REINERSCT

WHITEPAPER

Sicher im Internet

mit Chipkartenlesegeräten

Stand: 17.01.2020

Chipkartenlesegeräte erhöhen die Sicherheit bei Internet-Aktivitäten. Keine andere Schutzmaßnahme erreicht dieses Niveau.

Einleitung

Kaum eine Erfindung in der Geschichte hat sich so schnell verbreitet wie das Internet. Täglich nehmen die Nutzerzahlen zu und neue Anwendungen schießen aus dem Boden.Viele Dinge des täglichen Lebens – vom Einkauf über Behördengänge und Bankgeschäfte bis hin zur Pflege von Freundschaften – werden online bequem von zuhause und zunehmend auch mobil von unterwegs erledigt. Die neuen Technologien sparen Zeit und Wege, bieten eine ungeahnte Informationsvielfalt und Zugriff darauf zu jeder Zeit und von beinahe jedem Ort der Welt.

Doch die neue digitale Welt ist nicht nur für gutgläubige User attraktiv, sondern auch für Kriminelle. Es mehren sich Betrug und Missbrauch im Netz. Mit einer gestohlenen digitalen Identität kann man im fremden Namen und auf fremde Rechnung online einkaufen oder Gegenstände ersteigern. Wirtschaftliche Schäden erleiden längst nicht nur große Unternehmen, sondern zunehmend auch Privatpersonen, die allzu freigiebig mit ihren persönlichen Daten im Internet umgehen.

Deshalb sollten der Schutz der persönlichen Daten und ein verantwortungsvoller Umgang mit Internet-Technologien und elektronischen Medien höchste Priorität haben. Chipkartenlesegeräte erhöhen die Sicherheit bei Internet-Aktivitäten. Keine andere Schutzmaßnahme erreicht dieses Niveau. In diesem Whitepaper finden sich Anregungen, wozu Chipkartenleser eingesetzt werden können und warum sich ein Kauf der sichersten Kategorie rentiert.

Faktenlage

Über 28 Millionen Deutsche erledigen ihre Bankgeschäfte online. Damit nutzt beinahe jeder zweite Bundesbürger (45%) im Alter von 16 bis 74 Jahren Online-Banking.

Aktuell sind 51 Millionen Bundesbürger regelmäßig online. Das entspricht 72 Prozent aller Deutschen ab 14 Jahren. Für den Zugang zum Internet werden nicht nur PCs zuhause genutzt, sondern zunehmend auch mobile Geräte: 24 Prozent der User verwenden Laptops, Tablet-PCs oder so genannte PDAs („Personal Digital Assistant"; handliche Computer vor allem für Adress-, Kalender- und Aufgabenverwaltung) und 18 Prozent nutzen Mobiltelefone und Smartphones (Mobiltelefon mit Computerfunktionalität), um online zu gehen. Jedes dritte verkaufte Handy ist heute ein Smartphone. Im Jahr 2012 werden voraussichtlich 23 Millionen dieser Multimedia-Geräte in Deutschland verkauft (Plus 43% gegenüber Vorjahr). Sie sorgen auch für einen Boom bei der mobilen Internetnutzung. Der Umsatz mit mobilen Datendiensten lag im Jahr 2012 bei über 7 Milliarden Euro.

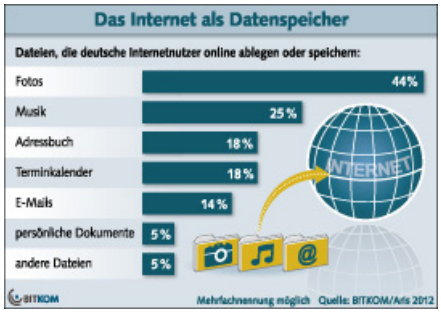
Online-Banking etabliert, Online-Shopping boomt

Über 28 Millionen Deutsche erledigen ihre Bankgeschäfte online. Damit nutzt beinahe jeder zweite Bundesbürger (45%) im Alter von 16 bis 74 Jahren Online-Banking.

85 Prozent der Internetnutzer haben bereits im Internet Waren und Dienstleistungen gekauft. Jeder dritte Deutsche hat im Jahr 2012 Software aus dem Internet heruntergeladen. Über 30 Millionen Deutsche haben schon einmal Waren oder Dienstleistungen bei einer Auktion im Internet ersteigert. Das entspricht über 50% Prozent aller deutschen Internet-Nutzer ab 14 Jahren.

Soziale Netzwerke sind begehrt

Fast drei Viertel (74 Prozent) aller Internetnutzer in Deutschland sind in einem sozialen Netzwerk – am häufigsten bei Facebook (45%) und Stayfriends (17%) – angemeldet, zwei Drittel nutzen sie auch aktiv. Knapp die Hälfte (47%) aller Unternehmen in Deutschland setzt soziale Medien ein. Fast ein Drittel (32%) aller Unternehmen ist bereits mit eigenen Seiten auf Facebook aktiv.



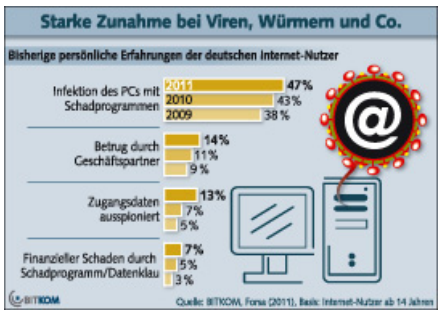
Cloud Computing auch bei Privatleuten beliebt

Vier von fünf Internetnutzern nutzen das Internet, um Inhalte dort zu speichern oder zu veröffentlichen (so genanntes Cloud Computing). 44 Prozent der Internetnutzer speichern Fotos im Netz. Jeder Vierte (25%) legt Musik online ab, jeder sechste (18%) speichert oder pflegt sein Adressbuch im Web.

Schlechte Erfahrungen im Netz

Drei Viertel aller deutschen Internetnutzer fühlen sich im Web bedroht, beispielsweise durch Viren, Betrug oder Datenmissbrauch. Tatsächlich schlechte Erfahrungen hat bislang jeder Zweite gemacht. Laut Polizeilicher Kriminalstatistik 2010 wurde in 250.000 Fällen das Internet zur Tatbegehung genutzt (+20% gegenüber Vorjahr). Der registrierte Schaden aller Cybercrime-Delikte (Straftaten mit Informations- und Kommunikationstechnik) ist auf rund 61,5 Millionen Euro gestiegen. Besonders stark zugenommen hat das so genannte Phishing im Zusammenhang mit Online-Banking. 2010 wurden dem BKA rund 5.300 Fälle gemeldet (+82% gegenüber Vorjahr). Die durchschnittliche Schadenssumme betrug rund 4.000 Euro pro Fall. Bei rund 36 Prozent der Nutzer wurde der Rechner von Viren befallen. Insbesondere die Ausspähung von Online-Zugangsdaten, etwa für Plattformen oder Internet-Shops, steigt an.

Bei rund 36 Prozent der Nutzer wurde der Rechner von Viren befallen. Jeder achte User (6,5 Millionen) ist beim Online-Shopping oder bei Auktionen von seinem Geschäftspartner betrogen worden. Jeder Zehnte (5 Millionen) gab an, dass in seinem Namen unerwünschte Mails verschickt wurden. Insbesondere die Ausspähung von Online-Zugangsdaten, etwa für Plattformen oder Internet-Shops, steigt an. 7 Prozent der Nutzer klagten, dass Unbekannte sich mit ihren Zugangsdaten in einem Internet-Shop oder Auktionshaus eingeloggt hatten. 6 Prozent der Nutzer von Sozialen Netzwerken und Online-Foren sind ebenfalls betroffen.



Zu wenig ausreichender Schutz

Nur 75 Prozent aller Internet-Nutzer verwenden ein Virenschutzprogramm und 70 Prozent eine Firewall. Jeder Fünfte surft völlig ohne Virenschutz oder Firewall. Nur jedes vierte kleine oder mittlere Unternehmen schult und informiert regelmäßig seine Mitarbeiter, nur jedes dritte hat ein IT-Sicherheitskonzept, das von der Geschäftsleitung getragen wird. 37 Prozent sichern ihre geschäftlichen Daten nicht täglich, 7 Prozent nie.

Der Digitale Mensch

Und plötzlich ist das Konto abgeräumt, die Alben mit den Babyfotos der Kinder gelöscht, alle Termine verschwunden, Unternehmen schicken Rechnungen für Warenkäufe, die man nie getätigt hat.

Der moderne Mensch besitzt diverse kostenlose E-Mail-Adressen, führt sein Bankkonto via Internet, kauft Theaterkarten, Reisen und Wein online, ersteigert Waren im Netz, ist Mitglied verschiedener sozialer Netzwerke, speichert seine Bilder, Dokumente und Adressbücher in einem Online-Speicher, erledigt Behördengänge im Web, kommuniziert über einen Kurznachrichtendienst und besitzt nicht selten eine eigene Homepage. Auf die entsprechenden Accounts greift er vom heimischen PC, vom Rechner im Büro und immer öfter auch mobil mit dem Smartphone zu. Benutzerkennungen und Passwörter häufen sich an – und um nicht durcheinanderzukommen, vergibt er der Einfachheit halber immer die gleichen Zugangsdaten. Kreditkartennummern und Bankverbindungen werden im Profil gespeichert, um sie nicht jedes Mal neu eingeben zu müssen.

Und plötzlich ist das Konto abgeräumt, die Alben mit den Babyfotos der Kinder gelöscht, alle Termine verschwunden. Noch schlimmer: vom eigenen Twitter-Account werden rassistische Äußerungen gepostet, Freunde und Geschäftspartner erhalten im eigenen Namen Spam und beleidigende Mails und Unternehmen schicken Rechnungen für Warenkäufe, die man nie getätigt hat.

Was klingt wie ein Horrorszenario, wird leider immer alltäglicher. Immer öfter berichten die Medien über solche Hackerangriffe mit Identitätsdiebstählen. Und immer öfter sind nicht Unternehmen, sondern Privatpersonen die Opfer. Jeder zweite Internetnutzer hat nach BITKOM-Angaben bereits schlechte Erfahrungen im Web gemacht. Mit anderen Worte: Wer bislang noch nicht betroffen war, hat einfach nur Glück gehabt.

Oft wiegt der finanzielle Verlust schwer und der Aufwand, seine Unschuld zu beweisen, ist enorm. Darüber hinaus sind die Daten und Dokumente nicht selten unwiederbringlich verloren – denn wer legt schon regelmäßig Sicherungskopien an und speichert sie gewissenhaft?

Deswegen lohnt es sich, das eigene Internet-Nutzungsverhalten zu überprüfen und Maßnahmen einzuleiten, um die Online-Sicherheit zu erhöhen.

Chipkartenlesegeräte

Mit Chipkartenlesegeräten können Chipkarten, wie z.B. der neue Personalausweis oder Bankkarten, angesteuert und gelesen werden. Chipkarten sind entweder kontaktbehaftet oder kontaktlos, sie müssen also entweder in ein Lesegerät eingesteckt werden oder nur darauf gelegt oder in die Nähe gehalten werden. Entsprechend unterschiedlich sind die Leser aufgebaut und ausgestattet. Sie sind in einer Vielzahl an Varianten, Größen und Formen erhältlich.

Chipkartenleser gibt es für die unterschiedlichen Anwendungsfälle im Privatbereich in vier verschiedenen Sicherheitsklassen:

Sicherheitsklasse 1:

Geräte dieser Klasse haben keine besonderen Sicherheitsmerkmale. Sie verbinden lediglich die Chipkarte mit dem Computer. Muss eine PIN eingegeben werden, muss der Nutzer dafür die Tastatur seines Computers benutzen.

Sicherheitsklasse 2:

Diese Leser sind mit einer eigenen Tastatur (auch PINpad genannt) ausgestattet, auf der die persönliche Geheimzahl (PIN) – ohne Umweg über den Computer – direkt am Gerät eingegeben werden kann. Das erhöht die Sicherheit und verhindert, dass die PIN von eventuell unbemerkt auf dem Computer befindlichen Schadprogrammen ausgespäht werden kann. Es ist aber nicht auszuschließen, dass Hacker die eingegebenen Daten vor Abschluss des Vorgangs manipulieren können.

Sicherheitsklasse 3:

Diese Geräte verfügen neben einer eigenen Tastatur auch über ein Display (Anzeige). Auf diesem werden z.B. bei einer Banküberweisung der zu zahlende Betrag und der Zahlungsempfänger angezeigt. Bei Secoder®-Lesern kann z.B. auch die Empfänger-Kontonummer angezeigt werden. Dadurch kann der Nutzer vor dem Absenden erkennen, wenn unbemerkte Schadprogramme den Empfänger, den Betrag oder die Kontonummer manipuliert haben sollten, und den Überweisungsprozess abbrechen. Leser dieser Klasse empfehlen sich für Online-Banking und andere Online-Transaktionen, z.B. mit dem neuen Personalausweis sowie elektronische Signaturen.

Sicherheitsklasse 4:

Falls sich ein Leser der Sicherheitsklasse 3 gegenüber der Anwendung eindeutig und nicht manipulierbar ausweisen kann, so handelt es sich um einen Leser der Sicherheitsklasse 4. Ein solcher Leser hat einen sicheren Schlüsselspeicher, i.d.R. eine zusätzliche smartCard (im SIM-Format) eingebaut. Um mit dem elektronischen Personalausweis eine qualifiziert elektronische Signatur zu erstellen, erfordert es zwingend einen Leser dieser Sicherheitsklasse.

Die Unterschiede auf einen Blick:

	Chipkartenleser Klasse 1	Chipkartenleser Klasse 2	Chipkartenleser Klasse 3	Chipkartenleser Klasse 4
Eignung für:	Altersnachweis, E-Ticketing	Altersnachweis, E-Ticketing, Homebanking, Signatur	Altersnachweis, E-Ticketing, Homebanking, Signatur, Sicheres Bezahlen	Altersnachweis, E-Ticketing, Homebanking, Signatur, Sicheres Bezahlen
Eigene Tastatur für sichere Dateneingabe	-	✓	✓	✓
Eigenes, sicheres Display	-	-	✓	✓

Anwendungsszenarien

a) Online-Banking

Millionen Menschen in Deutschland wickeln ihre Bankgeschäfte über das Internet ab. Die Kreditinstitute bieten dafür unterschiedlichste Verfahren an. Doch Vorsicht – nicht alle sind wirklich sicher.

TAN

Bei diesem Verfahren erhält der Kunde vom Kreditinstitut eine Liste mit TANs, die er der Reihe nach und jeweils nur einmalig nutzen kann. Diese Methode gilt heute als nicht mehr sicher.

iTAN

Hier erhält der Kunde von seinem Kreditinstitut eine Liste mit nummerierten TANs. Während einer Online-Transaktion wird der Kunde aufgefordert, eine nach dem Zufallsprinzip ermittelte TAN aus der Liste einzugeben. Nach Abschluss der Transaktion wird dem Kunden sowohl die Nummer als auch die dazugehörende TAN angezeigt. Auch diese Methode gilt heute als nicht mehr sicher.

mTAN

mTAN steht für „mobile TAN“ und wird oft auch „SMS-TAN“ genannt. Diese TAN wird erst während einer Online-Transaktion generiert und von der Bank per SMS auf das Handy des Kunden gesendet. Dieser gibt die mTAN ein und schließt die Online-Transaktion ab. Seit 2010 wird auch dieses Verfahren als unsicher eingestuft.

chipTAN

Für die Verwendung der chipTAN (Name bei der Volksbank: smartTAN) erwirbt der Kunde einen TAN-Generator. Der Kunde steckt seine ec-Karte in das Gerät, das Kreditinstitut blendet ein blinkendes Feld auf der Internetseite ein, der TAN-Generator wird direkt am Computer-Bildschirm exakt davor gehalten und automatisch wird eine TAN erzeugt. Diese so erzeugte TAN ist nur einmalig gültig.

HBCI mit Chipkartenlesegerät

Für das HBCI-Verfahren („Homebanking Computer Interface“) erwirbt der Kunde ein Kartenlesegerät (mindestens Sicherheitsklasse 2). Vom Kreditinstitut erhält er eine Chipkarte, auf der ein spezieller Online-Banking-Schlüssel gespeichert ist. Jede Banktransaktion wird von der Karte mit einer digitalen Unterschrift versehen. Bei jeder Online-Transaktion gibt der Kunde seine PIN direkt auf der Tastatur des Lesegerätes ein – somit können mögliche Schadprogramme, die sich unbemerkt in den Computer eingeschlichen haben, die PIN nicht ausspähen. HBCI nach Secoder-Standard gilt derzeit als das sicherste Verfahren. Erfolgreiche Angriffe auf diese Konfiguration sind bislang unbekannt.

> ***Und plötzlich ist das Konto abgeräumt, die Alben mit den Babyfotos der Kinder gelöscht, alle Termine verschwunden, Unternehmen schicken Rechnungen für Warenkäufe, die man nie getätigt hat.***

b) Online-Shopping

Anders als bei herkömmlichen Einkäufen im „realen" Laden, können bei Online-Geschäften via Computer weder der Kunde noch der Online-Shop wirklich sicher sein, dass der jeweils Andere tatsächlich der ist, für den er sich ausgibt. In der Folge kämpfen Online-Shops oft mit gefälschten Identitäten ihrer Kunden und unbezahlten Rechnungen und manche Käufer erhalten trotz pünktlicher Zahlung nicht die gewünschte Ware.

Wer seine Geschäftsbeziehungen im Internet absichern will, kann dafür den neuen Personalausweis einsetzen. Der neue Ausweis wird seit Ende 2010 ausgegeben und besitzt die so genannte Online-Ausweisfunktion. Mit ihr können Kunden im Internet ihre Identität nachweisen. Das passende Gegenstück für Online-Shops ist der eID-Service, mit dem der neue Personalausweis in das Webangebot eingebunden werden kann. Beide Seiten können sich damit gegenseitig ausweisen und somit sicher sein, mit wem sie tatsächlich Geschäfte machen.

Der Käufer benötigt dafür neben dem neuen Ausweis mit freigeschalteter Online-Ausweisfunktion sowie kostenloser Ausweis-App auch ein Chipkartenlesegerät. Experten empfehlen den Kauf eines Lesers mit Sicherheitsklasse 3. Idealerweise sollte der Leser vom Bundesamt in der Informationstechnik (BSI) zertifiziert sein. Selbstverständlich bei Online-Geschäften ist natürlich auch ein abgesicherter Computer mit aktueller Antiviren-Software und Firewall.

Neben sicheren Einkäufen im Netz bietet die Kombination aus neuem Personalausweis und Lesegerät auch weitere Möglichkeiten. Versicherungen bieten an, dass der Versicherte seine Daten nicht mehr manuell in Formulare eintragen muss, sondern dass die notwendigen Daten aus dem Ausweis übernommen werden können – das spart beiden Seiten Zeit und senkt die Fehlerquote durch falsche Eingaben.

Unternehmen ermöglichen das Log-in in geschlossene Benutzergruppen mit dem neuen Ausweis – und zwar auch dann, wenn man z.B. in Blogs oder sozialen Medien anonym bleiben will.

Online-Shopper können ihren neuen Ausweis auch nutzen, wenn sie beim Kauf von Waren mit Altersbeschränkung ihr Alter nachweisen wollen. Aus Gründen der Datensparsamkeit wird hierbei übrigens nicht das komplette Geburtsdatum übersandt, sondern nur bestätigt, dass der Käufer ein bestimmtes Alter erreicht hat.

In Kürze wird es auch möglich sein, mit Hilfe der Qualifizierten Elektronischen Signatur auch Vorgänge, die eine persönliche und rechtsverbindliche Unterschrift voraussetzen, sicher und medienbruchfrei elektronisch zu erledigen.

c) Behördengänge im Internet

Nicht nur privatwirtschaftliche Unternehmen haben den Wert von Online-Aktivitäten erkannt, auch Behörden bieten ihre Dienstleistungen zunehmend online an. Heiratsurkunden, Kindergeld oder Wunschkennzeichen beantragen, Stadtbüchereidienste nutzen, Meldebescheinigungen ausfüllen, Wohnortbestätigungen anfordern oder Elektroschrott anmelden – Bürger müssen sich für solche und ähnliche Vorgänge nicht mehr selbst ins Rathaus begeben, sondern können sie online erledigen.

Ob beispielsweise:

- die Bundesagentur für Arbeit (Registrierung/Online-Mitteilung über Kindergeld),
- die Deutsche Rentenversicherung (Identifizierung und Registrierung zum persönlichen Rentenkonto),
- das Kraftfahrt-Bundesamt („Punkteauskunft"),
- der Landkreis Ostallgäu (Online-Beantragung von Verwaltungsleistungen)
- oder die Stadt Aachen (Abwicklung von Verwaltungsleistungen ohne Registrierung)

immer mehr Behörden erkennen, wie effizient sich mit attraktiven eGovernment-Angeboten arbeiten lässt.

Um solche Angebote nutzen zu können, verlangen die Behörden in der Regel eine Authentifizierung mittels neuem Personalausweis. Dafür ist neben dem neuen Ausweis mit freigeschalteter Online-Ausweisfunktion auch ein Chipkartenlesegerät nötig. Auch für Online-Behördengänge empfehlen Experten den Kauf eines Lesers mit Sicherheitsklasse 3, der idealerweise vom Bundesamt in der Informationstechnik (BSI) zertifiziert ist. Selbstverständlich bei eGovernment-Aktivitäten ist natürlich auch ein abgesicherter Computer mit aktueller Antiviren-Software und Firewall.

Über REINER SCT

Mit unseren Whitepapern informieren wir regelmäßig über virulente Themen im Bereich der Online-Sicherheit, Zeiterfassung oder anderen aktuellen Trends und geben wertvolle Experten-Tipps, die für Unternehmen und Privatleute einfach umzusetzen sind.

Unsere Whitepaper finden Sie hier: **reiner-sct.com/whitepaper**

REINER SCT entwickelt, fertigt und vertreibt seit 1997 Lesegeräte für Chipkarten. Das Unternehmen ist spezialisiert auf hochwertige Homebanking-Sicherheitslösungen für Banken und deren Kunden sowie auf intuitiv anwendbare Zeiterfassungs- und Zutrittskontrollsysteme für kleine und mittelständische Unternehmen. REINER SCT entwickelt und produziert in Deutschland und bietet bis hin zum Vertrieb und Endkundenservice sämtliche Leistungen aus einer Hand.

Mit den neuen Chipkartenlesegeräten für den elektronischen Personalausweis ist REINER SCT Wegbereiter für den innovativen IT-Einsatz im öffentlichen Bereich. Das Unternehmen ist weltweit tätig und gehört zur REINER-Gruppe, die sich seit 1913 in Familienbesitz befindet. Es hat seinen Sitz in Furtwangen im Schwarzwald und beschäftigt 45 Mitarbeiter.

Weitere Informationen unter: **reiner-sct.com**

Impressum / Kontakt

REINER SCT
Reiner Kartengeräte GmbH & Co. KG
Baumannstr. 18
78120 Furtwangen
Tel.: +49 (7723) 5056-0
info@reiner-sct.com
reiner-sct.com