Auszug aus Kapitel 1 (Seite 1-5 von 1-60)

Der Banken-Hack

Die Aufgabe

Im Juni 2001 bekamen wir vom NDR den Auftrag die Sicherheit von Banksystemen und EC-Karten zu testen. Im Rahmen der Sendung ARD Ratgeber Technik sollte geprüft werden, wie sicher Homebanking heutzutage ist.
Die Sicherheitsfrage konnte man in zwei Richtungen formulieren:

1. Wie gut sind die Daten der Kunden geschützt, gibt es Angriffsmöglichkeiten auf einem Bankserver?
2. Wie sicher sind die Transaktionen, die beim Homebanking durchgeführt werden? Besteht dort eine Möglichkeit, Daten abzufragen, zu manipulieren, umzuleiten o.ä.?

Die Bedingung

Natürlich waren an diese Aufgabe bestimmte Bedingungen geknüpft, zu denen gehörten:

1. Es sollte kein Kunde geschädigt werden, was für uns bedeutete keine Transaktionen so zu manipulieren oder zu verfälschen, dass sie nicht stattfinden können.
2. Das Onlinebankingsystem der Banken sollte in seiner Funktion weder gestört, noch eingeschränkt sein.
3. Es sollte unauffällig geschehen, da man sonst Gefahr laufen würde, das die betroffene Bank vor dem möglichen Ausstrahlen der Sendung eine Einstweilige Verfügung erwirkt, um zu verhindern dass die Mängel aufgezeigt werden.

Vorgehensweise zur Lösung

Die Vorgehensweise für die ganze Sache sah zum Start wie folgt aus:
1. Zugangsweg zu Daten oder Server finden.
2. Eindringen in das System und Manipulations-Möglichkeiten erkunden.
3. Daten ausspähen
4. Transaktion manipulieren

Spontan fielen uns zwei Ansätze dazu ein:

- Zugriff auf den Webserver eines Instituts
- Trojanerplazierung bei Homebankingkunden und anschließend Zugriff auf den Server mit deren Daten

Leichter wäre, man greift auf den guten alten Trojaner zurück und spioniert ein paar PCs aus, um dann im richtigen Moment, wenn der Kunde Onlinebanking macht, zuzuschlagen. Nach ein paar Feldversuchen erschien uns diese Möglichkeit aber eher an den Haaren herbeigezogen. Man muss Kunden finden, denen einen Trojaner „zuspielen“, der Trojaner muss installiert werden usw. . Schließlich muss ein solcher Ansatz auch noch ständig überwacht werden, denn nach dem Ausspähen muss man ja auf die nächste Homebanking-Transaktion warten. Außerdem hätte das Auffliegen einer solchen Aktion derart viel Presserummel verursacht, dass der eigentliche Test kaum noch hätte stattfinden können.

Die sinnvolle Möglichkeit konnte dann also nur der Zugriff auf den Webserver eines Geldinstitutes sein. Das löste natürlich heftige Kontroversen aus, mit Blick auf die §202 und §263 des StGB. Im Endeffekt entschlossen wir uns dafür, es ersteinmal zu versuchen evtl. würden wir ja auf kleinere Lücken stoßen, die man aufzeigen könnte. Natürlich hatte keiner von uns ein genaues Konzept, wie man vorgehen sollte, und wir wussten auch nicht, wie die Systeme der Banken konkret aussehen. Also hieß es erst einmal Informationen sammeln.

Zugangsweg - Informationsrecherche über Social Engineering

Zunächst versuchten wir, über persönliche Kontakte an solche Informationen zu kommen. Es ist aber recht schwierig den eigenen Kundenberater nach Server-Details zu fragen, meist weiß er es selbst nicht oder schöpft Verdacht. Also musste eine andere Lösung gefunden werden.

Zuerst mußten wir uns über die Strukturen in der Bank informieren, dazu schrieben wir eine Mail an mehrere Banken, in der wir vorgaben Kunde zu sein, der von einem Hackerangriff auf den Webserver einer anderen Bank gehört hatte und nun von seiner Bank wissen wollte, wie sicher sein Geld bzw. das Online-Banking seiner Bank denn nun wirklich ist.
Die Mail musste so geschrieben werden, dass sie aufgrund des Aufbaues nicht mit einem Supportstandarttext beantwortet werden konnte. Also gaben wir uns netzwerktechnisch versiert und fragten zu guter Schluss frech nach, wie die Bank das Online-Banking und somit unsere Daten richtig schützt. Diese Mail schickten wir an 10 große Geldinstitute mit Onlinebanking-Portal.
Nach ca. 5 Tagen und 9 Standardmails mit dem Inhalt „Keine Sorge, Ihr Geld ist nirgends so sicher wie bei uns." Ihre XX –Bank“, ereichte uns überraschend folgende Mail aus der wir neben dem bekannten Satz „Keine Sorge, Ihr Geld ist nirgends so sicher wie bei uns." Folgendes entnehmen konnten:

--1. Die Infrastruktur

Die Infrastruktur des Online Banking Systems für die XY-Bank ist wie folgt ausgelegt:

Alle Anfragen für das Online Banking werden über einen Cisco-Router geführt, der nur den Port 443 (HTTPS-verschlüsselte Datenübertragung mit SSL) bereitstellt und nur Anfragen an den exklusiv dem Online Banking System vorgeschalteten Plug-Gateway mit integriertem Firewall durchlässt. Somit erfolgt eine gesicherte und verschlüsselte Übertragung der Banking Daten des Kunden ab Aufruf der Online Banking Seite.
Hinter dem Cisco-Router befindet sich zusätzlich ein exklusiv für die XY-Bank installiertes Intrusion Detection System, das Angriffe gegen das System protokolliert, meldet und auch abwehrt.

Das Plug-Gateway, das sich zwischen Cisco-Router und Bank Web-Server befindet nimmt folgende Aufgaben wahr:

Physikalische Trennung der Internet-Verbindung und der Verbindung zum Web-Server: Bei Aufbau einer Verbindung von einem externen System wird die Verbindung entgegengenommen und eine von der aus dem Internet kommenden Verbindung physikalisch getrennte Verbindung zum Web Server hergestellt, so dass keine Rückschlüsse auf die

internen Systeme von außen möglich sind

Alle Pakete werden durch die Firewall des Plug-Gateways analysiert und nur bei Erfüllung der Filterregeln (nur HTTPS Zugriffe sind gestattet) an den Webserver des Online Banking Systems durchgereicht. Weiterhin ist der Datenbankserver physikalisch vom Web-Server und der Anwendung getrennt, so dass ein direkter Zugriff vom Internet auf die Datenbank überhaupt nicht möglich ist.

2. Sicherheit
Ergänzend zu den Sicherheitsmaßnahmen der Infrastruktur (Hardware und Systemsoftware-Ebene) sind noch folgende Sicherheitsvorkehrungen für das Online Banking der Bank getroffen worden:
Die Verbindung zwischen Client und Server wird mit maximaler Verschlüsselung von 128 Bit aufgebaut. Dieser Standard gilt für Transaktionen im Internet als sicher.
PINs in der Datenbank sind verschlüsselt abgelegt und erlauben keinen Rückschluss auf die tatsächlich verwendete PIN.

4. Sicherheitsanalyse von Administrator vom 06.2001
Der Administrator hat 06.2001 selbst einen Scan gegen den öffentlichen Internetauftritt und das Online Banking System der Bank durchgeführt. Wie erwartet ist dabei das Online Banking System nur per https (Port 443) für den per 128 Bit verschlüsselten, sicheren Zugriff im Internet erreichbar. Der Versuch, weitere Informationen (Fingerprint) über das System (Hardware, Betriebssystem, Server etc.) zu erhalten, schlug fehl.—

Dieses ist ein sehr gelungenes Beispiel für Social Engineering, das uns einen sehr detaillierten Einblick in die Sicherheitsmaßnahmen der Bank-Webserver gab. Unsere Mail wurde mit hoher Wahrscheinlichkeit an einen Administrator des zuständigen Rechenzentrums weitergeleitet, der uns zu unserer grossen Verwunderung mit technischen Details überschüttete.

Scans für Detailinfos – Feinarbeiten

Was aus dem Mail nicht hervorging, was uns aber aufgrund einiger Scans (näheres s.u.) schon klar war, ist, dass alle Banken verschiedene Finanzsoftware-Produkte benutzen z.B. OFX (Open Financial Exchange). Diese sorgen z.B. für Integrationsschecks der Kontonummer, PINs und TANs und verwalten desweiteren die Kundeninformationen. Da sich nur spärliche Informationen zu dieser Server-Client Software finden ließen, wurde uns klar, dass wir nur über die Login Seite einer Bank an Kundendaten kommen könnten. Selbst wenn es möglich wäre, an Daten aus der OFX Datenbank heranzukommen, bliebe weiter unklar, ob diese nicht evtl. verschlüsselt sind etc..

Suche nach dem richtigen Ziel

Die Idee war also eine größere Bank zu finden mit direktem Anschluss des Servers zum Onlinebanking, um dort die Login Seiten so zu verändern, dass sämtliche Eingaben in eine Log-Datei wandern. Die Frage war nur, welche Bank?

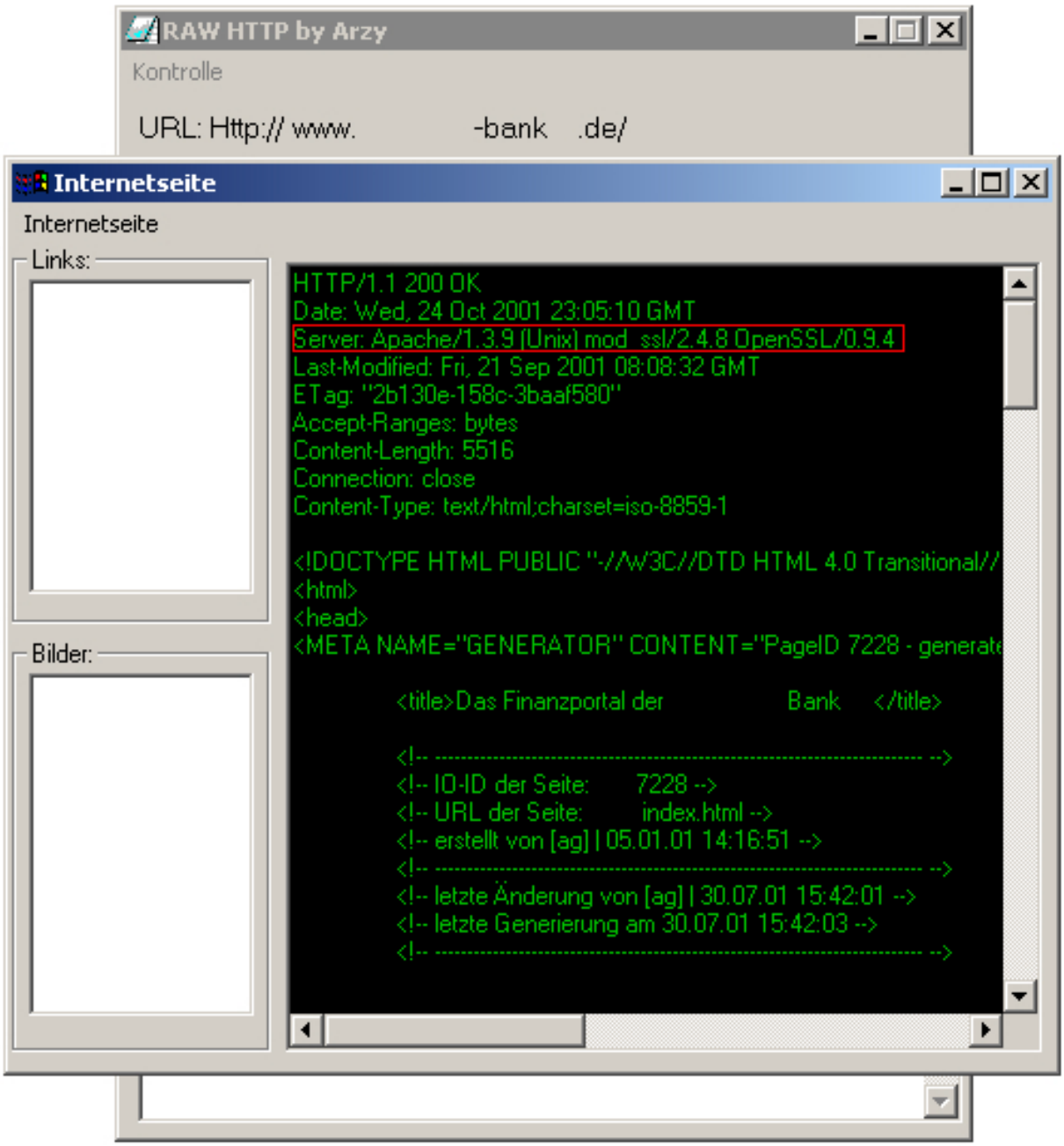
Sparkassen – Zuviel Kontrolle auf dem Server

Die Sparkassen schieden nach einem kurzem Blick auf die Infrastruktur aus, den bei ihnen ergab sich folgendes Problem, zwar hat fast jede Sparkasse eine eigene Seite doch das direkte Online-Banking wird über ein Rechenzentrum durchgeführt. Beispiel: www.ostspa.de der Server dieser Seite steht in Schwerin, die eigentliche Seite zum Login der Sparkassen Kunden auf ihr Konto läuft aber unter folgender Adresse https://ww2.homebanking-mecklenburg-

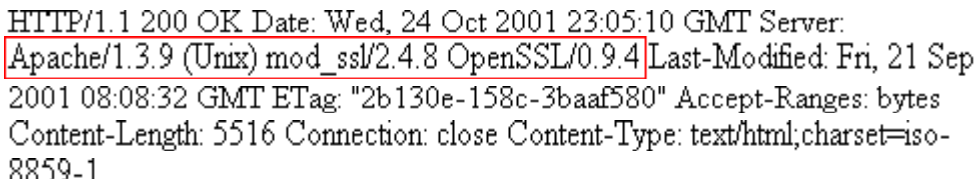
vorp.de/cgi/anfang.cgi/Ostseespk_Rostock, wobei sich dieser Server bei der DVG in Hannover befindet. Ein Angriff dort war uns etwas heiß, da z.B. in Hannover fast jede Sparkasse im Norden Deutschlands gehostet war und man davon ausgehen konnte, dass die Admins „auf den Rechnern „sitzen“ würden“ und schon ein Scan zu Testzwecken Aufmerksamkeit erregen würde.

Recherche: IIS Server gesucht

Also mußten wir unser Augenmerk auf größere Banken richten. Da es in der gesuchten Form eigentlich nicht so viele gab, konnten wir damit anfangen, jede einzelne Bank zu untersuchen. Für diesen Hack kam eigentlich nur ein IIS Server von Microsoft in Frage, da für diesen unseres Erachtens die meisten Exploits bekannt sind. Wir scannten also einige Banken ab, um nach den jeweiligen Servern zu schauen. Dazu benutzten wir das Tool RAW http (www.hackerzbook.de)



RAW HTTP



Anhand von RAW http ließen sich diverse Bankportale abscannen, um einen für den Angriff geeignetes System zu finden.

Es lieferte uns die wichtigsten Informationen über die Webserver der einzelnen Banken und Sparkassen.

Nach tagelangem Scannen fand sich die Seite der XXXXXXXXXXXbank, ein Portal über das sich sowohl die Kunden der XXXXXXXXXXXbank als auch die des Tochterunternehmens, der XXXXXXX- und XXXXbank, einloggen konnten.