Symantec verrät Hacker-Tricks – Die heimlichen Methoden der Cyber-Verbrecher

Cyberverbrecher haben es bevorzugt auf Kreditenkarteninformationen abgesehen, so ein Ergebnis des "Report on the Underground Economy". Im magnus.de-Videointerview verrät Symantec-Hackerexperte Stefan Wesche Tricks und Kniffe der Cyber-Verbrecher.

von Ulrich Klein – powered by PCgo! – vom 01.12.2008

Kreditkarteninformationen gehören nach den Sicherheitsexperten von Symantec zu den am meisten angebotenen Produkten und Servicekategorien der Hacker. 0,10 bis 25 Doller zahlen Hacker-Kunden hier, wenn die Karte über ein Limit von etwa 4000 US-Dollar aufweist. Laut Report liegt der potenzielle Maximalwert sämtlicher auf sogenannten Untergrund-Servern angebotenen Kredtikarten bei 5,3 Milliarden US-Dollar.

"Die Server als solche sind zwar einfach zu finden, die Herausforderung liegt mehr darin, die Benutzer dieser Server als Personen zu identifizieren", beschreibt Wesche die Schwierigkeit, Hacker dingfest zu machen. Der Trend im Hacker-Untergrund gehe zur Nutzung von IRC-Server, bei denen es sich um rein private Netzwerke handle, wo Zugangsdaten und Server-Adresse via Mundpropaganda die Runde machen.

Großer Reibach trotz Finanzkrise

Mit einem Anteil von 20 Prozent sind laut Symantec Kontonummern beziehungsweise Kontenzugangsdaten die zweithäufigste Kategorie inserierter Waren und Dienstleistungen. Während Konteninformationen für zehn bis 1.000 US-Dollar zu haben sind, sind die "geknackten" Konten durchschnittlich mit etwa 40.000 US-Dollar gedeckt.

Mit ein Punkt für die schwierige Verfolgung sei die große Anonymität im Internet, erklärt Wesche. "Insbesondere kann man sich bei vielen Foren anmelden, indem man nur einen Namen angibt", der falsch sein könne, sowie eine falsche E-Mail-Adresse. "Wenn man es auf die Spitze treiben will, kann man sich sogar von einen öffentlichen Internet-Cafe aus einloggen, so dass sich die IP-Adresse auf keinen Fall zuordnen lassen könnte". Aufgrund dieser Komplexität sei es für staatliche Organe so schwer, Schritte einzuleiten und Personen festzunehmen, um einen Handel mit gestohlenen Informationen im Internet zu unterbinden, weil der Cyber-Kriminelle seine Identität und Aufenthaltsorte ständig wechsle.

Das am häufigsten gehandelte Exploit während des Beobachtungszeitraums waren laut dem Report Site-spezifische Schwachstellen auf den Internetseiten von Finanzinstituten und Finanzdienstleistern, die im Schnitt für 740 US Dollar angeboten wurden. Die Preisspanne lag zwischen 100 und 2.999 US-Dollar. Phishing Scam Hosting Services kosteten im Schnitt zehn US-Dollar, insgesamt reichte die Spanne von zwei bis 80 US-Dollar.

"Der erste Schritt, den ein Cyber-Krimineller unternimmt, ist der Versuch, Zugang zum Rechner des Nutzers zu erlangen", beschreibt Wescher die Taktik der Online-Verbrecher. Sei der Zugriff auf den Rechner hergestellt, sei für den Hacker jegliche Art von Angriff auf vertrauliche Daten durchführbar.

Die übelste Masche

Die Angriffsmethoden der Hacker sind vielfältig. "Das Trickreichste, wovor man sich am schlechtesten schützen kann sind momentan so genannte Drive-By-Downloads", verrät Wesche. Dabei handle es sich um einen Angriff, wo eine legitime Website manipuliert werde. "Rein optisch entspricht die Website der Originalseite, allerdings wird in die Seite ein unsichtbarer Schad-Code eingepflanzt". Betrachtet der Nutzer die Seite im Browsser werde im Hintergrund automatisch ein Trojaner auf den Rechner heruntergeladen.

Bei einem solchen Trojaner könne es sich um einen Keylogger handeln, der nach der Installation jegliche Art von Tastatureingabe auf dem Rechner protokolliere und damit alle Zugangsdaten erhalte. So könne der Trojaner Daten zu Bankkonten und Kreditkarten später an den Hacker senden.

Zum Schutz empfiehlt Wesche Transaktionen nur auf vertrauenswürdigen Seiten zu tätigen. "Allerdings ist die Erkennung von gut gefälschten Seiten heute immer schwieriger", weiß Wesche um das Dilemma. Zudem sollten Nutzer eine Sicherheitssoftware wie Norten Security 2009 installieren, das einen Schutz vor Drive-by-Downloads bieten soll. Weiterhin sei es wichtig, seine Bank und Kreditkarteninformationen regelmäßig auf Unregelmäßigkeiten zu kontrollieren. Persönliche Daten sollten Internetnutzer online sparsam veröffentlichen, wenn keine zwingende Veranlassung bestehe.

Wesche prognostiziert für die Zukunft eine Zunahme an Trojanern, die dem Zweck dienen, an persönliche Informationen von Nutzern zu kommen. Symantec wisse, dass ein Trojaner einfach zu bekommen sei. Für 23 US-Dollar könne ein Trojaner den Besitzer wechseln.

Basis des Symantec 'Report on the Underground Economy' sind Daten, die von der Symantec Security Technology and Response Organisation (STAR) zwischen dem 1. Juli 2007 und dem 30. Juni 2008 von Untergrund-Servern erhoben wurden.