LG Bonn, Urteil vom 07. Juli 2009 – 7 KLs 01/09 –, Rn. 13 - 31

Zur Funktionsweise des Phishing allgemein

Unter "Phishing" versteht man das verdeckte "Abfischen" von Zugangs- und Transaktionsdaten, die ein Bankkunde für das Onlinebanking erhält, mit dem Ziel, diese Authentifizierungsdaten anschließend unbefugt zu Lasten fremder Konten einzusetzen.

Die Banken sicherten im tatkritischen Zeitraum ihre Online-Banking-Systeme durchweg mit PINs und TANs. Der Kunde erhielt eine persönliche Identifikationsnummer (PIN) , die beim Zugriff auf das Online-Konto abgefragt wurde und eine Liste mit Transaktionsnummern (TAN) , mit denen die einzelnen Verfügungen legitimiert werden mussten. Dabei konnte der Kunde - im Gegensatz zum heute vorherrschenden iTAN-Verfahren - die TAN selber von der Liste auswählen.

Das Abfischen der Daten erfolgt auf verschiedene Weise. In der Frühphase dieser Delikte wurden Bankkunden durch angeblich von ihrer Bank stammende, aber in Wirklichkeit gefälschte E-Mails dazu veranlasst, ihre Zugangsdaten (PIN) und eine ihrer persönlichen Transaktionsnummern (TAN) mitzuteilen. Diese Daten konnten dann unmittelbar für unbefugte Überweisungen verwendet werden.

Zunehmend entwickelten die Phishing-Täter - auch als Reaktion auf die Weiterentwicklung der bankeigenen Sicherheitssysteme - ihre Methoden weiter (vgl. : Goeckenjan, Phishing von Zugangsdaten für Online-Bankdienste und deren Verwertung, wistra 2008, 128 ff.). So werden mit Hilfe von E-Mails, welche massenhaft als SPAM versendet werden, Schadprogramme wie Trojaner , Würmer oder Viren auf die Rechner der Betroffenen übertragen, wenn diese die Mails öffnen. Die Schadprogramme können zum Beispiel bewirken, dass sich bei Eingabe der TAN ein Fenster öffnet, in dem der Bankkunde mit dem Hinweis darauf, dass die eingegebene TAN schon verbraucht sei, aufgefordert wird, eine weitere TAN einzugeben. Die zuerst eingegebene TAN wird automatisch an die Phishing-Täter übermittelt.

Auch kann durch Schadprogramme ein sogenannter "keylogger" auf dem befallenen Rechner eingerichtet werden, der verdeckt im Hintergrund sämtliche Tastatureingaben in Formularmasken protokolliert und sog. "Screenshots" (d.h. Standbilder von bestimmten Seiten) anfertigt.

Auch diese Daten werden von den Schadprogrammen automatisch an einen Bezugsrechner, den sogenannten Dropzone- bzw. Logserver übermittelt. Von diesem Server wird regelmäßig auch das Netz der von den Schadprogrammen befallenen Rechner gesteuert, das sogenannte "Bot-Netz".

Die auf einem dieser Wege erlangten Daten werden nunmehr dazu benutzt, die Online-Konten der Geschädigten mit den erlangten PINs und Kontonummern zu öffnen und dahingehend zu überprüfen, ob lohnenswerte Geldsummen vorhanden sind. Wenn dies der Fall ist, führen die Täter mit den ebenfalls "abgephishten" TANs unbefugt Überweisungen von den Konten der Geschädigten durch.

Die Gelder werden dabei üblicherweise zunächst auf Konten sogenannter "Finanzagenten" überwiesen, die zur Verschleierung des Geldflusses zwischengeschaltet werden. Deren Aufgabe besteht darin, die ihnen überwiesenen Gelder in bar abzuheben und mittels eines Auslandsgeldtransferdienstes wie z.B. "X2" oder "N5" in das - in der Regel osteuropäische - Ausland zu transferieren. Der Empfänger im Zielland, der sogenannte "Naler" , hebt das Geld in der Folge (meist unter falscher Identität) in bar ab und speist es wieder in das Bankensystem ein.

Durch Online-Zahlungssysteme wie "X3" oder "Q3" werden die Gelder schließlich den Tätern selbst zugänglich gemacht.

Die Anwerbung der Finanzagenten erfolgt regelmäßig durch das Internet. Unter einem Vorwand, der je nach Anwerbeseite sehr unterschiedlich sein kann, werden die Finanzagenten dazu bewegt, ihr Konto für die Überweisung zur Verfügung zu stellen. So kann es z.B. sein, dass die Anwerbeseite eine Scheinfirma präsentiert, die als Geschäftsinhalt angeblich die schnelle Transferierung von Geldern ins Ausland unter Vermeidung bürokratischer Hemmnisse offeriert. Dem Finanzagenten wird ein lukrativer Nebenverdienst dafür versprochen, dass er sein Konto zu Verfügung stellt. Dabei handelt es sich meist um eine prozentuale Beteiligung an den überwiesenen Geldsummen.

Das "Phishing" stellt sich somit als sehr personalintensives und komplexes System dar, das regelmäßig nur arbeitsteilig zu bewerkstelligen ist und das eines hohen Grades an Vorbereitung und Koordination bedarf:

Zum einen müssen die technischen Voraussetzungen geschaffen werden. Es werden Computerfachleute mit hinreichender Programmiererfahrung benötigt, um die Trojaner und die anderen verwendeten Schadprogramme anzufertigen. Daneben werden Personen benötigt, die die Trojaner durch Spammails, Spambanner oder über Sicherheitslücken in bekannten Programmen (sog. "exploits") im Internet verbreiten und mit den so infizierten Rechnern der Opfer ein sogenanntes Bot-Netz ("Bot": von Roboter) aufbauen. Über das Bot-Netz können die infizierten Rechner zentral gesteuert und ohne Kenntnis der Opfer benutzt werden. Die Bot-Rechner werden dabei nicht nur selber nach Konto-Informationen durchsucht, sondern können ihrerseits wieder zum Verbreiten der Spam und Phishing-Mails eingesetzt werden.

Weiter muss ein Logserver angemietet und administriert werden und die infizierten Rechner des Botnetzes müssen auf den Logserver ausgerichtet werden, damit die abgephishten Daten nutzbar werden. Alle diese Tätigkeiten müssen zudem technisch so ausgeführt werden, dass sie möglichst wenig nachverfolgbare Spuren im Internet hinterlassen.

Darüber hinaus müssen Personen gefunden werden, die die abgephishten Daten auf dem Logserver nach ihrer Aktualität sortieren, auf ihre Verwendbarkeit prüfen und die Online-Konten der Geschädigten nach Guthaben durchsuchen, die sich zum Überweisen eignen. Dabei sind jeweils unterschiedliche Besonderheiten der bankinternen Sicherheitssysteme zu beachten, an die die Vorgehensweise angepasst werden muss.

Zum anderen benötigt man ein funktionierendes System, mit dem die Finanzagenten angeworben und geführt werden. Dazu benötigt man neben den Anwerbeseiten im Internet vor allem Personen, die per E-Mail oder Telefon mit den Finanzagenten Kontakt aufnehmen und ihnen Anweisungen für das Weiterüberweisen geben. Diese "Dropführer" (Drop ist der szenegängige Begriff für die Finanzagenten) müssen dabei stets aufpassen, dass die Finanzagenten das Konzept nicht durchschauen. Zudem drängt im Fall einer Überweisung an einen "Drop" die Zeit; denn je schneller der Finanzagent reagiert und das Geld von seinem Konto abhebt, umso größer ist die Wahrscheinlichkeit, dass das Geld auch tatsächlich zu den Geldempfängern (Nalern) weitergeleitet werden kann. Denn in vielen Fällen fallen die Überweisungen den Geschädigten rasch auf und sie veranlassen schnellstmöglich die Rückbuchung der Überweisungen. Durch die Weiterleitung der Gelder per "X2" bzw. "N5" macht sich der Finanzagent selber regelmäßig der fahrlässigen Geldwäsche gemäß § 261 Absatz 5 StGB strafbar.

Als drittes Element bedarf es zum vollständigen "Phishing-System" noch der "Naler", also der Personen, die im Ausland das Geld - zumeist unter falscher Identität - bar abheben und wieder in den Bankenkreislauf einspeisen.

Erschwerend kommt hinzu, dass alle diese Teilbereiche koordiniert werden müssen. So müssen zum erfolgreichen Phishing die Trojaner-Programmierung und die Log-Server aufeinander abgestimmt sein, die Spamwellen müssen regelmäßig mit neuen Versionen der Trojaner versorgt werden und den Personen, die Überweisungen tätigen, müssen Drops zur Verfügung gestellt werden. Dabei müssen die Überweisenden genau beachten, von welchem Konto auf welchen Finanzagenten zu überweisen ist. Denn bestimmte Kombinationen von Banken sichern eine raschere und damit erfolgversprechendere Überweisung als andere Kombinationen. Schließlich müssen auch die "Dropführer" mit den Kontaktdaten der "Naler" in Osteuropa versorgt werden, damit sie ihren Finanzagenten die entsprechenden Weisungen erteilen können.

Alle diese Aufgaben können, da sie teilweise zeitgleich vorzunehmen sind, nicht von einer oder auch zwei Personen durchgeführt werden. Vielmehr ist erfolgreiches Phishing nur durch eine in hohem Maße organisierte Gruppe durchzuführen, die arbeitsteilig vorgeht.