

Phishing: Datenbetrug auf dem Höhepunkt – Was Wirtschaft und Verbraucher tun können

Statement von Prof. Dieter Kempf

Mitglied des Präsidiums

**Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.**

Vorsitzender

Deutschland sicher im Netz e.V.

Pressekonferenz

Berlin, 2. September 2008

- Es gilt das gesprochene Wort -

Meine sehr geehrten Damen und Herren,

auch von mir ein herzliches Willkommen zu unserer Pressekonferenz zum Thema „Phishing“. Dieser technische Fachbegriff, der für den professionellen Diebstahl von Bank-Geheimzahlen steht, ist heute leider einer breiten Öffentlichkeit bekannt. Angriffe auf Daten beim Online-Banking sind ein Risiko, vor dem sich nicht nur eine Minderheit schützen muss und schützen kann. 22 Millionen Deutsche nutzen die Internetangebote ihrer Bank, jeder Dritte zwischen 16 und 74 Jahren betreibt Online-Banking.

Als Hightech-Verband wollen wir, dass sich jeder sicher im Netz bewegen kann. Deshalb haben wir die steigenden Phishing-Zahlen seit zwei Jahren öffentlich gemacht und geben Verbrauchertipps. Unser Ziel ist, Sicherheit und Vertrauen zu fördern.

Das Thema hat in den vergangenen Wochen eine ganz besondere Aktualität bekommen. Sie alle haben die neue Diskussion um den illegalen Handel mit Daten von Verbrauchern verfolgt. Unter anderem ging es dabei um Konto-Informationen von Bankkunden. Wir haben zwar in vielerlei Hinsicht strenge Datenschutzvorschriften, aber offensichtlich noch Nachholbedarf bei der Bekämpfung schwarzer Schafe im Datenhandel. Eine Verschärfung von Sanktionen und eine bessere Ausstattung der zuständigen Datenschützer befürworten wir. Und wir müssen die Verbraucher konsequent über ihre Möglichkeiten aufklären. Ohne das Vertrauen der Kunden können seriöse Anbieter auf Dauer nicht erfolgreich sein.

[Datenschutz und IT-Sicherheit: Drei Dimensionen]

Datenschutz ist ein Schwerpunktthema im BITKOM – und das nicht erst seit gestern. Direkt nach Gründung des BITKOM haben wir hierzu einen Arbeitskreis eingerichtet. Die dort versammelte Expertise wollen wir Politik und auch Verbrauchern zur Verfügung stellen. Erlauben Sie mir kurz einen Überblick, welche Aspekte von Datenschutz und IT-Sicherheit aus unserer Sicht wichtig sind. Zum einen geht es um das, was PC-Nutzer aus freien Stücken an persönlichen Informationen im Netz eingeben. Zweitens geht es

um den Schutz der Anwender gegen Viren, Hacker und Betrüger, also Strategien gegen digitale Angreifer. Hier kommt das Thema Phishing ins Spiel. Und drittens geht es um Lösungen zur sicheren Identifikation – auch das will ich heute ansprechen.

Die meisten Menschen haben heute zahlreiche digitale Identitäten: als Kunde beim Online-Banking oder bei Online-Shops, als Nutzer von Internet-Marktplätzen oder als Teilnehmer von Communitys oder Foren. In all diesen Fällen sind ein wohlüberlegter Umgang mit persönlichen Daten und ein effizienter Schutz vor Missbrauch gefragt.

[Angriffe auf Bankkonten]

Die Gefahr, von Cyber-Kriminellen betrogen zu werden, ist trotz zahlreicher Aufklärungskampagnen bisher nicht gebannt. Beim Online-Banking, einem zentralen Thema der IT-Sicherheit, beobachten wir seit längerem steigende Opferzahlen. Der BITKOM befragt seit zwei Jahren die Landeskriminalämter, wie hoch die Fallzahlen und Schäden durch Phishing sind.

Hier sehen Sie die neuesten Ergebnisse: Die Zahl der Phishing-Fälle ist 2007 erneut stark gestiegen – um 25 Prozent. Das zeigen die neuesten Zahlen, die wir vor kurzem aus elf Bundesländern erhalten haben. Diese stehen für rund 90 Prozent der Bevölkerung und sind die Grundlage unserer bundesweiten Hochrechnung.

In mehr als 4.100 Fällen haben in Deutschland Kriminelle Geld von Konten ahnungsloser Bankkunden abgehoben. Der Geheimzahlen-Betrug hat damit seinen bisherigen Höhepunkt erreicht.

Eine Trendwende zeichnet sich erst für dieses Jahr ab: 2008 könnten die Opferzahlen erstmals sinken. Weil noch nicht alle teilnehmenden Bundesländer Zahlen für dieses Jahr genannt haben, handelt es sich aber um eine vorläufige Prognose. Statistisch gesehen ist sogar eine Halbierung der Fallzahlen denkbar.

Dass die Zahl der Opfer bisher gestiegen ist, hat mehrere Gründe: Zum einen nutzen immer mehr Menschen das Internet, aber längst nicht alle sichern sich wirkungsvoll ab. Ganz wesentlich ist allerdings, dass die Betrugsmethoden raffinierter werden. Die klassische Phishing-Mail, in der man über einen Link zur Eingabe der Geheimzahlen aufgefordert wird, hat weitgehend ausgedient. Heute setzen die Betrüger stärker Schadprogramme wie Trojaner ein, die im Hintergrund spionieren.

Wie sich Nutzer dagegen schützen können, soll gleich unser Thema sein. Aus unserer Sicht ist aber auch der Gesetzgeber gefragt, denn die rechtlichen Mittel gegen den Online-Betrug reichen nicht. Bisher ist der Kontodaten-Klau nicht eindeutig verboten – die Polizei kann meist erst aktiv werden, wenn bereits ein Schaden vorliegt. Es sollte aber schon der Versuch hart bestraft werden. Wir brauchen dringend ein belastbares Gesetz gegen Phishing. Natürlich wissen wir, dass ein solches Gesetz nicht alles ist, zumal die meisten gefälschten Bank-Webseiten nicht in Deutschland registriert sind. Aber es würde bei diesem bekannten Betrugsphänomen für juristische Klarheit sorgen und die Ermittlungen erleichtern.

[Illegale Geldströme]

Bedrohungen aus der virtuellen Welt gefährden sehr reale Werte – dafür ist Phishing das beste Beispiel. Die Schadenssumme bei den illegalen Bank-Transaktionen ist im vergangenen Jahr auf 19 Millionen Euro gestiegen, das ist etwa doppelt so viel wie zwei Jahre zuvor. Für 2008 zeichnet sich ein Rückgang ab, aber dabei handelt es sich um eine vorläufige Prognose. Der durchschnittliche Schaden pro Fall lag in den vergangenen Jahren bei 3.700 Euro. Für 2008 kommen wir im Schnitt auf 3.200 Euro. Maßgeblich für die Statistik sind die abgebuchten Beträge.

In einigen Fällen gelingt es glücklicherweise, betrügerische Überweisungen noch zu stoppen oder das Geld zurückzubuchen. Deshalb sollten Opfer zuerst die Bank alarmieren. Entsteht doch ein finanzieller Schaden: unbedingt Anzeige bei der Polizei erstatten. Das ist nötig, um Geld von der Bank zurückzubekommen. Falls der Kunde nicht grob fahrlässig gehandelt

hat, zeigen sich viele Banken in der Praxis kulant. Ob die Kunden einen Anspruch darauf haben, ist in der Rechtsprechung aber nicht eindeutig. Vorsorge ist deshalb unverzichtbar.

[So werden Transaktionen sicher]

Hier sehen Sie die wichtigsten Tipps zum Online-Banking. In meinem kurzen Vortrag kann ich nicht auf jeden einzeln eingehen, aber Details dazu finden Sie in Ihrer Pressemappe. Die entsprechende Presseinfo gehört zu den BITKOM-Tipps, einer Reihe von Veröffentlichungen, in denen wir unter anderem Sicherheitshinweise für Verbraucher geben.

Kurz gesagt – drei Dinge müssen zusammenkommen, damit Online-Banking eine sichere Sache ist: Bewusstes Nutzerverhalten, eine gute Sicherheitsausstattung des PCs und moderne Schutzverfahren der Banken.

Transaktionsnummern, TANs, sind heute meist nicht mehr beliebig einsetzbar, sondern an weitere Sicherheits-Hürden gekoppelt. Manche Kreditinstitute erhöhen den Schutz mit Kartenlesegeräten. Kunden sollten nachfragen und auf die modernsten Verfahren umstellen. Unterm Strich haben Betrüger wenig Erfolg, wenn sich gute Sicherheitstechnik und umsichtiges Verhalten ergänzen.

[Nutzer wollen sicheren Ausweis mit Chip]

Eine weitere Variante, Online-Dienste sicherer zu machen, ist ab 2010 der elektronische Personalausweis. Er soll mehr sein als ein klassisches Ausweisdokument. Da er chipbasiert ist, bietet er die Möglichkeit, sichere Transaktionen durchzuführen. Das begrüßen wir im BITKOM nachdrücklich. Ein solcher Ausweis hat Vorteile für alle. Verbraucher müssen keine gestohlenen Zugangsdaten mehr fürchten. Anbieter können sich sicher sein, dass ihre Produkte und Services nicht an die Falschen geliefert werden. Behörden können staatliche Leistungen leichter online anbieten, Bürger müssen seltener bei Ämtern erscheinen.

Dazu haben wir Forsa in der ersten Jahreshälfte um eine repräsentative Umfrage gebeten. Die Ergebnisse haben wir bereits veröffentlicht, aber beim

Thema Phishing sollten wir sie noch einmal erwähnen: 55 Prozent der deutschen Internet-Nutzer würden einen elektronischen Ausweis samt Lesegerät fürs Online-Banking nutzen, fast ebenso viele für staatliche Dienste wie die Steuererklärung. Für Online-Auktionen und Online-Shopping immerhin noch um die 40 Prozent. Nur für 15 Prozent der befragten Internet-Nutzer käme ein Einsatz des elektronischen Personalausweises nicht in Frage.

[Anwender sind zu Investition in Sicherheit bereit]

Die Anwender haben wir dann gefragt, wie viel sie für das nötige Lesegerät ausgeben würden: 61 Prozent der Internet-Nutzer sagten, bis zu 20 Euro sei ihnen ein solcher Service wert. Nur 11 Prozent würden ihn ausschließlich kostenlos nutzen wollen. Die zuweilen für ihre Technik-Skepsis kritisierten Deutschen stehen dieser Innovation also sehr offen gegenüber.

Das sollte auch die Banken ermutigen, ihren Kunden bereits heute verstärkt Kartenleser oder TAN-Generatoren anzubieten. Mit diesen Zusatzgeräten ist Online-Banking zurzeit am sichersten. Ganz offensichtlich sind die Kunden bereit, die notwendigen Beträge in die eigene Sicherheit zu investieren. Die meisten erwarten keinen Rundum-Schutz zum Nulltarif.

[Sichere Online-Identitäten]

Erlauben Sie mir zum Schluss noch einen Hinweis auf die Initiative „Deutschland sicher im Netz“, an der sich der BITKOM maßgeblich beteiligt. DsiN ist ein Gemeinschaftsprojekt mehrerer Verbände, Unternehmen und Institutionen unter der Schirmherrschaft des Bundesinnenministers. Auch hier bekommen Unternehmen, Privatanutzer und Jugendliche Tipps zum sicheren Surfen – damit ihre digitalen Identitäten bestmöglich geschützt sind.

IT-Sicherheit ist eine Herausforderung unserer Branche, in der sich die Bedürfnisse der Verbraucher mit den ureigensten Interessen der Wirtschaft decken. Kein Unternehmen kann sich leisten, dass seine Kunden das Vertrauen in die Produkte oder den Vertriebsweg verlieren.

Deshalb, meine Damen und Herren, sprechen wir diese Herausforderungen offen und nach vorne orientiert an. Ohne IT geht heute in der Gesellschaft und in der Wirtschaft nichts mehr. Daher ist die Sicherheit im Internet, davon bin ich fest überzeugt, ohne Abstriche ein gemeinsames Interesse von Unternehmen, Politik und Bürgern. In diesem Sinne freue ich mich auf den Vortrag von Herrn Ziercke und die anschließende Diskussion mit Ihnen.

Vielen Dank.