Wie kommt der Phisher eigentlich an sein Geld? – Update

Die durch eine Phishing-Attacke erbeuteten Gelder fließen stets über inländische Konten und werden von dort per Western Union ins Ausland transferiert (siehe unseren Beitrag vom 28.06.05). Aber wie kommt der Phisher eigentlich besonders elegant an ein inländisches Konto? Bis jetzt wurden die Kontoinhaber per Spam-Mail angeworben, die das Versprechen eines gut bezahlten Nebenjobs enthielt. Dieser bestand darin, ihr Konto für Geldtransaktionen zur Verfügung zu stellen. Sie sollten auf ihr Konto eingezahltes Geld in bar abheben und es per Western Union an die Täter nach Russland weiterleiten. Für diese „Dienstleistung“ sollten die Opfer dann 5-10% des Betrages als Provision erhalten. Das Geld stammte aus vorausgegangenen Phishing-Attacken.

Die Überweisung per Western Union ist die bevorzugte Transfervariante, weil sie die Spur des Geldes verwischt. Um eine entsprechende Überweisung vornehmen zu können, ist weder eine Bankverbindung noch eine Mitgliedschaft bei Western Union nötig. Das eingezahlte Geld wird an den Empfänger in bar ausgezahlt, nachdem er sich identifiziert hat. Danach ist es nicht mehr möglich, den Transfer rückgängig zu machen.

Jetzt haben die Phishing-Betrüger eine neue Variante der Anwerbung von Kontoinhabern entwickelt. Sie bieten in Jobbörsen niedrig bezahlte Aufträge an. Daraufhin melden sich gutgläubige Firmen oder Selbstständige und erfüllen den Job, z.B. Erstellung eines Internetlogos. Ihren Lohn bekommen sie dann vom Konto eines nichtsahnenden Dritten überwiesen, dessen Daten vorher per Phishing-Attacke ausgespäht worden sind. Sie erhalten allerdings wesentlich mehr als die vorher vereinbarte Summe. Unmittelbar danach werden sie per E-Mail darum gebeten, den überschüssigen Betrag per Western Union an die Betrüger zurückzuüberweisen, da es sich angeblich um ein Versehen gehandelt habe.

Dazu ein aktueller Fall: In einer in der Branche bekannten Internetjobbörse fand der selbstständige Softwareunternehmer Peter B.* eine Anzeige, in der ein Auftrag über die Erstellung eines Kalkulationsprogramms in Aussicht gestellt wurde. Nach einer Kontaktaufnahme per E-Mail einigte man sich schnell auf eine Bezahlung von 200 Euro. Nach Fertigstellung des Programms sandte es Peter B. per E-Mail an seinen Auftraggeber. Am Tag drauf traf auch der Lohn für seine Arbeit auf seinem Konto ein. Allerdings handelte es sich nicht um die vereinbarten 200 Euro, sondern um 2800 Euro. Unmittelbar danach

bemerkte Peter B., dass er eine E-Mail von seinem Auftraggeber erhalten hatte, in der dieser die Überweisung von den 2600 Euro als Versehen bezeichnete und ihn bat, ihm diesen Betrag zurückzuüberweisen. Da er sich gerade auf einer Geschäftsreise in Russland befände, sollte Peter B. den Betrag per Western Union nach Russland schicken. Daraufhin schöpfte Peter B. Verdacht. Er erkundigte sich bei seiner Hausbank, woher die Überweisung gekommen war. Diese stellte fest, dass das Geld vom Postbankkonto von Monika S.* überwiesen worden ist. Als Peter B. sie daraufhin anrief, stellt sich heraus, dass sie nichts von der Überweisung wusste. Monika S. rief sofort bei der Postbank an, die ihr mitteilte, dass sie im Laufe des Vormittages zwei Überweisungen zu jeweils 2800 Euro auf verschiedene Konten vorgenommen habe. Da sie selbst diese Überweisungen nicht vorgenommen hatte, ist anzunehmen, dass sie Opfer eines Phishing-Angriffs wurde.

Dieser Fall zeigt wieder einmal wie gefährlich Phishing-Attacken sind. Mittlerweile gibt es zwei Opfergruppen. Auf der einen Seite die Phishing-Opfer selbst, deren PIN und TAN erbeutet wurden. Auf der anderen Seite gutgläubige Dritte, deren Konten zum Transfer der gephishten Gelder ins Ausland missbraucht werden sollen. Dabei handelt es sich nicht mehr nur um Privatpersonen, die auf das Versprechen von leicht verdientem Geld hereinfallen, sondern auch um seriöse Unternehmer. Diese ahnen nicht, dass der ihnen angebotene Job nur zur Transaktion von Phishing-Geldern dient. Sie tragen dabei sogar ein doppeltes Risiko. Zum einen ist es so gut wie unmöglich, ihren Lohnanspruch gegen den im Ausland sitzenden Phishing-Betrüger durchzusetzen, zum anderen sehen sie sich auch zivilrechtlichen Ansprüchen der Phishing-Opfer ausgesetzt.

*Namen von der Redaktion geändert.

Isabelle Biallaß
Die Autorin ist wissenschaftliche Hilfskraft am Lehrstuhl von Prof. Dr. Georg Borges an der Ruhr-Universität Bochum.

Dennis Werner
Der Autor ist Diplom-Jurist und wissenschaftliche Hilfskraft am Lehrstuhl von Prof. Dr. Georg Borges an der Ruhr-Universität Bochum.