

Wie lassen sich Man-in-the-Middle-Angriffe erkennen?

Der elektronische Banküberfall ist alltäglich geworden. Dabei werden oft Schwachstellen ausgenutzt, die sich beim Anwender und nicht auf der Onlinebanking-Plattform befinden.

Vor allem müssen nun Massnahmen zur Erkennung des Missbrauchs ergriffen werden. *Urs Rufer*



Urs Rufer

ist Dipl. Informatik-Ing. FH und als Partner und Leiter Consulting & Projects bei terreActive AG für umfangreiche IT-Security-Projekte und Audits zuständig.

Die ersten Schwachstellen beim E-Banking befanden sich in der Software, die den Zugriff auf die Kontendaten der Kunden erlaubte. Durch einfache Manipulation der Anfrage konnte das Konto gewechselt und so auf vertrauliche Informationen zugegriffen werden. Sobald eine Schwachstelle behoben wurde, verlagerte sich der Angriff auf weitere Komponenten in der Kette der Systeme, die für die Erbringung der Dienstleistung verantwortlich war. In der Folge wurden Angriffe mittels SQL-Injection oder Cross-Site-Scripting entwickelt, die sofort durch geeignete Massnahmen wie etwa ein Web-Entry-Server verhindert wurden.

So ging der Wettlauf zwischen Angreifer und Verteidiger während Jahren hin und her. Mit dem Resultat, dass die bankseitigen Systeme und Anwendungen heute praktisch keine Schwachstellen mehr aufweisen. Deshalb ist inzwischen der Benutzer zum Ziel der Angreifer geworden. Da sich diese Systeme ausserhalb des Einflussbereichs der Anbieter befinden und die Angreifer mittlerweile sehr professionell und gut organisiert vorgehen, führt dies zu einer Zunahme der Vorfälle. Das Ziel der Bankinstitute ist dabei, solche Vorfälle zu verhindern und Missbräuche zu erkennen.

Wie soll die Bank reagieren?

Während erfolgreiche Phishing-Angriffe durch zusätzliche Authentisierungsmerkmale erschwert werden können, sind der Missbrauch von gültigen E-Banking-Sessions direkt im Browser oder in einer parallelen Verbindung zur Bank sehr schwer vermeidbar, solange die Computer der Kunden so anfällig für Schadprogramme sind und bleiben. Wie könnte also eine mögliche Reaktion der

Anbieter aussehen? Wie beim Kreditkartenmissbrauch, wo eine fixe Anzahl Missbräuche einkalkuliert sind und niemand auf den Komfort dieser Zahlungsmethode verzichten will, ist die Erkennung von Missbrauch durch Analyse der Transaktionen und Vergleich mit bekannten Mustern ein Ansatz zur Schadensbegrenzung.

Analog dazu können E-Banking-Systeme dahin ausgebaut werden, dass der Zugang

zur Anwendung und die anschliessenden Transaktionen analysiert werden und bei Verdacht auf Missbrauch eine vordefinierte Reaktion eingeleitet wird. Dabei ist denkbar, den Kunden telefonisch zu kontaktieren, die

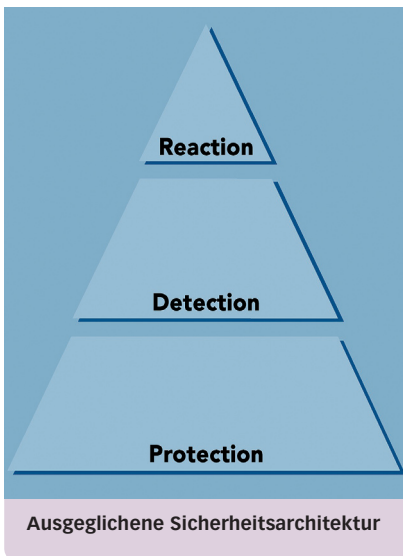
«Durch einfache Manipulation der Anfrage kann das Konto gewechselt und so auf vertrauliche Informationen zugegriffen werden.»

laufende E-Banking-Sitzung sofort zu unterbrechen oder die Vertragsnummer zu sperren.

Security Event Management

Im Zusammenhang mit einer ausgeglichenen Sicherheitsarchitektur (Protection, Detection, Reaction) hat sich der Begriff des Security Event Management als Schlüsseltechnologie im Detection-Bereich etabliert. Dabei wird versucht, durch Korrelation vorhandener Log-Informationen der Systeme und Anwendungen Sicherheitsevents zu modellieren und Unregelmässigkeiten beim Betrieb von Sicherheitsinfrastrukturen automatisch zu erkennen.

Angewendet auf den E-Banking-Bereich können Unregelmässigkeiten auf zwei Ebenen erkannt werden. Auf Applikationsebene kann Missbrauch aufgrund der Transaktion, typischerweise einer Zahlung oder Überweisung detektiert werden. Dabei können bestehende Analysen zur Vermeidung von Geldwäscherei herangezogen oder ein White-List-



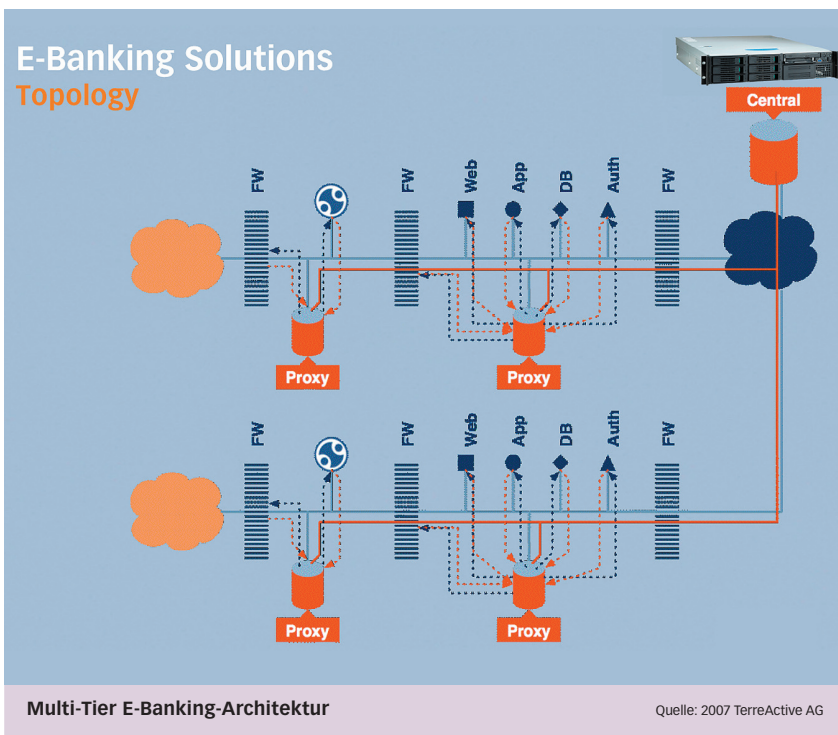
Mechanismus angewendet werden.

Leider haben solche Massnahmen einen negativen Einfluss auf den User-Komfort, was ihre Popularität stark mindert. Auf der Zugangsebene, wo der Kunde identifiziert und die gesamte Kommunikation verschlüsselt wird, lassen sich technische Details dieser Kommunikation aufzeichnen. Beim nächsten Verbindungsaufbau werden die neuen Daten mit den gespeicherten verglichen und bei Abweichungen eine Warnung (Security Event) ausgegeben. Ist beispielsweise ein anderer Browser im Einsatz, werden andere Verschlüsselungsparameter verwendet oder kommt die Anfrage aus einem Land (geografisches Abbilden der IP-

Adresse), das sich auf einer Blacklist befindet, lässt sich ein Event erzeugen, der dann die erwähnte Reaktion auslöst. Das Gleiche gilt selbstverständlich, wenn sich diese Parameter während einer laufenden Sitzung ändern. Die erforderlichen Daten lassen sich einfach aus dem Log eines Web-Entry-Servers und des Web-/Applikationsservers der E-Banking-Architektur extrahieren. Damit wird mit bestehenden Mitteln und bescheidenen Investitionen mehr Transparenz ins E-Banking gebracht und die Schadenssumme reduziert.

Was bringt die Zukunft?

Um die Sicherheit im E-Banking nachhaltig zu verbessern, muss der Client-Teil wieder in den direkten Einflussbereich des Anbieters gebracht werden, oder die verwendete Betriebssystem- und Browserumgebung muss so weit kontrolliert werden, dass jegliche Schwachstellen ausgeschlossen werden können. Ansätze gehen dahin, solche Umgebungen unveränderbar in virtuellen Umgebungen jeweils neu zu starten oder unterschiedliche Umgebungen für E-Banking, Gaming und Surfen zu unterhalten. Auf jeden Fall wird der Aufwand nicht kleiner, der Komfort hingegen schon. Und die Angreifer werden sich auch nicht zurückziehen, weshalb sich der Aufbau einer Security-Event-Management-Lösung zur Früherkennung von Missbrauch auch langfristig auszahlen wird. ■



Multi-Tier E-Banking-Architektur

Quelle: 2007 TerreActive AG