Thema für Bachelorarbeit / Masterarbeit
Systematische Intrusion Detection

Die Herausforderung

In fast jedem Internetserver gibt es heutzutage Schwachstellen und Sicherheitslücken. Angreifer können diese dann ausnutzen, um den Server zu verändern, zu manipulieren oder, im schlimmsten Fall, personenbezogene Daten entwenden und missbrauchen. Es gibt nun eine große Anzahl möglicher Ursachen für solche Probleme, die von einer unvollständig oder fehlkonfigurierten Anwendung, veralteten Betriebssystem-Versionen bis hin zu unsicheren Zertifikaten reichen. Für den Endanwender aber auch für den nebenberuflichen Systemadministrator sind diese Probleme nicht zu überblicken. Dazu zählt meist auch der ganzheitliche IT-Sicherheitsansatz. Im Internet gibt es verschiedene Testseiten, die gezielte Abfragen auf Internetserver starten und über deren Sicherheitsprobleme Bericht erstatten. Aber auch diese Systeme helfen nur beschränkt und sie sind in der Regel auf einzelne Dienste (Web, Mail, DNS) der Server bzw. Teilbereiche der IT-Sicherheit spezialisiert (SSL/TLS, Securityheader, Patchlevel, etc.).

Wünschenswert wäre daher ein Meta-System, das die wichtigsten Testseiten regelmäßig und automatisiert anstößt und anschließend auf einfache und übersichtliche Weise Bericht über die bestehenden Schwachstellen und Sicherheitslücken und entsprechende Handlungsempfehlungen erstellt.

Aufgabenstellung

Je nach Art der Arbeit (Bachelor, Master, Projekt), nach Interesse und Vorbildung des Bearbeiters soll im Rahmen dieser Arbeit ein solches Testsystem aufgebaut werden und in Absprache mit einer Behörde des Landes Mecklenburg-Vorpommern für die Internetserver im Wirkungsbereich dieser Behörde eingesetzt werden. (Damit die dann durchgeführten Tests auch rechtlich zulässig sind, wird von den Systemverantwortlichen eine schriftliche Beauftragung zur Durchführung dieser Maßnahmen vorgelegt, in der diese Systeme per IP-Adresse / URL eindeutig benannt werden.).

Die Arbeit soll die folgenden Aspekte untersuchen:

1. Identifikation und Validierung der Testseiten und der durch sie geprüften Sicherheitsbereiche / Informationen
2. Zusammengefasste, automatisierte Abfrage der Internetserver über die Testseiten
3. Strukturiertes Zusammenfassen und Ablage der Abfrageergebnisse
4. Dokumentation, Auswertung und Gliederung der Ergebnisse nach verschiedenen Sicherheitsaspekten

Vergütung

Die erfolgreiche Umsetzung dieser Aufgabenstellung wird mit einer Vergütung in Höhe von 5.000 € durch die Landesbehörde unterstützt.

Ansprechpartner: Prof. Clemens Cap