlich umgesetzt.

Betrachtet man Abbildung 1 wird deutlich, wie eng ein einfaches Portal mit der internen Infrastruktur des Unternehmens verzahnt ist.

Abb:1 Quelle:Fortinet



Ein erfolgreicher Angriff hat somit offensichtlich nicht nur Auswirkungen auf die Verfügbarkeit und Funktionsweise des Portals selbst, sondern unmittelbar auch auf wesentliche interne Daten und Prozesse.

Ein Online-Shop ist oft direkt mit internen Prozessen für Fertigung, Bestellwesen, Logistik und Datenbanken für Artikelstämme, Fertigungsteile und natürlich mit sensiblen Kundeninformationen wie Bank- und/oder Kreditkartendaten verknüpft. Viele kleine und auch große Unternehmen machen sich nicht bewusst, wie stark die eigenen Umsätze von der Verfügbarkeit der beschriebenen Portale, Shops oder anderen Anwendungen abhängen.

Auch wenn die eigentliche Produktionsumgebung oder die Kernkompetenz „Dienstleistung“ verfügbar sind, kann ein Ausfall beim Bestellwesen (Shop), der Auftragsabwicklung (Logistik, Kundendatenbanken) oder der Fertigungssteuerung katastrophal enden und große Verdienstaufschläge nach sich ziehen.

Zudem sind Unternehmen zum Beispiel im Bankenbereich auch aus Compliance-Gründen zum Einsatz von diversen Security Lösungen wie einer Web Application Firewall mit entsprechendem Reporting und Schwachstellen-Management der Applikationen verpflichtet. Das regelt der PCI DSS (Payment Card Industry Data Security Standard), der Kreditkartentransaktionen schützen soll.

Es handelt sich hier um einen Information Security Standard, der als Konsequenz auf die zunehmenden Angriffe auf Web-Anwendungen und -Services eingeführt wurde und der die sensiblen Daten der Kreditkartenbesitzer ebenso wie die Betreiber der entsprechenden Infrastruktur schützt.

Angriffe erkennen

Eine herkömmliche Firewall – auch wenn sie über ein Intrusion Prevention System (erkennt frühzeitig unberechtigte Eindringlinge) und eine Applikationskontrolle verfügt – ist nicht in der Lage, Web-Service-basierende Angriffe zu erkennen und abzuwehren.

Web Services sind die den Web-Applikationen zugrundeliegenden Funktionen, welche oft von mehreren Anwendungen gleichzeitig genutzt werden. Diese Web Services bedienen sich einer eigenen Beschreibungssprache (WSDL) und eines eigenen Protokolls (SOAP). Sowohl WSDL als auch SOAP beinhalten keinerlei Security-Mechanismen, beschreiben bzw. übertragen aber alle Parameter eines Web-Dienstes transparent.

Es ist klar, dass Manipulationen dieser Services somit sehr leicht möglich sind. Ein Beispiel hierfür sind XDoS-Attacks, die auf nur einem einzigen System mit wenigen Byte Code erzeugt werden können, da in XML rekursive Strukturen erlaubt sind.

Mit einem simplen Eingriff ist so beispielsweise eine Endlosschleife „programmierbar“ – die denselben Effekt hat, wie ein „normaler“ DoS-Angriff, für den in der Regel mehrere tausend Systeme manipuliert und fremdgesteuert werden müssten.

Ein weiterer typischer Angriff auf Web-Anwendungen und -Seiten ist das Verändern von Dateien, die Teil der Applikation oder der Website sind. Derartige Veränderungen erkennt meist weder die Applikation selbst, noch eine herkömmliche Firewall, weil sie in der Infrastruktur an einem anderen Punkt im Netzwerk integriert ist.

Im Gegensatz dazu befindet sich eine Web-Applikation-Firewall direkt vor der entsprechenden Web Server Farm und kann somit auch Files auf den Servern untersuchen und Veränderungen an Dateien sofort erkennen (sog. Anti-Defacement) – und ggf. die Original-Dateien zurückschreiben. Derartige Funktionalität ist mit normalen Sicherheitslösungen nicht realisierbar.

Die Liste der möglichen Angriffe ist lang und erinnert in der Namensgebung an bekannte Attacks aus der „klassischen“ Infrastruktur- und Applikations-Welt. Zu den bekanntesten Attacks zählen sicher Cross-Site-Scripting oder SQL-Injection.

Beim Cross-Site-Scripting (XSS) wird eine Sicherheitslücke in einer Webanwendung ausgenutzt, in dem Informationen als vertrauenswürdig dargestellt werden, so dass in diesem Zusammenhang ein Angriff gestartet werden kann. Das Ziel ist es, an die sensiblen Benutzerdaten zu gelangen.

Bei der SQL Injection versucht der Angreifer Zugang zu einer SQL Datenbank zu erlangen, in dem er Datenbankbefehle einschleust. Auch hier ist das Ziel in den Besitz von Daten zu gelangen oder Kontrolle über einen Server zu erhalten.

Performance sichern

Schließlich gilt es, neben einer ausreichenden Sicherheit auch die Performance von Web-Applikationen sicherzustellen. Die Zahl der Transaktionen nimmt ständig zu und die Schnelligkeit bei den Antwortzeiten bestimmen über die Nutzung und den Erfolg oder Misserfolg der jeweiligen Anwendung. Der Nutzer steigt oft sehr schnell auf einen anderen Anbieter um, wenn eine Applikation zu langsam reagiert oder sogar für einen Zeitraum nicht verfügbar ist, denn für nahezu alle Online-Angebote gibt es inzwischen leicht auffindbare Alternativen.

Gründe für schlechte Reaktionszeiten einer Web-Anwendung liegen häufig in einer nicht mehr den Anforderungen entsprechenden Dimensionierung der Web Server Farm. Zudem stellt jeder einzelne Web-Server Dienste bereit, die die Leistungsfähigkeit der Hardware mitunter stark beeinträchtigen. Dazu zählen rechenintensive Services wie SSL- oder XML Encryption und -Decryption ebenso wie XML-Security-Validierung.

Durch das Bereitstellen des notwendigen Zertifikats auf der vorgeschalteten Web Firewall, kombiniert mit diversen weiteren Optimierungs-Routinen wie Load Balancing oder XML-based Routing, kann eine externe Appliance die Web Server signifikant entlasten. Das resultiert in mehr möglichen Transaktionen und kann sogar zu Kosteneinsparungen durch eine Reduktion der benötigten Server führen.

Schwachstellen automatisch identifizieren

Web-Applikationen werden unter Zeitdruck entwickelt und sind ferner durch häufige Updates/Patches und Erweiterungen sehr fehleranfällig. Manchmal kann der Anwender erkannte Schwachstellen auch durch Neu-Konfiguration oder Patchen der Anwendung abstellen. An dieser Stelle sind Hilfsmittel gefragt, die kontinuierlich und automatisiert die eingesetzten Web-Anwendungen auf Sicherheitsdefizite hin scannen und entsprechende Reports generieren.

Selbstlernmodus für einfachste Integration

IT-Administratoren scheuen häufig – trotz der bereits erkannten Notwendigkeit – die Einführung von Web Application Security Lösungen. Grund dafür ist der als zu aufwändig angesehene Implementierungsaufwand. Oft liegen die Kenntnisse über die Details der zu schützenden Applikationen und Prozesse und das Wissen um die übrige IT- und Security-Infrastruktur nicht bei ein und derselben Person.

Die Erstellung von Sicherheits-Regelwerken erfordert hier also i.d.R. eine abteilungsübergreifende und meist zeitaufwändige Kooperation. Abhilfe schaffen hier Lösungen, die über einen Selbstlernmodus verfügen. Hierbei werden die zu schützenden Applikationen, deren Antwortverhalten sowie die Zugriffe durch Nutzer analysiert und ein dementsprechendes Basis-Regelwerk vorgeschlagen. Dieses kann dann sukzessive ergänzt werden. Auf diese Weise wird eine schnelle Wirksamkeit von Schutzmechanismen ebenso gewährleistet wie die Verfügbarkeit der Web-Anwendungen selbst.

☒ Lösungsansätze

Eine gewissenhafte Analyse von Abhängigkeiten zwischen kritischen Geschäftsprozessen und den dahinterliegenden Web-Diensten ist enorm wichtig. Häufig kommt es dann zu einem mehrstufigen Ansatz: Einsatz einer Web Application Firewall, dedizierter Schutz von XML-Services und Beschleunigung der Web-Anwendungen.

Aus Sicht des Betreibers sind hier integrierte Lösungen ideal, die die genannten Schutz- und Optimierungs-Maßnahmen kombiniert zur Verfügung stellen. Dies erspart Zeit für Einarbeitung und Konfiguration, da nur eine einzige Benutzeroberfläche und Nomenklatur zu erlernen ist.

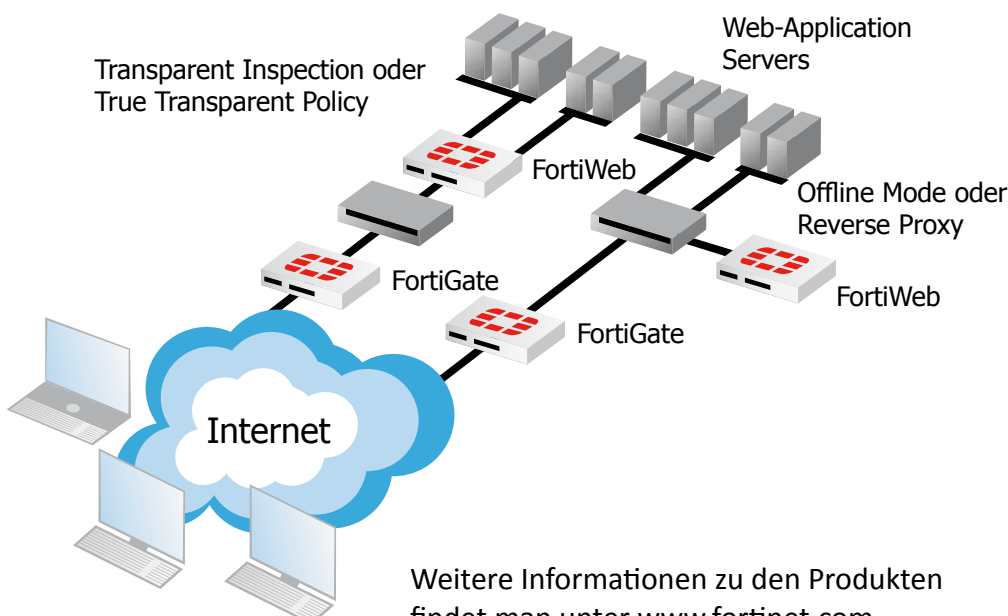
Überdies gewährt eine nahtlose Integration der verschiedenen Module höhere Transparenz auch hinsichtlich der Wirksamkeit der Maßnahmen, bessere Performance und deutlich geringere Kosten für Betrieb und Updates.

☒ Fortinet schützt Web-Anwendungen

Fortinet verfügt über jene integrierten Web-Security Appliance-Lösungen mit unterschiedlichen Leistungsdaten aber einheitlichem Feature-Set für Unternehmen jeder Größe, Application Service Provider (ASPs) und SaaS (Software as a Service)Anbieter.

Das Produkt FortiWeb stellt neben den Modulen Web Application Firewall, XML Firewall und Web Traffic Optimizer auch ein Applikations-basierendes Load Balancing und einen leistungsfähigen Schwachstellen-Scanner bereit. Mit der Möglichkeit des Auto-Learning ist es überdies möglich, den Traffic zu Web-Anwendungen regelmäßig zu analysieren und entsprechende Security-Profile automatisiert zu erstellen – ohne Eingriff in die vorhandene Netzwerkinfrastruktur oder die zu schützende Applikation.

Ein Policy Wizard sowie voreingestellte Regelwerke erleichtern den Einsatz und die Inbetriebnahme der FortiWeb Appliances ebenso wie die verschiedenen Anwendungsszenarien als Transparent Inspection, Reverse oder True Transparent Proxy, sowie Offline. Damit gelingt die Absicherung von Web-Portalen spielend.



Über den Autor



Jörg von der Heydt ist Channel- und Marketing-Manager Deutschland bei Fortinet und verfügt über langjährige Berufserfahrung im Bereich IT-Sicherheit. Nach seinem Studium der Elektrotechnik an der Uni Dortmund sammelte er bei Unternehmen wie Philips NK (heute Axians), Unisys und ABB umfangreiche Erfahrungen im Netzwerk-Infrastruktur- und Service-Business, bevor er dann bei Herstellern wie Nokia, Smarttrust und zuletzt Check Point zum Security Experten avancierte. Er hat im Laufe seiner Arbeit festgestellt, dass gerade im mittelständischen Bereich erhöhter Bedarf an praxisorientiertem Know-How und an Sicherheitskonzepten besteht, die genau auf diese Unternehmen zugeschnitten sind.

Über Ihre Fragen oder Anregungen freut er sich unter jvdheydt@fortinet.com.

Wünschen Sie mehr Informationen?:

Fortinet GmbH | T: +49-(0)69-710 423 500 | www.sicher-sein.net | www.fortinet.com