Opfer von Phishing-BetrÃ¼gern

Kategorie : Laaber
VerÃ¶ffentlicht von Atlan am 05-Oct-2010 15:26

Aus dem Pressebericht der PI Nittendorf vom 02.10.2010 zur besonderen Beachtung.
Ein Internet-Nutzer aus Laaber wurde Ende September Opfer von BetrÃ¼gern, die mittels der Phishing-Methode sein Girokonto leer rÃ¤umten.

Ihm entstand dabei ein Schaden von Ã¼ber 3.500 Euro. Das Geld wurde von den unbekannten BetrÃ¼gern auf ein niederlÃ¤ndischen Konto Ã¼berwiesen. Inwieweit das kontofÃ¼hrende Kreditinstitut fÃ¼r einen Schadensausgleich beim Kunden aufkommt, ist hier nicht bekannt.

Aufgrund dieses aktuellen Anlasses fÃ¼r alle Online-Banking-Nutzer wichtiges Hintergrundwissen zur Phishing-Methode:

Es gibt verschiedene Varianten von Phishing-Attacken, gemeinsames Ziel ist jedoch das AusspÃ¤hen von Zugangsdaten zu persÃ¶nlichen Accounts, um diese fÃ¼r eigene Zwecke zu nutzen (Onlinebanking, Online-AuktionshÃ¤user, Kreditkartendaten, Onlinezahlungssysteme usw.)

Variante 1 â Phishing-Mails:

Hierbei werden wahllos Massenmails verschickt. Diese Mails sollen den Anschein erwecken, dass sie von einer Bank stammen, wobei der Kunde aufgefordert wird, den mitgeschickten Link zur angeblichen Bankseite zu nutzen und dort seine persÃ¶nlichen Daten (Kontonummer, Passwort, PIN, TAN) einzutragen. Dabei wird in den Mails immer eine besondere Brisanz suggeriert, z.B. Umstellung des Systems, SicherheitsÃ¼berprÃ¼fung oder mÃ¶gliche Kontosperrung. Das soll dem Adressat zu einem schnellen Handeln verleiten, da er sonst mÃ¶gliche Konsequenzen fÃ¼rchtet. Bei den verlinken Seiten handelt es sich um gefÃ¤lschte Seiten, bei der die o.g. Daten abgefragt und somit dem Urheber dieser Seiten zugeleitet werden.

Kurz darauf benutzen die TÃ¤ter diese Informationen, um von dem Konto des Opfers eine Ãberweisung auf ein anderes Konto vorzunehmen.

Variante 2 â Trojaner:

Ein Trojaner installiert sich unbemerkt fÃ¼r den User auf dessen PC (versteckt sich meist hinter

"Nutzprogrammen" die aus dem Internet heruntergeladen werden oder Spam-Mails) und lauscht die

OnlineaktiviÃ¤ten ab. Erkennt er die Ãbermittlung von persÃ¶nlichen

Zugangsdaten sowie PIN und TAN-Nummern wird die Verbindung zur Bank unterbrochen und diese Daten nicht an die Bank, sondern wieder an den Urheber des Trojaners Ã¼bermittelt. Dem User wird meist eine Fehlermeldung angezeigt und in der Folgezeit ist ein erneutes Anmelden bei der Bank nicht mÃ¶glich. Damit sollen dem User mÃ¶gliche technische Probleme bei der Bank oder der Onlineverbindung vorgetÃ¤uscht werden, um zu verhindern, dass die gephishten Daten genutzt werden.

Die GeldbetrÃ¤ge werden dann entweder auf Konten im Ausland, Ã¼ber angeworbene, nichtsahnende â□□Geldkuriereâ□□ oder auf falsch erÃ¶ffnete Konten transferiert und abgerÃ¤umt.

Zusammenfassend kann gesagt werden, dass bei UnregelmÃ¤Ã□igkeiten und AuffÃ¤lligkeiten entgegen der bisher gewohnten DurchfÃ¼hrung beim Online-Banking alle Alarmsignale beim Nutzer hervorgerufen werden sollten. NÃ¤here Informationen dazu kÃ¶nnen auch bei jeder Bank dazu erfragt werden.