Sicherheitstipps

Thema: Internet

LKA-RP: Schützen Sie sich vor Passwort-Klau im Internet!

Mainz (ots) - Die Methoden der Passwort-Phisher werden immer subtiler.

Straftäter versuchen nicht nur mittels massenhaft versandter Phishing-Mails ("Password harvesting" aus "Ph" wurde sprachlich ein "F" und der Begriff "fishing", d.h. Abfischen von Passwörtern wurde geschaffen) im Internet an sensible Zugangsdaten von Nutzern und somit an das Geld dieser zu gelangen.
Vielmehr richten sich die Phishing-Attacken auch gegen Online-Banking-Nutzer zum Ausspähen von Zugangscodes, den so genannten PIN/TAN-Nummern. Fingierte Aufforderungen der vermeintlichen Hausbank die PIN und TAN wegen technischen Überprüfungen per eMail zu versenden, sind häufige Methoden der Straftäter. Grundsätzlich können aber bei allen Dienstleistungen im Internet, bei denen der Zugang über einen Benutzernamen und ein Passwort erfolgt (z.B. Auktionshäuser, eMail-Konto, etc.), die Zugangsdaten ausgespäht werden.

Eine andere Methode ist technischer Natur. Hierbei werden versteckt auf nicht ausreichend geschützte PC "Trojaner" installiert, die die eingegebene PIN- und TAN-Nummern nicht an die Bank, sondern an die Betrüger weiterleiten.

Die Transaktion des Geldes durch den Phisher erfolgt oftmals nicht direkt auf dessen Konto im Ausland, sondern zur Verschleierung werden die Gelder zunächst auf ein (deutsches) Konto eines "Finanzagenten" überwiesen. Dieser "Finanzagent" wird in zeitlichem Zusammenhang über das Internet angeworben und soll über sein Privatkonto den angeblichen Zahlungsverkehr für eine Firma gegen eine Provision von 5 bis 12 Prozent abwickeln. Die Tätigkeit des "Finanzagenten" ist nach dem deutschen Kreditwesengesetz anmelde- und erlaubnispflichtig. Ein Verstoß stellt eine Straftat dar. Insoweit haftet der "Finanzagent" gegenüber den geschädigten Bankkunden, auch wenn er glaubhaft versichert, den Betrug nicht erkannt zu haben. In Rheinland-Pfalz wurden die ersten "Finanzagenten" bereits wegen Geldwäsche verurteilt.

Sie können das Risiko, Opfer einer Phishing-Attacke zu werden, wesentlich reduzieren, wenn Sie folgende Verhaltenstipps/Hinweise beachten:

- Öffnen Sie keine eMails von unbekannten Absendern und klicken Sie nicht auf darin enthaltene Links. Löschen Sie diese Mails ungelesen.

- Ihre Bank wird niemals von Ihnen vertrauliche Daten (Konto-Nr., PIN, TAN, Telefonbanking-TAN) per eMail/Link abfragen.

- Bei Kontaktaufnahme mit Ihrer Bank geben Sie stets die Internet-Adresse direkt in der Adressleiste Ihres Browsers ein und achten Sie beim Online-Banking auf eine gesicherte Verbindung (erkennbar an der Adresszeile, beginnend mit https://...).

- Verwenden Sie ein Virenschutzprogramm sowie eine Firewall.

- Halten Sie zudem das von Ihnen verwendete Betriebssystem und die Internet-

Zugangssoftware (z.B. Internet-Explorer, Firefox, Opera, etc.) stets auf dem aktuellen Stand.

- Seien Sie misstrauisch. Sollten Sie während des Online-Banking-Vorganges Unregelmäßigkeiten feststellen, brechen Sie diesen sofort ab und informieren Sie unverzüglich Ihre Bank.

- Kontrollieren Sie regelmäßig Ihre Buchungsumsätze online.

- Lassen Sie sich nicht als "Finanzagent" via Internet anwerben; es droht eine Strafanzeige und eine Verurteilung wegen Geldwäsche.

Sollten Sie dennoch eine Abbuchung auf Grund einer Phishing-Attacke vermuten, ist schnelles Handeln geboten.

- Nehmen Sie unverzüglich Kontakt zu ihrer Bank auf und lassen Sie den Vorgang überprüfen. Von dort können bei Bestätigung des Verdachtes weitere Maßnahmen ergriffen werden.

- Erstatten Sie in diesen Fällen Anzeige bei Ihrer örtlich zuständigen Polizeidienststelle.

Weitere Informationen finden Sie im Internet unter **www.polizei-beratung.de** .