Datum: 06.03.2013

Haus & Garten

Online-Ausgabe

HausundGarten.ch
8024 Zürich
044/ 266 17 17
www.hausundgarten.ch

Medienart: Internet
Medientyp: Spezial- und Hobbyzeitschriften

Online lesen

Berner Fachhochschule
Haute école spécialisée bernoise

Themen-Nr.: 375.19
Abo-Nr.: 1074128

Smartphone für Geldgeschäfte riskant

Banküberweisungen via Smartphone sind unsicher – unabhängig davon, welche technische Lösung eine Bank gewählt hat. Das haben zwei Studenten der Berner Fachhochschule Technik und Informatik aufgezeigt.

Besonders einfach ist die Manipulation von Geldtransaktionen gemäss den Autoren Simon Klaus und Danijel Brei beim sogenannten MTAN-Verfahren. Es wird unter anderem von Credit Suisse, Raiffeisen, Bank Coop und einigen Kantonalbanken verwendet. Das Problem: Die Banken senden den Transaktionscode per SMS auf dasselbe Gerät, auf dem der Kunde die Überweisungen tätigt. So kann dieses selbständig Transaktionen tätigen und mit dem Code bestätigen, ohne dass der Kunde dies merkt.

Nicht selten öffnen die Smartphone-Besitzer die Türen für den unerlaubten Griff aufs Konto selbst, indem sie ohne aufzupassen Apps installieren, die diverse Berechtigungen fordern.

Für sichere Überweisungen braucht es laut Klaus und Brei eine zusätzliche Hardwarekomponente zur Identifizierung und Transaktionsbestätigung. Eine solche Lösung verwendet etwa die UBS mit ihrem Sicherheits-Token Zone Trusted Information Channel. Dies ist eine Art USB-Stick, der den Nutzer identifiziert und dessen Berechtigung überprüft. Für Smartphones gibt es noch keine solchen Lösungen. Deshalb gilt: Auf E-Banking mit dem Smartphone sollte man heute noch verzichten.

06. März 2013 | Mirjam Fonti, Redaktion saldo

Datum: 06.03.2013

Gesundheitstipp

Online-Ausgabe

Gesundheitstipp
8024 Zürich
044/ 266 17 27
www.gesundheitstipp.ch

Medienart: Internet
Medientyp: Spezial- und Hobbyzeitschriften

Online lesen

Berner Fachhochschule
Haute école spécialisée bernoise

Themen-Nr.: 375.19
Abo-Nr.: 1074128

Smartphone für Geldgeschäfte riskant

Banküberweisungen via Smartphone sind unsicher – unabhängig davon, welche technische Lösung eine Bank gewählt hat. Das haben zwei Studenten der Berner Fachhochschule Technik und Informatik aufgezeigt.

Besonders einfach ist die Manipulation von Geldtransaktionen gemäss den Autoren Simon Klaus und Danijel Brei beim sogenannten MTAN-Verfahren. Es wird unter anderem von Credit Suisse, Raiffeisen, Bank Coop und einigen Kantonalbanken verwendet. Das Problem: Die Banken senden den Transaktionscode per SMS auf dasselbe Gerät, auf dem der Kunde die Überweisungen tätigt. So kann dieses selbständig Transaktionen tätigen und mit dem Code bestätigen, ohne dass der Kunde dies merkt.

Nicht selten öffnen die Smartphone-Besitzer die Türen für den unerlaubten Griff aufs Konto selbst, indem sie ohne aufzupassen Apps installieren, die diverse Berechtigungen fordern.

Für sichere Überweisungen braucht es laut Klaus und Brei eine zusätzliche Hardwarekomponente zur Identifizierung und Transaktionsbestätigung. Eine solche Lösung verwendet etwa die UBS mit ihrem Sicherheits-Token Zone Trusted Information Channel. Dies ist eine Art USB-Stick, der den Nutzer identifiziert und dessen Berechtigung überprüft. Für Smartphones gibt es noch keine solchen Lösungen. Deshalb gilt: Auf E-Banking mit dem Smartphone sollte man heute noch verzichten.

06. März 2013 | Mirjam Fonti, Redaktion saldo

Datum: 06.03.2013

Ktipp

Online-Ausgabe

ktipp.ch
8024 Zürich
044/ 266 17 17
www.ktipp.ch

Medienart: Internet
Medientyp: Spezial- und Hobbyzeitschriften

Online lesen

Berner Fachhochschule
Haute école spécialisée bernoise

Themen-Nr.: 375.19
Abo-Nr.: 1074128

(0)

Artikel | saldo 04/2013

Smartphone für Geldgeschäfte riskant

Banküberweisungen via Smartphone sind unsicher – unabhängig davon, welche technische Lösung eine Bank gewählt hat. Das haben zwei Studenten der Berner Fachhochschule Technik und Informatik aufgezeigt.

Besonders einfach ist die Manipulation von Geldtransaktionen gemäss den Autoren Simon Klaus und Danijel Brei beim sogenannten MTAN-Verfahren. Es wird unter anderem von Credit Suisse, Raiffeisen, Bank Coop und einigen Kantonalbanken verwendet. Das Problem: Die Banken senden den Transaktionscode per SMS auf dasselbe Gerät, auf dem der Kunde die Überweisungen tätigt. So kann dieses selbständig Transaktionen tätigen und mit dem Code bestätigen, ohne dass der Kunde dies merkt.

Nicht selten öffnen die Smartphone-Besitzer die Türen für den unerlaubten Griff aufs Konto selbst, indem sie ohne aufzupassen Apps installieren, die diverse Berechtigungen fordern.

Für sichere Überweisungen braucht es laut Klaus und Brei eine zusätzliche Hardwarekomponente zur Identifizierung und Transaktionsbestätigung. Eine solche Lösung verwendet etwa die UBS mit ihrem Sicherheits-Token Zone Trusted Information Channel. Dies ist eine Art USB-Stick, der den Nutzer identifiziert und dessen Berechtigung überprüft. Für Smartphones gibt es noch keine solchen Lösungen. Deshalb gilt: Auf E-Banking mit dem Smartphone sollte man heute noch verzichten.

06. März 2013 | Mirjam Fonti, Redaktion saldo

Beitrag als PDF
Smartphone für Geldgeschäfte riskant
Download PDF 36 KB

Datum: 06.03.2013

BON À SAVOIR

Online-Ausgabe

Bon à Savoir
1001 Lausanne
021/ 310 01 36
www.bonasavoir.ch

Medienart: Internet
Medientyp: Publikumszeitschriften

Online lesen

Berner Fachhochschule
Haute école spécialisée bernoise

Themen-Nr.: 375.19
Abo-Nr.: 1074128

Smartphones et transferts bancaires ne font pas bon ménage

Rédaction online / 06.03.2013

Deux étudiants ont testé la sécurité des transactions bancaires effectuées avec un smartphone. A éviter!

Les téléphones dits intelligents ne le sont pas tant que ça lorsqu'ils sont confrontés à des problèmes de sécurité. La prudence élémentaire suggère donc de ne pas effectuer de transactions bancaires avec ces appareils vulnérables aux virus. Deux étudiants de la Haute école spécialisée de Berne ont testé concrètement les systèmes utilisés pour sécuriser les échanges et en particulier le protocole mTAN (mobile transaction number) adopté par de nombreuses banques (notamment Crédit Suisse, Raiffeisen, Coop et plusieurs banques cantonales). Le verdict de Simon Klaus et Danijel Brei est sans appel: quelque soit la technologie employée, les transactions sont risquées.

Un seul canal

La procédure d'identification mTAN se fait en trois étapes. Après avoir entré son identifiant et son mot de passe, le client reçoit par SMS un code qu'il doit à nouveau saisir pour confirmer son identité. Lorsque la transaction est effectuée avec un ordinateur, les données transitent par deux canaux différents: l'ordinateur et le téléphone. Alors que dans le cas d'un smartphone, toutes les données sont contenues dans un seul et même appareil. Or, les deux étudiants ont démontré qu'il était relativement aisé de pirater un smartphone afin de recueillir en une seule fois les données d'identification et le texte du SMS, à l'insu de la banque et du client.

Rappelons toutefois que le vol de données bancaires, certes plus compliqué sur un ordinateur (protégé par un bon antivirus), n'est pas pour autant exclu
(lire « Des paiements en toute quiétude
» TCF 11/2012 »)
. Selon une autre étude, les systèmes utilisant un lecteur de carte ou une clé USB lors de la procédure

Datum: 06.03.2013

BON À SAVOIR

Online-Ausgabe

Bon à Savoir
1001 Lausanne
021/ 310 01 36
www.bonasavoir.ch

Medienart: Internet
Medientyp: Publikumszeitschriften

Online lesen

Berner Fachhochschule
Haute école spécialisée bernoise

Themen-Nr.: 375.19
Abo-Nr.: 1074128

d'identification, renforcent considérablement la sécurité de la transaction. Mais de telles solutions n'existent pas pour les smartphones.

Philippe Chevalier/Mirjam Fonti

Datum: 22.03.2013

UNIA DIE ZEITUNG DER GEWERKSCHAFT. work

Verlagsgesellschaft Work AG
3000 Bern 15
031/ 350 24 18
www.workzeitung.ch

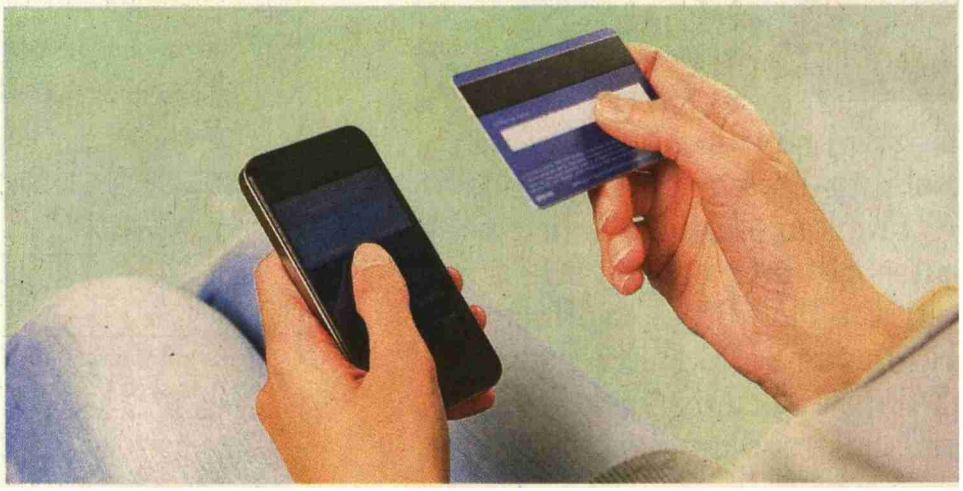
Medienart: Print
Medientyp: Fachpresse
Auflage: 90'643
Erscheinungsweise: 26x jährlich

Berner Fachhochschule
Haute école spécialisée bernoise

Themen-Nr.: 375.19
Abo-Nr.: 1074128
Seite: 13
Fläche: 33'161 mm²

saldo tipp im work

Dieser Text ist aus der Zeitschrift für Konsumentenschutz «Saldo» übernommen.



LIEBER FINGER WEG: E-Banking mit dem Handy. FOTO: FOTOLIA

Das Smartphone ist für Geldgeschäfte riskant

Banküberweisungen via Smartphone sind unsicher – unabhängig davon, welche technische Lösung eine Bank gewählt hat. Das haben Simon Klaus und Danijel Brei aufgezeigt, zwei Studenten der Berner Fachhochschule Technik und Informatik.

Besonders einfach ist die Manipulation von Geldtransaktionen beim sogenannten MTAN-Verfahren. Es wird unter anderem von Credit Suisse, Raiffeisen, Bank Coop und einigen Kantonalbanken verwendet. Das Problem: Die Banken senden den Transaktionscode per SMS auf dasselbe Gerät, auf dem die Kundin oder der Kunde die Überweisungen täti-

Oft öffnen Smartphone-Besitzer die Türen für den Griff aufs Konto selbst.

Datum: 22.03.2013

UNIA DIE ZEITUNG DER GEWERKSCHAFT. work

Verlagsgesellschaft Work AG
3000 Bern 15
031/ 350 24 18
www.workzeitung.ch

Medienart: Print
Medientyp: Fachpresse
Auflage: 90'643
Erscheinungsweise: 26x jährlich

Berner Fachhochschule
Haute école spécialisée bernoise

Themen-Nr.: 375.19
Abo-Nr.: 1074128
Seite: 13
Fläche: 33'161 mm²

gen. So können von aussen oder von einer Drittperson über dieses Gerät Transaktionen getätigt und mit dem Code bestätigt werden, ohne dass die Kundschaft es merkt.
Nicht selten öffnen die Smartphone-Besitzer die Türen für den unerlaubten Griff aufs Konto selbst, indem sie Apps installieren, die diverse Berechtigungen fordern.
Für sichere Überweisungen braucht es laut Klaus und Brei eine zusätzliche Hardwarekomponente zur Identifizierung und Transaktionsbestätigung. Eine solche Lösung verwendet etwa die UBS mit ihrem Sicherheits-Token «Zone Trusted Information Channel». Dies ist eine Art USB-Stick, der die Nutzerinnen und Nutzer identifiziert und ihre Berechtigung überprüft. Für Smartphones gibt es noch keine solchen Lösungen. Deshalb: Auf E-Banking mit dem Smartphone sollte man heute noch verzichten. MIRJAM FONTI

Eine Zusammenfassung der Diplomarbeit finden Sie unter **http://goo.gl/FJX8C**. Bei Postfinance finden Sie 5 goldene Regeln (**http://goo.gl/KnknB**) sowie ausführlichere Tipps für sicheres E-Banking (**http://goo.gl/hQCH1**).

Datum: 30.03.2013

Bieler Tagblatt

Berner Fachhochschule
Haute école spécialisée bernoise

Bieler Tagblatt
2501 Biel
032/ 321 91 11
www.bielertagblatt.ch

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 23'871
Erscheinungsweise: 6x wöchentlich

Themen-Nr.: 375.19
Abo-Nr.: 1074128
Seite: 4
Fläche: 58'093 mm²

«Menschenverstand genügt nicht»

BFH Technik und Informatik Die Studierenden Danijel Brei und Simon Klaus zeigen, wie einfach E-Banking-Systeme manipuliert werden können. Und wie Sicherheit möglich wäre.

Die Spezialisten: Danijel Brei, Simon Klaus und Reto Koenig (von links). Tanja Lander

Sie können sich ein Lächeln auf den Stockzähnen nicht verkneifen. Danijel Brei, Simon Klaus und Reto Koenig geniessen es sichtlich, ihre Erkenntnisse zu präsentieren. Die beiden Studierenden Brei und Klaus und ihr Dozent Koenig von der Berner Fachhochschule Technik und Informatik in Biel haben durchaus Grund dazu, stolz zu sein. Immerhin können sie aufzeigen, dass die vielgepriesenen E-Banking-Systeme in der Schweiz gravierende Sicherheitslücken aufweisen, wenn sie mit mobilen Geräten wie Smartphones oder Tablets funktionieren. Eigentlich müsste ein Aufschrei durch die Bankenwelt gehen.

Angriff auf zwei Arten

Brei und Klaus haben sich in ihrer Bachelor-Arbeit das sogenannte mTan-Verfahren im E-Banking vorgenommen. Dieses wenden in der Schweiz verschiedene Institute an, etwa die Credit Suisse, Raiffeisen, die Bank Coop und einige Kantonalbanken. In diesem Verfahren senden die Banken den Transaktionscode (der zur Bestätigung des Bankgeschäfts nötig ist) per SMS an ein mobiles Endgerät, also ein Smartphone oder ein Tablet. Das ist in diesem Zusammenhang insofern von Belang, als davon auszugehen sei, dass künftig die grosse Mehrheit der Nutzer mit Tablets arbeiten werde, so Koenig. «Man geht davon aus, dass ein SMS sicher ist», sagt er, «doch dem ist nicht so».

Zur Demonstration haben Brei und Klaus eine Übungsplattform entwickelt, ein Online-Banking-System der fiktiven YCT-Bank («You Can Trust», also: «Sie kön-

Datum: 30.03.2013

Bieler Tagblatt

Bieler Tagblatt
2501 Biel
032/ 321 91 11
www.bielertagblatt.ch

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 23'871
Erscheinungsweise: 6x wöchentlich

Berner Fachhochschule
Haute école spécialisée bernoise

Themen-Nr.: 375.19
Abo-Nr.: 1074128
Seite: 4
Fläche: 58'093 mm²

nen vertrauen» – ein gewisser Humor ist auch Informatikspezialisten nicht abzusprechen). Kern ihrer Arbeit sind aber zwei selber entwickelte Applikationen: Ein Web-Browser und eine SMS-Applikation. Diese können miteinander Daten austauschen. Ein Angriff aufs Konto des Nutzers kann auf zwei Arten erfolgen. Einerseits kann das von den Bieler Studenten entwickelte System selber Transaktionen auslösen. «Der Nutzer kriegt gar nichts mit», sagt Brei, denn der Browser löscht das SMS, das vom Nutzer die Bestätigung fordert.

In der zweiten Variante wird die Transaktion des Nutzers verfälscht. Die SMS-Applikation manipuliert das SMS an den Nutzer, so dass dieser das Gefühl hat, alles gehe mit rechten Dingen zu. In Wahrheit aber wird ein Teil des Betrags der Transaktion an ein fremdes Konto abgezweigt.

Leichte Kontamination

Banken, mit denen die Bieler in Kontakt waren, seien nach Angaben Koenigs überzeugt, dass es sehr schwer sie, ein Smartphone mit einem zweiten Programm zu kontaminieren. Allein: «Das ist es nicht.» In ihren Tests ist es Brei und Klaus mühelos gelungen, über eine frei verfügbare SMS-App in die Telefonie zu gelangen. Die Studenten haben dafür das Open-Source-Projekt «SMS Buddy» für ihre Zwecke abgeändert – ein Programm, das von mehreren Millionen Nutzern verwendet wird. Möglich ist auch ein Zugriff über den Web-Browser, ohne direkten Zugriff aufs Telefon. Weiter ist es möglich, die Kommunikation zwischen Handy und Laptop über Ultraschalltechnologie zu beeinflussen.

Zusatzgerät nötig

Problematisch ist zudem, dass die Kunden oft keine Kontoauszüge aus Papier mehr erhalten und so gefälschte Transaktionen kaum mehr erkennen können, denn: «Unser Browser kann auch den elektronischen Auszug fälschen, inklusive der digitalen Signatur», sagt Simon Klaus.

Die Bieler Informatiker weisen darauf hin, dass sicheres E-Banking durchaus möglich wäre. Dazu brauche es ein sogenanntes dediziertes Gerät. Von IBM, mit denen sie ebenfalls in Kontakt sind, gibt es etwa eine Lösung über ein abgesichertes Gerät, das über die USB-Schnittstelle an den Computer angeschlossen wird. Das vertrauenswürdige Display dieses Geräts zeigt an, was tatsächlich passiert, und diese Transaktion muss von Hand auf dem Gerät bestätigt werden. Diese Lösung verunmögliche den beschriebenen Angriff komplett, so Koenig.

Sicher aber sei, dass die Aufrufe von Melani, der Melde- und Analysestelle Informationssicherung des Bundes, nicht ausreichten: «Der gesunde Menschenverstand allein nützt gegen solche Bedrohungen nicht», sagt Reto Koenig.

Tobias Graden

Ursprung: die Wahlen in Norwegen

- BFH-Dozent Reto Koenig ist Informatik-Spezialist im Bereich **E-Voting** (elektronisches Abstimmen).
- Bei der Forschung am E-Voting-Projekt in **Norwegen** ist er auf das Problem gestossen, das im Haupttext beschrieben wird.
- Danijel Brei und Simon Klaus haben dieses nun im Kontext des E-Bankings untersucht.
- In Norwegen besitzen bereits über 90 Prozent der Bevölkerung ein Smartphone, E-Voting hat dort also grosses Potenzial – ebenso ein Angriff.
- Ohne sicheres Verfahren drohen also auch **gravierende demokratiepolitische Probleme**.

tg

Datum: 02.04.2013

ICT kommunikation

Online-Ausgabe

Kapi-Media
8604 Volketswil
079/ 437 79 33
www.ictk.ch

Medienart: Internet
Medientyp: Fachpresse

Online lesen

Berner Fachhochschule
Haute école spécialisée bernoise

Themen-Nr.: 375.19
Abo-Nr.: 1074128

Fachhochschule Bern entlarvt Schwachstellen beim mobilen E-Banking

Verfasst von ictk am 2. April 2013 - 10:40 Finanz-IT
News
Forschung & Entwicklung

Studierende und Forschende des Research Instituts for Security in the Information Society (Risis) der Berner Fachhochschule haben ein Angriffsszenario via Smartphone auf eine E-Banking Applikation erarbeitet und dabei aufgezeigt, wie einfach diese manipuliert werden kann.

Das Sicherheitskonzept der Bank geht laut Risis davon aus, dass die Erfassung der Transaktion und die Anzeige des Transaktionscodes nur vom Mensch gelesen werden kann und u ber unterschiedliche Gera te erfolgt. Diese Trennung wird nun mit Hilfe des Smartphones u berwunden und die Anzeige des Transaktionscodes kann so manipuliert werden, dass Schadprogramme autonom weitere, verborgene Transaktionen ta tigen ko nnen. Von diesen U berweisungen erfa hrt der Kunde erst, wenn er den elektronischen Kontoauszug u ber ein nicht manipuliertes Gera t einsieht, oder diesen per Post zugestellt erha lt und u berpru ft.

Studierenden gelang es der Untersuchung zufolge problemlos, das Angriffsszenario auf ein E-Banking System umzusetzen. Sie konnten die Transaktion sowie die Anzeige des Transaktionscodes leicht manipulieren. Aber auch E-Banking u ber konventionelle Computer ist angreifbar. Wird der Code u ber ein manipuliertes Smartphone angezeigt, kommunizieren die Schadprogramme der unterschiedlichen Gera ten zum Beispiel per Ultraschall, so die Risis-Beteiligten.

"Die Manipulation von smarten Gera ten und deren Applikationen ist im Cloud-Zeitalter sehr einfach geworden. Manipulierte Browser ko nnen Schadprogramme eigensta ndig und unbemerkt darauf installieren. Die Sicherheit etablierter E-Banking Lo sungen ist nicht mehr gewa hrleistet. Dagegen hilft auch der oft verku ndete gesunde Menschenverstand seitens der Nutzer nichts. Nur wenn Banken den Einsatz eines Security Tokens anbieten, bei dem die Anzeige und die Tastatur vertrauenswu rdig ist, kann ein sicheres E-Banking via Smartphone erfolgen", unterstreicht Reto Ko nig, Professor fu r Informatik an der Berner Fachhochschule.

www.risis.ti.bfh.ch

Datum: 02.04.2013

Online PC – Das Computer-Magazin

Online-Ausgabe

Online PC Zeitung
8134 Adliswil
044/ 712 60 10
www.onlinepc.ch

Medienart: Internet
Medientyp: Fachpresse
UUpM: 41'328

Online lesen

Berner Fachhochschule
Haute école spécialisée bernoise

Themen-Nr.: 375.19
Abo-Nr.: 1074128

Newsticker

02.04.2013

Berner Fachhochschule findet gravierende Sicherheitslücken beim E-Banking mit mobilen Geräten

Studierende und Forschende des Research Instituts for Security in the Information Society (RISIS) der Berner Fachhochschule haben ein Angriffsszenario via Smartphone auf eine E-Banking Applikation erarbeitet und aufgezeigt, wie einfach diese manipuliert werden kann.

E-Banking ist in unserer Gesellschaft weit verbreitet und gilt als sicher. Doch wie verhält sich das Sicherheitskonzept von Banken, wenn die Überweisung via Smartphone oder Tablet abgewickelt wird? Studierende und Forschende des Research Instituts for Security in the Information Society (RISIS) der Berner Fachhochschule haben ein Angriffsszenario via Smartphone auf eine E-Banking Applikation erarbeitet und aufgezeigt, wie einfach diese manipuliert werden kann.

Das Sicherheitskonzept der Bank geht davon aus, dass die Erfassung der Transaktion und die Anzeige des Transaktionscodes nur vom Mensch gelesen werden kann und über unterschiedliche Geräte erfolgt. Diese Trennung wird nun mit Hilfe des Smartphones überwunden und die Anzeige des Transaktionscodes kann so manipuliert werden, dass Schadprogramme autonom weitere, verborgene Transaktionen tätigen können. Von diesen Überweisungen erfährt der Kunde erst, wenn er den elektronischen Kontoauszug über ein nicht manipuliertes Gerät einsieht, oder diesen per Post zugestellt erhält und überprüft.

Studierenden gelang es problemlos, das Angriffsszenario auf ein E-Banking System umzusetzen. Sie konnten die Transaktion sowie die Anzeige des Transaktionscodes leicht manipulieren. Aber auch E-Banking über konventionelle Computer ist angreifbar. Wird der Code über ein manipuliertes Smartphone angezeigt, kommunizieren die Schadprogramme der unterschiedlichen Geräten zum Beispiel per Ultraschall.

"Die Manipulation von smarten Geräten und deren Applikationen ist im Cloud-Zeitalter sehr einfach geworden. Manipulierte Browser können Schadprogramme eigenständig und unbemerkt darauf installieren. Die Sicherheit etablierter E-Banking Lösungen ist nicht mehr gewährleistet. Dagegen hilft auch der oft verkündete gesunde Menschenverstand seitens der Nutzer nichts. Nur wenn Banken den Einsatz eines Security Tokens anbieten, bei dem die Anzeige und die Tastatur vertrauenswürdig ist, kann ein sicheres E-Banking via Smartphone erfolgen", so Reto König, Professor für Informatik an der Berner Fachhochschule.

Das Research Institute for Security in the Information Society (RISIS) beschäftigt sich mit Sicherheitsfragen in der Informationsgesellschaft. Darunter fallen prominent auch die Gebiete E-Banking und E-Voting. (Patrick Hediger)
www.risis.ti.bfh.ch

Aktuelle News >>

Hilfreiche Tipps >>