

## Thema: Weihnachten / Crimeware Shopping

Zeichen Artikel: 8.131 (mit Leerzeichen)

Zeichen Tipps: 903 (mit Leerzeichen)

### Die (Waren)sendung mit der Maus

#### Gefahren beim Einkaufen im Internet

Einkaufen mit Tastatur und Maus liegt im Trend. Unter den 16 bis 24-Jährigen nutzt schon jeder zweite die bequeme Shopping-Alternative zu Schmuddelwetter und langen Schlangen vor den Kassen. Aber wie sicher sind Transaktionen über das Internet? Gibt es einen Schutzschild für die Kreditkarte?

Zumindest Online ist die Welt für den Einzelhandel noch in Ordnung. Trotz Finanzkrise und Konsumstreik nutzen immer mehr Menschen ihren PC zu Hause, um einzukaufen. Ob Bücher, Musik, Mode oder Haushaltsgeräte, es gibt mittlerweile nichts mehr, was sich nicht auch online bestellen und an die Haustür liefern lässt. Nach einer Statistik des Branchenverbands BITKOM shoppen schon 41 Prozent der Deutschen über das Internet, Tendenz steigend. „Online-Shopping bietet viele Vorteile“, kommentierte BITKOM-Präsident Prof. Dr. August-Wilhelm Scheer die Zahlen. „Es ist preistransparent und bequem, ein Umtausch in aller Regel problemlos“.

Den Aspekt der Bequemlichkeit schätzen auch viele Büroangestellte. In einer Studie der IT-Organisation ISACA vom Oktober 2009 fanden 34 Prozent das Online-Shopping so bequem, dass sie ihre Weihnachtseinkäufe gleich im Büro erledigen wollen. Im Schnitt planen die Angestellten dafür über 14 Stunden ein, das dürften die Arbeitgeber nicht so gern sehen.

Doch der schnelle Einkauf per Mausclick sorgt auch aus anderen Gründen immer wieder für negative Schlagzeilen. Anders als bei einem Laden vor Ort muss sich der Käufer auf die Angaben verlassen, die er auf den Webseiten des Anbieters findet. Die können korrekt sein, eine Garantie gibt es nicht. Die erste Sicherheitsmaßnahme sollte daher der gesunde Menschenverstand sein. Extrem niedrige Preise für teure Markenartikel klingen nicht nur zu gut um wahr zu sein, sie sind es in der Regel auch nicht. Darum sehen Sie sich am besten zunächst gründlich beim Anbieter um. Ist das Impressum vollständig, mit Geschäftsführer, Adresse und Steuernummer? Sind die allgemeinen Geschäftsbedingungen an prominenter Stelle hinterlegt? Wenn Sie sich unschlüssig sind, bringt oft die Suche nach dem Anbieternamen bei einem Bewertungsforum wie Ciao.de Klarheit darüber, ob es sich um eine empfehlenswerte Firma handelt.

## Angriffe aus dem Hinterhalt

Doch auch wenn der Händler über jeden Zweifel erhaben ist, können andere Gefahren im Hintergrund lauern. Kriminelle nutzen das Internet verstärkt für ihre Aktivitäten. Es geht um viel Geld, allein in den USA haben Computernutzer über einen Zeitraum von zwei Jahren Schäden von knapp 8,5 Milliarden Dollar erlitten. Die Angreifer verwenden immer raffiniertere Programme, die weitgehend automatisch arbeiten und auf unterschiedliche Weise vorgehen. Der bekannteste Weg ist das Verschicken von Schadsoftware per E-Mail. Wird der Computer nicht von einem aktuellen Anti-Virus Programm geschützt, installiert sich das Programm mit einem Klick im Hintergrund und späht beispielsweise Passwörter, Kreditkartendaten und TAN-Nummern aus. Solche Programme werden als Trojanische Pferde oder kurz Trojaner bezeichnet, weil sie hinter einer vorgeblich harmlosen Fassade eine verdeckte Aufgabe ausführen. Hat sich solch ein Trojaner erst einmal eingemischt, bekommen Sie ihn nur mit Mühe wieder los. Die meisten Schadprogramme beherrschen zahlreiche Tricks um sich vor der Entdeckung zu schützen. Dazu kommt, dass Sie nichts von Ihrem ungebetenen Gast merken. Im Gegenteil, der Trojaner vermeidet alles, was auf ihn aufmerksam machen würde. Einige dieser Programme wehren sogar Angriffe von anderen Schadprogrammen ab.

Oft wird ein Trojaner dafür genutzt, um den Computer auf andere Webseiten umzulenken. Sie glauben, die vertraute Webseite des Online-Banking Anbieters auf dem Bildschirm zu sehen, sind aber in Wirklichkeit auf der gefälschten Seite des Online-Gauners gelandet. Diese „Phishing-Angriffe“ sind mittlerweile so ausgefeilt, dass sie selbst von erfahrenen Computernutzern nicht mehr erkannt werden. Gibt man auf der falschen Bankseite seine Login-Daten ein, erscheint eine Fehlermeldung mit der Bitte um Geduld aufgrund eines technischen Problems. Doch Benutzername und Passwort wurden längst zum Angreifer gesendet, der sie für die spätere Nutzung ablegt. Natürlich sind auch die Zugangsdaten zu Online-Shopping Angeboten begehrte Beutestücke. Besonders an Weihnachten werden elektronische Grußkarten für diesen Zweck missbraucht. Angebliche Weihnachtskarten von Schulfreunden, Nachbarn, Kollegen - den Phishern ist kein Vorwand zu banal, um die Empfänger dazu zu bringen, auf den Link in der Mail zu klicken oder die angehängte Datei auszuführen.

## Schutz per Wachhund

Der Schutz vor solchen und ähnlichen Attacken ist Sache einer Sicherheitssoftware. Diese Programme haben in den letzten Jahren einen enormen Wandel mitgemacht. Früher genügte es, den Computer vor Viren zu schützen. Dazu verglich die Sicherheitssoftware fremde Programme mit einer Liste, wurde eine Übereinstimmung gefunden, schlug die Software Alarm. Heute beherrschen die meisten Schadprogramme zahlreiche Tricks um sich zu tarnen

und zu verstecken, die Schutzprogramme mussten sich diesen Änderungen anpassen. Die Liste mit böartigen Programmen zum Vergleich gibt es immer noch, aber mittlerweile finden die digitalen Wächter die Schädlinge bereits dann, wenn sie sich verdächtig verhalten. „Behaviour Monitoring“ – Verhaltensüberwachung nennen die Hersteller diese Fähigkeit. Die Sicherheitsprogramme überwachen auch den Web-Browser und erkennen zuverlässig, wenn Sie auf eine Phishing-Seite umgeleitet werden soll.

Bei anderen Gefahren ist Ihre aktive Mitarbeit gefragt. So stellt der Bezahlvorgang einen neuralgischen Punkt im Online-Einkauf dar. Bei vielen schleicht sich ein mulmiges Gefühl ein, wenn es an die digitale Kasse geht. Bezahlt wird im Internet in der Regel per Kreditkarte oder über eine Lastschrift. Kontodaten oder Kartenummer preiszugeben stellt immer ein gewisses Risiko dar. Darum sollte der Shop-Betreiber auf jeden Fall eine verschlüsselte Verbindung für die Transaktion anbieten. Oft weisen die Anbieter an der virtuellen Kasse darauf hin, man kann die Verschlüsselung aber auch an einem kleinen Schloss-Symbol oder der geänderten Farbe der Adressleiste des Web-Browsers erkennen. Diese Verschlüsselung ist sehr sicher und kann mit vertretbarem Aufwand nicht geknackt werden. Hier droht Ihnen tatsächlich keine Gefahr.

### **Einmal Name und Adresse, bitte**

Brenzlig kann es werden, wenn es der Anbieter mit dem Datenschutz nicht so genau nimmt. Wie die Datenschutzskandale der letzten Monate zeigten, sind persönliche Daten eine heiße Währung, für die unter der Hand viel Geld gezahlt wird. Viele Webseiten, vor allem von ausländischen Anbietern, fragen seitenweise Informationen ab, bevor Sie auch nur ein Produkt zu sehen bekommen. Die Frage nach persönlichen Daten obwohl Sie nichts kaufen wollen, ist generell suspekt. Prüfen Sie auch gründlich, ob Ihnen die Webseite nicht irgendwo im Kleingedruckten oder außerhalb des sichtbaren Bereichs eine Einzugsermächtigung oder einen Kaufvertrag unterjubeln will. Noch einen Schritt weiter geht eine der goldenen Regeln des BITKOM. Die Experten raten dazu, jeden Schritt des Einkaufes mit einem Bildschirmfoto zu dokumentieren oder den Seiteninhalt auszudrucken. Das ist zwar eine reichlich extreme Maßnahme, sorgt aber dafür, dass Sie im Fall eines späteren Streits Beweismittel haben.

Und natürlich gilt auch für Online-Geschäfte das Fernabsatzgesetz. Sie das Recht die Ware ohne Angabe von Gründen innerhalb von 14 Tagen zurück zu senden, Sie treten damit rechtlich vom Kauf zurück, der Verkäufer muss den vollen Kaufpreis erstatten. Ob Sie dazu bestimmte Rahmenbedingungen einhalten müssen, zum Beispiel eine unbeschädigte Originalverpackung, sollte klar und deutlich auf der Webseite zu lesen sein. Fehlen solche Hinweise oder sind sie nur schwer zu finden, ist das schon ein Minuspunkt für die Seriosität

des Anbieters. Übrigens: auch die Polizei gibt auf ihrer Webseite „Online kaufen mit Verstand“ wertvolle Tipps für den sicheren Einkaufsbummel vor dem Bildschirm: <https://www.kaufenmitverstand.de/home/home.php>

### Tipps für sichere Einkäufe im Internet

Wenn Sie online shoppen, dann lieber mit dem Desktop-PC als mit dem iPhone oder einem anderen mobilen Gerät. Der Schutzfaktor ist auf dem stationären Computer meist höher.

Schützen Sie Ihre persönlichen Informationen wie Kreditkartennummern. Speichern Sie solche Daten nie unverschlüsselt auf dem PC und sichern Sie Ihr Handy durch ein Passwort, wenn darauf sensible Informationen liegen.

Statten Sie Ihre Computer und Smartphones mit Schutzsoftware aus. Dazu gehört auch das schicke Netbook und der Schul-PC des Jüngsten.

Nutzen Sie die Updatefunktion von Anti-Virus Software und Betriebssystem. Nur so werden Schwachstellen so schnell wie möglich geflickt.

Gehen Sie - auch im Web 2.0 - sparsam mit persönlichen Daten um. Solche Informationen erleichtern Social Engineering Angriffe enorm.

Wenn etwas zu gut klingt, um wahr zu sein, ist es das vermutlich auch nicht.

Der Artikel und Zitate daraus dürfen unter Nennung des Unternehmens Kaspersky Lab sowie des Autors frei veröffentlicht werden.

**Kaspersky Lab** reagiert im weltweiten Vergleich von Antivirus-Herstellern meist am schnellsten auf IT-Sicherheitsbedrohungen wie Viren, Spyware, Crimeware, Hacker, Phishing-Attacken und Spam. Die Produkte des global agierenden Unternehmens mit Hauptsitz in Moskau haben sich sowohl bei Endkunden als auch bei KMUs, Großunternehmen und im mobilen Umfeld durch ihre erstklassigen Erkennungsraten und minimalen Reaktionszeiten einen Namen gemacht. Neben den Stand-Alone-Lösungen des Security-Experten ist Kaspersky-Technologie Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsunternehmen. Mit den Kaspersky Hosted Security Services bietet das Unternehmen darüber hinaus Dienstleistungen im Bereich Malware- und Spam-Schutz sowie Content-Kontrolle für Unternehmen jeder Größe an. Weitere Details zum Unternehmen sind unter [www.kaspersky.de](http://www.kaspersky.de) zu finden. Aktuelles zu Viren, Spyware und Spam sowie Informationen zu anderen IT-Sicherheitsproblemen und Trends sind unter [www.viruslist.de](http://www.viruslist.de) abrufbar.

**Redaktionskontakt:**

essential media GmbH  
Florian Schafroth  
Florian.Schafroth@essentialmedia.de  
Tel.: +49-89-7472-62-43  
Fax: +49-89-7472-62-843  
Landwehrstraße 60-62  
80336 München

Kaspersky Labs GmbH  
Christian Wirsig  
christian.wirsig@kaspersky.de  
Tel.: +49-841-98-189-325  
Fax: +49-841-98-189-100  
Steinheilstraße 13  
85053 Ingolstadt

© 2009 Kaspersky Lab. The information contained herein is subject to change without notice. The only warranties for Kaspersky Lab products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Kaspersky Lab shall not be liable for technical or editorial errors or omissions contained herein.