RTR AKTUELL

FACHBEREICH TELEKOMMUNIKATION

Rundfunk & Telekom Regulierungs-GmbH
RTR

TK06/2006
VOM 19.06.2006

IMPRESSUM:
Medieninhaber (Verleger), Herausgeber, Hersteller und Redaktion:
Rundfunk und Telekom Regulierungs-GmbH
A-1060 Wien
Mariahilfer Straße 77-79
Tel.: +43 (0) 1 58058 - 0
Fax: +43 (0) 1 58058 - 9191
e-mail: rtr@rtr.at
http://www.rtr.at
FN 208312t
Verlags- und Herstellungsort: Wien

Zum Thema Sicherheit beim Online-Banking

Sicherheit beim Online-Banking ist wieder einmal ins Gerede gekommen. Zeitungen schreiben über eine neue „Betrugswelle“, die auf uns zukommt. Banken modifizieren laufend ihre Sicherheitsprozesse und scheinen somit die beängstigenden Medienberichte zu bestätigen. Überdies entsteht gelegentlich der Eindruck, dass Banken sich auf Kosten der Konsumenten absichern wollen. Ist Online-Banking wirklich unsicher?

Verschiedene Angriffsmethoden

Zu einem seriösen Umgang mit dieser Frage muss zunächst klargestellt werden, von welchen Angriffsmethoden die Rede ist. Ein erfolgreicher Angriff erfordert nicht unbedingt besondere technische Kenntnisse, wenn es dem Angreifer gelingt, jemandem vertrauliche Informationen zu entlocken (Social Engineering). Angriffe auf technischer Ebene können danach unterschieden werden, ob der Angriff auf die Systeme der Bank, auf den Kommunikationskanal oder auf den Rechner des Bankkunden gerichtet ist.

■ **Phishing**
Das Opfer wird durch Vortäuschung einer vertrauenswürdigen Kommunikation dazu gebracht, PINs und TANs preiszugeben. Häufig werden dabei bestehende Ängste der Bankkunden ausgenützt, indem diese per Massenmail dazu aufgefordert werden, sich wegen der Einführung eines neuen Sicherheitssystems online registrieren zu lassen. Die Registrierung, bei der geheime Authentifizierungsdaten abgefragt werden, erfolgt typischerweise über eine Website, welche jener der Bank täuschend ähnlich sieht. Größerer Schaden ist bislang wohl nur deshalb ausgeblieben, weil das sprachliche Niveau der Angreifer auf deren Website Professionalität vermissen lässt und somit Verdacht hervorruft.

■ **Man in the Middle**
Bei dieser Angriffsart wird die Kommunikation zwischen der Bank und ihrem Kunden von einem Angreifer belauscht und/oder manipuliert. Durch Authentifizierung mittels Secure Socket Layer (SSL) bzw. Transport Layer Security (TLS) wird die Gefahr eines solchen Angriffs weit gehend gebannt. Den Einsatz solcher Sicherheitsprotokolle erkennt man bei Websites daran, dass der URL mit „https://“ beginnt. Allerdings sollte der Bankkunde auch prüfen, ob das Zertifikat tatsächlich für den Webserver der Bank ausgestellt ist und ob das Zertifikat vom Rechner als gültig erkannt wird.

■ **Schadprogramme**
Schadprogramme im Rechner des Opfers können auf verschiedene Weise wirken: Sie können beispielsweise eine vom Bankkunden eingegebene TAN verändern, sodass der Auftrag von der Bank nicht ausgeführt werden kann. Die richtige TAN wird dann vom Schadprogramm selbsttätig für andere Bankgeschäfte eingesetzt. Derartige Programme setzen sich meistens im Browser fest.

Fortsetzung auf Seite 03

Zum Thema

Fortsetzung von Seite 02

Folgende Manipulationen sind typisch:

- Änderung der Browser-Einstellungen (Start- und Suchseiten),
- Eintragung bestimmter Websites in den Bereich der „vertrauenswürdigen Sites“, um Sicherheitsmechanismen zu umgehen,
- Eintragung bösartiger Nameserver, die Rechnernamen in falsche IP-Adressen auflösen,
- Installation eines trojanischen Pferds, welches dafür sorgt, dass die Konfigurationsänderungen vom Benutzer nicht dauerhaft rückgängig gemacht werden können,
- Nutzung von Browser Helper Objects (Bibliotheken zur Erweiterung der Funktionen des Internet Explorers), um Informationen abzufangen und zu manipulieren, die der Benutzer zu einem Internet-Server sendet,
- Installation eines Rootkits, um die Systemressourcen des Schadprogramms (Dateien, Prozesse, Speicherbereiche usw.) zu verbergen.

Schutz durch TAN-Verfahren unzureichend

Alle genannten Angriffsarten können verwendet werden, um TANs zu missbrauchen. Einige Banken haben daher das traditionelle Verfahren modifiziert: Beim iTAN-Verfahren (indizierte TAN) kann der Kunde seinen Auftrag an die Bank nicht mit einer beliebigen unbenutzten TAN bestätigen, sondern wird aufgefordert, beispielsweise die 34. TAN zu verwenden. Bei einem anderen Verfahren wird eine mobile TAN (mTAN) per SMS übermittelt. Beide Modifikationen bieten zwar einen gewissen Schutz vor Phishing, sind aber wirkungslos, wenn der Angreifer einen tatsächlichen Auftrag des Kunden an die Bank mit technischen Mitteln manipuliert (im Fall der mTAN kann jedoch ein Sicherheitsgewinn dadurch erzielt werden, dass im SMS auch das Empfängerkonto und der zu überweisende Betrag genannt werden).

Manche der einleitend angeführten Medienberichte verteufeln in Unkenntnis der Tatsachen neben dem TAN-Verfahren und seinen Varianten auch die elektronische Signatur. Bei solchen Darstellungen wird aber das Kind mit dem Bade ausgeschüttet, denn ist ein Überweisungsauftrag einmal mit einer sicheren elektronischen Signatur versehen, so kann ihn kein Angreifer der Welt unbemerkt verändern: Jede Modifikation der signierten Daten würde bewirken, dass die elektronische Signatur nicht mehr zu den Daten passt.

Die sichere elektronische Signatur beruht auf einem Schlüssel, der nur auf einer Chipkarte existiert und aus dieser nicht ausgelesen werden kann. Nicht einmal der Inhaber der Chipkarte kennt den Schlüssel. Somit kann er den Schlüssel auch nicht irrtümlich preisgeben. Ein Phishing-Angriff würde also ins Leere gehen.

Fortsetzung auf Seite 04

Aber auch gegen Angriffe auf technischer Ebene bietet die sichere elektronische Signatur wirkungsvollen Schutz, denn sie wird nicht in einem möglicherweise von Schadprogrammen befallenen Computer, sondern auf der Chipkarte berechnet.

Zum Thema

Fortsetzung von Seite 03

Der Signaturvorgang kann nur durch Eingabe einer PIN ausgelöst werden. Durch die Verwendung von Chipkarten-Lesegeräten mit eigener PIN-Tastatur kann ausgeschlossen werden, dass Schadprogramme im Computer die PIN ausspähen oder gar selbsttätig einen Signaturvorgang auslösen.

Könnte ein Schadprogramm den Bankkunden nicht dazu bringen, etwas anderes zu signieren als den vermeintlichen Überweisungsauftrag? Die Antwort lautet nein, sofern ein „Secure Viewer" verwendet wird: ein Programm, das die zu signierenden Daten vor Auslösung des Signaturvorgangs darstellt und dafür sorgt, dass diese Daten vor der Signaturerstellung nicht mehr verändert werden. Schadprogramme, die sich im Browser festsetzen, wirken sich auf Secure Viewer nicht aus. Überdies werden die meisten Secure Viewer einer strengen Prüfung nach anerkannten Sicherheitsvorgaben unterzogen, wobei u.a. die Unveränderbarkeit der zu signierenden Daten nachgewiesen werden muss.

Beispielsweise ist der vom Hamburger Unternehmen SecCommerce Informationssysteme GmbH hergestellte Secure Viewer „SecSigner", der von der BAWAG P.S.K. Gruppe beim Online-Banking eingesetzt wird, nach den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) und nach dem Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM) evaluiert (Evaluationsstufe „E 2", Mindeststärke der Mechanismen „hoch") und vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert. Überdies liegt eine ebenfalls vom BSI ausgestellte Bestätigung vor, der zufolge dieses Produkt den Anforderungen des deutschen Signaturgesetzes entspricht.

Für die Darstellung der zu signierenden Daten dürfen nur die vom Zertifizierungsdiensteanbieter empfohlenen Formate verwendet werden. Der Zertifizierungsdiensteanbieter haftet dafür, dass die von ihm empfohlenen technischen Komponenten und Verfahren den strengen Sicherheitsanforderungen des Signaturgesetzes entsprechen, und muss zu diesem Zweck eine eigene Haftpflichtversicherung abschließen.

Um keinen falschen Eindruck zu erwecken, sei klargestellt: Missbrauch kann auch bei Einsatz der elektronischen Signatur nicht vollständig ausgeschlossen werden. Das Risiko für die Bank und für ihre Kunden ist jedoch bei Einsatz der sicheren elektronischen Signatur um Größenordnungen geringer als bei den verschiedenen Varianten des TAN-Verfahrens. Unter allen derzeit eingesetzten Verfahren bietet die sichere elektronische Signatur nach einhelliger Meinung von Experten den wirkungsvollsten Schutz gegen praktisch alle Betrugsarten beim Online-Banking.

Internationales Neue Dokumente der European Regulators Group (ERG)

ERG veröffentlicht neue Version der gemeinsamen Position zu Regulierungsmaßnahmen

Bereits im April 2004 veröffentlichte ERG die erste Version einer gemeinsamen Position zu Regulierungsmaßnahmen. Ziel dieser zweiten revidierten Version war es, die Erfahrungen aus den bisherigen Marktanalysen im neuen Rechtsrahmen in ein neues Dokument einzuarbeiten. Nach einer Erstanalyse wurde der Fokus der Überarbeitung in folgenden Themenbereichen gesetzt:

- Emerging Markets,
- Investitionen (Konzept der Ladder of Investment),
- Kohärente Preisregulierung,
- Nichtdiskriminierung,
- Differenzierung von Regulierungsmaßnahmen in Terminierungsmärkten,
- Beziehungen zwischen Märkten,
- Aufhebung von Regulierungsmaßnahmen.

Während zu diesen Themen neue Überlegungen enthalten sind, wurden in den bisher bereits bestehenden Kapiteln Inhalte nur geringfügig überarbeitet.

ERG veröffentlicht Bericht zu regulatorischen Kostenrechnungssystemen in der Praxis

Die Ausgestaltung der in der Tarifregulierung zur Anwendung kommenden Kostenrechnungssysteme in Europa ist der Inhalt dieser neuen Studie der European Regulators Group. In diesem Dokument wurden quer über alle relevanten 18 Märkte der Märkteempfehlung die derzeit in europäischen Ländern angewendeten Kostenrechnungssysteme untersucht. Ein erster derartiger Bericht wurde bereits 2005 veröffentlicht und im neuen Bericht werden die Ergebnisse 2006 denen aus 2005 gegenübergestellt.

Im Detail wurden folgende drei Themen näher untersucht:

- Durch welchen Mechanismus werden Tarife bestimmt: In den meisten Fällen kommt Kostenorientierung zur Anwendung.
- Verwendete Kostenbasis (Bewertung) in der Kostenrechnung: Hier ist ein klarer Trend von historischen Kosten zu Wiederbeschaffungswerten zu erkennen.
- Art der Kostenzurechnung: Hier gehen immer mehr Länder zu LRIC über.

Fortsetzung auf Seite 06

Internationales

Update zur Entwicklung der Mobilterminierungsentgelte

Fortsetzung von Seite 05

Die ERG veröffentlicht ihr halbjährliches Update zur Entwicklung der Mobilterminierungsentgelte in Europa. In den meisten Ländern ist die Tendenz im Vergleich zu vor sechs Monaten weiterhin sinkend. Österreich liegt weiterhin in dieser Durchschnittsbetrachtung im europäischen Mittelfeld.

Referenzen:

- Revised ERG Common Position on the approach to Appropriate remedies in the ECNS regulatory framework, Final Version May 2006 ERG (06) 33
- Regulatory Accounting Practice: Report, April 2006, ERG (06) 23
- ERG MTR Snapshot ERG (06) 24

Alle Dokumente sind auf der Website der ERG (http://erg.eu.int) abrufbar.

Sonstiges

Terminaviso: 7. Salzburger Telekom Forum

Das 7. Salzburger Telekom Forum, das – wie in den letzten Jahren – von der Rechtsakademie und des Fachbereichs Öffentliches Recht der Rechtswissenschaftlichen Universität Salzburg gemeinsam mit der Europäischen Kommission, GD Informationsgesellschaft und der RTR-GmbH veranstaltet wird, findet heuer am 27. und 28. September 2006, in den Räumlichkeiten der Universität Salzburg, statt. Im Fokus der Veranstaltung steht das Thema Review 2006. Wie auch in den letzten Jahren, endet die Veranstaltung am Donnerstag mit einem Mittagsempfang der Salzburger Landesregierung.