Antiviren Apps nicht mehr erkannt werden. So reichen simple Umbenennung der Schad-Dateien oder minimale Modifikationen der Schad-Software aus, um von der Antiviren-App als unbekannt eingestuft zu werden. Die Schad-Software ihrerseits verliert dadurch nicht an Gefahrenpotenzial und kann ihre volle Wirkung auf dem ungeschützten Gerät entfalten. Damit steigt das Risiko sowohl für den Privatnutzer als auch für diejenigen Unternehmen, die den Einsatz privater mobiler Endgeräte im Unternehmensumfeld erlauben. Die AISEC-Forscher fassen ihre Ergebnisse in einem Technical Report zusammen. Dieser steht kostenlos unter *http://ais.ec/techreport* zum Download bereit.

Android-Bankraub: Schad-App hat es auf mTANs abgesehen

Gemäß einer Mitteilung von G Data (vom 24.04.2013)haben es Cyber-Bankräuber aktuell auf Android-Mobilgeräte abgesehen, um mTAN- und PIN-Nummern für Online-Bankkonten zu stehlen. Hierzu versuchen die Kriminellen mit Hilfe einer angeblichen Postbank-Mail die Nutzer zur Installation einer „SSL Zertifikat App" zu bewegen. Wählen die Anwender den in der E-Mail enthaltenen Link über ihr Smartphone oder Tablet an, gelangen sie auf eine Internetseite, auf der die vermeintliche SSL-Zertifikats-App und eine Installationsanleitung bereit stehen. Die schädliche Anwendung, die angeblich für mehr Sicherheit beim mobilen Online-Banking sorgen soll, späht nach der Installation die mTAN- und PIN-Nummern aus und versendet sie an die Täter. Kriminelle sind so in der Lage, Online-Bankgeschäfte zu manipulieren und bei Überweisungen Geldbeträge auf andere Konten umzuleiten. Kunden, die Ihr Android-Gerät mit G Data MobileSecurity 2 absichern, sind vor dem Schädling geschützt.

Beim Zwei-Wege-Authentifizierungsverfahren kommen u.a. auch Smartphones und Tablet-PCs zum Einsatz. Hierbei wird die Transaktionsnummer (TAN) von der Bank per SMS zum Smartphone oder Tablet gesendet. Für die Bankräuber 3.0. sind diese Geräte daher ein lohnende Angriffsziele, da viele Anwender auf eine Sicherheitslösung für ihr Mobilgerät verzichten.

Im aktuellen Fall geben die Täter sich als Kundenbetreuer der Postbank aus und versenden millionenfach gefälschte Service E-Mails mit der Aufforderung zur Installation der vermeintlichen „SSL Zertifikat App". Statt einer Banking-Sicherheits-App, wird ein Schadprogramm installiert, das alle empfangenen mTANs umgehend an die Kriminellen weiterleitet.

Der im E-Mail-Text enthaltene Link leitet bei einem Mobilegerät auf eine präparierte Webseite mit einem Postbank-Banner weiter, auf der die angebliche Sicherheits-App und eine Installationsanleitung hinterlegt sind. Wird die Webseite über einen PC aufgerufen, erscheint nur ein Hinweis, dass die Installation des Zertifikats erfolgreich war.

Nach der Installation der App verlangt die Anwendung vom Nutzer die Eingabe der Kontonummer und PIN-Nummern. Darüber hinaus fordert das Programm eine Reihe von Berechtigungen ein, die u.a. den Zugriff auf empfangene SMS-Nachrichten erlaubt. Die Täter sind so in der Lage, Daten zu stehlen, die für Online-Bankgeschäfte benötigt werden. Die Cyber-Bankräuber sind so in der Lage Überweisungsvorgänge zu manipulieren.

Leitfaden mit Analysen und Erklärungen der Angriffsarten bei Websites

In letzter Zeit sind erneut zahlreiche Hackerangriffe auf Internetseiten von Banken, Unternehmen und öffentlichen Institutionen bekannt geworden. Doch auch weniger prominente Websites weisen vielfach erhebliche Sicherheitslücken auf, dies ermittelte das Security-Beratungshaus mikado ag in einer eigenen Untersuchung (veröffentlicht am 22.04.2013). Dabei wurden Websites über automatisierte Penetrationstests auf mögliche Schwachstellen analysiert und in fast jedem zweiten Fall Sicherheitslücken der höchsten Risikostufe gefunden.

Das Beratungshaus hat daraus abgeleitet einen 15-seitigen Leitfaden unter dem Titel „Analyse und Erklärungen der Angriffsarten von Websites" herausgegeben. Er stellt nicht nur die Ergebnisse der Penetrationsstudie mit einer Darstellung des Verbreitungsgrades der Schwachstellen auf den untersuchten Websites nach Gefährdungskategorien dar, sondern bietet zudem eine Beschreibung der wichtigsten Angriffsarten. Sie werden mit zahlreichen Beispielen ergänzt. Dazu gehört etwa, dass die Bundesanstalt für Arbeit durch die Angriffsmethode „Improper Parameter Redirection" geschädigt wurde, bei der mittels eines präparierten Weiterleitungs-Links Besucher auf eine fremde Webseite gelotst werden, um dort Phishing-Angriffe durchführen zu können. Die Angriffsart „Blind SQL Injection" wiederum wurde für einen Angriff auf die Internetpräsenz von Sony genutzt, bei dem eine Million Kundendaten erbeutet wurden.

„Schwachstellen auf Webseiten werden vielfach unterschätzt, da viele Angriffsarten in ihrer Wirkungsweise nicht ausreichend bekannt sind", begründet Dürr die Herausgabe des mikado-Leitfadens. Deshalb werden in der Praxishilfe ausgehend von den Ergebnissen der Penetrationsstudie einige der verbreitetesten Angriffsarten ausführlicher erläutert und mit Links zu weiteren Informationen versehen.

Den 15-seitigen Leitfaden „Analyse und Erklärungen der Angriffsarten auf Websites" können Interessenten kostenlos unter *www.midas-scan.com/downloads/leitfaden-penetrationsstudie/* herunterladen.

ESET Secure Authentication: Sicherer Zugang zu VPN und Outlook Web App

Mit ESET Secure Authentication stellte der Antivirenhersteller ESET am 19.04.2013 eine erweiterte Zugangskontrolle für VPN-Verbindungen und Outlook Web App vor. Will sich der Anwender über sein Notebook einloggen, generiert das Tool ein Einmal-Passwort und zeigt es auf dem Smartphone an. Dieses muss er bei der Anmeldung zusätzlich zum statischen Passwort eingeben, um Zugang zu erhalten.

Diese 2-Faktor-Authentifizierung hebt Notebooks mit externer Netzwerkanbindung auf ein höheres Sicherheitsniveau. Statische Passwörter erweisen sich immer öfter als leichte Beute für Hacker – insbesondere beim Verlust des Geräts. Die Ausweitung des Sicherheitssystems auf zwei Passwörter, die sich zudem auf unterschiedlichen physischen Devices befinden, stellt für Cyberkriminelle eine deutlich größere Hürde dar. Das Verfahren ähnelt der mTan beim Online-Banking.