POLIZEI Hamburg

WIR INFORMIEREN :

Achtung: Betrügerische SMS

In einer SMS wird der Eindruck erweckt, der Empfänger hätte ein Paket bestellt und könne sich nun den Lieferstatus anzeigen lassen.

Hierbei versuchen bisher unbekannte Täter, die Empfänger dieser SMS dazu zu bringen, den in der Nachricht enthaltenen Link (Verweis auf eine Internetadresse) zu öffnen. Durch das Öffnen des Links gelangen Sie auf Internetseiten, auf welchen unter einem Vorwand personenbezogene Daten (z.B. Kredit-, Bank- oder Postdaten) abgefragt werden. Alternativ sollen Sie ggf. auch eine App herunterladen / installieren, über welche angeblich der Sendestatus des Pakets ersichtlich sei.

Bei der App handelt es sich um Schadsoftware, die, je nach Version, z.B. Ihre Kontaktdaten ausliest, eine Vielzahl gleichlautender SMS versendet oder dazu beiträgt, in Abläufe Ihres Onlinebankings eingreifen zu können. Während die SMS in den meisten Fällen den Wortlaut „Ihr Paket wurde verschickt...“aufweisen, variieren die enthaltenen Links und enthalten unter anderem die Domains “http://...duckdns.org/...”, “http://...tinyurl.com/...” oder “http://...shortrl.at/...”

Nach Installation der App versendet die Schadsoftware unter Ihrer Mobilfunknummer gleichlautende SMS an zuvor bereits erlangte oder zufällig generierte Mobilfunknummern. Wie in Ihrem Fall, dürfte es sich somit bei dem Absender der ggf. an Sie gerichteten SMS ebenfalls um ein Opfer einer Straftat und nicht um „den Täter“ handeln.

Was können Sie tun?

- Links, die Sie nicht angefordert haben, sollten Sie nie öffnen. Stammt die Nachricht von einem bekannten Absender, sollten Sie ggf. zuvor dort nachfragen.
- Installieren Sie Apps nach Möglichkeit nur aus „offiziellen“ Quellen (Google Playstore bzw. Apple App store). Insbesondere sollten sie bei Android die Möglichkeit unbekannte Apps zu installieren nicht aktiveren oder -falls sie dieses bereits getan haben- dieses wieder deaktivieren.
- Derzeit ist davon auszugehen, dass ein Schaden mindestens das Öffnen des Links, vermutlich aber auch die Installation der App voraussetzt.
- Haben Sie den Link geöffnet und ggf. auch der Installation einer App zugestimmt, sollten Sie das Gerät sofort vom Netz trennen / in den Flugmodus schalten.
- Um mögliche Schäden gering zu halten, informieren Sie Ihren Mobilfunkprovider und lassen Sie, sofern nicht schon bestehend,dort auch eine kostenlose Drittanbietersperre einrichten. Im Fall einer Installation der App sollten Sie darüber hinaus auch Ihre Bank in Kenntnis setzen und sich dort ergänzend beraten lassen.
- Um Ihr Mobilfunkgerät von der Schadsoftware zu befreien, reicht das Deinstallieren der App ggf. nicht aus. Wir empfehlen deshalb, setzen Sie Ihr Gerät in den Auslieferungszustandzurück. Bitte beachten Sie, dass dadurch auch alle anderen Daten gelöscht werden.

Ihre Polizei Hamburg