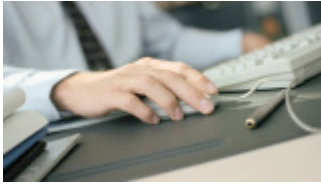


## Bankraub per Email



Trotz aller Bemühungen um größtmögliche Sicherheit – das Internet bietet einfallreichen Übeltätern immer neue Schlupflöcher für ihre kriminellen Machenschaften. Jüngstes Beispiel ist das so genannte „Pishing“. Beim „Pishing“, einer Wortneuschöpfung aus den englischen Begriffen „Password“ und „Fishing“, spähen Verfasser illegaler Emails sensible Kundendaten aus.

Internetsicherheitsunternehmen Messagelabs allein in den USA inzwischen über 250.000 Pishing-Emails pro Monat. Jetzt schwappt die Welle auch nach Deutschland: Vor einigen Tagen wurden Kunden der Postbank, der Deutschen Bank und des Internet-Marktplatzes Ebay Opfer von Pishing-Attacken.

Das Übel beginnt meist mit einer harmlosen Email, die scheinbar von einem Service- oder Sicherheits-Team des jeweiligen Unternehmens kommt. Darin wird beispielsweise behauptet, es seien kleine Fehler bei Abrechnungen oder harmlose Störungen bei der Datenverwaltung aufgetreten. Der Kunde wird daraufhin gebeten, seine Daten zu überprüfen. Über einen Link in der Email wird der Kunde auf eine Internetseite weiter geleitet, die exakt wie die Webseite des Unternehmens aussieht, in Wahrheit aber nur eine geschickt gemachte Kopie ist. Auf dieser gefälschten Seite, zu der ihn die gefälschte Email gelockt hat, wird der ahnungslose Kunde um Eingabe seines Passwortes, einer persönlichen Identifikationsnummer (PIN) oder einer Transaktionsnummer (TAN) gebeten, um sich zu identifizieren. Schon haben die Pishing-Versender Zugang zu persönlichen Informationen und können sie für Ihre Zwecke missbrauchen.

Von den gut getarnten Angriffen der Passwort-Diebe sind vor allem Banken, Kreditkarteninstitute, Finanzdienstleister oder Online-Auktionshäuser betroffen. Nach Schätzungen des amerikanischen Marktforschungsunternehmens „Gartner“ belaufen sich die Schäden, die Unternehmen und Privatpersonen im vergangenen Jahr durch Passwortraub entstanden sind, auf rund 1,2 Milliarden Dollar allein in den USA. Auch wenn in Deutschland bisher keine nennenswerten Schäden entstanden sind – Vorsicht ist geboten.

So setzen Unternehmen zunächst auf die Aufklärung ihrer Kunden: Postbank und Deutsche Bank informieren auf ihren Webseiten über die gefälschten Emails und geben Ratschläge zum Umgang damit. Doch auch technisch rüsten Banken und Online-Händler zum Schutz der Kunden auf. Ebay empfiehlt die Nutzung seiner neuen Toolbar, einem Zusatzprogramm, das vor der Eingabe persönlicher Daten auf nicht von Ebay verifizierten Internetseiten warnt. Banken dagegen verhandeln mit Entwicklern von Frühwarnsystemen und setzen auf so genannte digitale Signaturen, die die Identität des Nutzers zweifelsfrei klären.

Doch auch bis zum endgültigen Durchbruch dieser innovativen Sicherheitstechnik gilt es, sich zu schützen. Aber wie? Banken und Internethändler weisen ausdrücklich darauf hin, dass sie ihre Kunde niemals per Email nach vertraulichen Daten fragen würden. Landet also eine Email im Posteingang, die ebendies behauptet, sollten die Alarmglocken sofort klingeln. In Emails, die personenbezogene Daten abfragen wollen, sollte man mitgeschickte Links nie direkt anklicken. Diese könnten auf gefälschte Seiten führen oder auch Viren auf den eigenen PC einschleusen. Besser ist es, den Namen der Bank direkt im Browserfenster einzugeben, oder ihn aus der Favoritenliste auszuwählen. Handelt es sich tatsächlich um eine Email des seriösen Unternehmens, wird es seine Kunden über die Homepage zu aktuellen Problemen informieren. Ein gesundes Misstrauen ist also geboten, aber dann sind Pishing-Emails recht leicht von seriösen Kundeninformationen zu unterscheiden.