Landeskriminalamt Niedersachsen
Am Waterlooplatz 11, 30169 Hannover,

Tel. 0511/26262-63 01 / -63 02/ -63 03
Fax 0511/26262-6305
pressestelle@lka.polizei.niedersachsen.de

PRESSE-Information

Deutlicher Anstieg von Phishing Fällen

Wie kann ich mich schützen?

Gerade in den letzten Wochen werden Bürger in Niedersachsen immer häufiger Opfer von Phishing - Fällen. Das LKA Niedersachsen zählt in diesem Jahr bereits über 600 Fälle. Im gesamten letzten Jahr waren es ca. 1000 Fälle.

Wie gehen die Täter vor?
Den Betrügern gelingt es mit Hilfe von sog. Trojaner sich in den Kommunikationsweg zwischen Bankkunde und Bank zwischenzuschalten und Daten abzugreifen. Die Schwachstelle ist in den meisten Fällen der Internet-Browser. Ruft der Bankkunde die Internetseite seiner Bank auf, so erhält er – bedingt durch den Trojaner – gefälschte Mitteilungen, die den optischen und inhaltlichen Eindruck vermitteln, von der eigenen Bank zu stammen. Diese Fenster „poppen“ auf und legen sich über das normale Browserfenster. Ein Wegklicken ist oft nicht möglich. In diesem Popup-Fenster kommen Mitteilungen zu angeblichen Fehlern beim Online - Banking, zu Testteilnahmen oder zu falschen Überweisung, die eine Rücküberweisung nötig machen.

Folgt der Kunde dann den Anweisungen, kann dies schwerwiegende Folgen haben. Die Täter erfragen z. B. zu einer angeblichen "Fehlerbehebung" Zugangsdaten und/oder überweisungsrelevante Daten (z.B. TAN). Mit diesen werden dann manipulierte Überweisungen im Sinne der Täter durchgeführt, von denen der Bankkunde vorerst nichts bemerkt. Möchte der Bankkunde im Anschluss seine Überweisung oder den Kontostand kontrollieren, kann es passieren, dass die Täter durch die Schadsoftware den Browser oder Computer abstürzen lassen, um die Kontrolle zu verhindern.

Weitere typische Beispiele für das Vorgehen der Täter sind u. a. die „Rücküberweisung“, „Phishingmails“ aber auch eine sog. „Testüberweisung“. Eine detaillierte Erläuterung finden sie unter:

http://www.polizei-praevention.de/aktuelles/aktuelles-detailansicht/onlinebanking-weiter-stark-in-gefahr.html

Wie kann ich mich schützen?

- Halten Sie Ihr Betriebssystem immer auf einem aktuellen Stand. Dies gilt auch für zusätzliche Software (besonders für Internetbrowser und PDF-Reader, Adobe Flash - Player usw.).

- Nutzen Sie eine aktuelle Antivirensoftware mit einer Firewall. Wir empfehlen hier die Anschaffung kostenpflichtiger Software, da diese in der Regel einen umfassenderen Schutz bietet als kostenfreie Software. Nutzen Sie regelmäßig auch den Dienst des EU-Cleaners, den Sie auf www.botfrei.de bekommen können.

- Folgen Sie keinen Links aus Emails, die angeblich von Ihrer Bank stammen soll! Öffnen Sie auch keine Anhänge aus den Emails.

  Banken, Sparkassen und andere Kreditinstitute verschicken solche Emails nicht. Führen Sie im Zweifelsfall eine Kontrolle der Behauptungen durch, indem Sie sich über den Originallink einloggen und dort die z.B. angebliche "Sperrung" nachvollziehen. Alternativ können Sie auch bei Ihrer Bank direkt nachfragen.

Weitere wichtige Informationen finden Sie auf unserem „Ratgeber Internetkriminalität“
http://www.polizei-praevention.de/aktuelles/aktuelles-detailansicht/onlinebanking-weiter-stark-in-gefahr.html

Welche Banken sind betroffen?

In der Regel kann jede Bank betroffen sein, die Online - Banking über ein Web-Portal, also mittels Zugriff über Internetbrowser, betreibt. Vermehrt sind aber Phishingmails zu verzeichnen, die Banken vortäuschen, die deutschlandweit einen einheitlichen Auftritt haben (z.B. Postbank, IngDIBA usw.). Banken mit lokalem Bezug kontaktieren Ihre Kunden auch immer lokal und haben in der Regel auch einen lokalen Internetauftritt (z.B. Sparkassen und Volksbanken). Hier ist der Kundenstamm im Vergleich zu den landesweiten einheitlichen Banken eher gering. Die Trefferquote für die Täter wäre somit geringer und weniger erfolgversprechend.

Nadine Bunzler / Frank Federau
Pressestelle im LKA NI