

Summary

In der Diplomarbeit mit dem Thema „Sicherheit von Servern im Internet“ wird in der Einleitung (Kapitel 1) über den grundlegenden Bedarf an Sicherheit hingewiesen.

Viele Dienste sind in den letzten Jahren im Internet mit hoher Akzeptanz hinzugekommen, wie Online-Banking, Versandhandel bis hin zu Reisebuchungen. Doch die Sicherheit von Daten auf Servern und die Verbindungen zum Client wurden nicht immer stetig angepasst und darauf geachtet. Diese Diplomarbeit soll auf Gefahren hinweisen und Sicherheitsmängel aufzeigen.

Bevor aber näher auf die Gefahren eingegangen wird, ist es dem Autor wichtig, grundlegende Funktionsweisen und Übertragungstechniken im Internet aufzuführen und deren Funktionsweisen zu erklären. Zu Anfang werden die Protokollen der Internetschicht IPV4 und dem neuen IPV6 und deren Unterschiede dargestellt. Im Kapitel 2.3 werden die Protokolle der Anwendungsschicht beschrieben, die zum späteren Zeitpunkt besonders unter die Lupe genommen werden.

Angriff ist nicht gleich Angriff. Viele Begriffe stehen heutzutage im Raum. Deswegen werden diese in verschiedene Punkte sortiert und beschrieben und mit Begriffen wie Spoofing, Sniffing, Denial-of-Service Angriffe, klar definiert und spezialisiert.

Nach diesen grundlegenden Informationen über die Sicherheitslage im Internet und der Client-Server-Kommunikation, werden dem Leser im Kapitel 4 dann mögliche Abwehrszenarien und Gegenmaßnahmen ausführlich dargelegt, beginnend damit, dass Logging der Serveraktivitäten der erste wichtige Schritt und Voraussetzung für eine nachfolgende Analyse ist.

Ein weiterer Schritt ist, die in Kapitel 2 vorgestellten Schichten einzeln abzusichern. Meist gelingt das durch Verschlüsselung der Protokolle. Registrierung und Authentifizierung erschweren es Hackern, auf Daten zuzugreifen. Weiterhin werden Firewall-Systeme unter die Lupe genommen. Auf Seite des Clients helfen Browsereinstellungen, Verbindungen zu

Servern sicherer zu machen. Wichtig ist dabei, immer aktuelle Browserversionen zu verwenden, bei denen bekannte Sicherheitslücken geschlossen sind.

Im Kapitel 5 werden Vorbereitungen für eine Überprüfung der in vorherigen Kapiteln beschriebenen Techniken und Kommunikationswege getroffen. Der Autor beschreibt die Installation zweier Server. Zum einen die Installation eines Windows 2003 Servers und zum anderen die Linux- Distribution von Suse, Version 9.1. Auf beiden Servern werden Dienste eingerichtet und konfiguriert. Auch die mitgelieferte Firewall wird aktiviert, mit dem Ziel den Server besser vor Eindringlinge zu schützen.

Im Kapitel 6, dem letzten Kapitel wurde der Versuch gestartet, Angriffsvarianten aus Kapitel 4 zu testen. Dazu ist ein Netzwerk von mindestens drei Rechnern nötig, um Verbindungen zwischen Client und Servern mitzuhören. Erstaunlich mit welcher wenig Aufwand und speziellen, aber im Internet zum Download freie Tools, Verbindungen mitgelesen werden können. Bei unverschlüsselten Protokollen war es eine Leichtigkeit Benutzerdaten aus den Datenpaketen herauszulesen.

Manche Angriffe, wie zum Beispiel DoS Angriffe konnten nicht simuliert werden, da eine weit aus höhere Anzahl von Rechnern dem Autor zu Verfügung hätte stehen müssen.

Auch in diesem Kapitel wurde exemplarisch Browserschwachstellen getestet mit manch verblüffendem Ergebnis.

Am Ende der Tests wird das Augenmerk weg von der Verbindungssicherheit auf die Serversicherheit gerichtet. Mit Hilfe geeigneter Software wird nach Schwachstellen und Lücken der Server im Blick auf die verschiedenen Dienste gesucht.

Insgesamt gesehen ist die Sicherheit der Server aber deutlich besser als die der Kommunikationsverbindungen.