

Audiopakete zu „Phishing“

- **Mitschrift: Radiobeitrag und O-Töne**
- **Berlin, 2. September 2008**
- **O-Töne von Prof. Dieter Kempf, Mitglied des BITKOM-Präsidiums**

1. Sendefertiger Radiobeitrag

+++ Anmoderation +++

Phishing – das klingt so harmlos, nach Angelrute und idyllischen Seen. Aber so manchem Internet-Nutzer laufen bei diesem Wort Schauer über den Rücken. Denn Phishing kann richtig teuer werden: Gauner fälschen dabei Online-Überweisungen und lassen sich hohe Beträge auf ihr eigenes Konto senden. 19 Millionen Euro wurden so im vergangenen Jahr bundesweit erbeutet. Marko Schlichting hat Tipps, wie man sich vor Phishing schützen kann.

+++ Beitrag mit O-Tönen +++

Es beginnt mit einer einfachen E-Mail, an die zum Beispiel eine Mahnung angehängt ist. Wer neugierig ist und das alles öffnet, holt sich womöglich einen Trojaner auf den Rechner, sagt BITKOM-Präsidiumsmitglied Dieter Kempf.

Ein Trojaner ist ein Schadprogramm, das sich ohne Zutun des Nutzers selbst auf dem PC installiert. Und damit einfach Dinge, die auf dem PC geschehen, ausspioniert, also zum Beispiel Tastatureingaben, Mausbewegungen und so weiter. (14 Sek.)

Inzwischen ist das die häufigste Variante, wie Betrüger an geheime Kontodaten kommen – im Schnitt beträgt der Schaden je Phishing-Fall 3.700 Euro. Deshalb ist es erstens wichtig, dubiose E-Mails sofort zu löschen.

Das Zweite: Unbedingt immer neueste Antiviren- und Firewall-Programme der unterschiedlichen Hersteller nutzen. Dritter, aus meiner Sicht sehr wesentlicher Hinweis ist: Höhenbegrenzungen einführen. (11 Sek.)

Beispiel: Bei der Bank beantragen, dass online maximal 1000 Euro überwiesen werden können. Das begrenzt im Ernstfall die Schadenshöhe. Die Banken sind nämlich nicht verpflichtet, den Schaden zu ersetzen, aber wenn der Kunde nachweisen kann ...

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel. +49. 30. 27576-0
Fax +49. 30. 27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Christian Spahr
Pressesprecher
Telekommunikation & Recht
Tel. +49. 30. 27576-112
Fax +49. 30. 27576-400
c.spahr@bitkom.org

Präsident
Prof. Dr. Dr. h.c. mult.
August-Wilhelm Scheer

Hauptgeschäftsführer
Dr. Bernhard Rohleder

... dass er sich einer brauchbaren Firewall- und Virenschutzsoftware bedient und die auch regelmäßig auf den neuesten Stand gebracht hat. Dann reagieren die Kreditinstitute in aller Regel sehr, sehr kulant, ersetzen den Schaden. Wichtig ist eben: Das Kreditinstitut sofort informieren, die Konten sperren, Polizei informieren, und dann kann man nur noch hoffen. (16 Sek.)

Damit es gar nicht erst so weit kommt, fordert der Branchenverband BITKOM schärfere Gesetze gegen Phishing ...

... weil wir heute eine Rechtslage haben, die nur den tatsächlichen Betrugsfall sanktioniert. Wir fordern also: Bereits der Phishing-Versuch muss strafbar werden. (14 Sek.)

Immerhin scheinen die neuesten Sicherheitsmaßnahmen der Banken und die Tipps für die PC-Besitzer Früchte zu tragen: Im laufenden Jahr sind die Phishing-Zahlen erstmals seit langem wieder rückläufig.

2. Einzelne O-Töne:

1) Ist Phishing nach wie vor eine Gefahr für Nutzer von Online-Banking?

„Es ist leider in der Tat so, dass Phishing ein nach wie vor aktuelles Thema darstellt, auch wenn wir nach bisherigen Ermittlungen für das Jahr 2008 einen Rückgang der Fallzahlen und einen Rückgang der jeweiligen Schadenshöhen feststellen dürfen.“ (15 Sek.)

2) Welche ist die häufigste Methode von Phishing-Betrügern?

„Der mittlerweile häufigste Fall ist tatsächlich ein in einer sehr harmlosen E-Mail versteckter Trojaner. Ein Trojaner ist ein Schadprogramm, das sich ohne Zutun des Nutzers selbst auf dem PC installiert und damit einfach Dinge, die auf dem PC geschehen, ausspioniert – also zum Beispiel Tastatureingaben, Mausbewegungen und et cetera.“ (21 Sek.)

3) Wie kann man das Risiko minimieren, Opfer von Phishing zu werden?

„Wenn man den Absender nicht kennt oder wenn man weiß, dass man mit dem Absender eigentlich gar nichts zu tun hatte: Lieber mal eine E-Mail löschen als eine zu viel und zu früh aufmachen. Neben dieser allerersten Anweisung – allergrößte Vorsicht und Zurückhaltung – gibt's das Zweite: Unbedingt immer neueste Antiviren- und Firewall-Programme der unterschiedlichen Hersteller nutzen. Dritter, aus meiner Sicht sehr wesentlicher Hinweis ist: Höhenbegrenzungen einführen. Wenn ich zum Beispiel weiß, dass meine Internetzahlungen in der Regel 1000 Euro nicht überschreiten, warum mache ich dann nicht einfach eine Begrenzung auf 1000 Euro? Dann ist das eben der maximale Schadensbetrag, der mir entstehen kann.“ (35 Sek.)

4) Wer trägt im Ernstfall den Schaden – der Kunde oder die Bank?

„Also, in aller Regel ist es so, dass die Kreditinstitute sich sehr, sehr kulant zeigen, insbesondere dann, wenn dem Anwender der Nachweis gelingt, dass er nicht grob fahrlässig oder fahrlässig gehandelt hat. Dieser Nachweis gelingt am besten dadurch, dass er sich einer

brauchbaren Firewall und Virenschutzsoftware bedient und die auch regelmäßig auf den neusten Stand gebracht hat – dann reagieren die Kreditinstitute in aller Regel sehr, sehr kulant, ersetzen den Schaden. Wichtig ist eben: Das Kreditinstitut sofort informieren, die Konten sperren, Polizei informieren, und dann kann man nur noch hoffen.“ (29 Sek.)

5) Gibt es neue Maßnahmen, um das Online-Banking sicherer zu machen?

„Ein neues System, das so genannte ‚Extended Authentication Certificate‘, klingt sehr kompliziert – ist in Wirklichkeit nichts anderes als ein grüner Balken in der Adresszeile einer Internetseite, an dem man erkennen kann, dass derjenige, der die Seite eingestellt hat, tatsächlich derjenige ist, der er vorgibt zu sein. Das kann man auch erkennen an einem kleinen Vorhängeschloss auf den Webseiten. Aber zugegebenermaßen: Der grüne Balken ist natürlich wesentlich deutlicher.“ (30 Sek.)

6) Der Branchenverband fordert schärfere Gesetze gegen Phishing – warum?

„Wir fordern in der Tat schärfere Gesetze, weil wir heute eine Rechtslage haben, die nur den tatsächlichen Betrugsfall sanktioniert. Wir fordern also: Bereits der Phishing-Versuch muss strafbar werden.“ (14 Sek.)