

03.07.2014 - 10:58 Uhr

Last Minute-Schnäppchen: So tappen Urlauber nicht in die Falle / Sommerferien lassen bei Cyber-Kriminellen die Kassen klingeln

Bochum (ots) -

- Querverweis: Bildmaterial wird über obs versandt und ist abrufbar unter <http://www.presseportal.de/galerie.htx?type=obs> -

Der digitale Reisemarkt wächst von Jahr zu Jahr. Mittlerweile buchen gut 34 Millionen Bundesbürger ihren Urlaub im Internet (Quelle: BITKOM). Besonders in der Zeit vor den Sommerferien sind viele Schnäppchen-Jäger unterwegs, die auf der Suche nach dem Last Minute-Traumurlaub zum kleinen Preis sind. Das wissen auch Online-Betrüger und versuchen jedes Jahr aufs Neue, aus diesem Trend Kapital zu schlagen. Die Experten der G DATA SecurityLabs rechnen daher in den kommenden Wochen mit dem Aufkommen von Spam-Mails, die es auf urlaubsreife Internetnutzer abgesehen haben. Vorsicht da-her vor angeblichen Buchungsbestätigungen oder unseriösen Last-Minute-Angeboten, die ungewollt ins Postfach flattern. Viele der Mails sind mit einem infizierten Dateianhang versehen oder beinhalten Links zu dubiosen Webseiten, die in die Schadcode-Falle führen. G DATA Sicherheitsexperte Ralf Benzmüller kennt die aktuellen Maschen und erklärt, worauf Anwender generell achten sollten und wie sie sich schützen können.

Cyber-Kriminelle machen keine Ferien - so die Erkenntnis der G DATA Sicherheitsexperten aus den vergangenen Jahren. Doch worauf haben es die Täter abgesehen? Besonders begehrt sind Bank- und Kreditkartendaten. Diese werden in speziellen Untergrundforen zu Geld gemacht oder umgehend für weitere Straftaten missbraucht.

"Wer nicht Opfer von Onlinekriminellen werden möchte, sollte neben dem Einsatz einer Sicherheitssoftware sein gesamtes System immer auf dem aktuellsten Stand halten. Gerade letzterer Punkt wird gerne vernachlässigt und ermöglicht es Angreifern oftmals, den Rechner durch nicht geschlossene Sicherheitslücken in installierten Programmen zu infizieren", erklärt Ralf Benzmüller, Leiter der G DATA SecurityLabs. "Zusätzlich sollten Urlauber Online-Angebote und die Reputation des Anbieters im Netz genauestens überprüfen." Erhaltene Reise-Spam-Mails sollten generell gelöscht werden. Auf keinen Fall sollten Empfänger Dateianhänge öffnen oder Links anklicken. Auch von einer Beantwortung einer Spam-Mail rät der Experte dringend ab: "Hierdurch signalisieren Anwender den Kriminellen, dass die E-Mail-Adresse aktiv genutzt wird."

++ Vermeintlicher Reisegewinn

Bei vermeintlichen Gewinn-Mails sollten Empfänger stets misstrauisch sein. Unübersichtliche Formulare oder versteckte Zusatzkosten können aus dem Schnäppchen schnell eine Kostenfalle machen. Kürzlich stießen die G DATA SecurityLabs auf eine vermeintliche Gewinn-Benachrichtigung, die dem Empfänger eine Türkei-Reise verspricht. Für die Reise fallen laut der E-Mail nur die Gebühren für Buchung und Kerosin an. Wie hoch die wirklichen Gesamtkosten sind, wird jedoch verschwiegen. Bereits Anfang Juni 2014 verzeichnete G DATA eine erste Welle derartiger Spam-Mails, die Empfänger in die Kostenfalle locken sollen - weitere Informationen zu diesem Fall finden Sie im G DATA SicherheitsCenter: <http://ots.de/EROBE>

++ Tipps für die Reise-Buchung im Internet:

- Augen auf: Nutzer sollten Angebote genau prüfen und auch das Klein-gedruckte beachten. Etwaige Zusatzkosten sollten beachtet werden. Insbesondere bei Gratis- oder Billigangeboten sind gerne versteckte Kostenfallen vorhanden.
- Anbieter prüfen: Im Internet können Reiseveranstalter, Reisevermittler, Eigentümer von Unterkünften oder Fluggesellschaften Reisen anbieten. Internetnutzer sollten in jedem Fall prüfen, ob der Name, die Rechtsform des Unternehmens, der Name des Vertretungsberechtigten, die vollständige Adresse, Telefon- und Faxnummer, E-Mail-Adresse und Handelsregisternummer angegeben ist.
- Niemals direkt den gesamten Reisepreis bezahlen: Der Veranstalter kann frühestens vier Wochen vor Reiseantritt den kompletten Reisepreis verlangen. Dazu müssen der Sicherheitsschein und alle Reiseunterlagen ausgehändigt worden sein.
- Ab in den Papierkorb: Spam-Mails sollten sofort gelöscht werden. Dateianhänge oder Links bei Nachrichten von unbekanntem

Versendern sollten niemals angeklickt werden.

- Updates installieren: Das Betriebssystem und die verwendete Software sollten stets auf dem aktuellen Stand sein. So werden Sicherheitslücken geschlossen, die Kriminelle ausnutzen.
- Sicherheitslösung einsetzen: Der Einsatz einer umfassenden Sicherheitslösung ist empfehlenswert. Die Sicherheitssoftware sollte neben einem Virenschutz auch einen Echtzeitschutz beim Surfen und einen Spam-Filter beinhalten.

Kontakt:

Thorsten Urbanski
Public Relations Manager
Phone: +49 (0) 234 - 9762 239

Vera Schmidt
Pressereferentin
Phone: +49 (0) 234 - 9762 376

Christian Lueg
Pressereferent
Phone: +49 (0) 234 - 9762 160

E-Mail: presse@gdata.de

Königsallee 178b
44799 Bochum, Deutschland

Diese Meldung kann unter <https://www.presseportal.ch/de/pm/100011910/100758595> abgerufen werden.