EWS

veiz goes

en Tools
Welt» können
la MySpace
henlogo oder
e beschreiben.
nn man sich
logs austau-
richte schrei-
ngen abbilden
röffentlichen.
as Auktions-
m US- und dem
ndant gleich.
te Ebay der
ung.

er
turen
ai findet in
stival der
en statt. In
ung der Reihe
ons werden
tationen und
vorgestellt.
gibt es
Vorträge,
d Filme.
h

lplätze
arch.ch
Online-Karte
zeigt neu
ielplätze
en im
n die Karte
d detaillierte
über diese
tungen.

/S

Die Postcard lässt sich fälschen

Hacker vom Chaos Computer Club legen Mängel offen

VON MICHAEL SOUKUP (TEXT) UND BRUNO MUFF (ILLUSTRATION)

Die 2,1 Millionen Postcard-Besitzer haben ein Problem. Ihre Karten lassen sich kopieren und damit ihre Konten leer räumen. PIN hin oder her. Dies behauptet Bernd R. Fix, Physiker und Mitglied des Zürcher Ablegers vom Chaos Computer Club (CCC) – dem deutschen Hacker-Verein.

Der 45-jährige hat Bundesrat Moritz Leuenberger und Post-Chef Ulrich Gygi mehrmals darauf aufmerksam gemacht, dass die Sicherheitslücken seit 2002 bekannt, bis heute aber nicht geschlossen worden seien. Die Sicherheitslücke würde als vernachlässigbar klein eingeschätzt und deshalb millionenteure Anpassungen gescheut, hiess es. Für Postfinance sind die Vorwürfe hingegen «falsch und irreführend». Es sei kein Fall bekannt, in welchem Kunden durch eine gefälschte oder geklonte Postcard zu Schaden kamen.

Die Postcard ist baugleich wie die französische Carte bleue

nance abrupt die Sitzung. Denn mit dem Vertragsabschluss verpflichtet sich der Kunde, seinen PIN-Code geheim zu halten. Weil die Postfinance grundsätzlich davon ausgeht, dass ihr System 100 Prozent sicher und folglich ein unberechtigter Geldbezug immer als Folge eines PIN-Diebstahls zu betrachten ist, kann der Kunde einen Missbrauch kaum beweisen.

Bei der Postfinance abgeblitzt wandte sich der Hacker-Club im November 2002 an Bundesrat Moritz Leuenberger, den obersten Postchef. Er versprach, sich der Sache anzunehmen und die Mängel zu beheben. Doch auch Leuenberger zweifelte an den Vorwürfen: «Im Falle deliktischer Manipulationen der Postcard würde ein entschlossenes und koordiniertes Vorgehen der Justizbehörden greifen», schrieb er.

In der Hoffnung, dass Postfinance mit der Einführung einer neuen Kartengeneration das Sicherheitsproblem beheben würde, liess Bernd R. Fix die Sache auf sich beruhen. Bis er 2006 aus Neugier erneut einen genauen Blick auf das gelbe Kärtchen warf.

lplätze
earch.ch

r Online-Karte
h zeigt neu
pielplätze
gen im
In die Karte
nd detaillierte
n über diese
htungen.

WS

ur wenige
it

st weniger ein
ein Zuschau-
schreibt die
schungsfirma
t ihren Unter-
eröffentlicht nur
der Besucher
bseite YouTube
hmen. Beim
ckr sehe das
n Kreativität und
ich aus. Die bes-
uote weise das
n Wikipedia auf.

kaufen
niger CDs

nen Jahr wurden
z erneut weni-
Ds verkauft.
t der Branchen-
Demnach ging
m traditionellen
rkt zum sechs-
ge zurück. Die
rage 30 Millio-
Im Vergleich
5 sei dies ein
er. Der Online-
sich dagegen
en Franken
doppelt.

schlossen worden seien. Die Sicherheitslücke würde als vernachlässigbar klein eingeschätzt und deshalb millionenteure Anpassungen gescheut, hiess es. Für Postfinance sind die Vorwürfe hingegen «falsch und irreführend». Es sei kein Fall bekannt, in welchem Kunden durch eine gefälschte oder geklonte Postcard zu Schaden kamen.

Die Postcard ist baugleich wie die französische Carte bleue

Der Chaos Computer Club hat erstmals im April 2002 festgestellt, das die Postcard baugleich mit der alten französischen Bankkarte Carte bleue ist, bei der schon vor zehn Jahren schwere Sicherheitsmängel aufgedeckt wurden. Die gleichen Probleme konnten für die Postcard nachgewiesen werden.

Die Führungsspitze von Postfinance zeigte sich in einem Treffen mit den Hackern im September zunächst offen für die Kritik. Als diese jedoch auf eine zwingende Änderung der Teilnahmebedingungen zu Gunsten der Kundschaft pochten, beendete Postfi-

berger zweifelte an den Vorwürfen: «Im Falle deliktischer Manipulationen der Postcard würde ein entschlossenes und koordiniertes Vorgehen der Justizbehörden greifen», schrieb er.

In der Hoffnung, dass Postfinance mit der Einführung einer neuen Kartengeneration das Sicherheitsproblem beheben würde, liess Bernd R. Fix die Sache auf sich beruhen. Bis er 2006 aus Neugier erneut einen genauen Blick auf das gelbe Kärtchen warf. Denn die Post gibt seit vergangenem Sommer neue Karten heraus, die den internationalen Bankkartenstandard EMV erfüllen. Die Enttäuschung war gross: Nichts hat sich geändert. Ende Dezember ging Fix mit seinem Vortrag «A not so smart card» am Chaos Communication Congress in Berlin erstmals an die Öffentlichkeit.

Alle diese Ereignisse sind ausführlich dokumentiert und im Internet frei zugänglich. Es gibt seit Februar eine eigens zu diesem Thema aufgeschaltete Site namens

FORTSETZUNG AUF SEITE 111

CLUB DER EHRENHAFTEN HACKER

Der **Chaos Computer Club** (CCC) ist ein deutscher Verein von und für Hacker. Gegründet wurde er 1981 in Berlin in den Redaktionsräumen der Tageszeitung **«taz».** Die CCC-Mitglieder sehen sich als ehrenhafte Hacker der alten Schule, die gezielt auf Sicherheitslöcher aufmerksam machen. Und sich damit bewusst von den destruktiven **Crackern** und Virenschreibern abgrenzen. Berühmt wurde der Club durch den Hack der Hamburger Sparkasse 1984, bei dem man **135 000 Mark** erbeutete und das Geld tags darauf vor den Augen der Presse zurückgab. Es folgten diverse Hacks, unter anderem der Nasa. Durch konsequente Öffentlichkeitsarbeit gelang es, den CCC vor der Kriminalisierung zu bewahren. In **Zürich** besteht seit 2006 **ein Ableger.** Der Club steht laut CCCZ allen «denkfähigen Personen» offen.

FORTSETZUNG VON SEITE 109

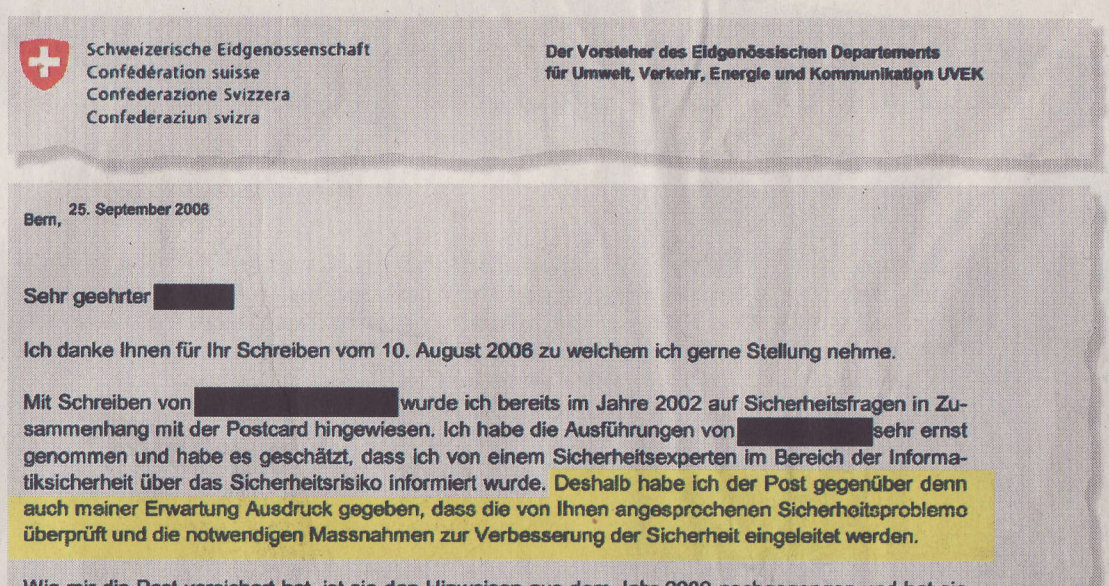
Postcard lässt sich…

postcard-sicherheit.ch. Hier soll die breite Öffentlichkeit informiert werden. Bis heute berichtete kein Schweizer Medium über den Streit zwischen CCC und Postfinance. Selbst dann nicht, als im Februar im renommierten deutschen Informatikmagazin c't» ein Artikel unter dem Titel Signatur der Schweizer Postcard geknackt» erschien.

Dabei ist das Knacken und Fälschen vergleichsweise einfach, wenn auch kein Kinderspiel. «Es ist mir klar, dass es andere, ergiebigere Missbrauchsmethoden gibt. Uns geht es darum, auf Lücken aufmerksam machen», so Fix. Jeder Informatik-Diplomand der ETH sei prinzipiell in der Lage, die notwendigen technischen Schritte auszuführen.

Die Daten auf dem Chip lassen sich problemlos auslesen

Zunächst gilt es, sich einen Chipleser zu beschaffen. Kosten: rund 50 Franken. Die PIN muss der Fälscher nicht kennen: Im Unterschied zu den EC-Karten der Banken ist sie bei der Postcard für die Authentifikation der Karte an einem Terminal unerheblich. Einziger Zweck ist, den Bezahlvorgang auf dem Kartenchip zu protokollieren. Die Daten auf dem Smartcard-Chip der gelben Karte lassen sich problemlos «auslesen». Dafür eignet sich auch die eigene Postcard.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Vorsteher des Eidgenössischen Departements
für Umwelt, Verkehr, Energie und Kommunikation UVEK

Bern, 25. September 2006

Sehr geehrter [redacted]

Ich danke Ihnen für Ihr Schreiben vom 10. August 2006 zu welchem ich gerne Stellung nehme.

Mit Schreiben von [redacted] wurde ich bereits im Jahre 2002 auf Sicherheitsfragen in Zusammenhang mit der Postcard hingewiesen. Ich habe die Ausführungen von [redacted] sehr ernst genommen und habe es geschätzt, dass ich von einem Sicherheitsexperten im Bereich der Informatiksicherheit über das Sicherheitsrisiko informiert wurde. Deshalb habe ich der Post gegenüber denn auch meiner Erwartung Ausdruck gegeben, dass die von Ihnen angesprochenen Sicherheitsprobleme überprüft und die notwendigen Massnahmen zur Verbesserung der Sicherheit eingeleitet werden.

Wie mir die Post versichert hat, ist sie den Hinweisen aus dem Jahr 2002 nachgegangen und hat sie in der sicherheitstechnischen Weiterentwicklung der Kartengeldsysteme laufend mit berücksichtigt. So wurden verschiedene technische Massnahmen zur Erhöhung der Kartensicherheit ergriffen. Im Weiteren wurden organisatorische Massnahmen getroffen, um bei allfälligen Angriffen auf das System bestmöglich vorbereitet zu sein. Die Umsetzung der Massnahmen wurde von Sicherheitsspezialisten auf ihre Wirksamkeit überprüft.

Die Sicherheit der Postcard rsp. der Kundinnen und Kunden von PostFinance liegt mir selbstverständlich sehr am Herzen. Ich habe Ihr Schreiben deshalb der Post weitergeleitet und sie erneut ersucht, allfällige Massnahmen zur Verbesserung der Sicherheit zu treffen.

Mit freundlichen Grüssen

Moritz Leuenberger
Bundespräsident

Ausriss aus dem Brief von Bundesrat Leuenberger an den Hacker-Club: «Massnahmen sind zu treffen»

Im Datensatz findet sich unter anderem die digitale Signatur, die der Identifikation der Postcard am Terminal im Laden dient. Sie ist eines der elementarsten Sicherheitsmerkmale der Postkarte, soll aber nach CCC-Angaben nur mit einem 320 Bit langen Schlüssel geschützt sein. Üblich sind aber heute Schlüssellängen von 2048 Bit. Um den geheimen Schlüssel der Postfinance abzuleiten, braucht man die Datenblöcke zweier Postcards und einen Computer. Danach lässt sich der Schlüssel laut CCC «innert Stunden knacken.»

Dazu Marc Andrey, Medienspecher von Postfinance: «Der als unsicher bezeichnete Schlüssel ist für die Sicherheit nicht relevant.» Denn diese hänge von einer Kombination von mehreren Elementen ab. «Aber warum hat es dann überhaupt diesen digitalen Schlüssel auf der Karte?», fragt sich Bernd R. Fix.

Mit dem geknackten Schlüssel kann der Hacker gleich der Postfinance Karten herausgeben, die von Terminals als echte Postcard identifiziert werden. Genau dies konnte in Frankreich durch Erstellung eines Kartenklons für die baugleiche Carte bleue bewiesen werden. Dafür benötigt der Hacker nur noch nackte Karten, die problemlos in einschlägigen Computergeschäften erhältlich sind. Und die achtstellige Kartennummer einer gültigen Postcard.

Die Karte sieht anders aus als die gelbe Postcard

Nun kann die Karte geklont und zu einer so genannten «YesCard» programmiert werden, die jede PIN annimmt. CCC-Hacker haben unlängst eine duplizierte Karte erfolgreich getestet – vorsichtshalber nur an einem Kartenlesegerät in einer Telefonzelle. Denn die Karte ist äusserlich nicht identisch mit der gelben Postcard, deshalb besteht im Laden ein erhebliches Entdeckungsrisiko. An Geldautomaten und Terminals, die auf der Magnetstreifentechnik basieren, funktioniert es überhaupt nicht.

Auf die Frage, warum Postfinance Fix nicht wegen Rufschädigung einklage, sagte Marc Andrey: «Aus verständlichen Gründen will Postfinance die Sicherheitselemente nicht offen legen. Das müssten wir bei einem allfälligen gerichtlichen Verfahren tun, wenn wir beweisen wollten, inwiefern gemachte Aussagen falsch sind.» Fix jedenfalls will demnächst den Beweis vor laufender Fernsehkamera erbringen.

Ratlos am Billettautomat

Die SBB testen eine neue Software

Die SBB testen neue Software für ihre Billettautomaten mit Bildschirmen. Seit dem 11. April sind zwei Selbstbedienungsschalter im Zürcher Hauptbahnhof damit ausgerüstet. Die SBB versprechen den Kunden mehr Auswahl und eine einfachere Bedienung an 1100 Automaten. Doch die Software ist unstabil und entspricht optisch in keiner Weise dem, was Anwender sich von professionellen PC-Programmen gewohnt sind.

Dies ergab ein Augenschein der SonntagsZeitung am Donnerstagabend. Kundenberater stehen im Bahnhof den Bahnreisenden bei, die Fahrscheine an den Testautomaten lösen. Die Helfer zeigen allerdings Nerven: «Ständig stürzt das Programm ab, die Kunden finden sich nicht zurecht» fasst ein Assistent den Tag zusammen. Das Lösen einer Fahrkarte nach St. Gallen bestätigt dies – erst im dritten Anlauf klappt der Vorgang. Zuerst taucht St. Gallen nicht in der Liste möglicher Zielbahnhöfe auf, dann springt das Programm zum Anfang zurück, später bricht es vor dem Bezahlen ab. Informationen und Schaltflächen sind getrennt voneinander über den Bildschirm verteilt.

«Systemabstürze haben unsere Teams vor Ort bisher nicht beobachtet», sagt SBB-Sprecher Roland Binz in einer Stellungnahme.

DANIEL METZGER