STUDIE: WIE DATENDIEBE NACH IHREN DATEN FISCHEN

Veröffentlicht am 10. November 2014 von Rüdiger

Spektakuläre Datendiebstähle führen uns immer wieder vor Augen, wie wichtig die Datensicherheit ist. Das Phishing stellt dabei eine besonders hinterhältige Form des Internetbetrugs da. Eine scheinbar normale Webpräsenz oder E-Mail wird beim Phishing zur Falle. Denn hinter der Webseite oder Mail stehen Hacker, die Sie zur Herausgabe Ihrer Zugangsdaten auffordern. Viele gutgläubige Nutzer kommen dieser Aufforderung nach, wie jetzt eine aktuelle Google-Studie beweist.

Es ist kein Zufall, dass das Wort **Phishing** eine Abwandlung des englischen Wortes Fishing (deutsch: Fischen, Angeln) ist. Denn wie beim Angeln **locken die Datenfischer Ahnungslose mit einem Köder**. Das kann etwa eine **vermeintlich vertrauenswürdige E-Mail** sein, die im Design Ihrer Hausbank gestaltet ist. Die Datendiebe sind aber auch mit **gefälschten Webpräsenzen** erfolgreich, auf die teilweise **jeder zweite Besucher** hereinfällt.

Der Suchmaschinenkonzern **Google hat nun eine Studie veröffentlicht**, die zeigt, wie wirkungsvoll diese Phishing-Art ist: Durchschnittlich gibt **jeder siebte Besucher auf einer falschen Webpräsenz seine Zugangsdaten preis**. Diese Blauäugigkeit hat oft fatale Folgen: Falls die Hacker Ihr E-Mail-Konto gekapert haben, **verlieren Sie in der Regel die Kontrolle darüber.** Die Internetkriminellen sperren Sie aus Ihrem eigenen Konto aus und durchforsten dieses auf der Suche nach wertvollen Daten.

Risiko Identitätsdiebstahl

Wenn sich die Hacker Ihres E-Mail-Kontos bemächtigen, droht der **Identitätsdiebstahl**. Das heißt, dass sie von Ihrem Konto aus, **Mails an Ihre Kontakte verschicken**. Da die Kontakte Ihren Namen im Absender lesen, vertrauen sie diesen Mails und geben oft Ihrerseits Zugangsdaten heraus. So kommt es zum **Flächenbrand**.

Was Sie tun können:

- **Gesunde Skepsis**: Es ist sehr unwahrscheinlich, dass jemand in guter Absicht Ihre Zugangsdaten verlangt. Lassen Sie also Vorsicht walten, wenn Sie in einer E-Mail nach Ihren Login-Daten gefragt werden.
- **Nicht klicken**: Besonders riskant ist der Klick auf einen Link in einer dubiosen E-Mail. Wenn Sie sich nicht sicher sind, sollten Sie den Verweis in das Adressfeld Ihres Browsers kopieren.
- **Starke Passwörter benutzen**: Mit sich häufig ändernden sicheren Passwörtern für Ihre privaten Accounts machen Sie den Hackern das Leben schwer. Mit dem kostenlosen Passwort-Generator KeePass ist die Passwort-Erstellung kein Problem.

Online-Betrüger versuchen mit gefälschten Webpräsenzen und vielen anderen Tricks die **Naivität mancher Menschen auszunutzen**. Unsere **Media Company schützt Ihre Partnerunternehmen** beispielsweise mit starken Passwörtern. Mit einem **skeptischen Blick** auf Mails und Webpräsenzen **müssen aber auch Sie sich schützen**. Sprechen Sie uns an, wenn Sie Fragen zur Datensicherheit haben.