Onlinebanking - vieles ist verbesserungswürdig

Presseinformation anläßlich der Präsentation der Studie am 12.12.2006 im Bundesministerium für Soziales, Generationen und Konsumentenschutz

Umfassende Studie testet alle wichtigen Onlinebankingsysteme Österreichs - mit Hilfe von Testkonten wurden die technischen, rechtlichen und organisatorischen Abläufe getestet - alle Systeme besitzen Basissicherheit - kein System ist jedoch optimal - Kunden könnten vor Phishing-Attacken besser geschützt werden - ein einziges, von zwei Banken betriebenes System kann als innovativ und überdurchschnittlich gut bezeichnet werden

Umfang Onlinebanking

Mit rund drei Millionen Konten ist Onlinebanking der bisher erfolgreichste eCommerce-Dienst. Analysiert wurden die Angebote von 19 exemplarisch ausgewählten Finanzinstituten, dabei wurden 10 technisch verschiedene Systeme, die von 7 verschiedenen Unternehmen entwickelt/betrieben wurden, berücksichtigt.

Phishing als immer größeres Problem

Die seit Ende 2005 massiv auftretenden Phishingattacken mit Einzelschäden von über 9.000,- Euro sind geeignet das Vertrauen in das Onlinebanking massiv zu gefährden. Abgesehen von den materiellen Schäden sind Kosten im zweistelligen Millionenbereich für zusätzliche Sicherheitsmaßnahmen und hohe Vertrauensschäden zu verzeichnen. Dem gegenüber werden Phishing-Attacken technisch perfektioniert und erreichen zielgerichteter ihre Opfer. Trojaner, Individualisierung und "Social Hacking" kennzeichnen die nun aufkommende dritte Phishing-Welle.

So wurde getestet

Getestet wurde mit Hilfe von Testkonten, wobei nicht bloß technische, sondern auch rechtliche und ablauforganisatorische Aspekte und auch die Benutzerfreundlichkeit und die Transparenz der Systeme berücksichtigt wurden. Die analysierten Lösungen decken mehr als 99% der in Österreich genutzten Onlinebanking-Lösungen ab. Alle Angebote wurden mit einem Optimalprofil verglichen, dass mit gegenwärtiger Technik leicht erreichbar wäre.

Kein System ist optimal

Zieht man das Schulnotensystem heran, dann sind zwei Angebote (ein technisches System) als gut, 11 Angebote (sechs verschiedene technische Systeme) als befriedigend und 6 Angebote (vier verschiedene technische Systeme) nur als genügend anzusehen. In keinem Fall wurde ein sicherheitstechnisch optimales, benutzerfreundliches und vertragsrechtlich unbedenkliches System angeboten, kein System erreichte 100%.

Finanzinstitut	Gesamt	Betreiber / Entwickler
BKS	82%	Drei-Banken-EDV GmbH
BTV 3Banken Gruppe	79%	Drei-Banken-EDV GmbH
Volksbank Wien	71%	ARZ Allgemeines Rechenzentrum / v7.20
Hypo Alpe Adria	69%	ARZ Allgemeines Rechenzentrum / v7.20
Hypo Tirol	67%	ARZ Allgemeines Rechenzentrum / v7.20
Bankhaus Spängler	65%	ARZ Allgemeines Rechenzentrum / v7.20
BA-CA	70%	BA-CA
Erste Bank	70%	Erste Bank
Bank Burgenland	66%	Erste Bank
OÖ Landesbank - Hypo OÖ	68%	Raiffeisen Informatik Zentrum ELBA VERSION csTAN
RAIKA WienNÖ	65%	Raiffeisen Informatik Zentrum ELBA VERSION csTAN
easybank AG	65%	BAWAG
PSK	63%	BAWAG
Sparda Wien	62%	BAWAG
BAWAG	62%	BAWAG
VKB Linz	65%	Raiffeisen Informatik Zentrum ELBA VERSION sTAN
Oberbank	64%	Raiffeisen Informatik Zentrum ELBA VERSION TAN
Generalibank	61%	Generalibank
SPARDA Linz	59%	IBM / v2.2.5/16032006

Alle Systeme besitzen Basissicherheit

Die Mindestvoraussetzungen für sichere Internetkommunikation, verschlüsselte Datenübertragung, passwortgesicherter Zugang und Verwendung von Einmalcodes (TANs) bei Transaktionen, sind bei allen Banken vorhanden.

Doch schon bei den verwendeten TAN-Verfahren gibt es große Qualitätsunterschiede. Immerhin in acht Fällen werden veraltete Verfahren verwendet (Marktanteil ca. 22%).

Als eigentliche Schwachstelle des Onlinebankings entpuppen sich jedoch weniger die verwendeten TAN-Verfahren, sondern die per Post verschickten Listen, die es Angreifern ermöglichen auch mehrere TANs in Erfahrung zu bringen. In einem Extremfall wurden einem Konsumenten 20 TANs auf einmal entlockt!

Innovationskiller Sicherheit?

Um einen nicht abzuschätzenden Vertrauensverlust zu vermeiden, sind alle Institute gezwungen ihre bestehenden Verfahren, welche auch immer, zu verteidigen und als "sicher" einzustufen. Damit ist keine beschleunigte Einführung innovativer Lösungen möglich. So dürften auch in naher Zukunft PIN/TAN-Listen in den verschiedensten Varianten Standard im Onlinebanking bleiben.

Eine Wende bei der Einführung moderner Sicherheitsverfahren könnte sich nur durch neue legistische Rahmenbedingungen ergeben. Erst wenn der Gesetzgeber bestimmte Mindeststandards vorschreibt (z.B. eine hardwarebasierte TAN-Generierung, die Einhaltung der ONR17700, eine ISO 27001-Zertifizierung der Banken, ...) gäbe es für die Institute einen unverdächtigen Grund ihre bisherigen alten Systeme vollständig zu ersetzen.

Innovative Lösung nur bei zwei Banken

Das Problem der sicheren Verwahrung von Einmalkennungen (den TANs) kann man durch verschiedenste technische Verfahren lösen.

Zwei Banken haben sich dazu entschlossen das Token-Code-Verfahren als ausschließliches System eingesetzt wird. Bei diesem Verfahren wird durch eine scheckkartengroße Hardware jede Minute ein neuer TAN erzeugt, der nur eine Minute lang gilt. Somit ist das Ausspähen mehrer TANs nicht möglich. Diese Lösung wurde als innovativ und überdurchschnittlich gut zu bewerten.

Andere Institute bieten mit dem Mobile-Code-Verfahren oder der digitalen Signatur Alternativen zum klassischen TAN-Verfahren an, diese Verfahren zusammen erreichen jedoch nur einen Marktanteil von weniger als 2% aller Onlinebankingbenutzer.

Kunden könnten vor Phishing-Attacken besser geschützt werden

Durch eine Fülle oft einfacher Maßnahmen könnte die Phishingresistenz entscheidend gestärkt werden.

So könnte die simple Einführung einer Bankservicecard, die alle wichtigen Informationen, wie Webadresse, Zertifikatsdaten, Hotline- und Sperrnummer schon viele Gefährdungen und Verunsicherungen beseitigen. Ebenso die bessere technische Unterstützung bei der Vergabe von Passwörtern (Stichwort: Vermeiden von Trivialpasswörtern) oder genauere Informationen zur Viren- und Trojanerabwehr.

Die Sperrmöglichkeiten des Onlinekontos bei Verdacht eines Missbrauches sind ebenso verbesserungsbedürftig. Insbesondere fehlen klare Vereinbarungen, wie rasch Sperren wirksam werden, weiters ist bei vielen Instituten keine Sperre rund um die Uhr möglich. Auch die Möglichkeit Transaktionslimits festzulegen fehlt weitgehend.

Probleme ergeben sich auch beim Onlinesupport und der technischen Dokumentationen. Genauere Informationen über die erforderlichen Browsereinstellungen könnte helfen Schwachstellen zu vermeiden. Oft war nach einer Supportunterstützung der Konsumentencomputer in einem unnötigen Ausmaß unsicherer als vorher.

Ungeliebtes Kind Onlinebanking?

Im Gegensatz zu den allgemeinen AGBs der Banken fehlt zum Onlinebanking ein gemeinsamer Standard.

Praktisch durchgängig wirken die Vertragsbedingungen zum Onlinebanking (Online-AGBs) wie Baustellen, bei denen laufend in unsystematischer Form Ergänzungen angebracht werden. Kettenverweise, Verwendung ungebräuchlicher Begriffe oder technischer Fachbezeichnungen und unbestimmte Verweise auf Internetseiten machen es einem Laien praktisch unmöglich zum Zeitpunkt des

Vertragsabschlusses zu erkennen, wozu er tatsächlich zugestimmt hat und wozu er sich vertraglich verpflichtet hat.

Die Sorgfaltsverpflichtungen der Internetbedingungen enthalten in vielen Fällen technische Details und unbestimmte Bestimmungen, die für einen Konsumenten jedenfalls als überraschend angesehen werden können und sowohl einer umfassenden Aufklärung, als auch einer ausdrücklichen Vereinbarung bedürfen würden, was jedoch in vielen Fällen nicht der Fall war.

Als besonders problematisch sind die Versuche anzusehen einen generellen Haftungsausschluss der Bank für Kommunikationsfehler zu vereinbaren. Zum Teil werden dabei gröblich benachteiligende Klauseln verwendet.

Bei keinem Institut wurden Zusagen zur Mindest-Verfügbarkeit des Onlinebankings getroffen, dies war auch bei den reinen Onlinebanking-Instituten der Fall. Wenngleich im Untersuchungszeitraum in den meisten Fällen die Verfügbarkeit gegeben war, kam es in Einzelfällen auch zu Bankzeiten zu längeren Ausfällen, in einem Fall wurde sogar die Onlinebankingsitzung "wegen Überlastung" zwangsweise unterbrochen.

Bedenklich ist auch die Vorgangsweise vieler Banken dem Kunden generell jegliche Haftung für Schäden aufgebürdet wird, die aus missbräuchlicher Verwendung von Identifikationsmerkmalen entstehen.

Ein Teil der datenschutzrechtlichen Zustimmungserklärungen ist intransparent gestaltet und vermischt die Zustimmung der Datenweitergabe zu Gläubigerschutzzwecken mit der Zustimmung zur Weitergabe zu Werbezwecken.

Die Zustimmungserklärungen zu Datenverwendung und -weitergabe widersprechen in einer Reihe von Fällen der zu diesem Thema ergangenen OGH-Entscheidung 4 Ob 179/02f.

PLUS und MINUS im Onlinebanking

PLUS
- Verschlüsselte Datenübertragung
- insgesamt relativ gute Verfügbarkeit
- mehrheitlich bemühter Support

MINUS
- teilweise veraltete TAN-Verfahren
- Zettelwirtschaft mit TAN-Listen
- mangelhafte Dokumentationen und Informationen
- undurchsichtige Prozesse: der Kunde weiß eigentlich nicht, wann er PIN/TAN und wann er nur PIN eingeben muss
- unübersichtliche Screengestaltung (Frames, ...)
- undurchsichtige Vertragsgestaltung
- unzulässige Haftungsübertragungen an Konsumenten
- nicht dem Datenschutzgesetz entsprechende Zustimmungserklärungen
- fehlende Registrierung beim Datenverarbeitungsregister

Viele Verbesserungen sind möglich

Das Phänomen "phishing" wird immer noch zu sehr als technisches Sicherheitsproblem abgehandelt, damit gerät die kommunikationspolitische Perspektive völlig aus dem Blickfeld.

"phishing" ist deswegen möglich, weil Onlinebanking nicht als Gesamtprozess organisiert ist, sondern in unzulässiger Weise die Verantwortung für viele Ablaufaspekte auf den Konsumenten abgewälzt wird. So versuchen einige Banken die Verantwortung für Fehler der Post, der Telekom-Betreiber und der Internetservicebetreiber vollständig auf den Kunden abzuwälzen.

Wichtige Änderungen, die heute leicht möglich wären:

- Anpassung der TAN-Verfahren an den derzeitigen Stand der Technik
- Schaffung von verständlichen Online-Banking AGB's und Korrektur der bestehenden intransparenten bzw. gröblich benachteiligenden Klauseln
- Einrichtung effizienter Sperr- und Meldestrukturen, die Rund-um-die-Uhr verfügbar sind und ein rasches Reagieren auf Phishingangriffe erlauben
- Bessere Berücksichtigung der Richtlinie des Österreichischen Normungsinstitutes ONR 17700 zur sicheren Webapplikationen
- Erhöhung der Benutzerfreundlichkeit durch verbesserte und effektivere Hilfs- und Informationsfunktionen
- Optimierung und Korrektur der Onlinebanking-Prozesse in Hinblick auf das in der Studie verwendete Referenzmodell
- Entwicklung konkreter Best-Practice-Vorschläge für den Betrieb der Kundencomputer
- Der Konsument sollte die Möglichkeit geboten werden die wesentlichen Onlinebanking-Abläufe und Merkmale systematisch zu lernen und seinen Computer auf Onlinebanking-Tauglichkeit überprüfen lassen zu können.
- Der Gesetzgeber bzw. die vollziehenden Behörden sollten Mindeststandards bei Onlinebanking definieren. Dies könnte im Zuge einer Verordnung im Rahmen des Datenschutzgesetzes zur Umsetzung der §14-Sicherheitsbestimmungen erfolgen.
- Internetserviceprovider (ISP) sollten in Zusammenarbeit mit Banken das Beobachtungsnetz bezüglich illegaler Webdienste verbessern und somit rascher unzulässige Server sperren können.
- Verbesserte internationale Zusammenarbeit der ISPs sollte sowohl den Zeitpunkt des Bekanntwerdens einer Phishingattacke nach vorne verlegen, als auch die Zeitspanne zwischen erkennen und reagieren (Sperre der verwendeten Internetmittel) verkürzen.
- Die Betriebssysteme sollten mit sicheren Kernels ausgestattet werden, sodass Trojanerangriffe unwahrscheinlich werden. Dazu wäre ein EU-weites Zulassungs- und Evaluationsverfahren erforderlich, wie es als CE-Kennzeichen bei jeder Art von Konsumgütern mittlerweile selbstverständlich geworden ist.
- Einrichtung einer zentralen Beschwerde-, Melde- und Strafverfolgungseinrichtungen für Identitäts- und Informationsdiebstahl und alle eCommerce-Belange.

Kontakt:

Mag. Gernot Prett, Büro Staatssekretär Dolinschek, BMSG, 71100/3379
Dr. Hans G. Zeger, Projektleiter der Studie
Mitglied des Datenschutzrates im Bundeskanzleramt und Obmann der "ARGE DATEN - Österreichische Gesellschaft für Datenschutz" (www.zeger.at, 0676/9107032)