Internetsicherheit: Phishing, Pharming, Skimming

Zeit, Ort: 15.09.2005, 11:00, HS 112

Referenten: Prof. Dr. Maximilian Herberger, Institut für Rechtsinformatik, Saarbrücken
Rigo Wenning, W3C/ERCIM, Sophia-Antipolis

Protokoll: Ass. jur. Iris Speiser

Zu Beginn des Arbeitskreises führte Prof. Herberger in das Spannungsfeld der Rechtsinformatik ein. Das Informationsrecht erfordere fundierte Kenntnisse der technischen Infrastruktur. Die Website www.daufaq.de zeige eindrucksvoll, dass das Problem der Unkenntnis noch immer vorhanden sei.

Im Anschluss an die kurze Einführung durch Prof. Herberger trug Rigo Wenning zum Thema Phishing vor. Der Begriff Phishing („Abfischen“) sei eine Form des Trickbetruges. Ziel sei, die Geschädigten per Mail durch Täuschung dazu zu bewegen, Zugangsdaten und Passwörter herauszugeben. In den meisten Fällen richten sich Phishing-Angriffe gegen Online-Banking-Kunden, gelegentlich aber auch gegen Kunden von Diensten wie eBay oder Paypal.

Beim Online-Banking würden verschiedene Informationen zwischen der Banken und dem Kunden ausgetauscht. In diese Kommunikation könne durch eine so genannten "Man-in-the-middle-attack" eingebrochen werden. Hierbei werde die direkte Verbindung zur Bank umgangen und ein Dritter zwischengeschaltet, der die Daten vor der Weiterleitung an die Bank verändere. Dies erfolge z.B. durch trojanische Pferde auf dem Rechner des Opfers.

Dabei ergäben sich jedoch einige Probleme für den „Phisher“: Er müsse geeignete Wege finden, seine betrügerischen Mails zu „spammen“, die von den Nutzern erlangten Daten sammeln, die Daten anwenden und den Rückfluss des Geldes organisieren - wobei der Rückfluss meistens durch Überweisung auf das Konto eines Naiven erfolge, der das Geld an den Phisher weiterleite.

Der Irrtum des Kunden werde in der Regel über SPAM-Mails generiert, die nicht als solche erkennbar seien, sondern den Anschein erweckten, von der Bank selbst zu stammen. Ein

neuerer Trick sei auch, den Mails den Anschein von individuellen Anschreiben zu geben, indem z.B. Teile der Kreditkartennummern der Betroffenen in die Mails integriert würden. Der Trick beruhe darauf, dass der erste Teil der Nummern innerhalb eines Instituts einheitlich und deshalb leicht zu ermitteln sei. Den unbekannten Teil lässt der Phisher dann vorgeblich aus Datenschutzgründen weg.

Inzwischen sei auch telefonisches Phishing bekannt, bei dem die Anrufer sich als Bankmitarbeiter ausgeben und den Kunden PINs und TANs entlocken wollten.

Um nicht identifizierbar zu sein, könne der Phisher selbst kein Konto unterhalten, bzw. das vom Opfer erbeutete Geld nicht direkt dorthin überweisen. Er bediene sich hierfür der Geldgier Naiver, die über „attraktive Jobangebote“ - die ebenfalls per SPAM verteilt würden - dazu gebracht würden, das Geld an die Hintermänner weiterzuleiten.

Es stelle sich die Frage, warum trotz der allgegenwärtigen Warnungen vor Phishing immer wieder Opfer auf so genannte Phishing-Sites hereinfallen. Hierfür gebe es verschiedene Ursachen. Zum einen gebe es Mängel in den Browser-Softwares sowie in den verwendeten Zertifikatsstandards X.509 und SSL, zum anderen Manipulationsmöglichkeiten in HTML-Formularen und bei Verwendung von Internationalized Resource Identifiers (IRIs). So sei es optisch nicht möglich, das russische „a“ vom lateinischen „a“ zu unterscheiden. Auf diese Art lasse sich die URL einer Bank vortäuschen, ohne dass dies für den Nutzer erkennbar sei.

Das im Browser in der Statusleiste angezeigte Vorhängeschloss sei auch keineswegs ein Garant für Sicherheit, es vermittele dem Nutzer vielmehr ein falsches Sicherheitsgefühl. So würden Zertifikate von Verisign von den meisten Bowsern standardmäßig als vertrauenswürdig eingestuft, obwohl derartige Zertifikate mit niedriger Sicherheitsstufe ohne Identitäts- oder Berechtigungsprüfung in einem automatisierten Verfahren erlangt werden könnten. X.509-Zertifikate seien für den Nutzer nicht prüfbar, da er vielfach nicht über die erforderliche Systemkenntnis verfüge. Das Schloss sei daher sinnlos, da die derzeitigen Implementierungen auch dem argwöhnischen Nutzer nicht weiterhelfen.

Das W3C habe im März zu diesem Thema einen Workshop abgehalten, an dem sowohl Vertreter von Banken, Browser & Sicherheits-Industrie, als auch aus Forschung und von Content Providern teilgenommen haben. Als Ergebnis seien etliche Empfehlungen an die

Entwickler und Anbieter ergangen.

So könne z.B. ein genormtes Sicherheitsinterface geschaffen werden, in das das Logo der jeweiligen Bank integriert werden könne und so dem Nutzer die Authentizitätsprüfung erleichtern könne. Ein solches Interface müsste gewissen Sicherheitsstandards genügen. So müsse der Teil des Bildschirms mit den Identifikationsdaten gegen Skripts und andere Manipulation geschützt werden. Dies könne durch Beschneiden der Browser-Funktionalitäten erreicht werden, da insbesondere CSS und komplexes HTML-Layout die Verschleierung der Herkunft der Seiten erlaube. Herr Wenning regte in diesem Zusammenhang die Schaffung eines „Sicherheits-Modus“ für Browser an, in dem gefährlich Funktionen wie „Skript-Ausführung“, Pop-Up-Fenster o.ä. deaktiviert wären. So könne der Nutzer auch ohne fortgeschrittene technische Kenntnisse zum Ausführen von Bankgeschäften in diesen Modus wechseln, ohne im „Normalbetrieb“ auf diese Funktionen verzichten zu müssen.

Das W3C bemühe sich derzeit darum, eine Konzertation der Browser-Entwickler zu fördern. Zudem versuche man Möglichkeiten zu schaffen, die es dem Content-Provider erlaube, Sicherheitsmerkmale mit ihrer Marke zu verbinden - z.B. durch eine „logo-type-extension“oder content labeling. Zwar gebe es sicherere Methoden der Authentifizierung, z.B. das HTTP-login, diese Möglichkeiten würden derzeit jedoch nur selten genutzt, da sie durch ihr nicht variierbares Design unattraktiv seien. Stattdessen würden HTML-Formulare, Cookies o.ä. genutzt, die sich besser in das individuelle Design einfügen ließen. Es sei daher erforderlich, technische Möglichkeiten zu schaffen, wie die Browser die Login-Informationen dennoch zuverlässig verwalten können, z.B. durch die Verbindung mit HTTP-Level Authentication.

Zum Abschluss seines Vortrages gab Herr Wenning noch einen kurzen Ausblick auf laufende Entwicklungsprojekte. So diskutiere die IETF derzeit Neuerungen der HTTP Authentication. Auch zahlreiche Online Identitätssysteme wie z.B. dix, Infocard, OpenID, Liberty Alliance u.a. würden stetig weiterentwickelt. Beim W3C befasse sich die W3C Security Working Group mit dieser Materie; Kommentare und Anregungen seien ausdrücklich erwünscht.

Im Anschluss an den Vortrag schilderte Prof. Herberger als Anregung für die Diskussion zwei praktische Fälle.

So habe er von einer Bank erfahren, die auf ihren Seiten ankündige, auf Wunsch den Fingerprint ihres https-Zertifikats in geeigneter Form in der Filiale zu überreichen. Dies zeuge von unzureichendem Systemkenntnissen und erscheine als wenig praktikable Methode, da sie dem Prinzip des Online-Banking zuwiderlaufe.

Weiterhin wies Herr Prof. Herberger auf eine Gerichtsentscheidung hin, die das Handeln des naiven Helfers eines Phishers als Beihilfe zum Computerbetrug eingestuft habe. Seiner Meinung nach sei die Tat jedoch bereits beendet, wenn der Naive ins Spiel komme, eine Beihilfe sei daher gar nicht mehr möglich. Zudem stelle sich die Frage, ob überhaupt eine wirksame Überweisung erfolgt sei, denn nur dann sei der für die Verwirklichung eines Betrugsdeliktes erforderliche Schaden entstanden.

Im Laufe der anschließenden Diskussion wurden einige Fragen im Zusammenhang mit Internetsicherheit aufgeworfen.

- Der Schwerpunkt des Vortrages habe sich mit Phishing befasst; gibt es auch eine Definition der Begriffe „Pharming“ und „Skimming“?
  Pharming sei die Umleitung eines an sich korrekten URL-Aufrufs (z.B. DNS-Spoofing), Skimming hingegen bezeichne die Manipulation von Geldautomaten und anderen bankkartenlesenden Geräten durch Vorsatzgeräte, die während des Einführens der Karte deren Inhalt auslesen.

- Gibt es gut funktionierendes Telefon-Banking?
  Die Risiken beim Telefonbanking seien die gleichen wie beim Online-Banking. Der Kunde könne einerseits veranlasst werden, eine falsche Telefonnummer anzurufen, andererseits versuchten Betrüger ihre Opfer anzurufen und diese unter dem Vorwand, Mitarbeiter der Bank zu sein, zur Angabe von Kontozugangsdaten zu bewegen (sog. „Vishing“).

- Ein Teilnehmer verwies auf einen Interessanten Ansatz zur Verfolgung von Phishing: die Strafverfolgung wegen Verstößen gegen das KWG. Schließlich gäben die Phisher vor, Bankdienstleistungen zu erbringen, ohne im Besitz der hierfür erforderlichen Lizenz zu sein. Dies sei leichter nachweisbar als der Betrug, da es nicht des Nachweises einer Täuschungshandlung oder eines konkreten Schadens bedürfe.

- Wäre es möglich, beim Online-Banking auf aktive Seiteninhalte wie Javascript zu verzichten?
  Technisch sei dies schon möglich, indem stattdessen serverseitige Skripte eingesetzt würden, dies belaste jedoch bei großer Nutzerzahl die Performance des Server, weshalb diese Möglichkeit von den Anbietern nur ungern genutzt werde.

- Ist das iTAN-Verfahren sicher?
  Das Verfahren erhöhe zwar die Sicherheit, da es den für einen Angriff zur Verfügung stehenden Zeitraum einschränke. Es sei jedoch auch bei diesem Verfahren möglich, die Information abzufangen, zu verändern und dann an die Bank weiterzuleiten.

- Ist mit HBCI sicheres Online-Banking möglich?
  HBCI sei ein sehr sicheres Verfahren, es helfe aber nicht gegen Trojanische Pferde auf dem Rechner des Nutzers. Zudem gebe es Berichte, dass es dem Chaos Computer Club gelungen sein soll, das HBCI-Interface zu hacken. Herr Wenning hält eine Kombination aus XHTML und XML-Signatur für die bessere Alternative.

- Ist Phishing nicht eher ein Problem der fehlenden Aufklärung der Nutzer und muss man nicht das Online-Banking als solches in Frage stellen, wenn man es nicht absichern kann?
  Dies sei nach Auffassung Rigo Wennings eine wirtschaftliche Frage, die die jeweiligen Banken beantworten müssten.