Ein Gemeinschafts-Spezial von FOCUS-MONEY, CHIP und REINERSCT

FOCUS MONEY — DAS MODERNE WIRTSCHAFTSMAGAZIN

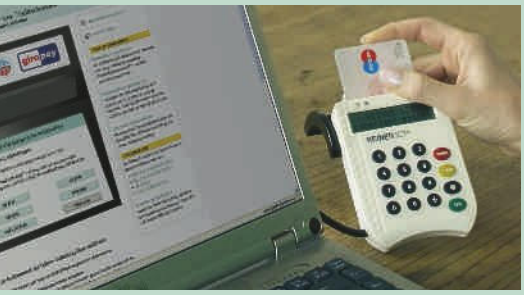
CHIP

Safer Banking • Safer Surfen • Safer Shoppen

Aus für Hacker

Wie die Chipkarte (Bank-)Geschäfte im Internet sicher macht

Ihr Geldautomat im Wohnzimmer!



Einfach und schnell von zu Hause aus die GeldKarte laden.

Um Ihre GeldKarte aufzuladen, können Sie sich ab sofort den Weg zum Geldautomaten Ihrer Bank sparen! Denn mit jedem handelsüblichen Chipkartenleser ist die Aufladung Ihrer GeldKarte mit bis zu 200,– Euro ab sofort auch online möglich!*) Sicher und ohne Gebühren**).

Mehr Infos unter www.GeldKarte.de

giropay

*) Voraussetzung ist die Teilnahme am Online-Banking Ihrer Hausbank, sofern diese am *giropay*-Verfahren teilnimmt (z.B. Sparkassen, Volks- und Raiffeisenbanken, Postbank).

**) Die Transaktion ist für Sie als Nutzer kostenlos. Sofern Ihre Hausbank Entgelte für Online-Überweisungen erhebt, gelten diese auch für Transaktionen mit *giropay*.

GeldKarte statt Münzen! Mit dem geladenen GeldKarte-Chip auf Ihrer ec-Karte zahlen Sie an über 600.000 Akzeptanzstellen in ganz Deutschland einfach, passend und bequem: z.B. für Parkgebühren, Fahrkarten, Briefmarken, Zigaretten und vieles mehr.

GeldKarte

Wie Kleingeld. Nur besser.

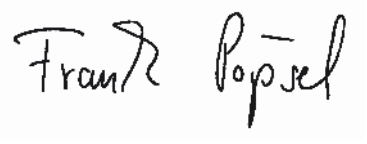
Frank Pöpsel,
Chefredakteur FOCUS-MONEY

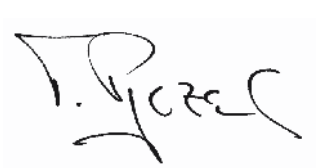
Thomas Pyczak,
Chefredakteur CHIP

Sicher ist sicher

Sind Sie E-Mail-Nutzer? Dann hatten Sie bestimmt auch schon eine dieser seltsamen Nachrichten im Posteingang: In radebrechendem Deutsch fordert Sie der Direktor Ihrer Bank auf, Benutzername, Passwort und Transaktionsnummern fürs Online-Banking zu übermitteln – zwecks einer angeblichen Sicherheitsprüfung. Auf solch plumpe Versuche des Ausspionierens geheimer Zugangsdaten dürfte heute kein Internet-Nutzer mehr hereinfallen. Das weiß inzwischen auch die Zunft der Ganoven. Die Methoden, an fremdes Geld zu kommen, sind denn auch wesentlich raffinierter geworden. Web-Seiten werden umgeleitet, die Eingaben auf PC-Tastaturen heimlich protokolliert und Spionageprogramme – sogenannte Trojaner – unbemerkt auf Rechner geschmuggelt.

Die Sicherheit beim Online-Banking wird zur echten Herausforderung. Doch welche Technik, welche Methode gewährt den besten Schutz? **In diesem Gemeinschafts-Spezial erläutern Ihnen FOCUS-MONEY, CHIP und Reiner SCT wie Banking sicher wird und welche Vorteile das Home Banking Computer Interface – kurz HBCI – bringt.** Immer mehr machen Gebrauch davon. Bei manchen Instituten greifen bereits über 20 Prozent der Kunden auf dieses sichere Verfahren zurück. Wussten Sie, dass Sie den Geldkarten-Chip auf Ihrer Bankkarte sogar schon online aufladen können und so den Geldautomaten direkt auf Ihrem Schreibtisch haben? Oder dass Sie die Karte auch zur Altersverifikation im Internet einsetzen können? Die Möglichkeiten sind vielfältig. Entdecken Sie sie.





Impressum

Redaktion: T. Schickling, K. Lohmeyer
Verlag: Die Verlagsbeilage erscheint in der FOCUS Magazin Verlag GmbH.
Verantwortlich für den redaktionellen Inhalt: Frank Pöpsel

Druck: Vogel Druck und Medienservice GmbH & Co. KG, Leibnizstraße 5, 97204 Höchberg

Fotos: A. Schick-Zech/FOCUS-MONEY, Fotolia (3), Dreamstime (4)

Titel: Fotos: iStockphoto, Samsung, MVG
Composing: FOCUS-MONEY

Internet-Sicherheit

Hände weg von meinem Geld

Der Deutsche gilt gemeinhin als vorsichtiger Mensch. Dass er sich angesichts einer der größten Gefahren für sein Erspartes kaum Sorgen macht, überrascht da sehr: In einer repräsentativen Umfrage des deutschen Bankenverbands gaben 80 Prozent der Befragten an, sich beim Online-Banking sicher oder sehr sicher zu fühlen. Eine trügerische Sicherheit. Denn die Angriffe aus dem Internet nehmen dramatisch zu. Sicherheitsexperten gehen davon aus, dass heute jeder mit dem Internet verbundene Computer alle zehn bis 15 Minuten attackiert wird.

Keine Freizeit-Hacker. Die Zeit der spektakulären Megaattacken durch pubertierende Jung-Hacker ist aber längst vorbei. „Die durch sportlichen Ehrgeiz motivierten individuellen Computer-Hacker sind in den meisten Fällen der professionellen Kriminalität gewichen“, schreibt das Bundesamt für Informationstechnik (BSI) in seinem aktuellen Lagebericht zur IT-Sicherheit in Deutschland. Die Hacker wollen keinen Ruhm mehr ernten. Sie wollen Geld.

Bankraub am PC: Nur noch Amateure überfallen mit vorgehaltener Waffe eine Bank

Online-Banküberfall: Wer heute noch mit vorgehaltener Waffe in eine Bank stürmt, ist ein Amateur. Profis überfallen Kreditinstitute und ihre Kunden inzwischen über das Internet. Risikolos. Ertragreich. Allein mit der einfachsten Methode, dem sogenannten Phishing (s. r.), sind schon Millionenraubzüge drin.

Rund 3000 Phishing-Fälle, bei denen arglose Internet-Nutzer ihre Banking-Zugangsdaten preisgaben, wurden für das Jahr 2006 in Deutschland gemeldet. Im Schnitt ergaunerten die Online-Diebe pro Fall 4000 Euro. Ein Gesamtschaden von rund zwölf Millionen Euro – und nur die Spitze des Eisbergs.

Etwa 21 Millionen Deutsche führen eines oder mehrere Konten online – oft nur unzureichend geschützt. Schwachpunkt ist in den meisten Fällen immer der Mensch: Vor allem TAN-basierte Verfahren bieten Kriminellen so viele Ansatzpunkte, dass sie zunehmend als unsicher gelten.

Wie professionell die Internet-Mafia heute vorgeht, zeigt ein Erfolg des Bundeskriminalamts (BKA), einer der wenigen großen Schläge gegen das organisierte Internet-Verbrechen: Im Frühjahr 2006 verhafteten BKA-Beamte in Frankfurt und anderen deutschen Städten sieben Mitglieder einer international agierenden Bande. Die deutschen und litauischen Staatsangehörigen hatten bereits zahlreiche Konten unter falschem Namen und mit Scheinwohnsitzen eröffnet, auf die sie sich geklautes Geld überweisen wollten.

Trojanische Pferde sind Programme, die sich unerkannt in PCs einschleichen

Die individuellen Computerhacker sind in den meisten Fällen der professionellen Kriminalität gewichen

Zum nächsten Schritt – dem Online-Banküberfall im großen Stil und dem Transfer des Geldes ins osteuropäische Ausland – kam es nicht mehr. Bei der Durchsuchung von zahlreichen Wohnungen der Bande fanden die Ermittler auch das Tatwerkzeug: einen sogenannten Trojaner. Die Software sollte sich auf den Rechnern der Opfer einschleichen und Passwörter, PINs und TANs ausspähen.

Ein seltener Erfolg für die Polizei. Meist sitzen die Online-Bankräuber sicher im Ausland, können weder ermittelt noch belangt werden. Um an das geklaute Geld zu kommen, setzen sie auf Mittelsmänner in Deutschland: Per E-Mail bieten sie ihnen lukrative Verdienstmöglichkeiten als „Online-Zahlungsmanager" oder „Fernassistent" an.

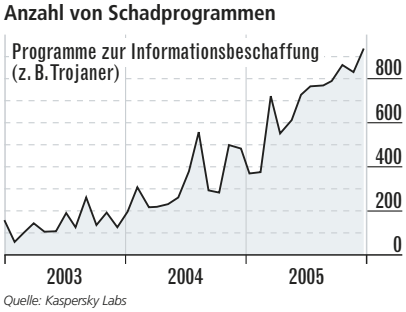
Als Gegenleistung für eine ansehnliche Provision müsse man nichts anderes tun, als Zahlungen in Deutschland zu empfangen und dann ins Ausland weiterzuleiten. Internet-Fahnder beobachten hier eine immer bessere Qualität: Inzwischen sind die Angebote in professionellem Layout und in fast perfektem Deutsch.

Ähnlich ist es bei den Phishing-Mails. „Das führte dazu, dass Kunden heute kaum mehr zwischen authentischen und gefälschten E-Mails unterscheiden können", schreibt das BSI. Die Web-Seiten, auf die diese Mails die Internet-Nutzer führen, werden immer mehr. Allein im Zeitraum von März bis April dieses Jahres erhöhte sich die Zahl der gefälschten Web-Seiten um 166 Prozent! So die Beobachtungen der Anti-Phishing Working Group, einem Zusammenschluss führender Sicherheits- und Software-Unternehmen.

Inzwischen sind auch die falschen Homepages kaum mehr von den Originalseiten der Kreditinstitute zu unterscheiden. Das geht bis hin zu der Web-Adresse. Zum Beispiel könnte die Originalseite ▶

Dramatische Zunahme der Attacken

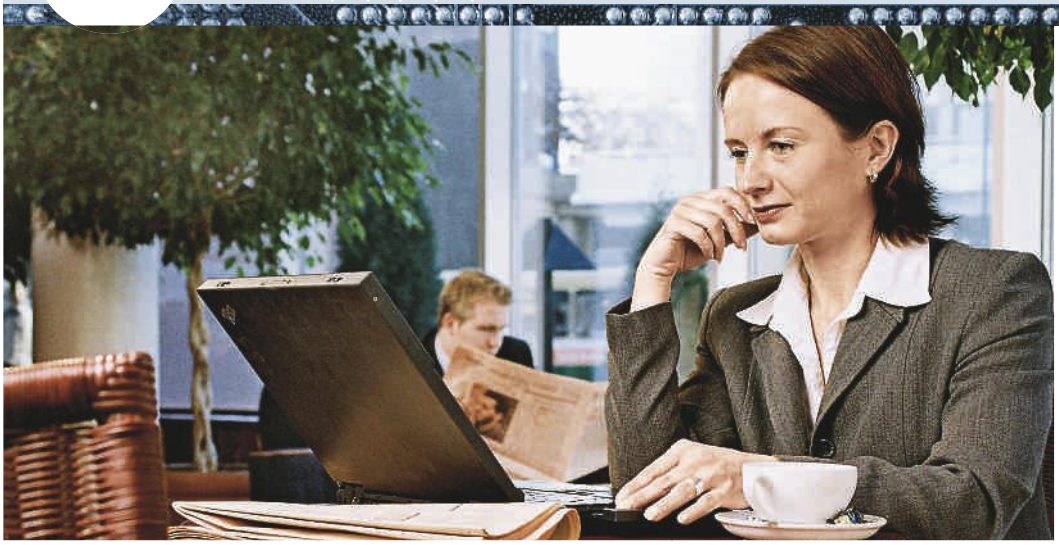
Die Fieberkurve zeigt steil nach oben: Die Antiviren-spezialisten von Kaspersky Labs führen genau Buch über die Zahl der Programme, die im Internet kursieren, um Nutzerdaten auszuspionieren.



Quelle: Kaspersky Labs

Die Methoden der Hacker

- **Phishing:** Die einfachste Methode, an Ihr Geld zu kommen. Hacker fragen einfach per Mail nach Ihren Zugangsdaten – getarnt als Ihre Bank. In den Mails befinden sich Links, die Sie auf gefälschte Bank-Web-Seiten führen.
- **Pharming:** Stellen Sie sich vor, Sie geben die Adresse Ihrer Bank in Ihren Internet-Browser ein und werden dann auf eine gefälschte Seite geführt, die der Ihrer Bank täuschend ähnlich sieht – das ist Pharming. Dabei schleusen die Hacker entweder ein kleines Programm direkt auf Ihren PC ein oder sabotieren die DNS-Server, die die Telefonbücher des Internet sind. Sie sagen dem Browser, wohin er surfen soll, wenn Sie eine Adresse eingeben.
- **Trojaner:** Der Name verrät es schon. Trojaner schleichen sich, oft als nützliches Dienstprogramm getarnt oder „Huckepack" mit einer anderen Software, auf Ihren PC. Dort spionieren sie alle Ihre wichtigen Daten aus und schicken sie dann an die Internet-Mafia. Diese und weitere Spionageprogramme werden als „Spyware" bezeichnet.
- **Keylogger:** eine Software oder sogar ein kleines Gerät zwischen PC und Tastatur, das jede Eingabe protokolliert und an den Hacker schickt.
- **Cross-Site-Scripting:** Hackern gelingt es durch manipulierte Links (meist in E-Mails), eigene Funktionen in Ihnen vertraute Web-Seiten einzubauen. Sie befinden sich tatsächlich auf Ihrer vertrauten Banking-Seite, doch der Hacker fängt alle Eingaben ab.
- **Exploits:** Fast jede Software hat Lücken, die Hacker für Angriffe verwenden können. Codes, die diese Lücken ausnutzen, heißen Exploits – aus ihnen können Viren entstehen.
- **Würmer:** Würmer sind Viren, die selbst alles unternehmen, um sich weiterzuverbreiten. Etwa indem sie sich selbst an alle Empfänger aus einem E-Mail-Adressverzeichnis eines infizierten PCs verschicken.
- **Rootkits:** Diese Schadprogramme greifen tief in Ihr Computer-System ein. Sie geben sich selbst Administrator-Rechte und können so Ihren PC komplett übernehmen. Herkömmliche Anti-Viren-Tools sind meist machtlos.



Bequem, aber gefährlich ist das Online-Banking in Cafés und Lounges über das Funknetzwerk WLAN

www.die-online-bank.de durch die Adresse www.die-on1ine-bank.de ersetzt werden, ohne dass es die meisten Nutzer merken würden. Verbreitet ist auch das „Pharming". Dabei gelingt es Hackern, Web-Anfragen nach Online-Banking-Seiten auf ihre eigenen, gefälschten Seiten zu locken. Dafür greifen sie entweder die DNS-Server an oder manipulieren direkt die Computer ihrer Opfer. Die DNS-Server sind so etwas wie die Telefonbücher des Internet; gibt man eine Web-Adresse in das Browserfenster ein, weist ein DNS-Server den richtigen Weg – oder eben nicht.

Arglos führt der Nutzer dann hier seine Überweisungen und andere Bankgeschäfte aus und liefert der Online-Mafia alles, was sie braucht, um sein Konto zu plündern.

Laut einer repräsentativen Umfrage von Microsoft sind in den USA bereits 17 Prozent aller erwachsenen Amerikaner schon einmal Opfer eines Online-Betrugs geworden. 81 Prozent von ihnen waren auf Phishing-Mails mit täuschend echten Logos und Anschreiben hereingefallen.

Das Internet, so zeigt sich, ist zur perfekten Spielwiese für die Organisierte Kriminalität geworden. Ganz einfach lassen sich aus sicherer Entfernung, völlig anonym, millionenfache Angriffe starten. An jedem ganz normalen Wochentag im zweiten Halbjahr 2006 beobachtete Antivirenspezialist Symantec weltweit rund acht Millionen Betrugsversuche. Und das nur bei durch Programme des Herstellers geschützten Rechnern! Selbst wenn sich lediglich bei einem winzigen Prozentsatz der Millionen attackierten Rechner eine Lücke findet, wenn nur ein paar Dutzend der unzähligen per Spam-Mail angeschriebenen Internet-Nutzer unvorsichtig sind, geht das Kalkül der Online-Mafia auf.

Das Schlimmste: Die Mafiabanden brauchen nicht einmal ein Computergenie in ihren Reihen, einfache Kenntnisse reichen völlig aus. Das Internet ist schon längst zum Basar geworden, auf dem alle Arten von bösartiger Software entweder frei verfügbar sind oder von Hackern zum Kauf angeboten werden. Wie bei einem Baukasten kann sich die Mafia an einzelnen Programmteilen bedienen und sich dann ihr persönliches Angriffsprogramm zusammenbasteln.

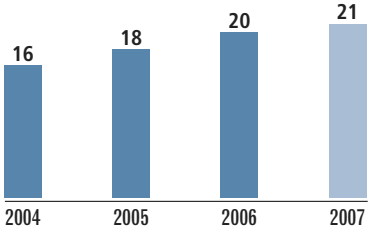
Sogar komplette sogenannte Bot-Netzwerke werden im Internet verkauft: Hacker haben unzählige Rechner ohne das Wissen ihrer Besitzer übernommen und können diese „Roboter" (Bots) fernsteuern. Völlig anonym schicken die Kunden dieser Hacker über diese PCs Massen-E-Mails mit Werbung, gefährlichen Viren, Trojanern und Spionageprogrammen (Spyware).

Symantec geht davon aus, dass weltweit rund sechs Millionen solcher Zombie-Computer existieren. Im ak-

Immer mehr Nutzer

Die Zahl der Online-Banking-Nutzer in Deutschland nimmt ständig zu – 21 Millionen sollen es Ende 2007 sein. Dabei ist die Zahl der online geführten Konten noch um einiges höher: Viele Internet-Nutzer haben mehrere Konten.

Online-Banking-Nutzer in Deutschland
in Millionen Euro, 2007 Prognose



Quelle: BITKOM (Zahlen für 2007 geschätzt)

Regelmäßig kommt es zum Wettlauf zwischen der Online-Mafia und den Antivirenspezialisten

tuell größten dieser Bot-Netzwerke sollen rund 1,7 Millionen Rechner zusammengefasst sein.

Bei ihren Attacken werden die Hacker immer schneller – blitzschnell nutzen sie jede neu erkannte Lücke in den Betriebssystemen (etwa Microsoft Windows) und Anwendungsprogrammen (zum Beispiel Outlook und Internet Explorer). Bei den „Zero day Exploits" (in etwa: „1-Tages-Ausbeutung") kommt es regelmäßig zum Wettlauf zwischen den Virenschreibern und den Programmierern bei den Herstellerfirmen und Antivirenspezialisten.

Gefährliches Werbegeschenk: Hacker verschicken Viren schon per USB-Stick

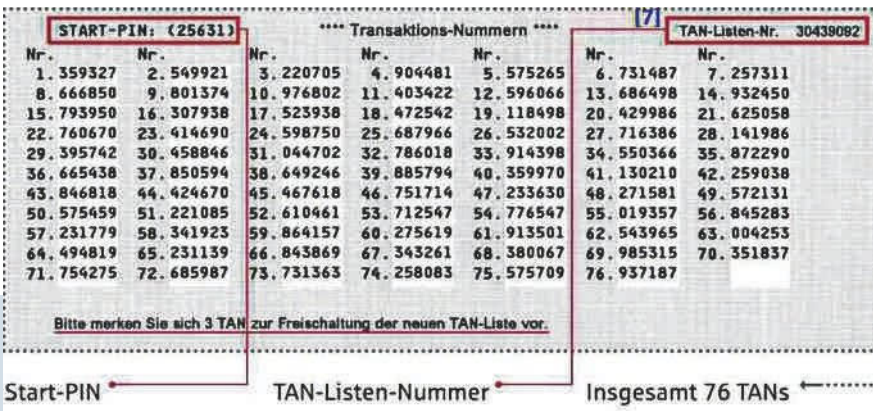
Die Online-Mafia will das Einfallstor nutzen, solange es offen ist, die Programmierer der anderen Seite wollen es so schnell schließen wie möglich. Listen mit bekannten Schwachstellen kursieren breit gestreut im Internet. Hacker sind ständig auf der Suche nach neuen und präsentieren ihre Fundstücke meist stolz der Konkurrenz. Sogar auf Ebay wurde 2005 schon einmal ein bis dahin unbekannter Exploit zum Kauf angeboten.

Besonders dramatisch: Selbst Virenschutzprogramme, Firewalls und regelmäßige Software-Updates versagen immer öfter ihren Dienst. „Die Sicherheitslage hat sich grundlegend geändert", sagt auch das BSI in seinem Lagebericht 2007. „Bei gezielten Angriffen können moderne Schadprogramme individuell an eine bestimmte Einsatzumgebung angepasst werden, so dass sie von Virenschutzprogrammen nicht erkannt werden."

Die Schwachstelle: Jeder Internet-Computer nutzt bestimmte Übertragungsprotokolle, um überhaupt mit dem World Wide Web kommunizieren zu können. Indem die Angreifer genau diese Protokolle nutzen und so tun, als seien sie etwa ein E-Mail-Programm, tricksen sie die Sicherheitsmechanismen wie z. B. eine Firewall aus.

Eine weitere erschreckende Entwicklung: Die Angriffe werden immer persönlicher und individueller. Vielfach haben die Online-Bankräuber schon vor der ersten Attacke genug über ihr Opfer herausge- ▶

„TAN und PIN" ist nach wie vor eine der am häufigsten genutzten Zugangsarten für Online-Banking – und für Hacker-Angriffe extrem anfällig.



Sicherungsmethoden beim Online-Banking

HOHES SICHERHEITSNIVEAU

HBCI/FinTS mit Chipkarte: „Home Banking Computer Interface" ist das sicherste System. Es schützt Ihre Daten selbst auf einem virenverseuchten PC. Transaktionen funktionieren nur, wenn Sie sich mit einer Chipkarte und Ihrer PIN per Lesegerät und Software an Ihrem Computer ausweisen.

MITTLERES SICHERHEITSNIVEAU

PIN und eTAN: Sie erhalten ein kleines elektronisches Gerät (Token) für den Schlüsselbund. Bei Transaktionen erhalten Sie von Ihrer Bank eine Nummer, die Sie in das Gerät eingeben. Es generiert dann eine TAN, die Sie in Ihrer Banking-Seite eintippen müssen. Beim eTAN-Plus-System funktioniert die TAN-Erzeugung nur in Verbindung mit der Kundenkarte Ihrer Bank.

PIN und mobile TAN: Um einen Online-Banking-Vorgang abzuschließen, müssen Sie eine TAN eingeben, die von der Bank per SMS auf Ihr Handy geschickt wird. Die mobile TAN ist meist nur wenige Minuten gültig. Das soll verhindern, dass Hacker mit ergaunerten TANs etwas anfangen können.

PIN und iTAN: Die TANs sind durchnummeriert. Die Bank fordert immer eine bestimmte TAN. Das erschwert es dem Hacker etwas, ergaunerte TANs beliebig einzusetzen – ist aber kein besonders aufwendiges Hindernis, etwa bei Pharming und Cross-Site-Scripting.

NIEDRIGES SICHERHEITSNIVEAU

PIN und TAN: Neben einer Geheimnummer (PIN) brauchen Sie für jeden Banking-Vorgang (z. B. Überweisung) eine beliebige Nummer von Ihrem TAN-Block. Sehr unsicher, weil Hacker, die PIN und beliebige TANs ergaunert haben, volle Verfügungsgewalt über Ihr Konto haben.

funden, um es mit seinem korrekten Namen und der richtigen Adresse anzusprechen. Vorsicht auch vor Werbegeschenken wie USB-Sticks. Denn gerade bei gezielten Attacken auf stark gesicherte Firmenrechner nutzen die Hacker heute einfach die klassische Post statt E-Mail: In einem Paket ist dann beispielsweise ein USB-Stick zu finden oder wahlweise auch eine CD-ROM mit einem Gratis-Spiel. Steckt der Empfänger dann das Geschenk in seinen Rechner, hat der Angreifer sein Ziel schon erreicht. Auch die beste Firewall und der beste Virenscanner können jetzt nichts mehr tun – der Schädling ist bereits auf dem Rechner.

Ist der PC infiziert, haben Nutzer von klassischen Online-Banking-Systemen mit PIN- und TAN-Sicherung bald nichts mehr zu lachen: Die trojanischen Pferde und andere Spionageprogramme zeichnen jeden Tastendruck auf und schicken Passwörter und andere Zugangsdaten direkt zu ihren Meistern. Besonders das Online-Banking mit HBCI und Chipkarte ist dagegen gefeit. Denn selbst wenn ein Trojaner, Keylogger oder Virus auf dem Rechner sein sollte, kann er bei diesem Mix aus Hard- und Software nichts anrichten.

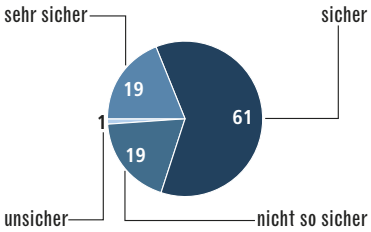
Der neueste Trick der Mafia, im August vergangenen Jahres auf einer Hacker-Konferenz öffentlich gezeigt: Hacker nützen die in neue Computerchips von Intel und AMD integrierten Virtualisierungsmöglichkeiten für ihre Zwecke aus. Die neuen Prozessoren ermöglichen es ihren Nutzern nämlich, neben ihrer normalen Arbeitsumgebung ein virtuelles System zu starten – ein simulierter Computer im Computer. Hacker können das ausnutzen und mit sogenannten VM-Rootkits PCs komplett übernehmen und einen virtuellen Computer schaffen, ohne dass es der Benutzer merkt. Dieser denkt, er surft ganz normal mit seinem PC, befindet sich aber längst in der virtuellen Umgebung des Hackers.

Im Moment ist das nur ein Gedankenspiel. „Zurzeit starten Virenschreiber kaum Angriffe mit neuartigen Methoden“, sagt Alexander Gostev vom Antivirenspezialisten Kaspersky Lab. Stattdessen würden sie seit etwa einem dreiviertel Jahr hauptsächlich auf Altbekanntes setzen. Hier, so Gostev, sei aber eine Entwicklung besonders deutlich: „Die Kommerzialisierung der Virenschreiber.“ Alle hätten nur noch ein Ziel: „Aus den alten Technologien so viel herauszumelken wie möglich.“ Entsprechend sei zwar nicht die Qualität, aber die Quantität der Angriffe gestiegen. Deshalb kämen Viren heutzutage auf allen Kanälen auf die Computernutzer zu: Nicht mehr

Großes Vertrauen

Eine Umfrage des deutschen Bankenverbands zeigt es: 61 Prozent der Deutschen fühlen sich beim Online-Banking sicher, 19 Prozent sogar sehr sicher. Nur 19 Prozent empfinden Bankgeschäfte im Internet als nicht sicher und nur ein Prozent als unsicher.

Wie beurteilen Sie die Sicherheit von Online-Banking? (in Prozent)



Quelle: Bundesverband Deutscher Banken

Die besten Security-Suiten

In Kooperation mit dem Virentestlabor AV-Test (www.av-test.de) ließ CHIP zehn aktuelle Security-Suiten einen extrem harten Sicherheitstest absolvieren. So musste die Software auch unbekannte Schädlinge erkennen und zuverlässig entfernen – die Kür für die Sicherheitsprogramme. Wichtiges Kriterium: Trotz des hohen Anspruchs an die Sicherheit durften die getesteten Programme den Computer nicht unnötig belasten und ausbremsen.

Platzierung	Security-Suite	Preis
1	Symantec Norton Internet Security 2007	60 Euro
2	F-Secure Internet Security 2007	40 Euro
3	G Data Internet Security 2007	40 Euro
4	Bitdefender Internet Security v10	70 Euro für 2 Lizenzen
5	Trend Micro PC-cillin Internet Sec. 2007	50 Euro

Sicher wie eine Burg ist kein PC-System. Hacker finden immer Wege

Sicherheits-CD. Security-Suiten können den PC schützen – bis zu einem gewissen Grad

Die Internet-Mafia arbeitet gerade an der nächsten großen Angriffswelle auf die Online-Konten

nur per E-Mail, sondern auch über Instant-Messenger, Online-Tauschbörsen und Online-Spiele.

Was die Sicherheitsexperten beunruhigt: Sie gehen davon aus, dass die Mafia auf Hochtouren an neuen Attacken arbeitet. Die nächste Angriffswelle wird kommen. Spätestens dann, wenn die bisherigen Methoden für die Online-Mafia nicht mehr genug Gewinn abwerfen. Also, wenn auf den meisten PCs auch die letzte bekannte Lücke geschlossen ist.

Vermutlich ist auch die Einführung von Windows Vista ein Grund. Nicht etwa, weil das neue Betriebssystem, wie von Hersteller Microsoft versprochen, besonders sicher wäre. Sondern, weil sich die Hacker im Moment erst noch ausführlich mit der neuen Umgebung beschäftigen, neue Ideen testen und Angriffsformen entwickeln – und warten, bis endlich genug Menschen rund um den Globus mit Windows Vista surfen, dass sich eine Attacke auch wirklich lohnt.

Höchste Zeit also, gegen die zu erwartende Megaattacke der Online-Mafia aufzurüsten. Mit aktueller Schutzsoftware, Hintergrundwissen über die Methoden der Hacker und Phisher und mit einer Umstellung weg vom einfachen PIN- und TAN-Verfahren zu sichereren Online-Banking-Methoden.

Denn es wäre den deutschen Online-Banking-Nutzern ja nicht zu wünschen, dass sie ihr Sicherheitsgefühl verlieren und es ihnen bald so geht wie den Surfern in Großbritannien: Dort haben mehr Menschen Angst vor Internet-Kriminalität als vor einem Einbruch.

Beschreibung	Plus	Minus	Fazit	Punkte im CHIP-Test
komplette Suite mit relativ hohem Preis	sehr guter Schutz	teure Hotline	bequemer und zuverlässiger Rundumschutz auch für Anwender ohne Expertenwissen	73
gute Suite mit sehr guten Testergebnissen	guter E-Mail-Filter	zu hohe Systemlast	ausgewogener Schutz in allen Bereichen, der Preis-Leistungs-Tipp der CHIP-Redaktion	70
schnelle Reaktion auf neue Gefahren	gute Erkennung	zu lange Scan-Dauer	Browser-Phishing-Filter könnte besser sein, Firewall legt bei einem Angriff den PC lahm.	69
Suite mit sehr guter Erkennungstechnik	guter E-Mail-Filter	zu späte Aktualisierung	eine gute und günstige Lösung, wenn man zwei Rechner gleichzeitig schützen will	69
spezialisierte Suite für besondere Fälle	schnelle Scan-Dauer	schlechte Firewall	besonders zu empfehlen bei bereits durch Schadprogramme infizierten Rechnern	67

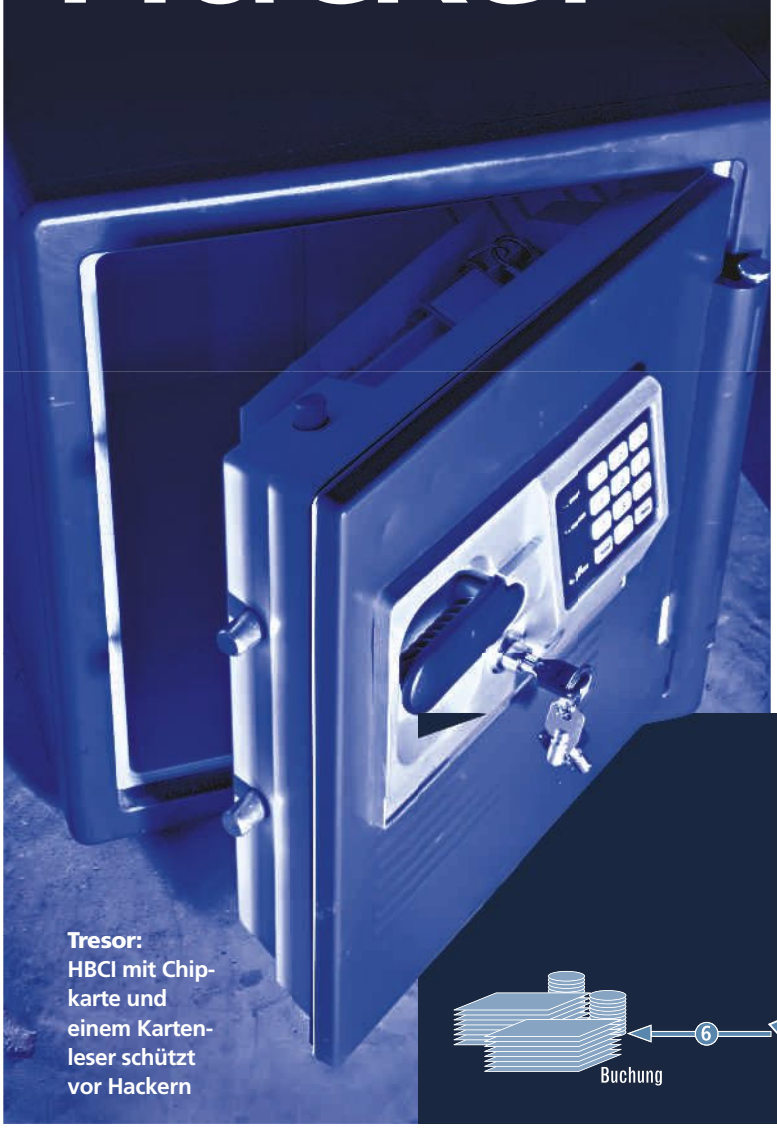
Quelle: CHIP

Tipps für sicheres Surfen

- **Automatische Updates:** Aktivieren Sie in Ihrem Betriebsystem (z. B. Microsoft Windows XP) unbedingt die automatische Update-Funktion – das gilt auch für alle anderen Programme, die dies anbieten. Hacker nutzen neue erkannte Lücken im System und in Programmen wie Internet Explorer oder Outlook sofort für Angriffe. Durch die Updates werden diese Lücken geschlossen. Aber: Bis die Programmierer eine Lösung gefunden haben, ist Ihr System verwundbar.
- **Aktuelle Security-Suite:** Ein Virenscanner allein nützt nichts. Den bequemsten Schutz bieten Security-Suiten (siehe Test unten links), die mehrere Schutzprogramme vereinen – neben dem obligatorischen Virenscanner etwa auch Firewalls, Spyware-Erkennung sowie Phishing- und Spam-Filter.
- **Firefox verwenden:** Der Microsoft-Browser Internet Explorer gilt als das größte Einfalltor für Hacker. Als sicherer gilt der kostenlose Firefox (Download unter www.getfirefox.de). Auch er ist nicht fehlerfrei, aber die große Gemeinschaft der Entwickler präsentiert meist extrem schnell Lösungen und automatische Updates für erkannte Lücken. Stellen Sie auf jeden Fall die Sicherheitsstufe Ihres Browsers als „hoch" ein.
- **Aufmerksam und kritisch sein:** Phishing-E-Mails setzen auf die Gutgläubigkeit ihrer Empfänger. Seien Sie vorsichtig bei jedweder elektronischen Post, die angeblich von Ihrer Bank kommt oder die Sie zum Anklicken von Links oder gar Anhängen wie Bildern und PDF-Dokumenten auffordert. Achten Sie beim Online-Banking auf die sichere SSL-Verschlüsselung (sichtbar am kleinen Schloss rechts unten im Browser) und die korrekte Adresse Ihrer Bank im Adressfenster des Browsers.
- **Nicht als Administrator surfen:** Surfen Sie niemals als Administrator im Internet – das bedeutet als der Nutzer, der alles auf Ihrem PC darf. Das überträgt sich auf die Viren. Bei Windows Vista ist es automatisch so, bei XP leider nicht. Hier sollten Sie neben Ihrem Haupt-Benutzerkonto ein weiteres mit weniger Rechten einrichten.

HBCI mit Chipkarte

Aus für Hacker

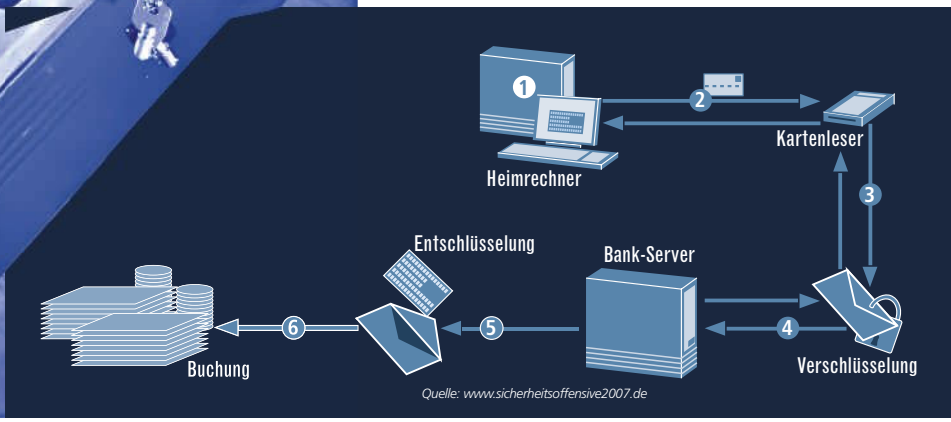


Tresor: HBCI mit Chipkarte und einem Kartenleser schützt vor Hackern

Deutschlands Internet-Gangster sind auf dem Vormarsch. Das belegt die aktuelle Kriminalstatistik des Bundesinnenministeriums. Danach kletterte die Zahl der Phishing-Attacken, bei denen Hacker Passwörter und TANs ausforschten, um 26,4 Prozent auf 2999 Fälle – Tendenz steigend. „Rund 90 Prozent aller Delikte von Computer-Gaunerei drehen sich um das Phishing", bilanziert Roland Henkel, Chef der Ermittlungsgruppe „Internetbetrug" bei der Frankfurter Polizei.

Hoch auf HBCI. Vor diesem Hintergrund sind Online-Bankern zuverlässige Abwehrsysteme gegen Web-Diebe wichtiger denn je. „Den besten Schutz vor Ganoven bei Geldgeschäften via Internet bietet derzeit wohl HBCI in Verbindung mit einer Chipkarte und einem Kartenlesegerät", sagt Thomas Krabichler, Projektleiter des wissenschaftlichen Instituts ibi Research an der Universität Regensburg. Das Kürzel HBCI steht für Homebanking Computer Interface. Die von der deutschen Kreditwirtschaft in den 90er-Jahren konzipierte Verschlüsselungstechnik wurde mittlerweile zum „Financial Transaction Services", kurz FinTS, verfeinert und weiterentwickelt.

Nahezu hackerresistentes Homebanking mittels HBCI läuft nicht nur auf allen Rechnern mit Windows, sondern auch unter Mac-OS von Apple oder Linux. Komfortabel für den Anwender ist zudem, dass er keine umfangreichen Vorkehrungen am



Quelle: www.sicherheitsoffensive2007.de

PC treffen muss, um sicher Online-Geschäfte zu tätigen. Nicht zu vergessen ist auch das einfache Handling in der Alltagspraxis. Zunächst muss der Nutzer alle Konten für das ausgeklügelte Sicherheitsverfahren bei seiner Bank freischalten lassen. Die Installation der HBCI-Software und des Chip-Kartenlesers am PC ist leicht. Will der Online-Banker etwa Geld transferieren, fährt er die HBCI-Software hoch, loggt sich mit seinen Zugangsdaten im Programm ein, füllt eine Überweisung aus, klickt mit der Maus auf „Senden" und autorisiert sich gegenüber der Bank als Kunde mit Chipkarte und Eingabe der PIN auf dem Kartenleser (s. Schausbild unten). Das Ganze funktioniert aber auch ohne Software. Die Deutsche Bank und die Bremer Sparkasse etwa bieten HBCI mit Chipkarte alternativ im Browser-Banking an.

Sicher und simpel. Top-Vorteil dieser Identifikationsmethode, die sich auch für Menschen mit wenig Hang zu komplizierter Technik eignet, ist: „Da die PIN nicht wie beim webbasierten Online-Banking über die PC-Tastatur auf den Masken der Banken eingetippt wird, können geheime Daten auch nicht durch Keylogging auf dem Rechner ausgespäht werden", sagt Candid Wüest, Sicherheitsexperte beim renommierten IT-Spezialisten Symantec.

Wirkungsvoll vor Datenklau aus dem Netz schützt zudem die gegenseitige Authorisierung von Bankkunde und Kreditanstalt: Chipkarte und Finanzinstitut tauschen dazu vor jedem Geldtransfer elektronisch signierte Nachrichten aus. Auf Grund der gegenseitigen Kenntnis sogenannter Signierschlüssel identifizieren sich Nutzer und Bank damit eindeutig. Plus: Transaktionsnummern, die mit Phishing-Mails ausspioniert werden könnten, braucht die Methode überhaupt nicht (s. auch rechts).

Auch wenn HBCI mit Chipkarte beim Internet-Zahlungsverkehr im Vergleich zu webbasierten Lösungen mit PIN und Transaktionsnummern wesentlich sicherer vor Hacker-Invasionen schützt: „Das Verfahren verliert leider seine Abwehrkraft, wenn Nutzer Chipkarte und PIN gemeinsam aufbewahren und diese gestohlen werden", warnt Wüest. Daher rät der erfahrene Sicherheitsexperte: „Chipkarte und PIN sollte man stets getrennt aufbewahren."

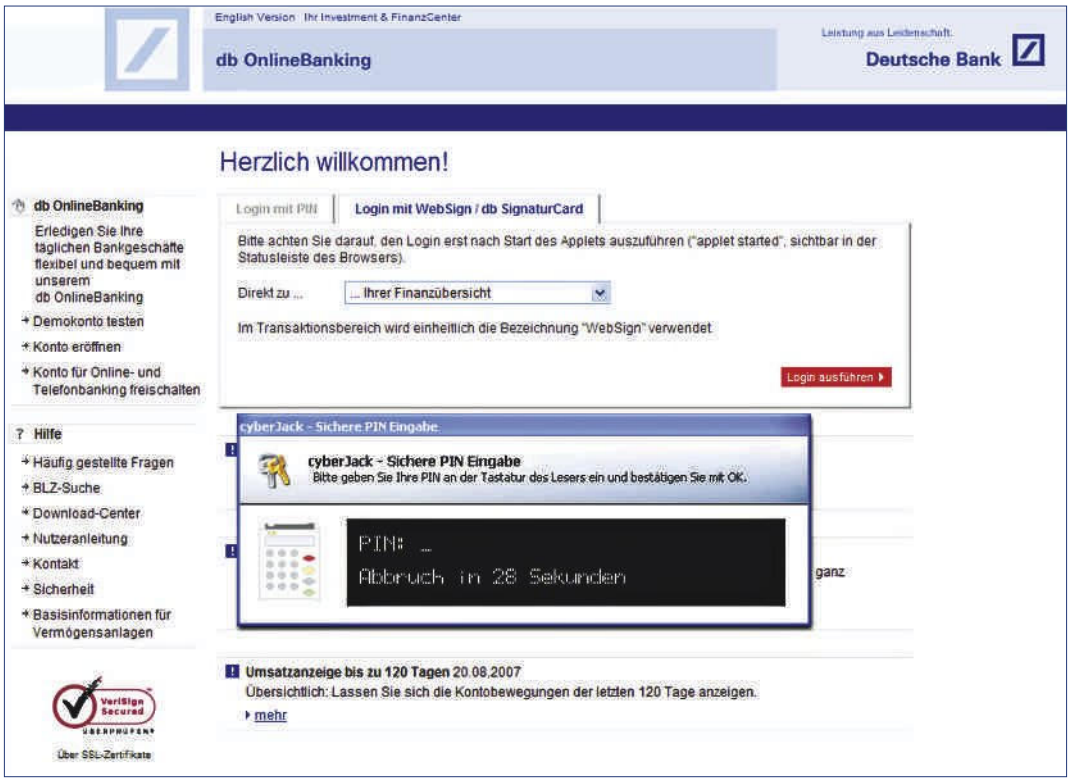
Doppeltes Netz. Theoretisch auszuschließen ist allerdings nie, dass ein Hacker die HBCI-Software manipuliert, so dass etwa Überweisungen unbemerkt auf sein Konto gehen. Um Betrügern keine Chance zu lassen, sollten HBCI-Banker ihren Rechner mit Virenschutz-Programmen (s. auch Seite 8/9) schützen.

So funktioniert HBCI mit Chipkarte in der Praxis

Zunächst füllt der Online-Banker das virtuelle Überweisungsformular im Vergleich zu webbasierten Lösungen lokal auf dem Rechner aus (1). Dann steckt er seine Chipkarte in den Kartenleser und identifiziert sich durch die Eingabe seiner PIN (2). Bevor der Zahlungsbeleg an die Bank geht, wird er vom Chip mit einem Signier- und Chiffrierschlüssel digital unterzeichnet und codiert. Clou: Code und Signatur sind für Hacker unsichtbar, da sich die Daten nur auf dem Chip und im gesicherten Bankenrechner befinden (3). Der Auftrag wird dann über gesicherte Leitungen an den Bank-Server übermittelt (4). Sobald der Institutsrechner die Überweisung hat, decodiert er diese und vergleicht die „Unterschrift" des Online-Bankers mit der auf dem Signierschlüssel der Bank (5). Nur wenn beide Daten übereinstimmen, erfolgt die Buchung (6).

HBCI: viele Vorteile

- **Kein Keylogging:** Online-Banker tippen ihre PIN nicht via PC-Tastatur ins Banking-System ein, sondern in den Chipkartenleser der Sicherheitsklasse 2 und 3. Ein Ausspähen der Geheimdaten mittels Keylogger (Hard- oder Software, die Tastatureingaben protokolliert) ist so unmöglich. Und: Die PIN wird nicht über das Internet an den Server der Bank transferiert, was ein Ausspionieren auf diesem Weg ebenfalls ausschließt.
- **Keine TAN-Listen:** HBCI mit Chipkarte kommt völlig ohne TAN-Listen aus. Das Ausspionieren der Transaktionsnummern von Gaunern via Phishing, Pharming und Trojanern greift so ins Leere.
- **Software-Oberfläche:** Nutzer arbeiten zumeist lokal auf dem Rechner mit einer HBCI-Software. Sie laufen nicht Gefahr, ihre Daten auf gefälschten Seiten einzugeben. Zudem ist der Zugang zur Banking-Software passwortgeschützt. Vorteil: Selbst wenn jemand die HBCI-Karte stiehlt, kann der Dieb noch lange nicht einfach die Software starten. Doch HBCI geht auch ohne Software. Die Deutsche Bank etwa bietet alternativ HBCI mit Chipkarte im Browser-Banking an.
- **Gegenseitige Autorisierung:** Chipkarte und Geldhaus tauschen vor der Transaktion signierte Nachrichten aus. Auf Grund der gegenseitigen Kenntnis der Signierschlüssel identifizieren sich Nutzer und Bank damit eindeutig.
- **Daten-Chiffre:** Der Geldtransfer wird im Chipkartenleser sicher vor Hackern elektronisch signiert und verschlüsselt. Auch erkennt der Institutsserver, ob die Nachricht eventuell manipuliert wurde.
- **Chipkarte als Sicherheitsmedium:** Ohne HBCI-Chipkarte ist eine Finanztransaktion nicht möglich. Selbst wenn jemand die PIN stiehlt, ist diese ohne Chipkarte wertlos. Anders als ein Magnetstreifen lässt sich der Chip nicht auslesen. Grund: Signier- und Chiffrierschlüssel sind im Chip-Betriebssystem SECCOS (Secure Chip Card Operating System) gut vor Hackern geschützt.
- **Flexibilität:** Mit der Finanzsoftware können gleich mehrere Bankverbindungen bei diversen Banken verwaltet werden. Umständliches Einloggen auf webbasierten Institutsseiten mit unterschiedlichen Zugangscodes entfällt.



HBCI-Banking der Deutschen Bank: einfach, übersichtlich und sicher

Chipkartenleser

Qual der Wahl

Sicherheit hat ihren Preis. Das wissen auch Online-Banker. Einer aktuellen Studie der IT-Beratung Pass aus Aschaffenburg zufolge ist daher fast ein Drittel der Finanzjongleure im Web dazu bereit, für effiziente Abwehrsysteme gegen Hacker mehr Geld in die Hand zu nehmen (s. Grafik S. 13).

Diese Geisteshaltung dürfte dem zwar unverletzlichsten, jedoch auch kostenintensivsten Banking-Verfahren HBCI mit Chipkarte und Kartenleser zum Durchbruch verhelfen.

Fallende Preise bei den modernen Chipkartenlesern steigern zudem die Akzeptanz der Verschlüsselungstechnik. „Auch sind derzeit bereits gut 2000 Banken in Deutschland fit für HBCI", bilanziert Ortwin Scheja, Abteilungsleiter bei Security Research & Consulting in Bonn. Doch welche Kartenleser eignen sich fürs Web-Banking? Und welche Sicherheitsklassen gibt es (s. Tabelle S. 13)?

Obwohl einige Hersteller von Laptops Chipkartenleser in ihre Portables integrieren, dominieren heute auf dem Markt externe Geräte, die über ein USB-Kabel am Rechner andocken. Einfache Modelle der Sicherheitsklasse 1 gibt es schon für etwas mehr als 20 Euro. Doch Vorsicht! Diese Kartenleser fungieren nur als Kontaktoberfläche für die Chipkarte. Da sie keine eigene Tastatur besitzen, müssen Nutzer die PIN via PC eintippen. Dementsprechend eignen sich diese Modelle zwar für das Auslesen einer GSM-Karte. Für sicheres Online-Banking aber taugen sie nicht.

Dazu braucht es mindestens Kartenleser der Sicherheitsklasse 2 mit eingebautem Tastaturblock. Preis: zwischen 40 und 70 Euro. „Über diesen können Nutzer ihre Geheimzahl direkt ohne Umweg über den PC vom Chipkartenmodul an die Chipkarte übertragen", erklärt Candid Wüest,

Kartenleser-Typen und ihre Eignung

Eigenschaften der Geräte	Chipkartenleser Sicherheitsklasse 1	Chipkartenleser Sicherheitsklasse 2	Chipkartenleser Sicherheitsklasse 3
im PC oder auf Tastatur integriert	+*	+*	–
eigene Tastatur für sichere Dateneingabe	–	+	+
eigenes manipulationssicheres Display[1)]	–	–	+
Transaktionsprüfmodule im Chipkartenleser	–	–	+
anerkannte Sicherheitszertifizierung	–	+*	+
Online-Firmware-Updates möglich	+*	+	+
Geräte besonders geeignet im Bereich	Jugendschutz, E-Ticketing	Homebanking, Signatur-anwendungen, Jugendschutz, E-Ticketing	sicheres Bezahlen im Web, Homebanking, Signatur-anwendung, Jugendschutz, E-Ticketing, Geld-karte laden

*teils; [1)]zur Anzeige von Transaktionsdaten

Quelle: Initiative Geldkarte

Fachmann beim IT-Spezialisten Symantec. Das nimmt Internet-Gaunern die Chance, die PIN über Keylogger am PC heimlich abzugreifen. Ist erst einmal die sichere PIN-Eingabe aktiv, wird das dem Anwender über eine optische Anzeige am Kartenleser oder akustisch signalisiert.

König der Kartenleser. „Das Nonplusultra für HBCI-Banking sind Geräte der Sicherheitsklasse 3", betont Insider Wüest. „Neben einer manipulationssicheren Tastatur haben sie ein Display, mit dessen Hilfe der Anwender die Transaktion verfolgen kann", ergänzt Scheja. Bankenexperten arbeiten gerade mit Hochdruck an einer Lösung, bei der künftig während des Bezahlvorgangs auf der Anzeige neben dem Namen des Empfängers auch der abzubuchende Betrag zu lesen sein wird. So kann der Nutzer die Angaben überprüfen, bevor er per Tastendruck die Überweisung freigibt. Preise der Kartenleser: je nach Modell bis zu 125 Euro.

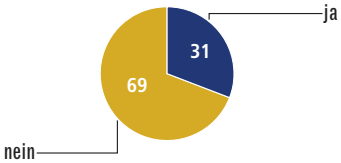
Egal, für welche Modellvariante sich der Verbraucher auch entscheiden mag – damit das Betriebssystem des Rechners auf den Kartenleser zugreifen kann, müssen auf diesem die passenden Treiber installiert werden. Besonders komfortabel sind Chipkartenleser, die ihre Treibersoftware automatisch via Internet aktualisieren. In der Lage dazu sind sämtliche Chipkartenleser-Modelle des Branchenprimus Reiner SCT aus Furtwangen. „Neben der Unterstützung alternativer Betriebssysteme wie Linux spricht für Geräte von Reiner SCT der reibungslose Support im Garantiefall", urteilt Eberhard Kreck, Vorstand der Volksbank Kirchhellen. Das Kreditinstitut setzt gezielt auf HBCI mit Chipkarte (s. dazu auch Interview S. 14).

Trotz etlicher Vorteile haben Chipkartenleser ein kleines Manko. Sie schränken die Mobilität ein. Wer auf Reisen alternativ zum HBCI-Banking sichere Deals ohne Kartenleser über eine browserbasierte Seite machen will, kann alternativ zu handlichen TAN-Generatoren mit einem Chipkarten-Slot greifen. Dieser generiert eine hackersichere Transaktionsnummer und zeigt sie auf dem Display des „Token" an. Diese Nummer tippt der Nutzer zur Legitimation seiner Transaktion in die Banking-Maske ein.

Hohe Bereitschaft

Die Zahl der Online-Banker in Deutschland steigt ständig. Fast ein Drittel der Finanzakteure im Netz würde in hackerresistente Abwehrsysteme Geld investieren.

Würden Sie für mehr Sicherheit auch bezahlen? in Prozent



Quellen: Pass Consulting

TAN-Generator mit Chipkarten-Slot: Das mobile Gerät erzeugt hackersichere TANs und zeigt sie auf dem Display

„Das Nonplusultra für HBCI-Banking mit Chipkarte sind Kartenleser der Sicherheitsklasse 3"

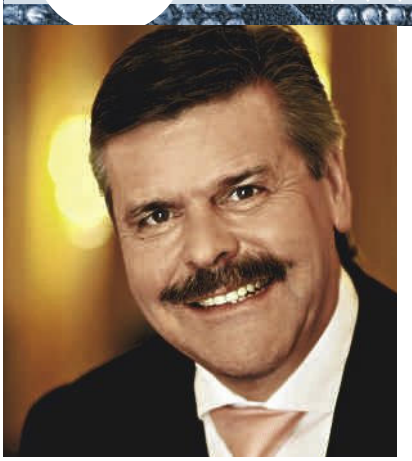
Candid Wüest, Internet-Sicherheitsexperte beim IT-Spezialisten Symantec

Banken mit HBCI-Technik

In Deutschland arbeiten bereits mehr als 2000 Kreditinstitute mit HBCI oder FinTS als hackerresistentem Verschlüsselungsverfahren, darunter die größten der Branche aus allen Bankengruppen (s. Liste unten). Welche Geldhäuser aktuell HBCI oder FinTS einsetzen, können Interessierte im Internet unter **www.hbci-finder.de** nachlesen.

1822 direkt	0180/3241822*
Bank 1 Saar	0681/30040
Berliner Sparkasse	030/86986969
Berliner Volksbank	030/30630
BW-Bank	0711/1240
Commerzbank	069/13620
Deutsche Bank	069/91000
Deutsche Kreditbank (DKB)	0180/3120300*
Dortmunder Volksbank	0231/54020
Dresdner Bank	069/2630
Frankfurter Sparkasse	069/24182224
Frankfurter Volksbank	069/21720
HSBC Trinkaus & Burkhardt	0211/9100
HypoVereinsbank	089/3780
Kreissparkasse Köln	0221/22701
Mainzer Volksbank	06131/1480
Merck Finck & Co.	0180/2104010*
Mittelbrand. Sparkasse	0331/890
Naussauische Sparkasse	0611/3640
Raiffeisenb. Aschaffenburg	06021/4970
Rostocker VR-Bank	0381/49670
Sparkasse Bremen	0421/1790
Sparkasse Celle	05141/9130
Sparkasse Hannover	0511/30000
Sparkasse Leipzig	0341/9860
Spark. Münsterland Ost	0180/1400501 50*
Sparkasse Nürnberg	0911/2300
Sparkasse Saarbrücken	0681/5040
Sparkasse Südholstein	0180/1010900*
Stadtsparkasse Düsseldorf	0211/8782211
Stadtsparkasse München	089/21670
Volksbank Freiburg	0761/21821111
Volksbank Gütersloh	05241/1040
Volksbank Kirchhellen	02041/1020
Volksbank Ruhr Mitte	0209/3850
Wartburg Sparkasse	01801/84055050*

Quelle: Informatikzentrum der Sparkassenorganisation SIZ, *Rufnummer mit erhöhter Gebühr



Eberhard Kreck,
Vorstand der Volksbank Kirchhellen eG Bottrop

FOCUS-MONEY: Warum haben Sie die altbewährten TAN-Papierlisten vollends gestrichen und durch das HBCI-Banking ersetzt?

Eberhard Kreck: Weil dieses Verfahren aus Sicht der Experten am meisten Sicherheit für Online-Finanztransfers bietet. Und Sicherheit genießt bei uns Priorität.

MONEY: Doch HBCI ist ohne zusätzliche Software und Chipkartenleser leider technisch nicht möglich. Welche Kosten entstehen Ihren Kunden dadurch?

Kreck: Das hängt ganz von den individuellen Ansprüchen jedes Einzelnen ab. Die komplette Hard- und Software plus Chipkarte für das HBCI-Banking bieten wir Interessenten jedenfalls bereits ab 60 Euro an.

MONEY: Schreckt diese doch relativ hohe Summe nicht viele Ihrer Partner ab, zumal Banking via Web-Browser keinen Cent extra kosten würde?

Kreck: Im Gegenteil. Für ein Höchstmaß an Sicherheit auch mehr Geld in die Hand nehmen zu müssen stellt die meisten unserer Kunden vor kein größeres Problem. Würden Sie sich denn heute ein Auto ohne Airbag kaufen, wenn es billiger wäre?

MONEY: Dennoch ist die HBCI/FinTS-Technologie unbestritten viel beratungsintensiver als herkömmliche webbasierte Banking-Lösungen am Markt. Klären Sie darüber auf?

Kreck: Natürlich. Wer sich für HBCI-Banking interessiert, wird über alle Vor- und Nachteile eingehend von unserem Fachpersonal informiert.

MONEY: Wie viel Prozent ihrer Kunden konnten Sie bislang zum Umstieg vom PIN/TAN-Verfahren auf HBCI überzeugen?

Kreck: Von den größeren Geschäftskunden, die ihren Zahlungsverkehr ausschließlich über unsere Software abwickeln, nutzen mehr als 60 Prozent diese Sicherheitstechnologie.

MONEY: Und die Privatkunden?

Kreck: Hier sind es immerhin 22 Prozent – Tendenz weiter steigend.

„Mehr als 60 Prozent unserer Geschäftskunden nutzen bereits HBCI mit Chipkarte“

MONEY: Welche Transaktionen laufen denn primär via HBCI ab?

Kreck: In erster Linie überweisen unsere Kunden auf diesem Weg Geld im In- oder ins Ausland oder rufen Kontostände ab. Einige laden sogar ihr Prepaid-Handy mit Hilfe dieses sicheren Verfahrens auf.

MONEY: Auch wenn HBCI vielseitig in der Anwendung ist, ist ein Manko jedoch die recht eingeschränkte Mobilität, da Chipkartenleser relativ sperrig sind. Welche Lösung offeriert Ihre Bank den Kunden, die auf Reisen sichere Finanztransfers per Laptop ohne Lesegerät abwickeln wollen?

Kreck: In diesem Fall bieten wir unseren Kunden unter anderem das sogenannte Sm@rtTAN plus-Verfahren in Verbindung mit mobilen Geräten an. Die erzeugte Transaktionsnummer wird mit dem eingegebenen Auftrag und der Browsersitzung verbunden. Damit kann das Geld nicht umgeleitet werden.

Deutscher
Sparkassenverlag

DSV*Gruppe*
So viel Lösung, wie Sie brauchen.

Sparen Sie Zeit, Geld und Wege
mit der qualifizierten elektronischen Signatur

Elektronische Geschäftsprozesse von A bis Z – mit der rechtsverbindlichen elektronischen Unterschrift. Nutzen Sie die nahezu unbegrenzten Möglichkeiten der Chipkarten der Sparkassen-Finanzgruppe mit S-TRUST Personenzertifikaten.

S-TRUST – Signaturlösungen für Industrie, Verwaltung, Finanzwirtschaft und Handwerk
Telefon: 0800 4 78 78 78 – E-Mail: info@s-trust.de – www.s-trust.de

VeriSign®

TRUST

Kartenleser & more unter www.sparkassen-shop.de

Hintergrund

Ein Chip, tausend Möglichkeiten

Geldkarte statt Kleingeld: Bezahlt werden mit dem Chip hauptsächlich Kleinbeträge

Spätestens nachdem seit Anfang dieses Jahres an jedem Zigarettenautomaten Hinweise kleben, werden viele Deutsche zum ersten Mal einen kleinen Begleiter entdeckt haben, den sie schon seit Jahren mit sich herumtragen: Den Chip auf ihrer Bank-Karte. Rund 75 Prozent aller EC- und Kundenkarten der deutschen Kreditinstitute haben ihn schon automatisch, ohne dass ihn der Kunde extra beantragen muss. Doch dass man mit dem Chip sein Alter nachweisen kann, ist zwar eine nützliche Möglichkeit – aber nur eine von vielen.

Denn schon wer etwa in München eine Straßenbahn betritt und kein Kleingeld dabei hat, erkennt den praktischen Alltagsnutzen des Chips: Er ist eine elektronische Geldbörse. In der Bahn und auch an fast jedem Ticketautomaten der Münchner Verkehrsbetriebe können Kunden mit Chip bezahlen – und sogar weniger, als wenn sie Bargeld einwerfen würden. In der Bremer Straßenbahn ist es sogar noch bequemer – da wird der Chip der Geldkarte gleich auch noch zum elektronischen Ticket.

In Deutschland nutzen nach einer Studie des Allensbach-Instituts bereits rund 15,1 Millionen Menschen die Geldkarte zum Bezahlen. Egal, ob im Parkhaus, an der Supermarktkasse oder dem Zigarettenautomaten. Meist sind es Kleinbeträge, im Jahr 2006 lag der Durchschnittswert pro Bezahlvorgang bei 2,47 Euro. Bis

Enormes Potenzial

Rund 68 Millionen Karten mit Geldkarten-Chip stecken derzeit in deutschen Geldbörsen – das sind etwa 75 Prozent aller EC- und Kundenkarten der deutschen Geldinstitute. Aber nur die wenigsten Kartenbesitzer wissen, wie viele Anwendungsmöglichkeiten es für den goldenen Chip gibt. Ein enormes Potenzial, das Leben leichter zu machen.

1 Bargeldersatz: Der Chip macht jede Standard-EC-Karte zur Geldkarte. Kunden können die Karte an jedem Geldautomaten ihres Instituts oder beim Online-Banking mit Hilfe eines an ihren PC angeschlossenen Kartenlesers gebührenfrei aufladen. Maximal 200 Euro passen auf eine Karte – immer mehr Verkaufsstellen akzeptieren sie.

2 Konzertkarte: Die fieberhafte Suche nach den verlegten Konzertkarten entfällt ab sofort – denn sie stecken in Ihrer Brieftasche. Der Chip Ihrer Geldkarte speichert nämlich auch Zutrittsdaten für Konzerte und andere Veranstaltungen. Die Kontrolleure am Einlass sind dann mit einem Chipkarten-Lesegerät ausgerüstet.

3 Fahrkarte: Dass man bei vielen Verkehrsbetrieben sein Ticket heute mit der Geldkarte bezahlen kann und sogar günstiger bekommt, ist fast schon ein alter Hut. Immer mehr Beförderungsunternehmen gehen einen Schritt weiter: Sie speichern die Fahrkarte direkt auf den Chip – das ist praktisch und verringert auch noch den Fahrkarten-Müll.

4 Altersnachweis: Ohne Chipkarte geht an deutschen Zigarettenautomaten nichts mehr. Der Chip sagt der Maschine, dass der Besitzer mindestens 16 Jahre alt ist. Diese Funktion ist aber noch weitergehend einsetzbar – etwa bei jugendschutzrelevanten Seiten im Internet oder jugendgefährdenden Computerspielen.

zu 200 Euro passen auf den Chip. Die Karte kann entweder an Geldautomaten oder auch über Kartenleseterminals am eigenen Computer per Online-Banking aufgeladen werden. Viele Banken bieten ihre Geldkarten mit Chips an, die gleichzeitig zum hackersicheren Online-Banking per HBCI nutzbar sind.

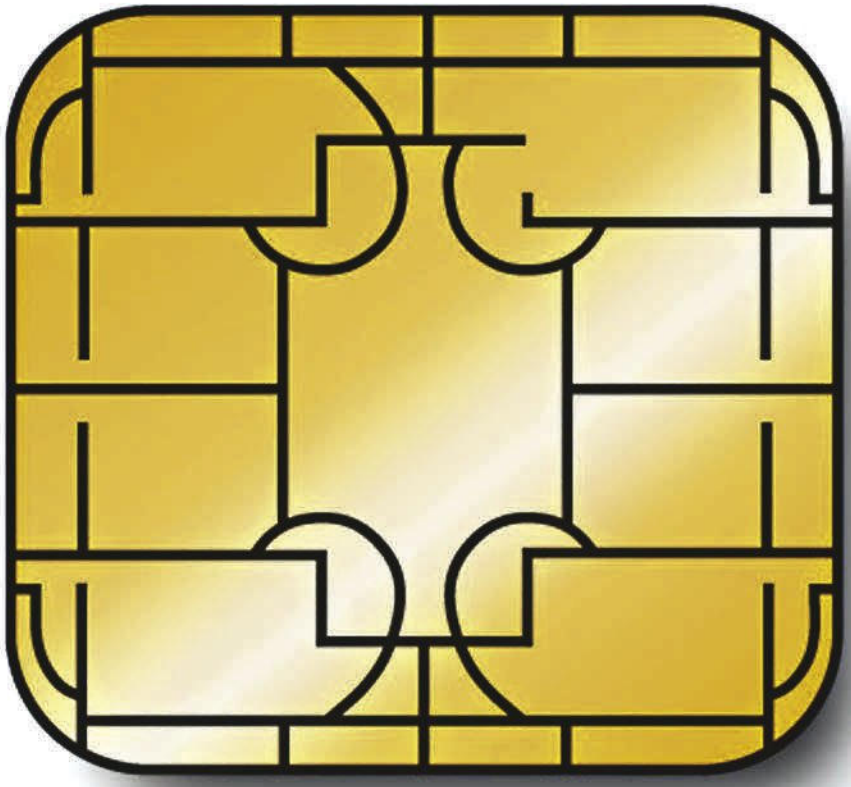
Doch wer schon ein Leseterminal an seinem Computer und eine reine Geldkarte hat, genießt weitere Vorteile, die über das bloße Bezahlen hinausgehen. So funktioniert der Alters-Check auch im Internet – auf inzwischen rund 140 000 Web-Seiten. Nur wer mit seiner Chipkarte nachweisen kann, dass er über 18 ist, wird auf diese Seiten gelassen.

Der nächste positive Effekt: Die meisten dieser Seiten – und viele andere auch – bieten eine Bezahlfunktion per Geldkarte, anonym und ohne dass Sie Ihre Kreditkartennummer eingeben müssen. Übrigens funktioniert das auch umgekehrt: Wenn Sie beispielsweise an einem Online-Gewinnspiel teilgenommen haben, können Sie sich den Gewinn gleich auf Ihre Karte buchen lassen.

In der Offline-Welt ist es ähnlich: So lassen sich gleich im Geschäft auch Bonuspunkte auf dem Chip speichern, die gesammelt und später eingetauscht werden können. Doch all das ist erst der Anfang. Wie es mit der Chipkarte weitergeht, lesen Sie auf der nächsten Seite. Mehr Infos im Internet: www.geldkarte.de

Chipkarte

Gold ist die Zukunft



Das Herzstück einer jeden Geldkarte ist der goldene Chip – er dient auch für die digitale Signatur

Wie unterschreibt man im Internet? Ganz einfach: mit seiner elektronischen Signatur vom goldenen Chip der Bankkarte. Dieses Legitimationsverfahren ist Teil des HBCI/FinTS-Standards und wird die Art revolutionieren, wie wir Geschäfte und Behördengänge erledigen – die Zukunft ist Gold. Die technologische Revolution läuft bereits: Zum Beispiel führen die Volks- und Raiffeisenbanken gerade eine neue Generation von Chipkarten und damit verbundenen Dienstleistungen weiträumig ein. Und die Sparkassen-Finanzgruppe hat eine solche schon fast flächendeckend eingeführt.

Die VR-BankCard des IT-Kompetenzcenters für Volks- und Raiffeisenbanken GAD ist von Haus aus HBCI-fähig und bereits für die elektronische Signatur vorbereitet. Schon ab Anfang 2008 soll es durch diese Karten auch möglich sein, mit Hilfe der elektronischen Unterschrift Bankgeschäfte online zu erledigen – also alles von der Überweisung bis hin zum Aktienkauf.

Doch der eigentliche Nutzen der Chipkarte fängt dort erst an. „Den Bankkunden eröffnet die elektronische Signatur einen echten Mehrwert – auch über das Bankgeschäft hinaus“, sagt Anno Lederer, Vorstandsmitglied der GAD, die, mit Sitz in Münster, als IT-Dienstleister, Rechenzentrum und Software-Haus rund 470 Banken betreut. „Beispielsweise könnte die VR-BankCard im Online-Bereich für rechtsverbindliche Verträge oder im Rahmen der virtuellen Behörde für die Kfz-Ummeldung oder die Meldung eines Wohnungswechsels eingesetzt werden. Stichworte sind hier das E-Government oder Bürgerportale.“

Verträge, Anträge und Aufträge sicher und ohne Angst vor Hackern abzuschließen, Behördengänge online zu erledigen, sichere und vertrauenswürdige E-Mails zu ver-

schicken – das ist der Sinn der elektronischen Signatur. Genauso ambitioniert wie die Pläne der Volks- und Raiffeisenbanken ist das Projekt der Sparkasseninformatik für die Online-Banking-Portale von Sparkassen in Baden-Württemberg, Hessen, Rheinland, Rheinland-Pfalz, Westfalen-Lippe und Bayern. Erstmalig implementiert die Sparkasseninformatik dabei eine Lösung, die, unter Nutzung von signaturgesetzkonformen Zertifikaten, auch Anwendungen außerhalb der Bank unterstützt. So werden diese bisher allein auf das Online-Banking ausgerichteten Sicherheitstechnologien offen für andere Anwendungen.

S-TRUST heißt das Trustcenter der Sparkassen-Finanzgruppe, das auf Basis der elektronischen Signatur Verschlüsselungstechniken anbietet, an denen sich Hacker die Zähne ausbeißen. Ein echtes Zukunftsmodell mit Potenzial: Rund 45 Millionen SparkassenCards gibt es derzeit, alle könnten theoretisch einmal als Träger der elektronischen Signatur dienen. Aktuell befinden sich bereits 24 Millionen, bei denen es sofort möglich wäre, beim Kunden. Alles, was diese nach Einführung der entsprechenden Schnittstelle auf den Web-Seiten der Bank noch brauchen, ist ein Kartenleser. Karten können per Software-Download für das Signaturverfahren aufgerüstet werden.

Die bequeme Anwendung und die Sicherheitsfunktionen von HBCI mit Chipkarte beim Banking, elektronischer Signatur bei Online-Geschäften und Geldkarte im Alltag überzeugen immer mehr Bankkunden. Das zeigen schon allein die steigenden Zahlen der Transaktionen mit der Geldkarte (s. rechts unten) – der goldene Chip hat definitiv eine große Zukunft.

Karten-Tankstelle: Auch hier können Kunden ihre Geldkarte aufladen

Mehr nützliche Links zum Thema im Internet unter:

www.hbci-finder.de
www.geldkarte.de
www.smartbasar.de
www.bsi-fuer-buerger.de
www.hbci-zka.de
www.homebanking-hilfe.de

Zunehmende Akzeptanz

Immer mehr Menschen werden sich des kleinen, goldenen Chips auf ihrer EC- oder Kundenkarte bewusst. Das zeigen die Zahlen einer aktuellen Allensbach-Umfrage, die die Initiative Geldkarte e.V. in Auftrag gegeben hat. Rund jeder dritte Chipkarteninhaber, der über die Geldkartenfunktion seiner Karte informiert ist, setzt sie als elektronischen Kleingeld-Ersatz ein. Damit ist die Nutzung der Geldkarte im Vergleich zu 2006 um die Hälfte von rund 20 auf 30 Prozent gestiegen. Rund 15,1 Millionen Menschen nutzen bereits die Geldkarte. Für Experten ist das ein deutliches Zeichen, dass die Akzeptanz des Chips generell zunimmt und die Kunden sich zunehmend auch für weitere Chip-basierte Anwendungen interessieren.

Elektronische Gesundheitskarte

Rezept und Krankenakte auf dem Chip

Das Rezept auf Papier hat bald ebenso ausgedient wie Krankenschein und Krankenakte. Alles wird auf einem Chip gespeichert. Momentan befindet sich die Gesundheitskarte noch in der Erprobung. Dass sie kommen wird, ist für Gesundheitsministerin Ulla Schmidt (SPD) gesichert. „Die elektronische Gesundheitskarte ist ein wichtiges Instrument zur Verbesserung der Lebens- und Versorgungsqualität der Patientinnen und Patienten“, sagt sie. Anders als die bisherige Versichertenkarte wird die neue Gesundheitskarte wichtige Daten über den Patienten enthalten – bis hin zur kompletten Krankenakte.

Das Rezept gehört bald der Vergangenheit an, es wird durch eine Chipkarte ersetzt

Praktisch bei einem Arztwechsel oder einem Unfall. Notfallärzte können so ganz schnell überprüfen, ob der Patient etwa eine Allergie gegen ein Medikament hat. Der Patient hat noch einen weiteren Vorteil: Mit demselben Chipkartenleser, den er fürs Online-Banking verwendet, kann er auch sein auf der Gesundheitskarte gespeichertes Rezept bei der Internet-Apotheke einlösen. Auch der Internet-Zugriff auf die persönlichen Daten der Patientenakte wird möglich. Mehr Infos: www.die-gesundheitskarte.de.

Beruhigend sicher.

HBCI-Banking per Chipkarte ist der bequemste und schnellste Weg, Ihr Geld und Ihre Daten sicher zu schützen. Die Schlüssel liegen dabei auf der Chipkarte, hochsicher aufbewahrt, außerhalb des angreifbaren PCs. Wie am Geldautomaten wird die PIN am sicherheitszertifizierten Chipkartenleser von REINER SCT eingegeben, und die Banktransaktionen werden verschlüsselt an Ihr Kreditinstitut weitergeleitet.

So entsteht eine extrem sichere Kommunikation auch bei extrem unsicheren Netzen. Das bestätigen übrigens auch unabhängige Experten. Fragen Sie Ihre Bank oder Sparkasse am besten sofort nach HBCI. Für sicheres Online-Banking und mehr. HBCI mit Chipkarte – Beruhigend sicher.

Weitere Infos: **www.reiner-sct.com**

REINERSCT

Smart Card Technology is our business