Identitätsschutz: Eine zentrale Herausforderung für IT und E-Commerce[1]

Der Schutz von Identitäten im Internet ist eine überaus komplexe Aufgabe, die neben technischen auch weitere, nicht zuletzt rechtliche Aspekte umfasst. Interdisziplinarität sowie Zusammenarbeit von Wissenschaft, Behörden und Unternehmen sind daher unabdingbar, um die Problematik sachgerecht zu erfassen und Lösungsansätze zu entwickeln.

I. Identitätsschutz als Voraussetzung für erfolgreichen E-Commerce

1. Identität – Grundlage verbindlicher elektronischer Kommunikation

Der Schutz von Identitäten ist eine zentrale Herausforderung für die Nutzung des Internets. Die Identität von Personen ist die Grundlage verbindlicher elektronischer Kommunikation und damit des elektronischen Geschäftsverkehrs, ebenso des E-Government. Denn die elektronisch übermittelte Erklärung, sei es ein Überweisungsauftrag, ein elektronischer Rechtsbehelf, eine Klage oder sonstige Verfahrenshandlung, wird einer bestimmten Person, dem Erklärenden, anhand von Identifizierungsdaten zugeordnet, die die Identität dieser Person festlegen.

Identifizierungsdaten (Identitätsmerkmale), begleiten uns von Geburt an in fast allen Lebenssituationen. Klassische Identitätsmerkmale wie Name, Geburtsdatum und -ort sowie Wohnungsanschrift werden seit Jahrhunderten zur Identifizierung verwendet. Mit der modernen Verwaltung und vor allem mit der EDV wurden Nummern eingeführt: Der Kunde, etwa eines Online-Versandhändlers, bekommt eine Kundennummer, unser Personalausweis ist nummeriert, bald soll sogar jeder Bundesbürger eine bundeseinheitliche, eindeutige und dauerhafte (Steuer)-Identifikationsnummer bereits ab der Geburt erhalten.[2] Nummern sind uns so vertraut, dass ihre Notwendigkeit kaum noch hinterfragt wird, obwohl viele personenbezogene Nummern offensichtlich entbehrlich sind.

---

[1] Um Fußnoten und Abbildungen erweiterte Fassung des Vortrags der Sprecher des Vorstands der Arbeitsgruppe Identitätsschutz im Internet e.V. (a-i3), Prof. Dr. iur. Georg Borges, Prof. Dr. rer. nat. Jörg Schwenk beim IT-Gipfel der Bundesregierung am 18.12.2006.

[2] Unter der neuen Identifikationsnummer werden Daten wie der Name (Familienname, frühere Namen, Vorname), ggf. der Doktorgrad, Tag und Ort der Geburt, Geschlecht, die gegenwärtige Anschrift der alleinigen oder der Hauptwohnung und der Sterbetag gespeichert. Siehe dazu BRat-Drucks. 705/06, S. 4.

Körperliche Eigenschaften, aus denen sich biometrische Daten gewinnen lassen, gehören zu den ältesten und zugleich den modernsten Identitätsmerkmalen.[3] So konnte man eine Person schon immer über ihr Aussehen oder ihre Stimme identifizieren – inzwischen gibt es biometrische Verfahren, die eine Gesichts-[4] oder Stimmerkennung[5] ermöglichen.

Zahlreiche Anwendungen im Internet basieren auf Authentisierungsverfahren, die vom Nutzer die Angabe von Nachweiszeichen, wie etwa PIN, TAN und Passwörter, für den Nachweis der eigenen Identität verlangen. Teilweise werden bei der Authentisierung auch Daten, die in eigens dafür erstellten Speichermedien enthalten sind (z.B. Signaturkarte), verlangt.

2. Identitätsmissbrauch – Gefahr für die elektronische Kommunikation

Ohne die Identifizierung von Personen anhand derartiger Daten kommt verbindliche elektronische Kommunikation nicht aus. Daher ist der Identitätsmissbrauch eine Gefahr für die elektronische Kommunikation, vor allem für den elektronischen Geschäftsverkehr.

Identitätsmissbrauch wird hier in einem engen Sinne verstanden: Gemeint ist die vom Täter hervorgerufene falsche Zuordnung einer Handlung zu einer Person. Man kann hier auch von Identitätsanmaßung sprechen. Identitätsmissbrauch liegt immer vor, wenn eine Handlung in Wirklichkeit nicht oder so nicht von der Person stammt, der sie nach dem Anschein zuzuordnen ist, wenn also beispielsweise ein Überweisungsauftrag nicht vom Kontoinhaber, sondern von einem Dritten veranlasst wurde.
Identitätsmissbrauch gab es schon immer und wird es immer geben. Schon im ersten Buch der Bibel wird vom Identitätsmissbrauch des Jakob berichtet, der sich als sein Bruder Esau ausgab, um eine Verfügung – den Segen und damit die Übertragung der Leitungsmacht – seines alten Vaters Isaak zu erschleichen.[6]

Aber erst die elektronische Kommunikation, namentlich das Internet, erleichtert den Identitätsmissbrauch und macht ihn attraktiv. Musste Jakob sich einst noch arg be-

---

[3] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet ausführliche Informationen zur Biometrie, auch zur historischen Entwicklung:
http://www.bsi.de/fachthem/biometrie/einfuehrung.htm.
Siehe dazu auch *Hornung*, Die digitale Identität - Rechtsprobleme von Chipkartenausweisen, 2005, S. 75; *Weichert*, CR 1997, 369 f.

[4] Einen guten Überblick über die Funktionsweise von Gesichtserkennung gibt das BSI: http://www.bsi.bund.de/fachthem/biometrie/dokumente/Gesichtserkennung.pdf.

[5] Eine niederländische Bank setzt ein Stimmerkennungsverfahren im Telefonbanking ein: http://www.voicevault.com/pdf/P06065uk.pdf.

[6] Gen. 26, 13 ff.

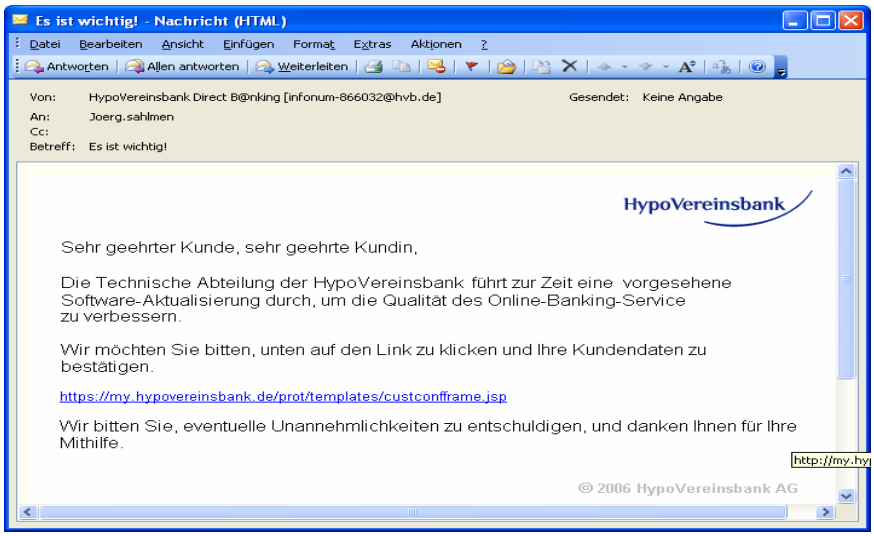
mühen als er sich ein Ziegenfell umband, um für den blinden Vater Isaak wie der behaarte Esau zu wirken, würde er heute dem Isaak eine E-Mail mit der Absenderkennung des Esau schicken und sich durch Passwort und Transaktionsnummern ausweisen.

3. Phishing und andere internetbasierte Betrugsformen

Als aktuelle Gefahrenschwerpunkte des Identitätsmissbrauchs sind Phishing und Identitätsdiebstahl zu nennen. Mit Identitätsdiebstahl ist nicht die Beschaffung von Identitätsdaten[7], sondern die Verwendung nicht geheimer Identifizierungsdaten gemeint, wie Name und Anschrift, etwa um eine Bestellung im Namen eines anderen aufzugeben. In beiden Fällen kommt es zu einem Identitätsmissbrauch.

Interessant ist für das Thema des Identitätsschutzes die Dimension des Phishing[8] und vor allem seine Dynamik. Auch wenn es keine genauen Zahlen gibt, wird die Dynamik aus den vorhandenen Angaben sehr deutlich. Die durch die Anti-Phishing Working Group ermittelte Zahl an Phishing-Angriffen lag im Oktober 2006 bei 26.877, im Oktober 2005 noch bei lediglich 15.820.

Besonders beeindruckend ist eine aktuelle Studie von Comsumerreports[9], wonach 8 % der insgesamt 2000 befragten Haushalte ihre persönlichen Daten aufgrund einer Phishing-Mail preisgegeben haben. Einen Schaden durch Phishing haben 0,7 % der Befragten erlitten. Dieser Wert ist auf Deutschland



Beispiel für eine Phishing-Mail, zahlreiche weitere sind abrufbar unter www.a-i3.org, Mail-Archiv – Phishing.

---

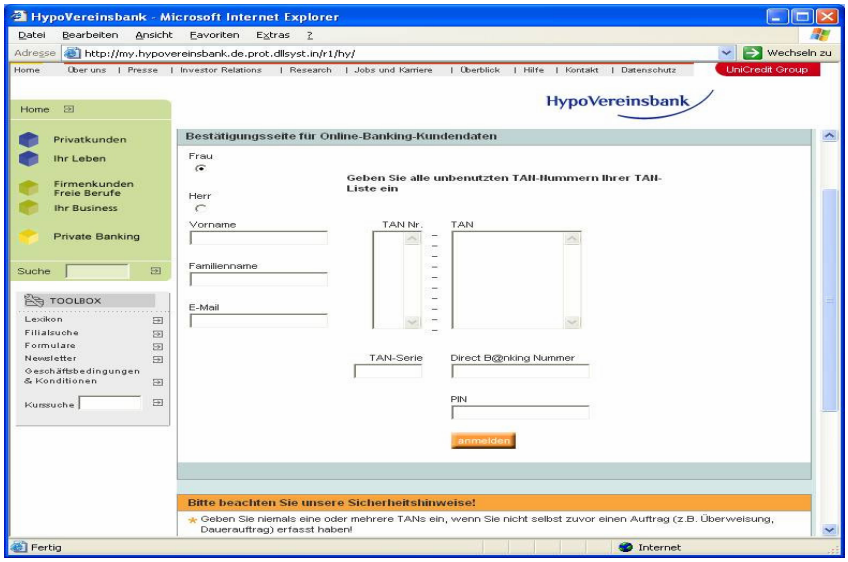
[7] Die Beschaffung von Identifizierungsdaten kann zum einen durch Angriffe auf den einzelnen Nutzer erfolgen. Zum anderen sind aber, insbesondere in den USA, immer wieder Fälle bekannt geworden, in denen sich Täter Zugang zu Datenbanken von Unternehmen und Behörden verschafft haben, um personenbezogene Informationen auszulesen. Eine Übersicht über die zahlreichen Fälle bietet die Website www.privacyrights.org/ar/ChronDataBreaches.htm (Stand 12.12.2006).

[8] Eine Erläuterung des Phishing und der anderen Angriffsmethoden ist unter www.a-i3.org, Themen - Phishing&Pharming, abrufbar (www.a-i3.org/content/view/931/202).

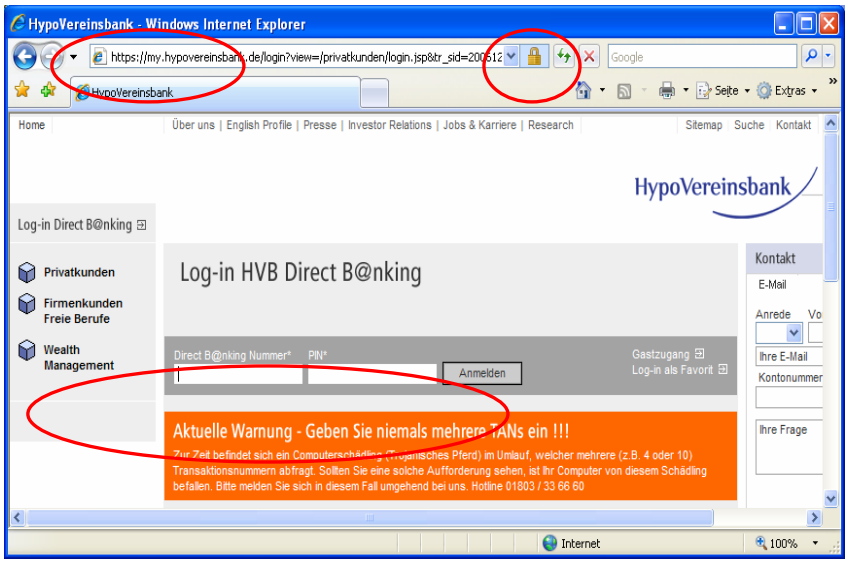
[9] www.consumerreports.org/cro/electronics-computers/online-protection-9-06/overview/0609_online-prot_ov1.htm

nicht ohne weiteres übertragbar, bestätigt aber, dass ein nicht unerhebliches Schadenspotential besteht, wenn die Sicherheitssysteme unzureichend sind.

Das klassische Phishing mit dem Versand gefälschter E-Mails und dem Link auf eine falsche Website, auf der die Kunden PIN und TAN eingeben sollen, wird zunehmend durch komplexere und gefährlichere Angriffe ersetzt. Eine aktuelle Studie von Gartner prognostiziert, dass Phishing-Angriffe gezielter, auf den einzelnen Nutzer zugeschnitten sein werden.[10] Außerdem nimmt die Bedrohung durch Malware-basierte Angriffe zu: Nach aktuellen Schätzungen werden derzeit 80 – 90 % der Schäden im deutschen Onlinebanking durch Trojaner verursacht. Es gibt inzwischen eine beeindruckende Vielfalt an verwendeten Trojanern und Angriffsstrategien. SSL und ähnliche Schutzinstrumente werden durch einige der aktuell verwendeten Trojaner mühelos überwunden. Nach Einschätzung zahlreicher Fachleute werden Trojaner in der näheren Zeit das wesentliche Werkzeug bei Angriffen gegen das Onlinebanking sein. Darauf reagierte jetzt beispielsweise die Hypovereinsbank mit einem auffälligen Hinweis an prominenter Stelle, der vor einem aktuellen Trojaner-Angriff warnt.



Beispiel für eine Phishing-Website



Schon das klassische Phishing hat deutlich gemacht, wie verwundbar der elektronische Geschäftsverkehr gegen diese Bedrohung ist und dass die traditionellen Schutzmechanismen, gegen Identitätsmissbrauch keinen ausreichenden Schutz bieten. Die Nutzer sind vielfach überfordert. Der durchschnittliche Nutzer kann

[10] Gartner-Studie vom 1.11.2006, „Phishing Attacks Leapfrog Despite Attempts to Stop Them“, S. 10.

Webadressen nicht lesen und daher gefälschte Domains nicht erkennen. Er versteht SSL nicht und missdeutet die Bedeutung des Schlosssymbols.[11] Er weiß nicht, dass die Informationen im Hauptfenster des Browsers nicht geschützt sind, dass also komplette Bankwebseiten durch einfaches Kopieren nachgeahmt werden können

Bei Trojanerangriffen stößt auch die Aufklärung des Kunden (dazu unten II.2.a) an ihre Grenzen: Die oben wiedergegebene Warnmeldung der Hypovereinsbank wird wirkungslos, wenn der Trojaner sich auf die Anforderung nur einer TAN beschränkt. Kunden können dann nicht mehr feststellen, ob die Eingabeaufforderung von ihrer Bank oder von einem Schadprogramm stammt.

Daher ist die wichtigste Lehre aus der Phishing-Problematik, dass die Sicherheit der elektronischen Kommunikation – gerade auch unter dem Gesichtspunkt des Missbrauchs von Identifizierungsdaten – eine Aufgabe ist, die dauernde Wachsamkeit und stete Fortentwicklung der Schutzmaßnahmen erfordert.

4. Bedrohung der Rechtssicherheit durch Identitätsmissbrauch

Das Ausmaß der durch Identitätsmissbrauch entstehenden Folgeprobleme ist nicht zu unterschätzen. Identitätsmissbrauch ist eine durchaus ernstzunehmende Bedrohung für die Rechtssicherheit der elektronischen Kommunikation. Im E-Commerce ist die Transaktionssicherheit gefährdet, was sich am Beispiel des so genannten Anscheinsbeweises verdeutlichen lässt. Mit dem Anscheinsbeweis wird im elektronischen Geschäftsverkehr traditionell der Nachweis der Identität des Nutzers, etwa des Bankkunden, geführt. Es wird hier ein Anscheinsbeweis dafür angenommen, dass eine Überweisung, die unter Verwendung von PIN und TAN veranlasst wird, vom Bankkunden stammt.

Wegen der Missbrauchsrisiken wird dieser Anscheinsbeweis von den deutschen Gerichten bei einfachem Passwortschutz nicht anerkannt.[12] Dies hat zur Folge, dass der Geschäftspartner kaum Beweismöglichkeiten für die Echtheit einer Erklärung, etwa ein Angebot oder eine Bestellung, hat und seine Rechte im Streitfall nicht durchsetzen kann.

Im Onlinebanking wird der Anscheinsbeweis, der vor zwei Jahren noch allgemein bejaht wurde, für das PIN/TAN-Verfahren in der aktuellen Literatur vermehrt bestritten – ausdrücklich wegen der Phishing-Problematik.[13] Wenn man dieser Einschätzung folgen würde, könnte die Bank nicht mehr nachweisen, dass eine bestimmte Über-

---

[11] http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf

[12] Siehe etwa OLG Köln, CR 2003, 55; erstinstanzlich LG Bonn, CR 2002, 293, 294; LG Bonn, CR 2004, 218, 219. OLG Naumburg, NJOZ 2005, 2222, 2224. Alle Urteile sind abrufbar unter www.a-i3.org, Recht – Urteile.

weisung von ihrem Kunden stammt und müsste in Streitfällen den Überweisungsbetrag selbst tragen. Eine solche Rechtslage hätte allerdings leicht problematische Anreize zur Folge. Die Missbrauchsrisiken gefährden daher die rechtliche Transaktionssicherheit im E-Commerce.

Für das Vertrauen in die Rechtssicherheit im Internet kommt es nicht zuletzt auf eine angemessene Reaktion auf Rechtsverletzungen wie Phishing an. Dazu gehört eine erkennbare, koheränte Verfolgung von Straftaten[14] ebenso wie eine sachgerechte Haftungsregelung. Überzogene Verhaltensanforderungen an Anbieter oder Nutzer können das Vertrauen in die Nutzung des Internets schädigen, vielleicht noch mehr als die Angriffe selbst. Aktuelle Entwicklungen mahnen auch hier zu erhöhter Aufmerksamkeit.

Die Rechtsprechung stellt teilweise extreme Anforderungen an Unternehmen. So vertrat beispielsweise das OLG Brandenburg in einem Fall des Identitätsdiebstahls bei einem Auktionshaus die Ansicht, das Auktionshaus müsse den „Identitätsklau“ durch Dritte verhindern.[15] Eine solche Wertung, die sich durchaus auf andere Bereiche übertragen ließe, ist nicht unproblematisch, da Angriffe nie völlig ausgeschlossen werden können.

Auf der anderen Seite werden auch Schutzpflichten von Nutzern gefordert, die ihn möglicherweise überfordern. Der Nutzer kann nicht beliebig viele Passwörter geheim halten, er kann, wie dargestellt, komplexe Fälschungen nicht erkennen, er kann komplexen technologischen Schutz weder einrichten noch damit umgehen. Eine Überforderung des Nutzers durch überzogene Verhaltenspflichten oder Haftungsrisiken untergräbt sein Vertrauen in das Internet. Ein massiver Vertrauensverlust, der bisher durch das Phishing glücklicherweise nicht eingetreten ist, wäre fatal.

Nicht anders wird es im E-Government liegen. Sollte es in Verwaltungsverfahren in nennenswertem Umfang zu Identitätsmissbrauch kommen, etwa durch gefälschte Erklärungen, wird es schwer werden, den Bürger für die elektronische Verwaltung zu begeistern. Besonders bedrohlich erscheint die Möglichkeit der Verfälschung von Abstimmungen und Wahlen. Dies gilt genauso für die Privatwirtschaft, etwa die elektronische Abstimmung in der Hauptversammlung einer börsennotierten Aktiengesellschaft, die künftig möglich sein soll.[16]

---

13 *Kind/Werner*, CR 2006, 353, 359 f.; *Erfurth*, WM 2006, 2198, 2205.

14 Vor dem Landgericht Frankfurt findet derzeit ein Prozess gegen sieben Angeklagte statt, die mit Hilfe von Trojanern Zugangsdaten zu insgesamt 69 Online-Bankkonten ausgespäht haben sollen, www.a-i3.org, News vom 15.12.2006 (https://www.a-i3.org/content/view/1004/214/).

15 OLG Brandenburg, ZUM 2006, 220 m. Anm. *J. Meyer*. Das Urteil ist ebenfalls abrufbar unter www.a-i3.org, Recht – Urteile.

16 Vgl. Art. 8 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Ausübung der Stimmrechte durch Aktionäre von Gesellschaften, die ihren eingetragenen Sitz in ei-

II. Die Bewältigung der Herausforderung

Die Aufgabe, den Schutz von Identitäten als Grundlage für Vertrauen in den elektronischen Geschäftsverkehr zu gewährleisten, ist eine Herausforderung an Unternehmer wie an die öffentliche Hand bei deren Bewältigung Forschung und praktische Umsetzung Hand in Hand gehen müssen.

1. Problemstruktur und Anforderungen

Die Anforderungen an die Lösungsansätze ergeben sich aus der Problemstruktur. Am Beispiel des Phishing werden die beiden wesentlichen Schwachstellen deutlich: Technische Sicherheit kann nie lückenlosen Schutz bieten, schon weil nicht jede künftige Missbrauchsmöglichkeit antizipiert werden kann. Folglich ist eine stetige Verbesserung der Technik erforderlich, um neuen Gefahren zu begegnen.

Der zweite Problemschwerpunkt liegt in der Überforderung des durchschnittlichen Internetnutzers. Er ist in vielfältiger Weise anfällig für Angriffe, da er nicht die Kenntnisse und Fähigkeiten hat, um sich selbst hinreichend zu schützen. Umso mehr sind Information und Aufklärung geboten, um dem Nutzer die relevanten Informationen zu geben. Erforderlich ist auch die Definition angemessener Verhaltensstandards, also der Maßstab an Sorgfalt, der vom Nutzer erwartet werden kann und für den er das Risiko trägt.

2. Erfolgreiche Lösungsansätze

a) Technische Lösungen – sichere Authentisierung im Onlinebanking

Die derzeit im Bereich des Onlinebanking eingeführten technischen Lösungen, die im aktuellen Heft der Zeitschrift Finanztest (Ausgabe 1, 2007) einer breiten Öffentlichkeit vorgestellt werden, wurden in Bankenkreisen und auf dem 1. Interdisziplinären Symposium Phishing und Onlinebanking, das im April 2006 gemeinsam von der Arbeitsgruppe Identitätsschutz im Internet (a-i3) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ausgerichtet wurde, diskutiert.[17]

Das indizierte TAN-Verfahren, das seit Herbst 2005 von einigen Banken eingeführt wurde, hat die Zahl der Phishing-Angriffe auf diese Banken deutlich reduziert. Zwar bietet es keinen vollständigen Schutz, da es anfällig gegen so genannte Man-in-the-

---

nem Mitgliedstaat haben und deren Aktien zum Handel auf einem geregelten Markt zugelassen sind, sowie zur Änderung der Richtlinie 2004/109/EG, KOM 2005/0685. Der Vorschlag ist abrufbar unter: http://eur-lex.europa.eu/LexUriServ/site/de/com/2005/com2005_0685de01.pdf

17 Die Arbeitsgruppe Identitätsschutz im Internet e.V. (a-i3) führt Schulungen zu diesen Themen durch, und informiert im Bedarfsfall in öffentlichkeitswirksamer Weise über zukünftige, realistische Bedrohungen. Informationen zu dem Symposium sind abrufbar unter www.a-i3.org, Forschung – a-i3/BSI-Symposium (https://www.a-i3.org/content/view/948/234/).

middle-Attacken ist[18], bewirkt aber, dass die auch international agierenden Phisher auf einfachere Ziele (z.B. Banken mit dem alten TAN-Verfahren) ausweichen.

Das zuerst von der Postbank eingeführte mobile TAN-Verfahren bietet Schutz gegen alle heute bekannten Angriffe, da hier alle transaktionsrelevanten Daten (Zielkonto, Betrag, mTAN) von der Bank zum Kunden über einen sicheren GSM-Kanal übertragen werden.

Beispiel: eTAN

Ein gutes Beispiel für Investitionsschutz durch eine genaue Analyse der technischen Bedrohungslage bieten die verschiedenen Varianten der eTAN-Verfahren. Direkt nach Bekanntwerden der ersten Phishing-Fälle wurden Geräte als Lösung angepriesen, die eine einmalig verwendbare TAN entweder zeitabhängig oder abhängig von einer einzugebenden, zufällig gewählten „Challenge“, erzeugten. Man kann jedoch leicht zeigen, dass diese Geräte gegenüber der iTAN-Lösung nur eine marginale Sicherheitsverbesserung bewirken, bei hohen Investitionen insbesondere in die Schulung der Nutzer.

Eine kleine Variante, in der Praxis meist als eTAN+ bezeichnet, verbessert die Situation enorm: Wenn der Kunde zusätzlich noch (Teile der) Zielkontonummer eintippt, sinkt die Erfolgswahrscheinlichkeit für einen Angreifer mit jeder eingegebenen Ziffer um den Faktor zehn. Angriffe jedweder Art (Phishing, Pharming, Trojaner) sind damit nicht mehr möglich, und dies bei annähernd gleichen Kosten wie für die „einfache“ eTAN-Lösung.

Gegenüber HBCI bietet eTAN+ die Chance, mehr als nur Banktransaktionen abzusichern: Für jede Aktion im Internet wäre so überprüfbar, ob sie von einem autorisierten Nutzer initiiert wurde. Die notwendige Interoperabilität ließe sich über eine Service-orientierte Architektur der Hintergrundsysteme (SOA) abbilden.

b) Information und Aufklärung der Nutzer

Genauso wichtig sind Information und Aufklärung der Nutzer über die Problematik, wie sich am Beispiel des Phishing zeigen lässt. Phishing ist gefährlich, solange der Nutzer nicht damit rechnet, das gefälschte E-Mails und gefälschte Bankwebseiten im Umlauf sind.

Hier hat sich viel getan. Unternehmen, Behörden und Organisationen weisen auf die Gefahren des Phishing hin. Das Bundesamt für Sicherheit in der Informationstechnik

---

[18] Pressemeldung der a-i3 vom 11.11.2005 abrufbar unter www.a-i3.org, Über uns – Pressemeldung,

(BSI) und die Arbeitsgruppe Identitätsschutz im Internet (a-i3) haben Informationsportale speziell zur Internetsicherheit bzw. zum Identitätsschutz im Internet aufgebaut, die stark genutzt werden. Zahlreiche Unternehmen und Behörden weisen auf diese Angebote hin. Selten sind bisher Angebote zur individuellen Beratung rund um Sicherheitsfragen und Identitätsschutz. Die Verbraucherschutzverbände sind hier aktiv, vor allem bietet das Beratungstelefon der a-i3 zum Phishing den Bürgern kostenlosen und barrierefreien Zugang zu Expertenrat rund ums Phishing.

Wie erfolgreich Information und Aufklärung sein können, zeigt sich derzeit im Zusammenhang mit Finanzagenten, die für den Transfer der gephishten Gelder ins Ausland eingesetzt werden und häufig über E-Mail und gefälschte Webseiten angeworben werden. A-i3 hat eine Dokumentation dieser Anwerbeversuche aufgestellt, die über unser Portal abrufbar ist[19], und identifizieren damit diese Art von Betrug. Die Zugriffsstatistik der Website (www.a-i3.org) zeigt, dass viele Zugriffe auf diese Dokumentation über Suchmaschinen erfolgen, mit denen die Nutzer speziell nach den Websites der vermeintlichen Unternehmen gesucht haben. Die Personen, die als Finanzagenten angeworben werden sollen, informieren sich also im Internet über den potentiellen Arbeitgeber, stoßen auf diese Dokumentation und werden dadurch gewarnt und davor bewahrt, als Mittelsmann für Phisher tätig zu werden. Dieser Zusammenhang wird durch das Beratungstelefon bestätigt, da dort häufig die Adressaten der vermeintlichen Jobangebote anrufen, um sich zu vergewissern.

c) Erforschung der Gefährdungspotentiale und Lösungsmöglichkeiten

Die Erforschung von Gefährdungspotentialen und die darauf aufbauende Entwicklung von Lösungsmöglichkeiten sind von zentraler Bedeutung. Beim Phishing sind etwa Banken, IT-Industrie, Behörden wie BKA, BSI und andere sowie Wissenschaft, etwa Fraunhofer-Institut, HGI oder a-i3, intensiv tätig. Die Europäische Union fördert ein Projekt zur technischen Erforschung des Phishing, das unter anderem von Symantec und der Universität Leuven betrieben wird.

Auf der normativen Seite werden Rechtsprechung und Gesetzgebung zum Phishing analysiert und durch wissenschaftliche Untersuchungen begleitet, in Deutschland derzeit am intensivsten durch die a-i3. Auch dies hat Auswirkungen. So ist etwa die Klarstellung, dass Phishing und Geldtransfer strafbar sind, die Grundlage für eine konsequente Strafverfolgung.[20]

Wie das Beispiel der verschiedenen TAN-Varianten zeigt, lohnt es sich durchaus, Gefährdungspotenziale zu ermitteln, bevor entsprechende Schadensfälle aufgetreten

---

https://www.a-i3.org/images/stories/pressemeldung/pressemeldung_itan_lang.pdf

19 Abrufbar unter www.a-i3.org, Mail-Archiv – Geldwäsche (https://www.a-i3.org/content/category/14/57/218/).

20 Zu dem laufenden Prozess vor dem Landgericht Frankfurt a.M. siehe oben Fußnote 14.

sind. So wurde ein Man-in-the-middle-Angriff, vor dem a-i3 bereits im November 2005 gewarnt hat, im Juli 2007 gegen die amerikanische Citibank durchgeführt[21]. Die Citibank verwendete dabei das einfache eTAN-Verfahren.

Aktuelle Forschungsprojekte der a-i3 umfassen einen Dialog mit Mobilfunkbetreibern zum besseren Verständnis der Sicherheit von mobilen TAN-Verfahren und die prototypische Implementierung von Trojanern, um den finanziellen und zeitlichen Aufwand zur Umsetzung von Crimeware-Attacken besser abschätzen zu können (Es versteht sich von selbst, dass diese Trojaner-Prototypen niemals publiziert werden.).

III. Aufgaben für die Zukunft

Im Ergebnis gibt es eine Reihe guter Ansätze, um das Problem des Phishing und ähnliche Formen des Identitätsmissbrauchs in den Griff zu bekommen. Gleichwohl bleiben dringende Aufgaben für die Zukunft:

1. Verbesserung der elektronischen Signatur

Die elektronische Signatur bedarf der Verbesserung. Eine aktuelle Studie zur Sicherheit signaturgesetzkonformer Softwarelösungen hat gezeigt, dass Dateien, die mit einer qualifizierten Signatur versehen sind, unbemerkt verfälscht werden können.[22] Da die elektronische Signatur die zentrale Grundlage für Authentisierung und Verfälschungsschutz darstellen soll[23], kommt es entscheidend auf die Sicherheit der Signaturverfahren an. Hier muss nachgebessert werden.

2. Erweiterung der Aufklärung von Nutzern

Information und Aufklärung der Nutzer sollten weiter verbessert werden, um den Erfolg noch zu steigern. Die vorhandenen Informationsangebote sollten besser bekannt gemacht werden. Hierzu können öffentliche Hand und Privatwirtschaft mit geringem Aufwand erheblich beitragen.

---

21 http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html

22 *Langweg*, "Malware Attacks on Electronic Signatures Revisited". In: J. Dittmann (ed.): *'Sicherheit 2006'. Konferenzband der 3. Jahrestagung Fachbereich Sicherheit der Gesellschaft für Informatik*, 2006, S. 244-255.

23 Dies zeigt nicht zuletzt die Einführung des § 371a der Zivilprozessordnung (ZPO) im Jahr 2001, damals § 292a ZPO, der erstmals eine gesetzliche Regelung des Anscheinsbeweises enthält. Nach § 371a ZPO begründet die qualifizierte elektronische Signatur einen Anschein dahin, dass die signierte Datei vom Inhaber der Signaturkarte signiert wurde. Dazu *Borges*, Verträge im elektronischen Geschäftsverkehr, 2003, S. 505 ff.

Eine Verbesserung der vorhandenen Angebote kann insbesondere dadurch erreicht werden, dass die Beteiligten, soweit möglich, ihre Leistungen koordinieren. Das Risiko widersprechender Informationen wird hierdurch erheblich verringert. Zudem würden erhebliche Synergien bei der Informationsbeschaffung erzielt, die derzeit noch durch verschiedene Stellen erfolgt.

3. Erforschung, Formulierung und Durchsetzung von Verhaltensstandards

Große Bedeutung wird der Erforschung, Formulierung und praktischen Umsetzung von Verhaltensstandards zukommen.

Im Bereich der Anforderungen an Unternehmen erscheint ein Selbstregulierungsmechanismus sachgerecht, der Forschung und Erfahrungen aus der Praxis aufnimmt und der möglicherweise, ähnlich dem *Corporate Governance Kodex*, in ein Regelwerk münden könnte.

Für die Anforderungen an Nutzer sind vor allem Rechtsprechung und Wissenschaft gefragt, eine differenzierte, sachgerechte Regelung zu entwickeln. Hier werden Fallgruppen zu bilden sein. Als Beispiel kann hier etwa die brisante Problematik von W-LAN sowie der Virenschutz herangezogen werden. Nach aktuellen Berichten sind 22 % der WLANs offen und nur ein Sechstel der Funknetze sind sicher verschlüsselt.[24] Dem durchschnittlichen Nutzer ist das Problem aber nicht bewusst, und er ist nicht in der Lage, ein sicheres WLAN einzurichten. Folglich kann der Nutzer die daraus entstehenden Risiken nicht tragen, solange nicht die Industrie einfache, nutzerfreundliche Lösungen anbietet und der Nutzer nicht hinreichend informiert wird.

Anders liegt es beim Virenschutz: Hier stehen dem Nutzer heute preiswerte oder gar kostenlose, einfache, zuverlässige Systeme zur Verfügung. Dies spricht dafür, dass der Einsatz von Virenschutzsoftware dem Verbraucher zumutbar ist.

Zur Gewährleistung des Identitätsschutzes durch Fortentwicklung der Technik und Entwicklung angemessener Verhaltensregeln sind vor allem Unternehmen, Wissenschaft und Rechtsprechung berufen.

4. Flankierung durch Rechtsprechung und Gesetzgebung

Die Politik kann diese Prozesse flankierend unterstützen, durch Förderung geeigneter Projekte und Gestaltung der öffentlichen Diskussion. Punktuelle Gesetzgebungs-

---

[24] Siehe dazu z.B. *Endres*, c´t 2006, Heft 25, S. 98 unter Berufung auf eine Studie der RWTH Aachen. Zur Störerhaftung bei einem ungesicherten Funknetz siehe z.B. das Urteil des LG Hamburg, MMR 2006, 763 m. Anm. *Mantz*.

maßnahmen[25] können hilfreich oder gar unabdingbar sein, sind freilich auch schwierig, wie das Beispiel der geplanten Strafrechtsänderung[26] zeigt. Die Diskussion sollte unter Einbeziehung von Praxis und Wissenschaft mit hoher Intensität und Dringlichkeit geführt werden. Dasselbe gilt für die Verbesserung des Signaturgesetzes.

Prof. Dr. Georg Borges
Lehrstuhl für Bürgerliches Recht, deutsches und internationales Handels- und Wirtschaftsrecht, insbes. Recht der Medien und der Informationstechnologie

Ruhr-Universität Bochum
Universitätsstraße 150, GC 7/146
44801 Bochum

E-Mail: georg.borges@rub.de

Tel.: (+49) (0)234 / 32-26775
Fax: (+49) (0)234 / 32-14700

Prof. Dr. Jörg Schwenk
Lehrstuhl für Netz- und Datensicherheit

Ruhr-Universität Bochum
Universitätsstraße 150, IC 4/160
44801 Bochum

E-Mail: joerg.schwenk@rub.de

Tel. (+49) (0)234 / 32-26692
Fax: (+49) (0)234 / 32-14347

---

25 Auf dem Gebiet des Identitätsdiebstahls („Identity Theft“) und des Phishings haben zahlreiche Staaten der USA Gesetze erlassen. Eine Übersicht dazu ist hier abrufbar: http://www.ncsl.org/programs/lis/privacy/idt-legis.htm . Von Interesse ist - insbesondere im Bereich des Onlinebanking – ein Vorschlag einer Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt v. 1.12.2005, 2005/0245 (COD), abrufbar unter https://www.a-i3.org/images/stories/recht/zahlungsdiensterichtlinie.pdf. Weitere Informationen auch unter www.a-i3.org, Recht – Gesetzgebung.

26 Der Gesetzesentwurf der Bundesregierung ist abrufbar unter:
http://www.bmj.bund.de/media/archive/1317.pdf.
Zum Teil heftig kritisiert wurde der Entwurf vom Bundesrat, BRat-Drucks. 676/1/06
http://www.bundesrat.de/cln_050/SharedDocs/Drucksachen/2006/0601-700/676-1-06,templateId=raw,property=publicationFile.pdf/676-1-06.pdf
Siehe auch die Stellungnahme des Branchenverbands BITKOM:
http://www.bitkom.org/files/documents/Stellungnahme_BITKOM_StrAendG_11_10_06.pdf
Zusammenfassend zum Ganzen www.a-i3.org, News vom 14. 11.2206 (https://www.a-i3.org/content/view/953/235/) und *Stuckenberg*, F.A.Z. vom 6.12.2006, S. 25.