COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/online-straftaten-bleiben-gefaehrlich,1936347

Verisign Betrugsbarometer

Online-Straftaten bleiben gefährlich

Datum: 08.06.2010
Autor(en): Thomas Pelkmann

Die Zahl der gemeldeten Fälle von Online-Betrügereien ist in den vergangenen Monaten stabil geblieben. Leichte Zuwächse gab es bei der durchschnittlichen Schadenshöhe.

Jeder sechste deutsche Internet-Nutzer ist innerhalb der vergangenen zwölf Monate Opfer eines Online-Betrugs geworden. Das stellt das **VeriSign**[1] Betrugs-Barometer fest, für das zweimal jährlich Internet-Nutzer in Deutschland befragt werden. Die Zahl von Fällen sei damit gegenüber den Vorjahren stabil geblieben, heißt es in der Untersuchung.

Leicht angewachsen ist dagegen die durchschnittliche Schadenssumme, die sich von 179 auf 183 Euro pro Opfer erhöht hat. Das entspricht einem Anstieg von allerdings gerade einmal zwei Prozent. Der Schaden hält sich auch deshalb in Grenzen, weil immerhin jedes fünfte Opfer (21 Prozent) den gestohlenen Beitrag vollständig erstattet bekam. Im Jahr zuvor konnten sich nur 17 Prozent über eine Erstattung freuen. Ein Drittel der Befragten, 37 Prozent, rechnet dagegen nicht damit, ihr Geld überhaupt zurückbekommen zu können.

"Der höhere finanzielle Schaden", heißt es bei Verisign, "hängt damit zusammen, dass Käufer in Deutschland unvorsichtiger werden, wenn sie **vertrauliche Informationen im Internet**[2] übermitteln". Zwar geben 77 Prozent der Befragten an, dass sie bei Transaktionen oder der Weitergabe persönlicher Informationen Websites mit erhöhter Sicherheit verwenden. Mehr als drei Viertel achten also auf sichere **Authentifizierung**[3] und erkennbare Prüfmerkmale wie zum Beispiel **Sicherheitssiegel**[4].

Allerdings ist hier der Trend leicht rückläufig (minus vier Prozent). Das weise darauf hin, so Verisign, dass Internetnutzer mit ihren Daten online immer unvorsichtiger umgehen.

Das Mittelalter achtet am meisten auf Sicherheit

Das größte Sicherheitsbewusstsein haben der Umfrage zufolge Internet-Nutzer aus der Altersgruppe der 35- bis 44-jährigen; 85 Prozent prüfen die Sicherheitsangaben einer Website, bevor sie diese nutzen. Dazu passt auch, dass die Internetnutzer dieser Altersgruppe in den letzten zwölf Monaten am wenigsten anfällig für Online-Identitätsdiebstahl waren. In dieser Altersklasse lag die Zahl der Betrugsopfer bei nur elf Prozent.

Grundsätzlich gilt, dass Nutzer, die bei **Transaktionen**[5] mit sensiblen Daten nur Websites mit erhöhter Sicherheit verwenden, seltener finanziell geschädigt werden.

"Das aktuelle VeriSign-Betrugsbarometer zeigt eine klare Beziehung zwischen dem Wissen über Online-Sicherheit und den finanziellen Verlusten durch Online-Identitätsbetrug", kommentiert Joachim Gebauer von VeriSign das Ergebnis der Umfrage. Er ruft Verbraucher dazu auf, ihre Einstellungen zur Privatsphäre zu überprüfen und auf Sicherheitszertifikate und Prüfsymbole zu achten.

Unternehmen könnten sich im Feld der Anbieter profilieren, indem sie die Sicherheit ihrer **Websites**[6] erhöhten. So zeigten sie den Verbrauchern, dass sie für ihre Sicherheit sorgen.

5 Tipps für Ihren Schutz

Zum Schutz vor bedenklichen Webseiten empfiehlt Verisign die folgenden fünf Maßnahmen.

1) Schützen Sie Ihren Computer. Installieren Sie auf Ihrem Computer eine Firewall und eine Anti-Virus-Software. Unterbrechen Sie die Verbindung zum Internet, wenn Sie sie nicht benötigen. Richten Sie auf Ihrem Notebook ein Passwort ein, um Ihre persönlichen Daten vor fremdem Zugriff zu schützen.

2) Wählen Sie ein sicheres Passwort. Ändern Sie Ihr Passwort regelmäßig und **wählen Sie dafür eine Zeichenkombination**[7], die nicht leicht zu erraten ist. Geben Sie Ihr Passwort nicht an Dritte weiter.

3) Überprüfen Sie, ob die Website sicher ist. Bevor Sie vertrauliche Daten eingeben, sollten Sie überprüfen, ob die URL mit https beginnt. Das "s" im Namen der Webseite steht für "Sicher". Meiden Sie eine Seite, wenn deutlich erkennbare Fehler in der Schreibweise zu finden sind und keine Sicherheitsinformationen angezeigt werden. Verwenden Sie stets die neuesten Browser-Versionen, die bei verschlüsselten und geprüften Verbindungen eine grün hinterlegte **EV-SSL-Adressleiste**[8] anzeigen.

4) Laden Sie keine E-Mail-Anhänge herunter oder klicken Sie auf einen Link in einer E-Mail, deren Absender Sie nicht kennen oder dem Sie nicht vertrauen. **Stellen Sie keine persönlichen Daten in einer E-Mail zur Verfügung.**[9] Banken fragen in einer E-Mail nie nach Passwort, Benutzername, PIN oder anderen sensiblen Daten. Nur Betrüger wenden solche Tricks an.

5) Verwenden Sie ein sicheres Wi-Fi Netzwerk. Benutzen Sie ein Passwort, um Ihr Heim-Netzwerk zu sichern. Vermeiden Sie Internetkäufe oder Banktransaktionen in öffentlichen Netzwerken.

Links im Artikel:

1 **http://www.verisign.de/**
2 **http://de.wikipedia.org/wiki/Phishing**
3 **http://de.wikipedia.org/wiki/Secure_Sockets_Layer**
4 **https://www.ssl247.de/ssl-certificates/validation/extended**
5 **https://www.tecchannel.de/sicherheit/identity_access/401380/bezahlen_im_internet/index8.html**
6 **https://www.computerwoche.de/schwerpunkt/w/Website.html**
7 **https://www.cio.de/knowledgecenter/security/2221380/index2.html**
8 **http://www.verisign.de/static/EV_DataSheet_DE.pdf**
9 **https://www.cio.de/knowledgecenter/security/2221598/**
