Absichern von Onlinebanking und anderen Internetdiensten, die sensible Informationen verarbeiten

cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

Die besten Schutzmechanismen für Web-Applikationen auf der Serverseite sind machtlos, wenn die Browser der Anwender beispielsweise bereits mit Trojanern kompromittiert sind. Promon hat ein System entwickelt, mit Hilfe dessen die Browser der Anwender ohne vorherige Installation von Software für den Verlauf einer Sitzung und unter Kontrolle des Web-Servers gesichert werden können.

Eine der größten Herausforderungen in der IT-Sicherheit sind Trojaner- und Spyware-Angriffe auf das Endgerät (Client). Da Webseitenbetreiber weder Informationen noch Kontrolle über den Client haben, müssen sie darauf vertrauen, dass die Anwender die richtigen Maßnahmen gegen Hacker-Angriffe treffen. Die traditionellen Antivirus- und Authentifizierungs-Lösungen bieten jedoch keinen ausreichenden Schutz gegen die hochentwickelten Angriffe auf den Client. Es ist somit nur eine Frage der Zeit, wann das Endgerät mit Schadsoftware infiziert wird.

Promon Shield bietet Betreibern von Web-Applikationen bzw. Portalen die Möglichkeit, ihren Dienst auch auf dem System des Anwenders ohne Installation von Software zu schützen.

Promon Shield wird vom Anbieter in dessen Website integriert und dem Anwender auf diesem Weg zur Verfügung gestellt. Der Anwender muss weder Administrator-Rechte besitzen noch vorab Installationen vornehmen. Der Schutzmechanismus ist automatisch aktiv, auch hier ist nahezu keine Interaktion des Anwenders nötig. Um Kompatibilitätsprobleme auf dem Client zu vermeiden, arbeitet Promon Shield ausschließlich in der zu schützenden Anwendung und lässt alle weiteren Komponenten des Anwendersystems unberührt.

Dies gilt nicht nur für Web-Applikationen, sondern auch für Stand-Alone-Software-Programme. Der Anbieter des Programms integriert den Schutzmechanismus und stellt den Anwendern somit eine geschützte Software zur Verfügung.

Beispielsweise wurde Promon Shield in die multibankenfähige Online-Banking-Software Starmoney von Star Finanz integriert.

Um die Wirksamkeit des Promon-Schutzschilds zu überprüfen, haben Sicherheitsexperten des S-CERT vom Informationszentrum der Sparkassenorganisation (SIZ) das Programm einer Vielzahl von Angriffen ausgesetzt.

Die Untersuchung wurde in drei Phasen durchgeführt: In der ersten Phase lag der Fokus auf dem Ausspähen von Daten (Data Leakage). Mit vorhandenen Tools wie einem Keyboard-Logger wurde überprüft, ob sich mit deren Hilfe vertrauliche Daten ausspähen lassen. Neben sechs kommerziellen Keyboard-Loggern wurden auch Trojaner verwendet, die u. a. Keyboard-Logging-Funktionalitäten beinhalten. Die Untersuchung stellte fest, dass alle verschiedenartigen Keyboard-Logger-Angriffe durch das Promon-Shield erfolgreich abgewehrt wurden.

Darüber hinaus wurde in der zweiten Testphase zunächst mit aktuellen, weit verbreiteten Banking-Trojanern untersucht, inwieweit es möglich ist, bösartigen Programm-Code in den laufenden StarMoney-Prozess einzuschleusen und dort zur Ausführung zu bringen. Neben aktuell weit

verbreiteten Trojanern wurden dann bewusst auch ältere Varianten und Trojaner-Familien verwendet, die zurzeit nicht mehr im Umlauf sind, um auch die Schutzwirkung gegen bereits ältere Techniken zu verifizieren. Hierbei wurde festgestellt, dass das Promon-Schutzschild alle Trojaner erfolgreich abwehrte. Es konnte in den meisten Fällen damit erreicht werden, dass sich bösartiger Code in StarMoney-Software weder injizieren noch ausführen ließ. In einigen Fällen gelang es den Trojanern zwar, sich zu infiltrieren, jedoch gelang es ihnen danach nicht, entsprechend aktiv und damit bösartig zu agieren. So war StarMoney zum Teil nicht mehr startbar, wenn der Trojaner seinen Code injizierte.

Neben den zuvor aufgeführten konkreten Angriffen sind weitere Szenarien mit dem Ziel denkbar, ein tiefergehendes Verständnis der implementierten Schutzmechanismen zu erhalten und darauf aufbauend, neue Angriffe zu entwickeln. Zu diesen weitergehenden Szenarien zählt das Reverse Code Engineering. Typischerweise werden dazu Debugger eingesetzt, die die Software durchlaufen, analysieren und nachkonstruieren.
Im Rahmen der Untersuchungen wurde daher ebenfalls geprüft, ob und inwieweit Debugger in die StarMoney-Software eingebunden werden können, wenn diese durch das Promon-Schutzschild geschützt werden. Im Rahmen der Untersuchungen zeigte sich, dass es grundsätzlich möglich war, StarMoney.exe im Debugger zu laden und zu starten. Zur Laufzeit erkannte StarMoney jedoch, dass es nicht vom korrekten StarMoney-Hauptprogramm des Herstellers Star Finanz gestartet wurde und brach die weitere Programmausführung ab. Das Promon-Schutzschild erkannte in allen Fällen die Reverse Code Engineering-Angriffe und verhinderte ein schrittweises Debuggen von StarMoney, allerdings war ein punktueller Einblick in den Programm-Code und die Speicherinhalte mit Hilfe dieser Technik möglich.

Zusammenfassend lässt sich sagen, dass das von der Star Finanz implementierte, präventive Promon-Schutzschild in StarMoney einen sehr guten, umfangreichen Schutz bietet und für Angreifer eine hohe Hürde darstellt.