



## **Pressebericht vom 26.10.2005**

### **Inhaltsübersicht**

#### **STADTGEBIET NÜRNBERG**

##### **(1558) Mit „Phishing“-Angriff hohen Geldbetrag entwendet**

Phishing – eine Form des Trickbetruges über das Internet. Hier versuchen Kriminelle, Bankkunden zur Preisgabe ihrer Geheimzahlen zu bewegen. Meistens geschieht dies über die Zusendung entsprechender E-Mails, aber auch Zugangsdaten zu Versandhäusern, Internetauktionsbörsen und Kontaktportale sind Ziel dieser Tätergruppe. Mit den gestohlenen Zugangsdaten verursachen die „Phisher“ erheblichen Vermögensschaden.

Dies musste auch ein 49-jähriger Online-Kunde einer Bank aus Rheinland-Pfalz im Februar 2005 feststellen. Während der Mann über die Internetseite seiner Bank eine Überweisung abwickeln wollte und dabei seine geheime TAN (Transaktionsnummer) eingab, brach sein Computer die Verbindung zur Hausbank plötzlich ab. Bei der erneuten Anwahl der Seite und Wiedereingabe der gleichen TAN erhielt er die Mitteilung, dass diese bereits vergeben wäre. Wenig später musste er feststellen, dass von seinem Konto mehrere Tausend Euro abgebucht worden waren.

Wie sich bei den umfangreichen und langwierigen Ermittlungen herausstellte, war auf seinem Rechner ein sog. „Abbruchtrojaner“ unbemerkt installiert worden. Dies kann z.B. durch das Anklicken einer beliebigen Seite im Internet geschehen sein. Der Trojaner brach nach Eingabe der Geheimzahl die Verbindung zur Bankseite ab, die angegebene Nummer verschickte er an seinen „Programmierer“. Dieser wiederum nutzte die TAN, um den Betrag auf sein eigenes Konto zu überweisen.

Als dringend tatverdächtig wurde vom Fachkommissariat der Nürnberger Kriminalpolizei ein 31-jähriger Nürnberger ermittelt, auf dessen Konto die Überweisung erfolgte. Seinen Angaben nach fungierte er allerdings nur als Geldkurier für eine ausländische Firma. Über ein Zeitungsinserat wäre er an die Firma geraten.

Wegen Computerbetruges, Datenveränderung, Ausspähen von Daten und Geldwäsche wird der 31-Jährige angezeigt. Überdies muss er den gesamten Geldbetrag an den Geschädigten zurückzahlen.

Die Kriminalpolizei rät davon ab, das Bankkonto für Zahlungseingänge zur Verfügung zu stellen, die anschließend ins Ausland transferiert werden sollen. Des Weiteren wird empfohlen, ein Virenprogramm sowie eine Firewall auf dem Computer zu installieren, welche regelmäßig aktualisiert werden. Diese Programme sind kostenlos im Internet abrufbar. Dadurch wird die Gefahr einer Infizierung mit einem Schadprogramm minimiert.

Sollten Sie eine vermeintliche E-Mail Ihrer Bank bekommen, folgen Sie auf keinen Fall dem angegebenen Link zur Aktualisierung Ihrer Kundendaten. Ihre Bank wird Ihre persönlichen Daten, insbesondere PIN und TAN, niemals per E-Mail abfragen.