Arbeitsgruppe Identitätsschutz im Internet

Tagungsbericht

a-i3/BSI-Symposium 2007: Identitätsmissbrauch in Onlinebanking & E-Commerce – Phishing, Trojaner & Co. – Angriffe, Schutzmaßnahmen, Haftung. Bochum, 24. - 25. April 2007

Am 24. und 25. April 2007 fand an der Ruhr-Universität Bochum das 2. interdisziplinäre Symposium der Arbeitsgruppe Identitätsschutz im Internet (a-i3) und des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu dem Thema „Identitätsmissbrauch in Onlinebanking & E-Commerce – Phishing, Trojaner & Co. – Angriffe, Schutzmaßnahmen, Haftung“ statt.

Das Problem des Identitätsmissbrauchs im Internet hat auch im Jahr 2007 nichts von seiner Brisanz verloren. Die Kriminellen entwickeln immer wieder neue Methoden um Passwörter zu erbeuten. Mittlerweile sind nicht nur Banken, sondern verstärkt auch andere E-Commerce Anbieter, vor allem Internet-Auktionshäuser, betroffen. Aktuelle Trends der technischen und rechtlichen Entwicklung wurden auf der Tagung durch zahlreiche Teilnehmer aus der gesamten Bundesrepublik, Österreich, der Schweiz und Luxemburg diskutiert.

Die Tagung wurde am ersten Tag durch Prof. Dr. Peter Awakowicz, den Prorektor für Forschung der Ruhr-Universität Bochum, eröffnet. Prof. Dr. Georg Borges, Sprecher des Vorstand der Arbeitsgruppe Identitätsschutz im Internet, und Frank Felzmann vom Bundesamt für Sicherheit in der Informationstechnik begrüßten die Teilnehmer und stellten die Tätigkeit ihrer Organisationen im Bereich Phishing vor.

Einführungsvorträge zu Technik und Angriffsszenarien von Phishing und Co. von Prof. Dr. Jörg Schwenk, und zu den Rechtsfragen des Phishing von Prof. Dr. Georg Borges erläuterten das umfangreiche Themenspektrum der Tagung.

In dem ersten Vortrag erläuterte PD Dr. Carl-Friedrich Stuckenberg, LL.M. (Universität Bonn/a-i3) Fragen der Strafbarkeit von Phishing und Geldtransfer. Er ging von der klassischen Phishing-Attacke aus, die er in vier strafbare Verhaltensseiten einteilte: Das Versenden der Phishing-Mail, das Betreiben der Phishing-Website, das Verwenden der „gephishten“ Daten und den Geldtransfer ins Ausland. In seinem Vortrag erläuterte Stuckenberg auch die Auswirkungen des Gesetzesentwurfs zur Bekämpfung der Computerkriminalität auf die Strafbarkeit von Phishing.

Dem folgte ein Vortrag von Staatsanwalt Marco Thelen (Staatsanwaltschaft Bonn) zu den Aspekten der Strafverfolgung bei Phishing an. Er berichtete, dass vor allem Phishing mit Hilfe von Trojanischen Pferden zunehme. Bei der Strafverfolgung von Phishing ergäben sich jedoch zahlreiche Probleme: Die Banken seien bei der Anzeigenerstattung und der Mitteilung von verfahrensrelevanten Informationen sehr zurückhaltend. Es gebe immer noch

Onlinebankingkunden, die auf Phishing-Mails antworten oder mit völlig ungesicherten Rechnern Onlinebanking betrieben. Im Gegensatz dazu seien die Phisher höchst professionell. Weitere Probleme ergäben sich durch die behördeninterne Zuständigkeitsverteilung, die die Zuständigkeit bezüglich des Finanzagent und der Phisher verschiedenen Staatsanwaltschaften zuordnen würde. Auch das Verbot der Onlinedurchsuchung würde die Ermittlungen hemmen.

Sodann referierte Dr. Stefan Werner (Dresdener Bank AG) zu der Haftung des Finanzagenten beim Phishing. Er nimmt an, dass der Überweiserbank ein Anspruch aus Eingriffskondiktion gegen den Geldkurier zusteht. Sind Empfänger- und Überweiserbank identisch, kann die Bank vor Rechnungsschluss diesen Anspruch über ihr Stornorecht aus Nr. 8.1 AGB-Banken selbst durchsetzen. Ein bereicherungsrechtlicher Anspruch des Phishing-Opfers gegen den Finanzagenten dürfte allerdings in der Regel ausscheiden.

Auf diesen Block rechtlicher Vorträge folgten die ersten technischen Redner. Prof. Dr. Jörg Schwenk (Ruhr Universität Bochum/a-i3) berichtete über Angriffstrends und Lösungsansätze. Er berichtete, dass das klassische Phishing rückläufig sei. Es gebe zahlreiche Lösungsansätze wie SPAM-Filter, Blacklisting, i-TAN. Allerdings sei die Bedrohung durch technisch hochwertigere Verfahren keinesfalls gebannt. Er ging auf die Bedrohung durch Pharming ein und stellte stellte Vor- und Nachteile möglicher Lösungsansätze (SSL, AV-Programme, DNS-Überwachung, DNSSEC, m-TAN) vor. Auch Malware stelle ein großes Problem dar. Als Lösung würden u.a. AV-Programme, schnellere Analyse, Javascript-Filter, Trusted Computing und e-TAN vorgeschlagen.

Dem folgte ein Vortrag von Hanno Langweg (Hochschule Gjøvik/Universität Bonn) zu der Sicherheit von HBCI und digitalen Signaturen. Er erläuterte, dass FinTS bzw. HBCI nur teilweise schütze. Es bestünde die Möglichkeit, dass lokale Malware die Eingaben überwacht und die Ausgaben oder die Dateiablage manipuliert. Beispielsweise könne die Anzeige dessen, was signiert wird manipuliert werden, so dass die falsche Kontonummer signiert, aber die richtige angezeigt wird.

Danach referierte Frank Sudholt (T-Mobile Produkt & Applikation Security) über die Sicherheit handybasierter Authentisierung. Er stellte die verschiedenen Authentisierungsmethoden vor, insbesondere propagierte er die Verwendung Mobiltelefonen. Diese sind mit einer Chipkarte ausgestattet, die zur Passwortgenerierung verwendet werden kann.

Der letzte Themenbock des ersten Tages war die verbesserte Sicherheit im Onlinebanking: Matthias Stoffel (SIZ-Informatikzentrum der Sparkassenorganisation GmbH) stellte nach einem Überblick über die aktuellen Angriffszenarien und –ziele Möglichkeiten vor, wie durch neue Authentifizierungsmaßnahmen erhöhte Sicherheit erreicht werden kann. Er

beschrieb in wie weit die i-TAN verbessert werden kann und erläuterte die Grundlagen von m-TAN, e-TAN und digitaler Signatur.

Danach informierte Ulrike Linde vom Bundesverband deutscher Banken über die Weiterentwicklung des TAN-Generators. Schon die Einführung des i-TAN-Verfahrens würde die Sicherheit für Privatkunden verbessern. Durch eine Weiterentwicklung könne eine noch höhere Sicherheit erreicht werden. Die Banken arbeiteten auch an einer Verbesserung der Authentisierungsverfahren für Geschäftskunden.

Die Veranstaltung wurde am zweiten Tag durch Dr. Udo Helmbrecht, den Präsidenten des Bundesamts für Sicherheit in der Informationstechnik, und Herr Prof. Dr. Peter Windel, den Dekan der juristischen Fakultät der Ruhr-Universität Bochum, eröffnet.

Wolfgang Weber (eBay GmbH) berichtete über Phishing im allgemeinen E-Commerce. Neben dem klassischen Phishing per E-Mail, käme auch so genanntes „Botnet-Phishing“ zum Einsatz. Werde ein Computer aus dem Internet genommen, trete bei dieser Variante ein nächster an seine Stelle. Gephishte Daten von Internet-Auktionshäusern würden entweder verkauft oder zum Warenbetrug verwendet. eBay versuche, den Betrugsversuchen entgegenzuwirken indem es das Sicherheitsbewusstsein seiner Nutzer steigere.

Thomas Roesseler, (World Wide Web Consortium (W3C), Arbeitsgebiet Datenschutz und Sicherheitstechnologien), referierte zum Thema „Die Zukunft der Internetbrowser“. Roessler stellte einige Beispiele vor, bei denen Sicherheitsfunktionen „am Browser vorbei entwickelt“ worden seien. Mit einfachen Mitteln könnten Nutzer dazu gebracht werden, Sicherheitsvorrichtung zu ignorieren und ihre Daten preiszugeben. Auch dass SSL-Schlosssymbol im Browserfenster biete keine Garantie mehr für die Echtheit der Seite. Nach dem aktuellen Stand seien die Browser durch für den Verbraucher unverständliche Informationen und unerfüllbare Verhaltenstipps bei eventuellen Bedrohungen eher Teil des Problems als Teil der Lösung. Zentral sei es dabei herauszuarbeiten, welche Entscheidungen der Nutzer selbst treffen müsse und welche Informationen er dazu benötige. Die entsprechenden Sicherheitsinformationen müssten auf eine nutzbare, verständliche und robuste Weise dem Nutzer präsentiert werden.

Im Anschluss behandelte Prof. Dr. Georg Borges in seinem Vortrag das rechtliche Verhältnis zwischen Bank und Kunde. Im Mittelpunkt standen dabei Haftungs- und Beweisfragen bei Phishing Angriffen. Borges stellte zunächst die verschiedenen Rechtsbeziehungen dar, die vom Risiko des Phishings betroffen sind um dann näher auf das Verhältnis Überweiserbank - Phishing-Opfer einzugehen. Eine Pflichtverletzung des Kunden durch Eingabe vertraulicher Daten auf einer Phishing – Website sei, so Borges, bei offensichtlichen Verdachtsmomenten wohl zu bejahen, z.B. bei der Aufforderung 10 TAN auf

der Seite einzugeben. Ob der Kunde allerdings verpflichtet sei, aktuelle Virenschutzprogramme vorzuhalten, könne noch nicht eindeutig beantwortet werden. Jedenfalls stelle es aber eine Pflichtverletzung dar, wenn der Kunde einen Missbrach nicht unverzüglich seiner Bank mitteile. Insgesamt, so Borges, sei die Haftung des Kunden noch weitgehend ungeklärt. Auf Seiten der Banken bestehe die Pflicht, die Kunden über die Gefahren des Phishing etc. so aufzuklären, dass ein durchschnittlicher Kunde nicht im Unklaren bleiben könne. Ob aus der allgemeinen Pflicht der Banken, Daten des Kunden vor Zugriffen Dritter zu schützen, die Verpflichtung resultiere neue Verfahren mit höherem Sicherheitsstandart einzuführen, sei noch offen.

Zu den beweisrechtlichen Fragen führte Borges aus, dass bei den aktuellen Online-Banking Verfahren grds. ein Anscheinsbeweis bestehe. Erschüttert werden könne dieser Anschein z.B. beim PIN/TAN Verfahren durch den Nachweis oder die konkrete Möglichkeit von Phishing. Ob der Anschein erschüttert werden könne, hänge wesentlich von der Sicherheit des Authentifizierungsverfahrens ab.

Felix Lindner, Leiter von SABRE Labs, ging speziell auf die neuen Verfahren zur Klassifikation von Schadprogrammen mittels des Vergleichs von Programmstrukturen ein. Einfache Byte-Signaturen könnten nur einen winzigen Teil des Schadprogramms erfassen und seien daher leicht zu umgehen und folglich nicht gut geeignet, neue Varianten bereits bekannter Schadsoftware zu erkennen. Ein Vergleich der Struktur der Call- und Flowgraphen decke dagegen das gesamte Programm ab. Linder beschrieb anschließend die genaue Funktionsweise und auch die zu lösenden Probleme beim Graphvergleich. Im Ergebnis sei festzustellen, dass auch unbekannte Bots sinnvoll in Familien geordnet würden. Die Nach-Benennung der Bots durch AV-Software zeige, dass die Einordnung oft übereinstimme.

Ebenfalls zum Thema „Neue Analyseverfahren für Malware“ erörterte nachfolgend Carsten Willems, von der CWSE GmbH, Aspekte der verhaltensbasierten CWSandbox. Da die manuelle Analyse zu lange dauere, um die zunehmende, sich autonom verbreitende Schadsoftware zu erfassen, sei ein höheres Maß an Automatisierung notwendig. Diese automatische Analyse sei mit der CWSandbox ohne eine menschliche Interaktion möglich. Der Vorteil der Verhaltensanalyse, die nur das Verhalten während der Programmausführung beobachte, sei die Schnelligkeit und Einfachheit. Die CWSandbox liefere daher fast immer ausreichende Ergebnisse in sehr kurzer Zeit. Diese automatische Verhaltensanalyse sei daher ein wertvolles Werkzeug Im Bereich der Malware-Bekämpfung.

Den Abschluss des zweitätigen Symposium bildete die Podiumsdiskussion zum Thema „Crimeware – Forensik und Schutzmaßnahmen“. Unter der Moderation von Armin Barnitzke, stellvertretender Redakteur der Computer Zeitung, führten

die vier Podiumsteilnehmer in Kurzvorträgen in das Thema ein. Willhelm Dolle von der HiSolutions AG ging unter anderem auf die Probleme und Herausforderungen der Computer – Forensik ein. Einen kurzen Überblick über die Arbeit der Firma GData gab Ralf Benzmüller. Sebastian Rohr von Microsoft Deutschland und Rainer Witzgall von der Avira GmbH stellten anschließend Ihre Sichtweise der Problematik dar.

Diskutiert wurde zunächst, wie ein Verbraucher reagieren müsse, wenn er Schadsoftware auf seinem Rechner entdecke. Selbst wenn ein Schadprogramm eindeutig identifiziert werden könne, sei es zumindest für den durchschnittlichen Verbraucher nicht ohne weiteres möglich, dieses anschließend auch vollständig und zuverlässig zu entfernen. Um eine möglichst hohe Sicherheit zu erlangen sei daher dazu zu raten, den Computer „platt zu machen“. Diese Vorgehensweise sei zwar technisch empfehlenswert, ziehe aber das Problem nach sich, dass der Nutzer nur noch schwer seiner Bank gegenüber beweisen könne, dass sich Schadsoftware auf dem Rechner befunden hat. Sicherheitskopien der gespeicherten Daten hätten nicht denselben Beweiswert wie die Originale. Auch die Protokolle der Virenscanner, die möglicherweise das entsprechende Programm erkannt haben, seien ohne größeren Aufwand zu manipulieren und daher weniger zur Beweisführung geeignet.

Aus dem Publikum wurde die Frage gestellt, ob die Anti-Viren Softwarehersteller das Ziel, vor sämtlichen im Umlauf befindlichen Schadprogrammen zu schützen, mittlerweile aufgegeben hätten. Dies wurde von den Teilnehmern auf dem Podium bestritten. Aufgrund der schnellen Entwicklung in diesem Bereich sei es aber äußerst schwierig immer alle neuen Programme umgehend zu erfassen. Von den schon länger im Umlauf befindlichen Schadprogrammen, könnten allerdings nahezu alle von einer entsprechenden Schutzsoftware entdeckt werden.

Isabelle Biallaß, Paul Dienstbach