Datenschutz-Berater

Informationsdienst der Verlagsgruppe Handelsblatt

DSB 12/2006
(30. Jahrgang)
DSB G05311

INHALT

NACHRICHTEN

SWIFT: Neuregelung nötig

Nachdem die Artikel 29-Gruppe der Europäischen Datenschutzbeauftragten die bisherige Datenübermittlungspraxis von SWIFT als unrechtmäßig bezeichnet hat, soll die Weitergabe an US-amerikanische Behörden neu geregelt werden. SEITE 4

Vorratsdatenspeicherung (I)

Der Arbeitskreis Vorratsdatenspeicherung hat zur Beteiligung an einer „Sammel-Verfassungsbeschwerde" aufgerufen. SEITE 4

Finanzinformationssysteme

Der Europäische Gerichtshof hat mit seinem Urteil vom 23. November 2006 den Austausch von Kundendaten zwischen Finanzdienstleistern für rechtmäßig erklärt. SEITE 6

BigBrotherAwards 2006

Die Ständige Konferenz der Kultusminister wurde für ihren Vorschlag, Schüler künftig für schulstatistische Zwecke mit einer persönlichen ID zu versehen, als eine der „größten Datenkraken der Nation" ausgezeichnet. SEITE 7

Computerkriminalität 2005

Für das Jahr 2005 hat die Polizeiliche Kriminalstatistik einen Anstieg des registrierten Computerbetrugs um 11,9 Prozent verzeichnet. SEITE 8

DATENSICHERHEIT

Sichere Netzübergänge

Das Bundesamt für Sicherheit in der Informationstechnik hat einen Leitfaden mit Hinweisen zur Planung und Einrichtung sicherer Netzübergänge veröffentlicht. SEITE 9

IT-Sicherheitsstudien

Zwei neue Sicherheitsstudien dokumentieren die weiter gewachsene Bedeutung der IT-Sicherheit und Ordnungsmäßigkeit der IT-Systeme und Anwendungen. SEITE 10

Mehr Sicherheit mit mTan

Der Versand transaktionsbezogener Einmal-Passwörter auf alternativen Wegen verspricht höhere Sicherheit beim Online-Banking. SEITE 11

RECHT & POLITIK

Vorratsdatenspeicherung (II)

Das Bundesministerium der Justiz hat einen Referentenentwurf zur Neuordnung verdeckter Ermittlungsmaßnahmen ausgearbeitet. SEITE 13

DATENSCHUTZPRAXIS

30. Datenschutzfachtagung

Am 16. und 17. Oktober 2006 fand die 30. DAFTA in Köln statt. SEITE 16

RECHTSPRECHUNG

Schweigepflichtentbindung

Nach dem Beschluss des Bundesverfassungsgerichts vom 23. Oktober 2006 verletzt eine versicherungsvertragliche Obliegenheit, zur Feststellung des Versicherungsfalles eine umfassende Schweigepflichtentbindung zu erteilen, das informationelle Selbstbestimmungsrecht des Versicherungsnehmers. SEITE 18

Verhaltensbedingte Kündigung

Mit der unerlaubten Installation einer Anonymisierungssoftware verletzt ein Arbeitnehmer seine arbeitsvertraglichen Pflichten in erheblichem Ausmaß. Eine solche verbotene Nutzung des Internet-Zugangs zu privaten Zwecken rechtfertigt eine verhaltensbedingte Kündigung. SEITE 19

Anbieterkennzeichnung

Die Angabe einer über zwei Links erreichbaren Anbieterkennzeichnung bei einem Internetauftritt kann den Informationspflichten eines Teledienstanbieters entsprechen. SEITE 20

Aneignung von Kundendaten

Ein ausgeschiedener Mitarbeiter, der Kundenlisten seines früheren Arbeitgebers schriftlichen Unterlagen entnimmt, die er während des früheren Dienstverhältnisses gespeichert hat, verschafft sich damit unbefugt ein Geschäftsgeheimnis. SEITE 21

ISSN 0170-7256

stocken. 45 Prozent der befragten Organisationen schätzen den Sicherheitsbedarf auf dem IT-Sektor aufgrund neuer Kommunikationstechnologien höher ein als noch vor wenigen Jahren. Fast die Hälfte aller Befragten geht davon aus, dass durch den Einsatz neuer Technologien wie RFID-Chips, Voice-over-IP oder Mobile-Business-Anwendungen zusätzliche Sicherheitskosten entstehen, die hoch oder sogar sehr hoch ausfallen können. ■

Internet: www.caemea.com/de/papers/studie_it-sicherheit_2006_2007.pdf; www.telekomforum.de

Stichworte: Sicherheitsumfragen, Telekom-Forum, Computer Associates

Banken - Mehr Sicherheit mit mTAN

Rund ein Viertel der Bankkunden in Deutschland nutzt Online-Banking. Eine erfolgversprechende Strategie für mehr Sicherheit ist der Versand von transaktionsbezogenen Einmal-Passwörtern auf alternativen Wegen, welche die Internet-Transaktionenen besser absichern als bisherige TAN-Verfahren.

Von MARKUS KRAMER, Dortmund.*

Alles schien sicher beim Identifikationsverfahren, das die Banken für die Auftragsabwicklung beim Online-Banking entwickelt haben: Der Bankkunde weist sich durch die Eingabe einer Persönlichen Identifikationsnummer (PIN) aus und verwendet für die Autorisierung der einzelnen Buchungsvorgänge Transaktionsnummern (TAN), die er blockweise in ausgedruckter Form von der Bank erhält. Jede TAN kann nur einmal benutzt werden und verfällt danach.

Verhältnismäßig schnell aufkommende Manipulationsstrategien setzten zunächst an der Kombination „menschliches Wesen und TAN-Liste auf dem Schreibtisch" an. Jeder kennt die Fluten von E-Mails, mit denen Bankkunden veranlasst werden sollten, Identifikations- und Transaktionsnummern preiszugeben oder auf einer gefälschten Webseite einzugeben. Parallel zu steigenden Sicherheitsvorkehrungen verfeinerten auch die Betrüger ihre Methoden: Die E-Mails dienen vorrangig dazu, Schädlinge auf dem Rechner des Kunden einzuschleusen. Beim Pharming werden die Kunden unbemerkt auf die gefälschte Seite der Bank weitergeleitet. Dafür muss die E-Mail noch nicht einmal mehr geöffnet werden. Wer Opfer eines Pharming-Angriffes geworden ist, kann noch so große Sorgfalt walten lassen: Selbst wenn er die URL seiner Bank von Hand im Browser eingibt, landet er auf der Betrüger-Seite. Aktuell kommen auch Schadprogramme zum Einsatz, die die Tastatureingaben oder die Bewegungen des Mauszeigers auf dem Bildschirm aufzeichnen und die Informationen an den Hacker schicken. So genannte Backdoor-Trojaner ermöglichen den direkten Zugriff auf den Anwender-Rechner und die Manipulation laufender Vorgänge - der Hacker kann selbst Überweisungen tätigen. Dagegen helfen auch Firewalls und gut gepflegter Virenschutz nicht.

Herkömmliche Authentifizierungsverfahren

Gegen die Versuchung durch die TAN-Liste auf dem Schreibtisch hilft nur: keine TAN-Liste auf dem Schreibtisch. Die Alternative ist die transaktionsbezogene oder Einmal-TAN, die für anstehende Transaktionen angefordert und nach Benutzung beziehungsweise nach einer kurz bemessenen Zeitspanne ungültig wird. Die steht beispielsweise in Form so genannter iTANs zur Verfügung. Bei diesem Verfahren, das von vielen Banken in Deutschland eingesetzt wird, hat der Kunde zwar immer noch eine TAN-Liste zur Hand. Ein Betrüger kann allerdings nichts damit anfangen, denn die TANs sind „indiziert", durchnummeriert. Welche TAN für den aktuell anstehenden Vorgang benutzt werden soll, entscheidet nicht der Anwender, sondern der Zufallsgenerator der Bank. Damit ist der Kunde vor den klassischen Phishing-Attacken geschützt.

Auch beim eTAN-Verfahren kommt ein Zufallsgenerator zum Einsatz, und zwar in der Hand des Kunden. Sobald der Kunde die Daten für die gewünschte Transaktion auf der Internetseite der Bank eingibt, wird eine Nummer auf der Seite erzeugt. Die gibt er in das taschenrechnergroße Gerät ein, das darauf hin eine elektronische Nummer, die so genannte eTAN, generiert. Durch das Eingeben dieser Nummer auf der Bankseite wird die Transaktion ausgeführt. Die eTAN ist nur kurze Zeit gültig.

Viele Banken bieten ihren Kunden Verfahren über das vom deutschen Zentralen Kreditausschuss standarisiertes Protokoll für Online-Banking Homebanking Computer Interface (HBCI) an. Das Verfahren macht TANs überflüssig. Es arbeitet mit auf dem Rechner installierter Spezialsoftware, Lese-

gerät und Chipkarte. Die Karte ist mit einer PIN geschützt, die der Kunde über das Lesegerät eingibt. Alle Überweisungsdaten werden für jeden Vorgang aufwendig verschlüsselt und sind so vor Manipulationen geschützt. Die Sicherheit hat jedoch ihren Preis; das Verfahren ist technisch aufwendig und nicht mobil.

Mobile TAN - Den Übermittlungskanal wechseln

Zum Schutz der Privatsphäre von Kontoinhabern sollten Banken auch über den Wechsel des Übermittlungskanals, über den die TAN an den Kunden geschickt wird, nachdenken. Statt auf den Rechner kommt sie per SMS aufs Handy und kann daher von Schadprogrammen nicht ausgelesen werden. Schutz vor Pharming-Attacken bietet das Verfahren mit mobilen TANs insofern, als einer gefälschten Webseite die Logik fehlt, um eine valide TAN zu generieren. Sicherheitshalber ist die mobile oder mTAN nur kurze Zeit gültig. Generell gilt: Je kürzer die Geltungsdauer, desto höher der Sicherheitsgewinn. Laufzeiten von mehr als zwei bis fünf Minuten sollten vermieden werden. In der SMS werden das Empfängerkonto und der Betrag wiederholt, so dass Manipulationen erkennbar sind. Mit der Eingabe der mTAN schließt der Kunde den Überweisungsvorgang ab.

Allerdings wird die mTAN erst von wenigen Banken, unter anderen der Postbank, angeboten, meist auf optionaler und kostenpflichtiger Basis. Dass in einem Land wie Deutschland, in dem es mehr Mobiltelefone gibt als Einwohner, die mTAN ein Schattendasein führt, liegt nach Einschätzung des SMS-Operators TynTec an den Mängeln beim Versand einer herkömmlichen SMS. Anbieter herkömmlicher SMS Dienste, wie SMS-Wiederverkäufer und Aggregatoren, die die erforderlichen Kontingente für den SMS-Versand bereitstellen, liefern die SMS lediglich beim SMS-Server (SMS-C) eines Netzbetreibers ein, über das die SMS in das globale GSM-Netz (auch SS7-Netz genannt), eingespeist werden. Die eigentliche Zustellung auf das Mobiltelefon des Kontoinhabers erfolgt über den Netzbetreiber. Dies bedeutet aber, dass herkömmliche SMS-Dienstleister keine Zusage hinsichtlich der zeitlichen Zustellung einer SMS abgeben können, da sie keine End-to-End-Kontrolle über die Nachricht haben. Bei Versendung eines privaten Grußes ist das nicht weiter tragisch. Kommt allerdings eine mobile TAN verspätet oder gar nicht an, haben Bank und Kunde ein Problem, da die Transaktion nicht ausgeführt werden kann. Außerdem kann bei Drittanbietern nicht ausgeschlossen werden, dass die SMS auf mehreren fremden Servern zwischengespeichert wird. Dies alles macht die SMS im Grund ungeeignet für Anwendungen im Banken-Umfeld, bei denen sehr hohe Anforderungen im Sinne von Zustell- und Zugriffssicherheit erfüllt sein müssen.

SMS mit Qualitätsgarantie

Für SMS mit derartigen sensiblen und zeitkritischen Informationen stellt das Münchener Unternehmen TynTec GmbH sogenannte „bank-konforme SMS- Services" bereit. Der SMS-Operator, der als Mitglied der GSM Association Netzwerkanbieterstatus hat, bietet eine garantierte Zustellung von SMS innerhalb von fünf bis maximal 15 Sekunden sowie entsprechende Service Level Agreements. TynTec unterhält über die Partnerschaft mit europäischen, amerikanischen und asiatischen Netzbetreibern einen direkten, redundanten Zugang zum globalen GSM-Netz sowie ein eigenes, proprietäres SMS-C (Short Message Service Center). Auf dieser Basis und der damit verbundenen End-to-End-Kontrolle über jede SMS kann das Unternehmen Finanzinstituten seine strikten Service Level ausstellen. Darüber hinaus kann TynTec auch GSM-Signalisierungsinformationen direkt auswerten und den Banken für jede SMS ein „GSM Delivery Receipt", eine Bestätigung über die Zustellung an das Mobiltelefon, in Echtzeit liefern. Die SMS bleiben bei der Übermittlung von der Bank-Anwendung bis an das Empfänger-Handy im hochgesicherten Rechenzentrum von TynTec; sie werden in keinem Fall über ein SMS-C eines anderen Netzbetreibers zugestellt oder auf Dritt-Servern zwischengespeichert.

Neben der zuverlässigen und schnellen Übermittlung spielt auch der Schutz von Informationen vor dem Zugriff Dritter eine bedeutende Rolle. Die Nutzung der „bank-konformen SMS-Services" erfolgt aus den Unternehmensanwendungen über APIs (Application Programmable Interfaces) auf der Basis des SMS-Standardprotokolls SMPP 3.4 oder über http. Für den Schutz bei der Übermittlung von der Bank an das SMS-C von TynTec sorgt eine VPN-Verbindung (1024 bit IPSec). Die Weiterleitung bis zur Luftschnittstelle ist über A5-1 Asymmetric Encryption Algorithm geschützt, den globalen GSM-Standard zur Verschlüsselung aller Informationen, die über die SS7-Signalisierungsstrecke versandt werden. ■

* Markus Kramer ist Business Development Manager bei der TynTec GmbH.

Stichworte: Online-Banking, eBanking, TAN, mTAN, SMS, TynTec