

Einleitung

Jeder hat heutzutage beinahe täglich mit ihnen zu tun und genießt den Komfort den sie einem bieten. Die Rede ist von Webanwendungen. Mittlerweile sind diese Anwendungen nahezu unverzichtbar. Sie bieten mittlerweile sehr große Möglichkeiten, Prozesse zum simplifizieren. Da das Web beinahe jedem zugänglich ist, können nicht nur die potentiellen Benutzer auf den angebotenen Service zugreifen. Insbesondere ist die Anwendung auch für diejenigen frei zugänglich, deren Ziel es ist, solche Systeme auszuspionieren oder zu hintergehen.

Aus diesem Grund ist einer der wichtigsten Aspekte solcher Anwendungen die Sicherheit und diese in ausreichendem Maße zu gewährleisten. Dieser Punkt wird häufig beim Optimieren von Prozessen vernachlässigt. Webanwendungen werden oft in Betrieb genommen, ohne zu wissen ob die Sicherheit der Anwendung ausreichend Beachtung gefunden hat.

Viel mehr als in der Vergangenheit, werden Geschäftsprozesse im Internet abgebildet und durchgeführt. Dabei sind Prozesse zwischen Geschäftspartnern als auch Prozesse zwischen Unternehmen und deren Kunden (eBusiness).

Dabei reicht der Bereich dieser Anwendungen von sehr einfachen bis hin zu sehr komplexen Systemen. Unabhängig davon, sollte den Gesichtspunkten der Sicherheit immer ausreichend Beachtung geschenkt werden. Oft wird aufgrund von Zeit- oder Geldmangel diesem Aspekt nicht genügend Aufmerksamkeit geschenkt, so dass die Sicherheit nur im geringen Maße gewährleistet werden kann.

Zur besseren Klärung der Zuständigkeiten bei der Sicherheit von Webanwendungen, existiert ein 5 Ebenen Modell, welche diese klar definiert. Mittlerweile wird dieses Modell oft in sechs Ebenen aufgeteilt:

- Netzwerk und Host(*)
- System
- Technologie
- Implementierung
- Logik,
- Semantik
- Vorschriften und Bestimmungen(*)

(*) nicht direkt der Webanwendung zugeordnet

Im weiteren Verlauf werden diese Ebenen noch genauer unter die Lupe genommen.

Ein weiter Punkt sind die Gegenmaßnahmen die zu ergreifen sind und Sicherheitslücken zu vermeiden. Dazu existieren einige allgemeine Methoden um dies zu garantieren, von denen einige der wichtigsten später noch genauer besprochen werden. Im folgenden Kapitel nun aber zuerst zu den Grundlagen des Ablaufs und dem Aufbau einer Webanwendung.

Fazit

Die Sicherheit von öffentlich zugänglichen Webanwendungen gewinnt immer mehr an Bedeutung um Unternehmen oder Personen keinen Schaden zuzufügen. Infolgedessen sollten immer die notwendigen Massnahmen ergriffen werden um die Schädigung des Systems oder Personen zu verhindern. Dies kann nur durch eine gründliche Analyse der gegebenen Situation und den Prozessen der zu entwickelnden Anwendung geschehen, um die Risiken zu erkennen und diese zu minimieren. Oft ist dies nicht immer einfach zu realisieren und bei großen Anwendungen auch nur mit großem Aufwand zu erreichen. Jedoch können schon durch das Einhalten von Programmierrichtlinien die größten Schwachstellen eliminiert werden. Die Sicherheit hat einen so großen Stellenwert, dass es sich lohnt auch einen größeren Aufwand in Kauf zu nehmen und Sicherheit bei der entwickelten Anwendung einen hohen Stellenwert beizumessen. Zusätzlichen Schutz bietet verschiedene WAF-Software(Web Application Firewall).