HTBLuVA Wien XX

Abteilung: INFORMATIONSTECHNOLOGIE
Ausbildungsschwerpunkt: SYSTEMTECHNIK

DIPLOMARBEIT

WebSecure

Ausgeführt im Schuljahr 2012/2013 von:
Paul Pfeiffer-Vogl 5AHITT
Harun Koyuncu 5AHITT
Patrick Ullrich 5AHITT
Kevin Schneider 5AHITT

Betreuer/Betreuerin:
Michael Borko, Bakk. techn.
Mag. Hans Brabenetz

Wien, am 14.05.2013

tgm | Technologisches Gewerbemuseum | Höhere Technische Bundes- Lehr- und Versuchsanstalt
Wexstraße 19-23 | A-1200 Wien | ☎ +43 1 33126 | FAX: +43 1 33126 204 | E-Mail: info@tgm.ac.at

Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Ort, Datum

Paul Pfeiffer-Vogl (Product Owner)

Harun Koyuncu

Patrick Ullrich

Kevin Schneider

INHALTSVERZEICHNIS

1. ABSTRACT

WebSecure is an online service, which gives a service provider the possibility of checking his system on possible safety gaps or any technical weaknesses. In the case of the utilization of WebSecure-Service the customer is instantly informed, if there is an acute safety problem for his server. In order to make the management and handling of the service as easy as possible, a website has been set up, in which an automatic payment, authorization and execution system is provided.

So that the attack mechanism is able to work properly, the service itself has to come to knowledge of which possible ways of inspecting a server are given. At the same time, the service has to be updated constantly, in order to recognize even the newest safety gaps. These attack mechanisms get the information from so-called exploit-databases and the results of analysis tools. In this database any safety weaknesses are continually updated and laid off in a specified structure. This data information is processed by an Agent and then taken over into an own database. After this analysis of the system the attack mechanism can work properly.

Due to the fact that the attack from a single server on a target server can easily be traced with the help of the IP-address, modern blockmechanisms are able to impede further attacks on the server. This is where the Cloud-system comes into play. Several Agents are installed on each of these Cloud-servers to produce a dispersed system. Since the computing power is distributed, a performed attack according to the time can be completed.

KURZFASSUNG

WebSecure ist ein Online-Service, welcher einem Serverbetreiber die Möglichkeit bietet sein System auf Sicherheitslücken bzw. Schwachstellen zu überprüfen. Dabei soll der Kunde bei dem Einsatz vom WebSecure-Service aufmerksam gemacht werden, wenn ein akutes Sicherheitsrisiko auf seinem Server besteht. Um den Kunden eine möglichst einfache Bedienung des Services zu gewährleisten, wurde eine Webseite mit automatisierten Bezahlungs-, Autorisierungs- und Exekutionssystem bereitgestellt.

Damit überhaupt ein Angriff stattfinden kann, muss das Service selbst das Wissen erlangen, auf welche Art der Server untersucht werden kann. Genauso, muss der Service ständig aktuell gehalten werden, damit dieser weiß, wo neue Sicherheitslücken aufgetreten sind. Dieses Wissen beziehen die Angriff-Tools von sogenannten Exploit-Datenbanken und von Ergebnissen der Analyse-Tools. In dieser Datenbank werden die Sicherheitslücken ständig aktualisiert und in einer festgelegten Struktur abgespeichert. Die Daten werden von einem Agent ausgelesen und in eine eigene Datenbank übernommen.

Nach der Analyse des Systems können gezielte Angriffe auf den Server gestartet werden.

Da nun aber mit einem einzelnen Rechner die Untersuchung auf den Zielserver leicht anhand der IP-Adresse zu identifizieren ist, blockieren moderne Sicherheitsmechanismen die weiteren Zugriffe auf den Server. Deshalb kommt ein Cloud-System ins Spiel.

Es werden nun mehrere Agents auf den Cloud-Rechnern installiert, um ein verteiltes System zu schaffen. Da die Rechenleistung verteilt ist, kann ein leistungsstarker Angriff ausgeführt werden.