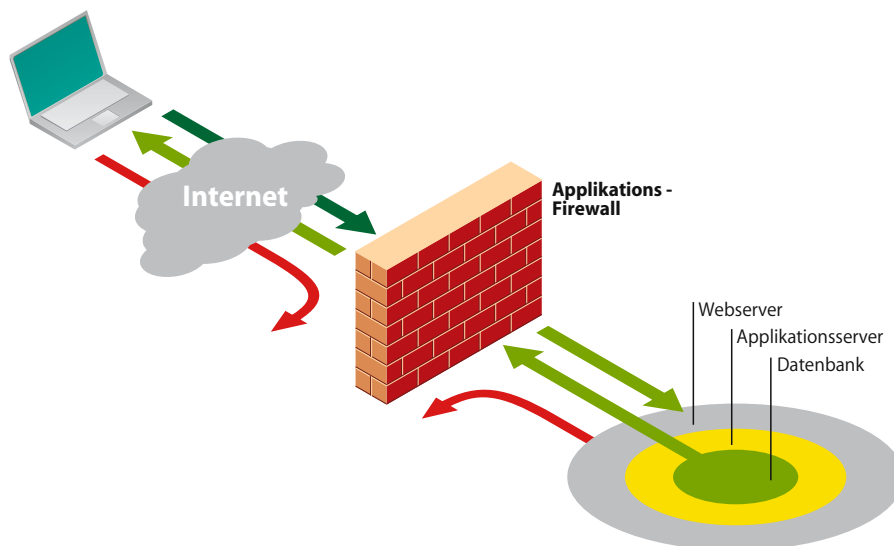


Schutzschild für Webportale

Webportale sind besonders beliebte Angriffsziele. Sie sind durch ihre Komplexität zumeist leicht angreifbar und versprechen Zugang zu interessanten Daten. Im schlimmsten Fall können sie komplett lahm gelegt werden – ein Schreckensszenario für viele Unternehmen.

Da klassische Firewalls hier keinen ausreichenden Schutz bieten, brauchen Webportale spezielle Applikations-Firewalls.



Die Tage, in denen Websites aus ein paar statischen HTML-Seiten bestanden haben, sind endgültig vorbei. Um die benötigte Funktionalität zu erzielen, müssen Webseiten heute in vielen Fällen dynamisch generiert werden. Anders wäre es nicht möglich,

Die Filterwirkung einer Applikations-Firewall: Den Webserver erreichen nur noch saubere Anfragen und die Datenbank kann ausschließlich die für den jeweiligen Benutzer relevanten Daten ins Internet zurückliefern.

die aufwändigen Webapplikationen zu verwirklichen, über die heute viele Geschäfte abgewickelt werden. Internetbanking, Online-Shops und die meisten Internet-Auftritte größerer Firmen sind Beispiele für Systeme, deren Seiten dynamisch generiert werden. Die Seiten, die der Benutzer in seinem Browser dann zu sehen bekommt, sind der Output von komplexen Lösungen, die aus drei Schichten bestehen: einem Webserver, einem Applikationsserver und einem Datenbankserver. Das bedeutet aber, dass ein externer Benutzer über das Web indirekt Zugriff auf Datenbankserver im Unternehmen bekommt. Angreifer haben das längst erkannt und eine Vielzahl von Methoden entwickelt, um

an vertrauliche Daten zu gelangen. Meistens wird dabei der Umstand genutzt, dass Webapplikationen die Benutzereingaben unzureichend prüfen. Im schlimmsten Fall lässt sich auf diesem Weg uneingeschränkter Zugriff auf die Datenbankserver erlangen. Diese offenen Angriffswege ließen sich rein theoretisch durch ein entsprechendes Design der Webapplikation von vornherein verschließen. Es gibt sogar eine ÖNORM (ON17700), die Grundregeln für den Aufbau sicherer Webapplikationen bietet. In den seltensten Fällen werden diese Grundregeln bei der Entwicklung tatsächlich vollständig beherzigt – verschiedene Penetrationstests unabhängiger Beratungsunternehmen haben

Einladung zum Bacher Systems Breakfast 10. Mai 2007

Mehr über die **Absicherung von Webportalen** erfahren Sie auf dem nächsten Bacher Systems Breakfast am 10. Mai 2007 (9:30 bis 12:00) im Atelier Augarten. Die Teilnahme ist kostenlos, um rechtzeitige Anmeldung unter www.bacher.at/breakfast wird gebeten.



Newsletter 3/2007

Informationen für IT-Sicherheit und IT-Infrastruktur

bei bis zu 90% aller Webapplikationen Schwachstellen aufgezeigt, die sich für gravierende Manipulationen nützen lassen. Ein komplettes Redesign einer bestehenden und an sich gut funktionierenden Webapplikation wäre aber zumeist extrem teuer und ist somit keine wirtschaftliche Option. Und auch klassische Firewalls oder SSL Verschlüsselungstechnologien sind keine ausreichenden Schutzmaßnahmen. Firewalls analysieren die Inhalte im HTTP-Protokoll nicht tief genug und durch SSL werden Attacken nur verschlüsselt übertragen – was nichts an ihrer Wirksamkeit ändert.

Abwehr direkt am Gateway

Kostengünstig und wirkungsvoll lassen sich die Sicherheitslücken rund um Webportale nur mit speziellen Applikations-Firewalls schließen. Produkte wie zum Beispiel Airlock von Visonys sind speziell dafür geschaffen, einen Schutzschild zwischen der externen Welt und dem Webserver aufzubauen. Sie übernehmen die Authentifizierung, filtern den HTTP-Datenstrom und verteilen die Last unter den Webservern. Eingesetzt werden Verfahren wie URL Encryption, Form Validation oder Cookie Protection, womit eine Vielzahl von Angriffsvarianten unterbunden werden – Cross-Site Scripting, SQL-Injection, Command Execution oder Path Transversal werden verhindert. Externe Benutzer kommen nicht mehr direkt zum Webserver durch, sie kommunizieren ausschließlich mit der Applikations-Firewall, von der die

Anfragen gefiltert an den Webserver weitergegeben werden. Die folgenden drei Beispiele zeigen, wie Webapplikationen und ihre Daten geschützt werden:

Ein Angreifer kann etwa mit Hilfe von Cross-Site Scripting die Session-ID eines legitimen Benutzers übernehmen. Er greift dann auf Informationen zu, die nur für diesen Benutzer bestimmt sind. Je nach Applikation könnten Kreditkartennummer, Informationen zu Bestellungen oder andere Daten gestohlen werden. Mit der beschriebenen Applikations-Firewall wird dieses Manöver verhindert und die Vertraulichkeit der Benutzerdaten bleibt sichergestellt.

Eine andere Attacke besteht zum Beispiel darin, mittels einer so genannten SQL-Injection uneingeschränkten Zugriff auf die (der Webanwendung zugrunde liegende) Datenbank zu erhalten. Das bedeutet für einen Angreifer, dass er nicht nur alle Daten auslesen, sondern im Extremfall auch beliebig verändern kann. Damit ist die Datenbank allen Manipulationen ausgeliefert, von purem Vandalismus bis zu gezielter Sabotage. Mit einer Applikations-Firewall wird erreicht, dass externer Zugriff dieser Art auf die Datenbank unmöglich wird – die Integrität der Daten bleibt gesichert.

Mit einem Manöver auf Basis von Command Executions kann ein Angreifer zum Beispiel die volle Kontrolle über den Webserver erlangen. In weiterer Folge steht es ihm offen, mit den Ressourcen des Servers nach seinem

Belieben zu verfahren. Wenn er eine Überlastung des Servers produziert, kann er auf diese Weise ein Denial-of-Service erzeugen. Was in weiterer Folge bedeutet, dass Webapplikation und Daten den regulären Anwendern nicht mehr zur Verfügung stehen. Mit einer Applikations-Firewall werden solche Angriffe unterbunden und die Verfügbarkeit der Daten bleibt gesichert.

Trainings bei Bacher Systems

IT-Infrastruktur

Solaris 10 OE Containers

3.5. - 4.5.2007 / € 1.050,-

Solaris 10 OE Systemadministration II

7.5. - 11.5.2007 / € 2.790,-

Solaris 10 OE für erfahrene Systemadministratoren

21.5. - 25.5.2007 / € 2.790,-

Veritas Storage Foundation 4.1 für Solaris

21.5. - 25.5.2007 / € 3.100,-

Solaris 10 OE Systemadministration I

18.6. - 22.6.2007 / € 2.790,-

IT-Sicherheit

Check Point Security Administration NGX I 1.1

7.5. - 8.5.2007 / € 1.350,-

Check Point Security Administration NGX II 1.1

9.5. - 11.5.2007 / € 1.990,-

Check Point Security Admin. NGX I auf Nokia Plattform 1.1

11.6. - 12.6.2007 / € 1.350,-

Check Point Security Admin. NGX II auf Nokia Plattform 1.1

13.6. - 15.6.2007 / € 1.990,-

Alle Preise pro Person exkl. MwSt.

Firmenspezifische Kurse auf Anfrage.

Anmeldungen: training@bacher.at

Kursinfos: www.bacher.at/training

Package
NGX I+II
€ 2.900,-
statt € 3.340,-

Package
NGX I+II
auf Nokia
€ 2.900,-
statt € 3.440,-

Änderungen vorbehalten

Offenlegung gemäß § 25 Mediengesetz; Medieninhaber: Bacher Systems EDV GmbH, Clemens Holzmeister Straße 4, 1100 Wien Reg. zu FN 54202i, Handelsgericht Wien, GF: Manfred Köteles, Mehrheitsgesellschafter: Manfred Köteles, Martin Mörtinger Unternehmensgegenstand: Handel mit Computer-Soft- und Hardware IT-Beratung; Blattlinie: Verbreitung von Information für sichere IT-Infrastruktur

