HELPDESK

Sicherheit von Online-Banking

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

ILLUSTRATION: CW/THÜ

Frage: Wie sicher ist Online-Banking wirklich? Sind grundsätzliche Ängste noch begründet?

Modernes Online-Banking ist technisch gesehen verhältnismässig sicher. Die Verschlüsselungsmechanismen in solchen Umgebungen können als sehr stark klassifiziert werden. In den meisten Fällen wird dabei auf offene und über Jahre bewährte Mechanismen gesetzt, die selbst durch Regierungen für den Austausch und die Ablage hochsensibler Daten genutzt werden (z.B. DES/AES, MD5/SHA1). Nur ganz wenige Angreifer bringen das für eine kryptoanalytische Attacke auf diese Ebene erforderliche mathematische Geschick mit. Gelegenheitsangreifer sind mit derlei Mechanismen überfordert und werden andere Ansätze und Angriffsflächen suchen müssen.

Ein Angriff auf eine Authentisierung ist der Klassiker in geschützten Umgebungen. Bruteforce-Attacken versuchen durch das Ausprobieren sämtlicher Zeichenkombinationen der Passwörter einen legitimen Zugang zu finden. Die Zeitdauer, die eine solche stumpfsinnige Attacke erfordert, ist jedoch enorm gross. Bei einer nummerischen PIN mit vier Stellen ist ein Schlüsselraum von 10 000 Möglichkeiten gegeben und damit zirka 5000 Versuche erforderlich. Werden kurzlebige TAN (Transaktions-Nummern) oder SecurID-Token sowie automatische Kontensperrung nach mehreren fehlerhaften Authentisierungsversuchen eingesetzt, führt auch diese Methode für einen Angreifer nicht zum Erfolg. Komplexe und häufig geänderte Passwörter sind eine zusätzliche Hürde, die ein Nutzer errichten kann.

> «Die Sicherheit von Online-Banking scheitert meistens an der Leichtgläubigkeit der Nutzer.»

Direkte Angriffe auf Webserver und -applikationen des Online-Bankings sind naheliegend. Pufferüberlauf-Schwachstellen oder SQL-Injection sind ein beliebtes Mittel, um erweiterte Rechte auf einem Webserver zu erlangen. Die Chancen, derlei Schwächen in einer gut behüteten Umgebung zu finden – und Banken werden mittels periodischer Sicherheitsüberprüfungen um diesen Status in ihrem Online-Banking bemüht sein – ist relativ gering.

Ein gewiefter Angreifer wird viel eher den Privatrechner des Nutzers attackieren und darüber eine Hopping-Attacke versuchen. Schlecht abgesicherte Privat-PCs werden sodann als Zwischenstationen missbraucht und dadurch andere Ressourcen mit legitimen Zugriffsrechten, wie halt eben das Online-Banking, angesteuert. Remote-Control-Utilities wie das klassische Subseven werden dabei nach erfolgreichem Einbruch als Hintertür installiert und garantieren fortwährenden Zugang auf das übernommene System. Mit Patches stets auf dem neuesten Stand gehaltene Rechner, eine aktualisierte Antiviren-Software sowie eine gut umgesetzte Firewall-Komponente wird das Risiko eines derartigen Missbrauchs minimieren.

Die grösste Gefahr im Online-Banking ist und bleibt damit vorerst der Mensch an sich, der durch psychologische Tricks manipuliert und zu kompromittierenden Handlungen bewegt werden kann. Ein Benutzer, der durch die Leichtgläubigkeit gegenüber einem Phishing-Mail zum ungewollten Opfer wird, ist viel eher gegeben als eine ernstzunehmende Schwachstelle auf einem Webserver oder in einem Verschlüsselungsalgorithmus.

Sucht man ein Online-Angebot auf, gilt es vor der Nutzung dessen auf einige Merkmale zu achten. In der Adresszeile des Webbrowsers sollte die richtige URL der Webseite ausgegeben werden. Wird HTTPS/SSL genutzt, sind Fehlermeldungen in Bezug auf das Zertifikat (z.B. fehlerhafte URI) ernst zu nehmen. Sensitive Daten nur herausgeben, wenn es sinnvoll erscheint. Solange der gesunde Menschenverstand während des Online-Bankings mitsurft und die Banken auch weiterhin ihre Hausaufgaben machen, kann also von sicherem Online-Banking gesprochen werden. ■

Der Autor
Marc Ruef ist Buchautor und Security Consultant beim Sicherheitsunternehmen Scip AG, Zürich, www.scip.ch.

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch