Phishing Angriff – eine authentische Geschichte

Diese Geschichte handelt von einem echten Fall, der sich in Deutschland zugetragen hat. Die Namen sind natürlich verändert, aber die Fakten bleiben.

Eines schönen Morgens, es war der 2.7. dieses Jahres, geht Claudia S. zu ihrem Geldautomaten, um Bargeld zu holen. Es ist früh, kalt ist es draußen, und so beeilt sie, sich um zu einem Termin zu gelangen.
Keine Zeit bleibt, den Kontostand abzufragen und die Auszüge aus dem Automaten zu holen. Das Konto dürfte aber an sich nicht leer sein, denn es sollte mehr als genug Geld vorhanden sein da Claudia größere Gutschriften erwartete.
Das dem nicht so war, sollte sich wenig später heraus stellen bei einem Kontostand von knappen 2,- €.
So dachte sich Claudia S., hat sich nicht weiter Gedanken darüber gemacht und eilte zu ihrem Termin.
Nach dem Termin, gegen 10:00 Uhr, ist Claudia S. dann wieder zu Hause und will sich via eBanking die Umsätze anschauen, um die Kontobewegungen zu prüfen.
Das Gehalt ist eingegangen, und auch eine weitere Gutschrift ist auf dem Konto ersichtlich.

Aber was ist das? 5000,- € sind an einen gewissen Herrn G. überwiesen worden, der ein Konto bei der Volksbank in Wiesbaden hat.
Claudia S. ist sicher, sie kenne keinen Herr G. und hat auch keine Überweisung vorgenommen. Warum auch?
Schliesslich folgt ein Anruf bei der Hausbank, die Kulmbacher Bank, um den Sachverhalt schnell zu klären und das Geld zurück zu holen.
Das Horrorszenario beginnt mit dem Rückruf der Bank, die sogleich Claudia S. zu verstehen gibt, es handele sich hierbei um einen Fall von Phishing, und sie selbst sei das Opfer.

Die Bank gibt Claudia S. zu verstehen, dass mit einer gültigen TAN per eBanking bereits am 29.06.2007 eine Überweisung über 5000,- € an Herr G. getätigt wurde.
Zurückholen kann man das Geld nach Aussage der Bank nicht, da es sich um eine gültige Überweisung mit einer gültigen TAN handele.
Das Geld scheint weg, der Computer infiziert mit einem Trojaner, der den Computer von Claudia S. so ausspionierte, dass die Angreifer an eine gültige TAN gelangen konnten.
Der Banker gab sogleich den Hinweis, dass dieser Vorgang unmittelbar bei der zuständigen Polizei zur Anzeige gebracht werden müsse.
Claudia S. erinnert sich dann bei der Polizei an Details, die nicht unwesentlich scheinen im Zuge der nun folgenden Ermittlungen.
So gibt Claudia S. an, wenige Tage vor der falschen Überweisung, Trojaner auf dem Computer gefunden zu haben und diese wohl auch durch eine Anti-Virus Software entfernen ließ.
Anscheinend scheint dies nicht mit der gewünschten Gründlichkeit der Software geschehen zu sein, denn eine weitere, unentdeckte Spionagesoftware befand sich nach wie vor auf dem Computer.
Die Frau erinnert sich auch wieder daran, dass sie selbst einige Tage vor der unberechtigten Überweisung für sich Überweisungen getätigt habe.
Es erschien die Meldung, dass die TAN bereits verbraucht sei.
Das TAN System, so sei anzumerken, ist kein numerisches, fortlaufendes TAN System, sondern man kann stets irgendeine noch nicht benutzte TAN aus dem gelieferten TAN Block wählen und eingeben.

Man kann davon ausgehen, dass eine Schwachstelle im Internet Explorer Ausnutzung gefunden hat.
Die Verbindung zur Bankwebseite wurde kurz abgebrochen, die bereits eingetragene TAN konnte von einem Dritten abgefangen werden, damit diese von ihm für die falsche Überweisung genutzt werden konnte.
Dieser Dritte kam so in den Besitz einer gültigen TAN.
Die Bank bestätigte, dass die angeblich verbrauchte TAN für besagte Überweisung der 5.000 Euro (von den Betrügern) benutzt wurde.
Aber Stopp, das Geld ist doch an eine deutsche Bank überwiesen worden.
Da muss es doch wenigstens echte Möglichkeiten geben, das nachvollziehen zu können.
Und genau das konnte dann auch durchgeführt werden. Man kontaktierte die Volksbank Wiesbaden und prüfte die Einzelheiten des Transfers der 5000,- €, die ja bei Herr G. auf dem Konto eingegangen sein müssten.
Oder ist das Geld nach einer beliebten Betrügermethode bereits per Western Union weiter transferiert worden und befindet sich schon im Ausland?
Zunächst untersucht die Polizei den Computer von Claudia S. und kann in der Tat noch einen Schädling ausmachen, den sie aber nicht entfernen dürfen.
Dieser dürfte für die Phishing Attacke zuständig gewesen sein.
Die Bank jedenfalls hat sich in diesem Fall anständig, bemüht das Geld wieder zu beschaffen. Was sich natürlich als unmöglich heraus stellen dürfte, wenn das Geld bereits ins Ausland transferiert wurde.
Die Fakten waren exakt so, und die Hoffnung das Claudia S. je an ihr Geld kommt, flossen in Tränen und schlaflosen Nächten dahin.
Es stellte sich dann heraus, dass der Herr G. in Wiesbaden existierte und dass dieser seit einiger Zeit seltsame Transaktionen auf seinem Konto durchgeführt hatte.
Die Wiesbadener Volksbank nahm Kontakt zu ihrem Kunden Herr G. auf und forderte ihn zur Rückzahlung sowie zur Selbstanzeige auf.
Es stellte sich heraus, dass Herr G. über eine Zeitungsanzeige auf Betrüger reingefallen war, die ihm für Transaktionen entsprechende Honorare in Aussicht stellten, wenn er sein Konto dafür zur Verfügung stellt.
Somit konnten die Betrüger vermutlich bei diversen Personen Geld abziehen und auf das Konto des Herrn G. transferieren. Dieser überwies das Geld gemäß Abmachung unmittelbar weiter über Western Union.
Am darauf folgenden Tag bestätigen sich die Angaben auch der Wiesbadener Volksbank.
Herr G. hatte sich selbst angezeigt.
Er hatte bereits 11.000 Euro so über sein Konto transferiert.
Der 61-jährige Rentner habe für die Bereitstellung seines Kontos eine Provision von 3% erhalten, so die eigene Aussage.
Gegen Herrn G. wird nun wegen Verstoß gegen das Geldwäschegesetz ermittelt. Ein harter Vorwurf, dem sich den Rentner ausgesetzt fühlt, wollte er doch seinen Ruhestand genießen.
Wenige Tage später meldet sich die Bank aus Wiesbaden und verkündet, das Geld sei wieder zurück überwiesen worden auf das Konto von Claudia S..
Vermeintlich, aber dazu gibt es keine klaren Hinweise, sei das Geld vom Rentner Herr G. direkt wieder zurück überwiesen worden.
Eine Versicherung sei nicht eingesprungen. Gegen die Betrüger wird weiterhin ermittelt.
Claudia S. kommt mit einem „blauen Auge" davon und wird sich nun mit den Vorwürfen konfrontiert sehen, nicht ausreichend für die eigene Sicherheit am heimischen Computer getan zu haben.

Was sich wie eine Geschichte liest, ist ein wahres Ereignis, das sich vor wenigen Tagen

genauso zugetragen hat.
Abschließend bleibt die Erinnerung an die Steigung von Sicherheit gerade auch in privaten Haushalten.
Claudia hat aus den Fehlern gelernt und wird in der Zukunft natürlich noch sensibler mit entsprechenden Bankdaten umgehen und für aktuelle Anti-Virensoftware sorgen.
Grundsätzlich kann nur empfehlenswert sein, auf seinem Computer eine immer aktuelle Anti-Virus Software installiert zu haben und auch immer die Updates auszuführen.
Weiterhin gibt es Firefox als alternativen Browser, der nicht so anfällig ist wie der Internet Explorer und die Ausnutzung nicht so „leicht" gemacht wird wie mit dem Internet Explorer.
Denn das Einschleusen des Trojaners geschah vermutlich über eine Schwachstelle im Internet Explorer.
Gute Anti-Virus Hersteller können auch Schädlinge erkennen, die nicht in der Datenbank enthalten sind.
Viele Schädlinge weisen ja immer ähnliche Verhaltensmuster auf und können so bei Manipulation am System identifiziert werden.
Vorsicht ist auch dann geboten, wenn eine Transaktion innerhalb des Online-Banking plötzlich abgebrochen wird oder eine TAN als bereits benutzt.
Auch sind die Webseiten der Banken mit einem https:// versehen und das Schlüsselsymbol für eine sichere Datenübertragung ist unten in der Browserleiste ersichtlich.
Ein gesundes Mißtrauen sollte man schon an den Tag legen, wenn etwas ungewöhnlich erscheint, Browserseiten nicht mehr angezeigt werden können, die Verbindung zur Bank abbricht oder der Computer sich generell anders verhält als man es gewohnt ist.
Hier sollten spätestens die Alarmglocken angehen, der Computer sollte zunächst vom Internet getrennt und eine Untersuchung nach Schädlingen sollte eingeleitet werden.
Nicht jeder Betroffene dürfte so viel Glück haben und bekommt sein Geld wieder zurück.
Denn ist eine Überweisung erstmal ausgelöst mittels einer gültigen TAN, ist das Geld weg.

Text: Marko Rogge
http://www.marko-rogge.de

Anmerkung:
Dieser Artikel ist mit der Genehmigung der Geschädigten entstanden. Alle weiteren identitäten sind nicht deutlich genannt, so dass hier keine Verletzung von Schutzrechten vorliegt.
Sollten Sie Fragen zu diesem oder anderen Artikeln von mir haben, so nehmen Sie Kontakt zu mir auf: mail@marko-rogge.de .