

Der Schutz von Webapplikationen wird immer wichtiger

Mit der Anzahl und der Bedeutung von Webapplikationen steigen auch die potentiellen Angriffe: Immer häufiger entstehen hohe finanzielle Schäden durch schlecht - oder gar nicht - geschützte Webapplikationen. Für uns ist das Grund genug über die Möglichkeiten zum Schutz Ihrer Webapplikationen zu informieren.

Warum sollte man Webapplikationen schützen?



Als Betreiber eines Online-Shop-Systems sind Sie beispielsweise der Gefahr ausgesetzt, dass die Konkurrenz immer über Ihre aktuellsten Preise informiert ist, weil Sie die Suchfunktion Ihres Shops ausnutzen könnten, um sich alle Produkte auf einen Blick ansehen zu können. Noch Schlimmeres ist denkbar, wenn Ihr Shop-System durch eine SQL-Injection alle Kundendaten ausliefert.

Setzen Sie eine Webapplikation ein, die nicht mehr weiterentwickelt wird, sind Sie zwangsläufig einer Menge Gefahren ausgesetzt. Gegen neu erkannte Sicherheitslücken gibt es keine Schutzmöglichkeiten, es sei denn, Sie schützen die Applikation mit einer WAF (Web Application Firewall), nur so können Sie sicher sein, dass Sie die Kontrolle darüber haben, was Ihre Webapplikation überhaupt ausführt und was nicht.

Die üblichen Angriffe im Überblick:

SQL Injection

Dynamische Webapplikationen reagieren normalerweise auf Interaktionen die in Form von GET und/oder POST Parametern übergeben werden. Ein Angreifer versucht bei diesem Angriff diese Parameter so zu verändern, dass die Webapplikation Werte ausgibt, die normalerweise nicht ausgegeben werden sollen. Für so einen Angriff ist nicht einmal viel Know-How nötig, es finden sich zu Hauf Anleitungen im Netz.

Cross-Site Scripting

Ihre Besucher surfen auf Ihrer Webseite, aber eine dritte Instanz hört mit Kundendaten, Zugangsdaten usw. werden über den Besucher an den Angreifer gesendet obwohl Sie Ihre Applikation per SSL und gültigem Zertifikat zur Verfügung stellen. Der Angreifer hat es geschafft, Code in Ihre Applikation einzuschleusen, dieser könnte bei jedem Besucher ausgeführt werden.

Pufferüberlaufangriffe

Ähnlich wie der DoS-Angriff hat diese Attacke die Absicht Ihre Webapplikation lahmzulegen, Ihrer Konkurrenz würde die Idee gefallen, schließlich kann dieser Angriff zur Folge haben, dass Ihre komplette Präsenz im Internet verschwindet Sie sind nicht erreichbar, also geht der Besucher und/oder Kunde zum nächsten Anbieter. Technisch gesehen ist dieser Angriff nichts anderes als ein Überlasten Ihres Systems, sodass es nicht in der Lage ist, anderen zu Antworten. Natürlich kann es auch vorkommen, dass das System abstürzt oder irreparable Schäden an Ihren Datenstrukturen hinterlässt.

Data Leakage

Weniger ein Angriff, aber dafür umso gefährlicher erlaubt Ihre Webapplikation dem Angreifer Einsicht auf z.B. interne IP Adressen und andere Informationen, kann er diese mit anderen Informationen zusammenführen und einen Angriff in aller Ruhe planen. Leider wird es oft unterschätzt wie viele Informationen durchsickern.



Web Application Firewalls ein konsequenter Schritt in die richtige Richtung

Mit einer WAF sind Sie in der Lage viele Gefahren von vornherein abzuwehren, als Appliance oder virtuelle Maschine schützt eine WAF Ihre Webapplikationen effektiv.



CuC setzt dabei besonders gerne die Web Application Firewall von Barracuda Networks ein. Die exklusive Kombination aus Know-How und langjähriger Erfahrung - CuC ist einziger Barracuda Diamond Partner in Norddeutschland - hilft Ihnen, Webapplikationen wirklich effektiv zu schützen.

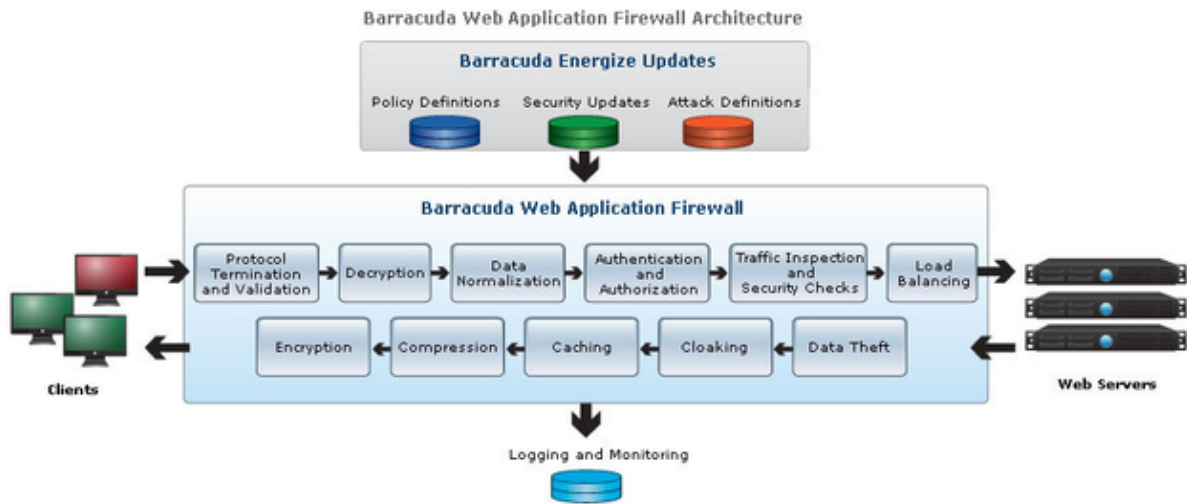
Spätestens seit 2009, als die Barracuda Web Application Firewall von den ICISA Labs (bzgl. Payment Card Industry Data Security Standard) zertifiziert wurde (Link: www.barracudanetworks.com/ns/news_and_events/certification.php) stand fest, dass dieses Produkt zukunftsweisend im Bereich der Web Application Firewalls sein würde.

Viele Firmen setzen die Barracuda bereits produktiv ein und schützen so Ihre Webapplikationen. Einen Überblick über einige wichtige Kunden von Barracuda finden Sie hier:

www.barracudanetworks.com/ns/customers/customer_by_country.php

Wußten Sie schon, dass Sie mit einer Barracuda Web Application Firewall zusätzlich in der Lage sind, durch Load Balancing Ihre Webapplikationen hochverfügbar zu machen?

Funktionsweise der Barracuda Web Application Firewall:



Essentielle Komponente einer effektiven Abwehrstrategie sind dabei auch die Barracuda Energize Updates, die stets auf die neuesten Attacken vorbereiten.

Gerne laden wir Sie zu einem unverbindlichen Informationsgespräch ein. Herr Fickel betreut Sie in allen Fragen zu den Barracuda Networks Produkten (Kontakt oben rechts).