Arbeitsgruppe Identitätsschutz im Internet

Bundesamt für Sicherheit in der Informationstechnik

Forscher diskutieren Gefahren, Trends und Lösungen des Online-Bankings

Interdisziplinäres Symposium – Phishing und Online-Banking – Gefahren, Trends, Lösungen – 27. April 2006 – Zentrum für IT-Sicherheit, Bochum

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Arbeitsgruppe Identitätsschutz im Internet (a-i3) an der Ruhr-Universität Bochum veranstalteten am 27. April 2006 das 1. Interdisziplinäre Symposium zu Phishing und Online-Banking. Ziel der Expertentagung war es, aktuelle Sicherheitsprobleme im Online-Banking und Lösungsansätze hierzu aus technischer und juristischer Sicht zu erörtern. Experten aus Bankwesen, Rechtswissenschaft und Technik waren eingeladen, um über zukünftige Gefahren, die Strafbarkeit des Phishing, Haftungsfragen und mögliche Gegenmaßnahmen zu diskutieren.

Phishing ist auch in Deutschland im Lauf des Jahres 2005 ein ernst zu nehmendes Problem geworden. Es umfasst den Diebstahl von Zugangsdaten (PIN/TAN), die Anwerbung von „Finanzagenten“ zum Zweck der Geldwäsche, und eine ständige „Verbesserung“ der Angriffsmethoden (SPAM-Versand, Botnetze, Trojanische Pferde).

Entsprechend ihrem interdisziplinären Charakter wurde die Tagung durch die Dekane der beteiligten Fakultäten der Ruhr-Universität, Prof. Dr. rer. nat. Ralf Peter Brinkmann (Elektrotechnik und Informationstechnik) und Prof. Dr. Roman Seer (Rechtswissenschaften) eröffnet. Anschließend wurden die Teilnehmer des Symposiums durch die Veranstalter Prof. Dr. Georg Borges (a-i3, Bochum) und Frank Felzmann (BSI, Bonn) begrüßt, die die Tätigkeiten ihrer Organisationen im Bereich des Phishing vorstellten.

Im ersten Vortrag berichtete Christoph Fischer (BFK edv-consulting, Karlsruhe) über aktuelle Phishing-Fälle, und verglich die Risiken im Online-Banking in Deutschland mit denen in Europa. Sein Fazit war, dass Phishing durch speziell für Banken zugeschnittene Malware rasant zunehmen wird.

Prof. Dr. Jörg Schwenk (a-i3, Bochum) stellte eine Klassifikation bislang untersuchter Phishing-Angriffe vor. Die meisten Angriffe können in zwei Phasen unterteilt werden: In der 1. Phase wird der Kunde auf eine gefälschte Webseite geleitet (z.B. durch gefälschte E-Mails oder Pharming-Angriffe), in der 2. Phase wird durch vertrauensbildende Designelemente versucht, den Benutzer zur Preisgabe seiner Zugangsdaten zu bewegen. Verschiedene Verbesserungen des TAN-Verfahrens (iTAN, eTAN, mTAN) wurden in Bezug auf Man-in-the-Middle Attacken hin untersucht, und die Sicherheit von eTAN und mTAN gegen heute vorstellbare Phishing- und Pharming-Attacken festgestellt.

Dr. Maximillian Dornseif von der Universität Mannheim ging speziell auf die Problematik der Malware im Zusammenhang mit Phishing ein. Er betonte die Verfügbarkeit von Zero-Day-Exploits für alle Rechnerplattformen, und die Tatsache, dass herkömmliche Virenfilter gezielte Malware-Attacken nur schwer erkennen können.

Der Strafbarkeit von Phishing und dem damit verbundenen Geldtransfer widmete sich PD Dr. Carl-Friedrich Stuckenberg, LL.M. (a-i3, Bonn). Er vertrat die Ansicht, dass alle Phasen einer klassischen Phishing-Attacke nach geltendem deutschen Recht strafbar sind, betonte jedoch auch, dass die Strafverfolgung mit großen Schwierigkeiten konfrontiert sei. Das Versenden der Mail ist seiner Ansicht nach als Fälschung beweiserheblicher Daten (§ 269 StGB) und als Betrug (§263 StGB) strafbar. Pharming-Angriffe fallen laut Stuckenberg unter den Straftatbestand der Datenveränderung gem. § 303a StGB. Auch der „Geldkurier“, der die „gephishten“ Gelder per Baranweisung ins Ausland transferiert, macht sich nach Ansicht Stuckenbergs strafbar: Einschlägig sei der Tatbestand der Geldwäsche (§ 261 StGB), der auch leichtfertig verwirklicht werden kann (§ 261 Abs. 5 StGB). Wird der Geldtransfer als „Nebenjob“ betrieben, sei sogar die Gewerbsmäßigkeit i.S.d. § 261 Abs. 4 StGB zu bejahen.

Die zivilrechtlichen Fragen der Haftung und Risikotragung bei Phishing wurden von Prof. Dr. Georg Borges (a-i3, Bochum) erörtert. In seinem Vortrag untersuchte er zunächst die materiellrechtlichen Fragen der verschiedenen Phishing-Varianten: Grundsätzlich trage die Bank das Risiko einer gefälschten Überweisung. Eine Rechtsscheinhaftung des Kunden kommt nach Borges in aller Regel nicht in Betracht. Allerdings begehe der Kunde eine zu einem Schadensersatzanspruch der Bank führende Pflichtverletzung, wenn er trotz offensichtlicher Verdachtsmomente seine Daten einem Phisher preisgibt. Beim Pharming hingegen scheidet laut Borges eine Pflichtverletzung

in der Regel aus. Offen sei die Frage, ob der Kunde zum Einsatz von aktuellen Virenschutzprogrammen u.ä. verpflichtet ist. Die Banken träfen Informationspflichten, sie seien aber wohl nicht zur Einführung neuer Sicherungssysteme verpflichtet. In prozessrechtlicher Hinsicht stellte Borges fest, dass ein Anscheinsbeweis zugunsten der Bank durch die theoretische Möglichkeit von Phishing und Pharming nicht grundsätzlich ausgeschlossen wird. Allerdings könne er im Einzellfall durch den Nachweis von Phishing und Pharming erschüttert werden.

Vor der Podiumsdiskussion wurden Konzepte für sicheres Online-Banking vorgestellt. Die Moderation übernahm Bert Ungerer (heise Verlag).
Herr Stein vom Sparkasseninformatikzentrum stellte den HBCI-Standard vor, der unter der Bezeichnung FinTS neue Technologien (XML) mit bewährten Sicherheitsfeatures (Chipkarten mit symmetrischer und asymmetrischer Kryptographie) vereint.
Die Herren Fischer und Heinen (Deutsche Postbank AG) stellten das gestufte Sicherheitskonzept der Postbank vor: Das iTAN-Verfahren, das alle Kunden der Postbank mittlerweile anstelle des bekannten TAN-Verfahrens nutzen müssen, und das kostenpflichtige mTAN-Verfahren mit verbesserten Usability- und Sicherheitsfeatures.
Dr. Jacobsen (BVR) stellte als praktische Implementierung des eTAN-Konzepts die Sm@rt-TAN Plus vor, die eine Balance zwischen Usability und Sicherheit durch Festlegung der einzugebenden Daten erlaubt.
Aus der akademischen Welt kommt Monn€yP€nny, eine Open-Source-Lösung, die von Prof. Dr.-Ing. Walter Roth (FH Südwestfalen) entwickelt wurde. Monn€yP€nny stellt eine vollwertige HBCI-Implementierung dar, und sichert sich gegen Malware durch Booten von CD ab.

In der anschließenden Diskussion wurden Fragen zum Entwicklungsstand der einzelnen Lösungen gestellt. Außerdem wurde am Beispiel der kostenpflichtigen mTAN diskutiert, wer die Kosten für mehr Sicherheit zu tragen habe.