REINERSCT

Whitepaper

Mobilität & Sicherheit

Stand: 09.07.2013

Inhaltsverzeichnis

1. Einleitung 3
2. Fakten 4
3. Gefahren 6
4. Lösungen 7
5. Hilfreiche Links 9
6. RSCT-Whitepaper 10
7. Über Reiner SCT 10

Impressum/Kontakt 11

> Niemand ist Angriffen schutzlos ausgeliefert. Auch ohne tiefere IT-Kenntnisse kann sich jeder Nutzer, egal ob Privatanwender oder Unternehmen, vor Computerkriminalität wirksam schützen.

1. Einleitung

Noch nie war unsere Gesellschaft so mobil wie heute. Für viele Menschen ist es selbstverständlich, private Urlaubsreisen in exotische Länder zu machen oder geschäftliche Meetings auf anderen Kontinenten zu absolvieren. Junge Kreative haben keinen festen Arbeitsplatz mehr, sondern suchen sich in der Stadt, in der sie sich gerade aufhalten, Coworking-Spaces. Entsprechend ist auch der Anspruch gewachsen, ortsunabhängig aktuelle Nachrichten zu erhalten, E-Mails zu checken, Texte zu bearbeiten, den Kontostand abzufragen und Überweisungen zu tätigen oder mit Freunden und Geschäftspartnern über soziale Netzwerke zu kommunizieren.

Neue Technologien, die solche Möglichkeiten erschließen, sind bereits erfunden und etabliert. Ob Tablet-PC, Smartphone oder Cloud Computing – innovative Geräte und Anwendungen bieten Zugriff auf eine ungeahnte Informationsvielfalt zu jeder Zeit und von beinahe jedem Ort der Welt. 40 Prozent der Deutschen nutzen das Internet inzwischen mobil. Laut Technologieberater Accenture verwendeten im Jahr 2011 28 Prozent der Surfer dafür ein Smartphone. Mobile Geräte sind mit umfassenden Funktionen ausgestattet, die es erlauben, auch unterwegs Termine zu vereinbaren, Kontaktdaten auszutauschen und Verträge oder Umsatzzahlen zu erstellen oder weiterzuleiten. Zuhause genügt ein Knopfdruck und alle Daten sind mit dem stationären Rechner synchronisiert – praktisch!

Für die Hälfte aller Nutzer ist das mobile Internet „ein wichtiger Bestandteil des Alltags“. Doch diese Mobilität bringt auch Gefahren mit sich, wenn Geräte, Netze und Daten nicht gut gesichert sind. Die gute Nachricht: Niemand ist Angriffen schutzlos ausgeliefert. Auch ohne tiefere IT-Kenntnisse kann sich jeder Nutzer, egal ob Privatanwender oder Unternehmen, vor Computerkriminalität wirksam schützen.

Wie das funktioniert, wollen wir mit diesem Whitepaper aufzeigen. Es sensibilisiert für den sicheren Umgang mit den eigenen Daten in mobilen Szenarien und befasst sich mit der Frage, mit welcher Soft- und Hardware mobile User ihre Daten sichern können.

2. Fakten

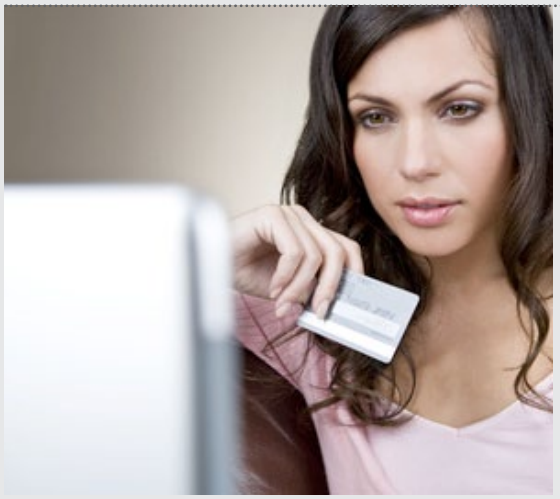
Der Trend zur mobilen Internetnutzung beschleunigt sich. Laut aktuellen Prognosen des ITK-Bundesverbandes BITKOM e.V. werden die Verkaufszahlen von Smartphones – also Mobiltelefonen mit Computerfunktionalität – in Deutschland von 22,9 Millionen Stück im Jahr 2012 auf 31,5 Millionen im Jahr 2015 steigen. Das entspricht einem Wachstum von 38 Prozent. Während derzeit 70 Prozent aller verkauften Mobiltelefone Smartphones sind, werden es in drei Jahren 90 Prozent sein.

Tablet-Nutzung steigt rasant

Der deutsche Markt für Tablet Computer – das sind tragbare Rechner, die über einen berührungsempfindlichen Bildschirm mit den Fingern gesteuert und via WLAN oder Mobilfunknetz drahtlos mit dem Internet verbunden werden – ist 2012 um fast 84 Prozent auf 2,1 Milliarden Euro gewachsen. Der Geräteverkauf hat sich im gleichen Zeitraum mehr als verdoppelt: Die verkauften Stückzahlen stiegen von 2,1 Millionen Geräten im Jahr 2011 auf rund 4,4 Millionen im Jahr 2012, ein Plus von 122 Prozent. 2013 soll der Absatz die 5-Millionen-Marke übertreffen.

Mehr als die Hälfte surft mobil

Laut der Studie „Mobile Internetnutzung“ der Initiative D21 nutzen mittlerweile über die Hälfte aller Internetsurfer Smartphones, Tablets & Co, um ihre Mails abzurufen, online einzukaufen oder um sich in sozialen Netzwerken mit anderen auszutauschen. Während im Vorjahr jeder dritte Surfer einen mobilen Netzzugang genutzt hat (35 Prozent), ist es in diesem Jahr bereits jeder Zweite (53 Prozent).



Mobiles Online-Banking

Entsprechend boomen auch die mobilen Anwendungen: So wollen laut D21-Studie „Online-Banking“ 47 Prozent der Smartphone-Besitzer ihr Gerät künftig für digitale Bankgeschäfte nutzen. Übertroffen wird diese Zahl noch von Tablet-Usern (65 Prozent). Laut Aussage von BITKOM nutzt fast jeder fünfte Besitzer (17 Prozent) eines Smartphones das Gerät zum Abfragen von Kontoständen, Überweisungen oder den Kauf von Wertpapieren. Das sind fast fünf Millionen Deutsche. Jeder siebte Besitzer eines Smartphones (15 Prozent) prüft mobil seinen Kontostand, acht Prozent überweisen auf diese Art Geld von ihrem Bankkonto.

Laut BITKOM würden viele Nutzer gerne zusätzlich zum Mobile Banking sämtliche Zahlungsgeschäfte digital vornehmen und ihren Geldbeutel durch eine „Mobile Wallet“ auf dem Smartphone ersetzen. Jeder Siebte (14 Prozent) kann sich vorstellen, auf sein Portemonnaie komplett zu verzichten und nur noch mit dem Smartphone zu bezahlen. Das sind knapp 10 Millionen Personen.

Apps boomen

Auch der Trend zu Apps hat sich im Jahr 2012 weiter verstärkt. Apps sind Programme, die speziell für Mobilgeräte wie Smartphones und Tablet Computer entwickelt werden. Im vergangenen Jahr wurden laut BITKOM in Deutschland mehr als 1,7 Milliarden Apps heruntergeladen. Das entspricht einer Steigerung von rund 80 Prozent im Vergleich zu 2011 – damals wurden knapp eine Milliarde Apps installiert. In Deutschland nutzen 83 Prozent der Smartphone-Besitzer Apps. Fast jeder Zweite (45 Prozent) lädt nur kostenfreie Programme herunter. Durchschnittlich hat jeder Smartphone-Besitzer 23 Apps für die verschiedensten Anwendungen installiert.

Allerdings können Apps schädliche Funktionen haben oder ein Einfallstor für Schadprogramme wie Viren sein. So können schädliche Apps unbemerkt SMS-Nachrichten an teure 900er-Nummern senden oder auf Kontaktdaten auf dem Smartphone zugreifen. Häufig verbergen sich in kostenlosen Apps Abo-Fallen, die den Nutzern beim Anklicken von Werbebannern untergeschoben werden.

3. Gefahren

Diese schöne digitale Welt birgt also auch Gefahren und Einfallstore für Kriminelle. Laut „Lagebild Cybercrime 2011 des BKA“ nimmt vor allem der Diebstahl digitaler Identitäten zu. Bei der digitalen Identität handelt es sich um alle Arten von Nutzer-Accounts, also zum Beispiel um Zugangsdaten zu E-Mail-Postfächern oder Konten für Online-Banking und Online-Shopping. Wer sich beispielsweise mit Benutzername und Passwort via ungesichertem Smartphone in sein Bankkonto, das Social Network oder seinen Online-Versteigerungs-Account einloggt, macht es Betrügern leicht, die Daten auszuspähen und ungehindert zu missbrauchen. Die Schäden in solchen Fällen sind gewaltig.

Smartphones für Betrüger lukrativ

Mobile Endgeräte wie Smartphones waren 2011 ein zunehmend lukratives Ziel für die Täter. Vermehrt wurden Smartphones mit Schadsoftware infiziert, um beispielsweise an die Daten möglicher SMS-basierter Authentifizierungsverfahren, wie sie z.B. beim Online-Banking verwendet werden, zu gelangen. Laut der Polizeilichen Kriminalstatistik 2012 beläuft sich die Zahl der erfassten Fälle von Cyberkriminalität im engeren Sinne– dazu zählen beispielsweise Computerbetrug, Betrug mit Zugangsberechtigungen und das Ausspähen oder Verändern von Daten – auf den Rekordwert von 63.959 Fällen (+7,5% gegenüber Vorjahr). Die Computersabotage ist um 134 Prozent angestiegen. Der verursachte Schaden aller Cybercrime-Delikte liegt bei mindestens 80 Millionen Euro.

Jeder Zweite bereits Opfer

Eine Umfrage des BITKOM im Jahr 2012 ergab, dass 52 Prozent der privaten Internetnutzer bereits persönliche Erfahrungen mit Internetkriminalität gemacht haben. Das entspricht 28 Millionen Menschen. Bei 36 Prozent oder 20 Millionen Nutzern sind Computer mit Viren oder anderen Schadprogrammen infiziert gewesen. 16 Prozent oder 8,5 Millionen Internetnutzer geben an, dass ihre Zugangsdaten zu verschiedenen Diensten ausspioniert wurden. Jeder achte (12 Prozent) Internetnutzer ist bereits Opfer eines Betrugs im Zusammenhang mit Online-Shopping geworden. Es folgt mit 10 Prozent betroffenen Internetusern der unfreiwillige Versand von Spam-Mails vom eigenen E-Mail-Account.

Angst bremst

Die Angst vor Cybercrime und die negativen Erfahrungen jedes Einzelnen haben Auswirkungen auf das Verhalten vieler Menschen. Sieben von zehn Internetnutzern schränken laut Bitkom bewusst Kommunikation oder Transaktionen im Internet ein. 42 Prozent versenden vertrauliche Informationen oder Dokumente nicht per E-Mail, ein Viertel verzichtet auf Online-Banking und ein Fünftel ganz oder teilweise auf Online-Shopping. Jeder zehnte Nutzer nimmt grundsätzlich keine Transaktionen im Internet vor.

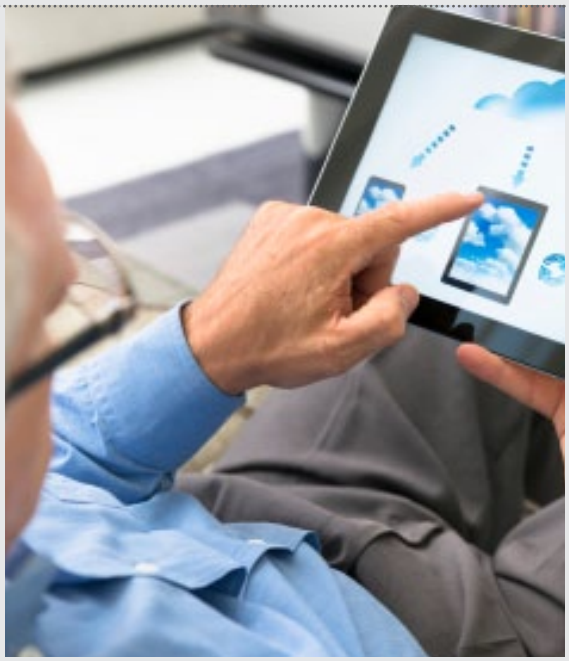
> Die Angst vor Cybercrime und die negativen Erfahrungen jedes Einzelnen haben Auswirkungen auf das Verhalten vieler Menschen.

4. Lösungen

Die Angst vor Cybercrime und das damit verbundene eingeschränkte Nutzerverhalten muss alarmieren. Denn Digitalisierung und Vernetzung sind – vor allem für Unternehmen und mobile Arbeiter – wichtige Treiber für Innovation und Wachstum, von denen die Gesellschaft weitreichend profitiert. Dieser Fortschritt wird durch Cyberkriminalität gebremst.

Es stellt sich also die Frage, wie Cyberkriminalität wirksam bekämpft werden kann. Grundsätzlich gilt: Niemand ist Angriffen schutzlos ausgeliefert. Auch ohne tiefere IT-Kenntnisse kann sich jeder Nutzer, egal ob Privatanwender oder Unternehmen, vor Computerkriminalität wirksam schützen. Nachfolgend erläutern wir moderne Szenarien.

a) Cloud Computing



Immer mehr private Anwender und Unternehmen nutzen die Vorteile des Cloud Computing. Die Nutzer legen ihre Daten nicht mehr auf dem eigenen Rechner ab, sondern nutzen virtuellen Speicherplatz von Dienstleistern in der „Wolke". Von jedem Ort der Welt mit Internetverbindung können sie dann auf ihre Daten zugreifen – vollkommen geräteunabhängig. Die weit verbreiteten Internetanwendungen wie E-Mail, soziale Netzwerke oder Videodienste laufen bereits fast ausschließlich in der Cloud.

Nach Erhebungen des ITK-Bundesverbandes BITKOM ist Cloud Computing eines der zentralen Trendthemen unserer Zeit und entwickelt sich rasant: Der Markt für Cloud Computing wird in Deutschland von 5,3 Milliarden Euro im Jahr 2012 auf 17,1 Milliarden Euro im Jahr 2016 wachsen.

Doch auch bei diesem Thema hat die Medaille zwei Seiten. Denn beim Cloud Computing werden die Daten in der Regel nur beim Übertragen vom Rechner in die Wolke verschlüsselt – in der Cloud selbst liegen sie meistens ungeschützt. Auch der Zugang zu den Daten ist zumeist nur mit einem einfachen Passwort abgesichert. Wer es kennt oder knackt, hat freie Bahn für Missbrauch. Das kann für Cloud-Nutzer teuer werden.

Wie wichtig der Schutz der Cloud-Daten ist, haben die führenden deutschen Computer-Zeitschriften kürzlich bestätigt. Die Magazine „PCgo", „Business & IT", „PC Magazin" und „PC Praxis" empfehlen den Einsatz von Cloud-Verschlüsselungstools, wie z.B. „cloudCockpit" aus dem Hause REINER SCT (www.reiner-sct.com/cloudcockpit).

b) Mobile Online-Transaktionen

Manchmal können wichtige Dinge einfach nicht warten. Da müssen und wollen Banküberweisungen, Online-Versteigerungen oder Vertragsabschlüsse sofort erledigt werden – auch wenn wir uns gerade auf Bahnreisen, mehrtägigen Geschäftsaufenthalten oder Privatreisen im Ausland befinden.

Doch wer Transaktionen mit mobilen Geräten vornimmt, muss in ganz besonderem Maße auf die Sicherheit achten. Hier wird vielfach das Risiko unterschätzt. Während die meisten Nutzer ihre stationären PCs zuhause oder im Büro mit Virenschutzsoftware ausgerüstet haben, nutzen sie ihre Smartphones und Tablets oftmals ungeschützt. Dabei bieten die gängigen Hersteller von Anti-Virus-Programmen sogar kostenlose Versionen für Mobilgeräte an. Dennoch muss jedem bewusst sein, dass die Virenschutzsoftware erst dann reagieren kann, wenn ein Problem bekannt wurde. Sie kann also nur eine zusätzliche Möglichkeit sein.

Experten sind einhellig der Meinung, dass die aktuell höchste Sicherheit erreicht wird, wenn User bei ihren Transaktionen eine zweite Hardware einsetzen. Egal ob man seine Banküberweisung mit dem PC, Tablet oder Smartphone erledigen will, die TAN sollte niemals über das gleiche Gerät eingegeben werden. Denn dann können die Daten abgefangen und manipuliert werden. Auch wer moderne Verfahren zur Erzeugung von Transaktionsnummern nutzt – also z.B. SMS-TAN, photoTAN via Smartphone oder TAN-Generator oder chipTAN via Scheckkarte und Leser – sollte aufpassen. Auch hier gilt: Sicher sind diese Methoden nur dann, wenn die TAN in ein vollkommen unabhängig arbeitendes, separates Lesegerät eingegeben wird. So sind die Übertragungswege von TAN und Überweisungsauftrag getrennt und der Vorgang kann nicht manipuliert werden. Einer der führenden Hersteller sicherer Lesegeräte ist die Schwarzwälder Firma REINER SCT.

Inzwischen gibt es ultraflache Chipkartenlesegeräte für die Hemdtasche, auf denen Kontoführungs-Programme für Windows und Mac OS X abgelegt werden können. So ist auch unterwegs sicheres Online-Banking möglich. Die mobilen Leser, die sogar kabellos via Bluetooth funktionieren, eignen sich auch für das Online-Bezahlen mit der Geldkarte oder sichere Authentifizierungen.

4. Hilfreiche Links

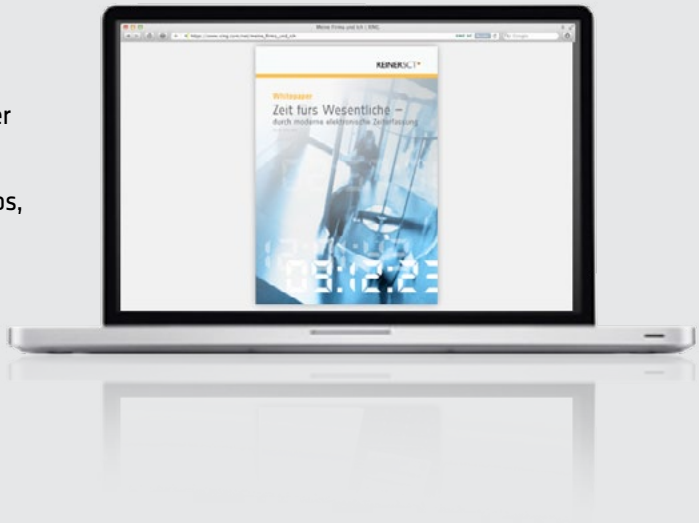
Weblinks zum Thema Mobilität & Sicherheit:

- Merkblatt D21 und Bayerisches Staatsministerium der Justiz und für Verbraucherschutz:
  „Gut zu wissen! Gefahren des mobilen Internets“
  http://www.initiatived21.de/wp-content/uploads/2013/04/GefahrendesmobilenInternets_web.pdf
- D21-Studie „Mobile Internetnutzung“
  http://www.initiatived21.de/wp-content/uploads/2013/02/studie_mobilesinternet_d21_huawei_2013.pdf
- D21-Studie „Online-Banking“
  http://www.initiatived21.de/wp-content/uploads/2013/01/studie_onlinebanking_fiducia_2013.pdf
- Institut für Internet-Sicherheit der Westfälischen Hochschule:
  „Tipps Basissicherheit für mobile Geräte“:
  http://www.internet-sicherheit.de/service/tipps-zur-sicherheit/basissicherheit-mobile-geraete
- Deutschland sicher im Netz:
  www.dsin.de
- BITKOM – Bundesverband Informationstechnologien, Telekommunikation und neue Medien e.V.:
  www.bitkom.org
- BSI – Bundesamt für Sicherheit in der Informationstechnik:
  www.bsi.de
- REINER SCT:
  www.reiner-sct.de

5. REINER SCT Whitepaper

Mit unseren Whitepapern informieren wir künftig 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:
www.reiner-sct.de/whitepaper



6. Über REINER SCT

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.

REINER SCT
Reiner Kartengeräte GmbH & Co. KG
Goethestr. 14
78120 Furtwangen
Tel.: +49 (7723) 5056-0
Fax: +49 (7723) 5056-778
info@reiner-sct.com
www.reiner-sct.com