Online-Betrug und wie man sich dagegen schützen kann

Wo sich viele Menschen sammeln gibt es immer auch ein paar schwarze Schafe. Das gilt natürlich auch für das Internet. Allerdings kann hier jeder Betrüger leicht viele Millionen Menschen erreichen. Welches die häufigsten Betrügereien sind und wie man sich schützen kann ist Gegenstand dieser Surftipps-Ausgabe.

Social Engineering ist das Schlüsselwort für einige der raffiniertesten Betrugsmuster. Professionelle Callcenter stehen hinter den konstruierten Personen, die sich per E-Mail melden und um Hilfe bitten oder sich selbst für partnersuchend anbieten (spätere Heirat nicht ausgeschlossen). Immer wird der (und hier sind es tatsächlich nur Männer) Angesprochene mit weiteren Informationen und Fotos geködert. Natürlich sind immer mindestens Reisekosten vorauszuzahlen. Ist das geschehen, so wird das Flugzeug verpasst, die Mutter krank oder ein anderes Unglück verhindert die Abreise. Auch dieses ist durch eine Zahlung abzuwenden. Äußerst wendig und geschickt wird die Hoffnung aufrechterhalten und weitere Zahlungen gerechtfertigt.

Bereits seit den Siebzigerjahren und damals noch per Fax operiert die Nigeria Connection bzw. wird diese Methode angewendet. Zu Beginn meldet sich eine Person, die angeblich ein Vermögen eines Verstorbenen entdeckt hat oder verwaltet und nun Hilfe bei dessen „Nutzung" benötigt. Selbstverständlich gegen eine stattliche Provision von in der Regel mehreren Millionen. Auch hier werden sehr flexibel und einleuchtend Gründe angeführt, warum nur eine einzige Vorauszahlung zwischen dem Angesprochenen und der Millionenprovision steht. Ist diese erfolgt tun sich andere Hindernisse auf, die ebenfalls mit Zahlungen zu überwinden sind. Erschwerend wirkt hier, dass man, einmal begonnen, erpressbar wird, da es sich um die Beihilfe zu einer Straftat handelt.

Sicherheitstipp 1

Wie lukrativ auch immer ein Angebot wirken mag. Reagieren Sie nicht darauf. Falls der Impuls zu stark ist, recherchieren Sie nach Mustern des Angebots und informieren Sie sich zu aktuellen Betrugsfällen (siehe Links).

Noch immer eine der besten Übersichten bietet die TU Berlin mit ihrer Hoax-Seite http://hoax-info.tubit.tu-berlin.de/

Anfragen zu Daten, Kennworten und auch harmloseren Informationen können höchst plausibel wirken. Hier werden die Briefköpfe von Banken usw. kopiert, sprachlich nüchtern präsentiert und auf Ihre Reaktion spekuliert. Password Fishing oder Phishing ist die Bezeichnung für derartige Anfragen.

Sicherheitstipp 2

Anfragen die scheinbar von Ihrer Bank oder Kreditkartenfirma oder auch von Freunden kommen, sollten gegebenenfalls immer per Telefon (bei der Info-Nummer auf Ihrer tatsächlichen Abrechnung) geklärt werden, niemals per E-Mail.

Von gekaperten E-Mailkonten werden regelmäßig Notrufmails an alle Adressbuchkontakte also auch Freunde und Bekannte versendet. „Schickt mir Geld, ich bin auf Reisen und in Not, daher nur an Western Union schicken."

Sicherheitstipp 3

Zahlen Sie NIEMALS per Western Union, egal welche Begründung ihr Gegenüber dafür hat. Dort ist Ihr Geld nicht nachverfolgbar und damit meist verloren.

Sicherheitstipp 4

Verwenden Sie keine Passwörter, die genauso im Wörterbuch stehen (egal in welcher Sprache) sondern immer Kombinationen. Wörterbuchdateien auf der Suche nach Ihrem Mailpasswort durchlaufen zu lassen gehört zu den einfachsten Übungen für Internet-Gauner.

Ziel vieler SPAM-Mails ist, Sie zum Klicken auf Links, zum Downloaden und Installieren von vermeintlich nützlicher Software oder Dateien zu bekommen. Tatsächlich wird der Rechner dann zum Versand von SPAM ferngesteuert zu so genannten Bot-Netzen (vom englischen Robot) zusammengeschaltet, nicht selten mit hunderttausenden Rechnern anderer ahnungsloser Nutzer. Gänzlich unattraktiv für Bot-Netze sind Rechner, die regelmäßig ausgeschaltet werden bzw. nicht online erreichbar sind. Technische Details und sogar Biographien der bedeutendsten Spammer aus technischer Sicht gibt es bei www.spamhaus.org/rokso/index.lasso

Sicherheitstipp 5

Legen Sie sich eine Mehrfachsteckdose mit einem Netzschalter zu, um ihr DSL-Modem (zumindest) über Nacht auszuschalten oder schalten Sie gleich Ihren Rechner mit aus.

Ein hochkompetenter und inspirierender Vortrag zum Thema SPAM und Hintermänner von Peer Heinlein findet sich auf www.heinlein-support.de/web/heinlein/download-vortraege/

Ganz erstaunliche Betrugsfälle aus der Realität finden sich zusammengestellt hier http://computer.t-online.de/online-betrug-mann-ueberweist-200-000-us-dollar-an-internet-bekanntschaft/id_44656000/index

Einige der verwendeten Betrugsmuster werden in einem Beitrag von SPIEGEL-Online erläutert www.spiegel.de/netzwelt/web/0,1518,692888,00.html

Niemand weiß genau wieviel Viagra und andere Medikamente als Kopie und Fälschung verkauft werden. Allein vom veröffentlichten Umsatz Pfizers auszuschließen ist der Bedarf immens. Warnen Sie auch Ihre Patienten vor Pharmabetrug. Der Bundesverband der Verbraucherzentralen warnt vor Onlineversand und Betrug und bietet auch eine Positivliste von Versandapotheken
www.vzbv.de/go/presse/1205/4/17/index.html

Von ganz anderer Natur sind Kettenaussendungen nach dem Muster: eine bekannte Marke verschenke ein begehrtes Gerät, wenn man diese Mail an 10, 20 oder 50 eigene Mailkontakte weitersendet. Natürlich gibt es weder das Geschenk noch eine andere „Belohnung", sondern die erfolgreiche Verteilung einer meist infizierten Mail an möglichst viele Mail-Adressen. Hier werden auch arme Kinder, Kranke und bemitleidenswerte Geschöpfe jeder Art angeführt um eine Weiterleitung zu erreichen.

Sicherheitstipp 6

Leiten Sie keine E-Mails weiter, schon gar nicht an mehrere Adressen, die nicht von Ihnen persönlich bekannten Absendern stammen; und selbst dann nicht, da auch einer Ihrer Bekannten natürlich auf den Trick hereingefallen sein kann. Senden Sie in diesem Fall einen freundlichen Hinweis mit dem Link zu diesem Artikel oder dem HOAX-Info der TU Berlin (siehe Abbildung), um für Aufklärung zu sorgen.

Manche Newsletter dienen nur dazu neue Adressen zu generieren bzw. deren Gültigkeit zu bestätigen.

Sicherheitstipp 7

Klicken Sie niemals auf „unsubscribe", denn dadurch bestätigen Sie dem Spam-Versender, dass Ihre Adresse gültig ist und er wird sie weiterverkaufen. Ausnahmen sind nur namentlich bekannte Newsletter, die Sie tatsächlich einmal abonniert haben.

Soziale Netzwerke wie XING, LinkedIn, Facebook, Lokalisten usw. dienen neben den Nutzern auch Betrügern, die Informationen über Sie herausfinden wollen. Auch anonyme Nutzer sind oft durch das einzigartige Muster ihrer Gruppenzugehörigkeit zu identifizieren, wie eine Studie zeigte.

Sicherheitstipp 8

Seien Sie zurückhaltend mit Mitgliedschaften in sozialen Netzwerken. Fragen Sie sich vorab, was der konkrete Nutzen für Sie ist. Geben Sie möglichst wenig Informationen über sich und Ihre Kontakte preis. Einmal eingegebene Information lässt sich nur schwer bis gar nicht wieder entfernen aus dem Gedächtnis des Web.

Immer wieder gibt es auf eBay oder anderen Verkaufsplattformen Angebote, die mehr als verlockend klingen. Gerade bei teureren Artikeln wie Laptops, Schmuck oder Autos ist hier äußerste Vorsicht angebracht. Mit wechselnden Methoden werden die angelockten Käufer ausgenommen, meist ohne Ware zu liefern.

Sicherheitstipp 9

Was zu gut klingt um wahr zu sein, ist es in der Regel auch. Widerstehen Sie allzu attraktiven Angeboten. Auch bei realen Angeboten lohnt es sich meist nicht beim allerbilligsten Anbieter einzukaufen, da letztlich oft versteckte Kosten das Angebot verteuern. Für die Bezahlung gilt Tipp 3!

Abschließend sei angemerkt, dass es neben den Profi-Betrügern auch immer jugendliche Hacker gibt, die sich mit einer erfolgreichen E-Mail-Lawine, die sich um den Globus verteilt, Anerkennung ihrer Freunde verdienen wollen. Das macht es nicht unbedingt besser, erklärt aber manche der tatsächlich nicht „ausbeutenden" Mails.

Sicherheitstipp 10

Nichts ist gefährlicher als eigene Überlegenheit anzunehmen nach dem Motto: „Mich kann das alles nicht betreffen." Da sich die Methoden und Geschichten ständig weiterentwickeln und manche einen erheblichen Grad an Plausibilität und Glaubwürdigkeit erreichen, kann nur kritische Wachsamkeit schützen, gepaart mit aktualisierter Virenschutz- und Sicherheitssoftware sowie einem ebensolchen Browser und Betriebssystem. Bei seltsamen E-Mails gilt: Ignorieren ist der beste Selbstschutz. Also lesen Sie solche Nachrichten am Besten gar nicht durch. Bereits die Beschäftigung mit einer solchen Nachricht erhöht das Risiko, wie eine Studie zeigen konnte.

Autor

Dr. Marc M. Batschkus, Arzt, Medizinische Informatik, Spezialist für eHealth, eLearning & Mac OS X, Steinstraße 40, 81667 München, E-Mail: mail@batschkus.de