Der Teufel steckt im Detail - Wie Sie Phishing-Mails erkennen

Sven Krumrey 01.03.2016
26 Kommentare

Mails mit ernstem Inhalt in einem offiziellen Ton, mit Mahnungen oder angeblichen technischen Problemen verunsichern wohl alle Leser. Dahinter steht oftmals der Versuch, Ihr Geld zu ergaunern, wie ich letzte Woche schon erläuterte. Wie kann man aber miesen Betrügern auf die Spur kommen, wo verraten sie sich? Zuerst muss man sich von dem Gedanken lösen, *dass nur jene Ihre Daten haben, die dazu auch befugt sind*.

Wie sind die Hacker an meine Daten gekommen?

Phishing-Mails wirken doppelt glaubwürdig, wenn der Name, die Adresse oder sogar die Bankverbindung *bereits eingetragen sind*. Die Daten für diese Einträge können aus unterschiedlichsten Quellen stammen. Es kann eine Firma gehackt worden sein, wo Sie früher einmal Ihre Daten hinterlegt haben. **Riesige Sammlungen mit so erbeuteten Kunden-Profilen können in dunklen Ecken des Internets gekauft werden.** Hatten Sie mal einen Trojaner auf dem Rechner? Diese Programme sammeln munter Ihre Eingaben und erstellen mitunter ausgefeilte Benutzerprofile. Haben Sie eventuell Ihre Daten bei Gewinnspielen oder ähnlichen Seiten hinterlegt? Anbieter kostenloser Dienste finanzieren sich z.T. auch dadurch, dass die die Datensätze ihrer Kunden meistbietend verkaufen. Da lohnt es sich, doppelt vorsichtig zu sein, bevor man „echte Daten“ wie Namen, Adresse oder gar Bankdaten übermittelt. Eine E-Mail-Adresse kann man leicht wechseln, den Wohnort oder das Konto weniger.

Woran Sie Phishing Mails erkennen können

Schauen Sie genau darauf, *was alles ungewöhnlich ist*. Hat Ihnen dieser Absender schon mal geschrieben? Wie sind die Rechtschreibung und der Satzbau? Viele nutzen z.B. Google Translate, um Texte in fremden Sprachen zu erstellen. Dann stehen meist die richtigen Wörter da, aber in ungewöhnlichen Kombinationen. Ihre Bank, PayPal oder wer auch immer der Absender sein will, können das als versierte Muttersprachler besser.

Eile ist geboten!

Das ist der Tenor, der viele Phishing Mails auszeichnet. *Wenn Sie nicht gerade finanziell am Abgrund stehen oder als Hobby dritte Mahnungen sammeln, wird sich keine seriöse Firma so äußern.* Gerade dieser Druck, der aber aufgebaut wird, soll Sie zu voreiligen Schlüssen und zu der übereilten Überweisung oder Daten-Preisgabe verleiten. Kontensperrungen und Pfändungen sind immer das letzte Mittel und kommen nicht aus heiterem Himmel. Bleiben Sie in dieser Situation ruhig, denken Sie nach und melden sich erst mal über einen regulären Weg (Telefon / E-Mail) bei den Firmen und **nutzen Sie dabei keine Kontaktmöglichkeiten, die in der Mail selbst angegeben sind**. Hier könnten durchaus weitere Kriminelle sitzen, um sie von der Seriosität des Anliegens zu überzeugen.

Keine Bank braucht Ihre Daten, PINs und TANs! Wenn Mails darauf hinauslaufen, dass Sie plötzlich Benutzername, Passwort oder gar Codes für Transaktionen eintragen sollen, so steht kein vertrauenswürdiges Anliegen dahinter. Die Schreiber sind findig, immer neue Gründe zu suchen, damit Sie etwas „bestätigen", „verifizieren" oder „für weitere Nutzung eingeben". Ihre Bank hat all diese Daten aber schon, sonst könnten Sie sich dort gar nicht einloggen. Auch wird gerne vorgegeben, *Ihr Account sei gesperrt oder jemand hätte versucht, ihn zu hacken*. Daher auch hier der Ratschlag: Anrufen und die Sache klären. Ist gerade eine Welle von Mails unterwegs, wird man Sie vielleicht schon nach dem ersten Satz sanft unterbrechen - und schnell die Angelegenheit bereinigen.

Öffnen Sie keine Anhänge und klicken Sie keine Links an, wenn Sie sich unsicher sind! Auch mit guten Antivirus-Programmen ist man nicht vor Trojanern und ähnlicher Schadsoftware *komplett sicher*. Besonders beliebt: In PDF-Dokumenten Links verstecken (wo man sich angeblich z.B. den Versandstatus eines Pakets anzeigen lassen kann), die dann zu einem Downloadlink für Trojaner führen. So ist der eigentliche Anhang zwar sauber, *der Zielort des Links darin aber nicht*. Böse!

Die Wahrscheinlichkeit ist sehr gering, dass sie der Erste sind, der diese Mail bekommen hat. Zahlreiche Seiten setzen sich mit dem Thema auseinander und zeigen auch tages-aktuelle Beispiele. Wenn Ihnen z.B. eine Formulierung seltsam vorkommt, kopieren Sie sie einfach in die Google-Suche. Wahrscheinlich treffen Sie gleich auf Leidensgenossen und die Angelegenheit ist schnell geklärt.

Aktuell gibt es bei **Facebook** eine weitere Masche. Nutzer mit den gefälschten Facebook-Profilen Ihrer Freunde fragen unter einem Vorwand nach Ihrer Handynummer. Statt einer Nachricht von ihm bekommen Sie aber eine SMS mit einem Code. Während man noch rätselt, was das soll, versucht der falsche Freund, *diese Nummer von Ihnen zu erfahren*. Schafft er das, wird von Bezahldiensten wie PayPal , Buy with Mobile oder dessen Ableger Zong Geld über Handyrechnung abgebucht. Daher: **Stellen Sie Ihre Freundesliste auf unsichtbar, wenn Sie Facebook-Nutzer sind**!

Sind Links in der Mail enthalten? Halten Sie einfach die Maus darüber, ohne zu klicken. *Die meisten Mail-Programme zeigen so schon den Link an, der dahinter verborgen ist.* So können Sie vergleichen, ob es sich wirklich um die Firma handelt. Achten Sie auch auf Details, denn die Betrüger nutzen gerne Adressen, die sehr ähnlich sind.

Immer noch unsicher? Gehen Sie einfach im Browser auf die Seite der Firma (bevor Sie einen Link aus der Mail angeklickt oder einen Anhang geöffnet haben!) und loggen Sie sich ganz normal ein. Egal, ob bei Banken, Amazon oder Paypal, werden Sie auch dort eventuelle Nachrichten des Anbieters lesen können. Finden sie dort keine, so können Sie die Mail beruhigt löschen.

Wer sich tiefer in die Technik einarbeiten will, kann auch den **Mail Header analysieren**. Denn was bei uns in dem Email-Programm als einfacher Name erscheint, enthält viele Informationen mehr! Nähere Informationen lesen Sie bei den Kollegen von PC Welt.

Man merkt, **das beste Sicherheits-System ist immer noch zwischen unseren Ohren**! Seien Sie kritisch und bleiben Sie ruhig, wenn Sie Mails bekommen, die Sie nicht sofort einordnen können. *Lassen Sie einen kompletten Scan Ihres Antivirus-Programms über den Rechner laufen.* Die meisten Trojaner werden sofort erkannt und können unschädlich gemacht werden. Modernes Online-Banking, kritischere Anwender und gute Antivirus-Lösungen erschweren solche Angriffe ebenso, dennoch gehen Schätzungen von jährlichen Schäden in Milliardenhöhe weltweit aus. Und falls es doch mal passieren sollte: Selbst englische Minister sind davor nicht gefeit. 2009 erregten derb sexuelle Aussagen von ihnen via Twitter erhebliche Aufmerksamkeit. Sie hatten Benutzername und Passwort ihrer Accounts leichtherzig in einer Phishing-Mail eingegeben.

Kommentare

Werner Gantschnigg 03.03.2016, 09:55

Phishingmails bekomme ich fast jeden Tag. Ein neuer Trend ist folgendes:
Es kommt ein Mail mit einer Rechnung im Anhang von einer mir unbekannten Firma mit dem Titel in ungefähr diesem Wortlaut:
Rechnung nr. xxxx vom xxxxxx lt Auftrag von (Name eines Bekannten!) in perfektem Deutsch.
Das machte mich stutzig, weil ich genau weiß, dass dieser Bekannte zur Zeit keine Bestellung machen kann (Krankenhausaufenthalt). Ein Blick auf die Homepage dieser Firma brachte gleich Klarheit. Sie hatten groß eine Warnung auf der Startseite, dass ihre HP gehackt wurde und Mails in Ihrem Namen verschickt wurden. Ich finde das vorbildlich von dieser Firma.
Ich vermute mal, dass in der angehängten Rechnung ein Makro-Virus versteckt war. Ich hab natürlich alles gleich gelöscht.

Rolf Betke 03.03.2016, 09:53

Hallo,
Erst vor kurzem habe ich eine ungewöhnliche Attacke erlebt. An einem Wochenende habe ich eine SMS erhalten, dass ich meinen Führerschein beim Carsharing Anbieter vorlegen müsste, ich könnte es aber auch online tun. Prinzipiell nichts ungewöhnliches, nur diese Nachricht als SMS und die Online-Verifikation weckten meinen Verdacht. Aber die Gestaltung und auch die Sprache der Nachricht waren perfekt gemacht. Als ich persönlich in der Geschäftsstelle vorsprach, sagte man mir noch, das wäre alles ok und man würde das jetzt so machen, weil viele ihre Mail nicht lesen. Am Abend kam dann die Meldung des Anbieters, dass es sich bei der Meldung um einen Phisingangriff handele. Leider musste ich dann mitansehen, dass einige Nutzer Opfer dieses perfiden Angriffs geworden sind.
Herr Krumrey, ich wünschte Beiträge, wie dieser Artikel hier von Ihnen, würden von der Schule bis zum Seniorenheim vermittelt!