ACHTUNG #SMISHING!

Falsche SMS enthält Link mit Schadsoftware

Mitte April 2021 flutet eine wahre Smishing-Welle viele Smartphones: Handy-Nutzer erhalten SMS-Nachrichten mit einer vermeintlichen Paketbenachrichtigungen. **Betroffen sind gleichermaßen Android-, als auch Apple iOS-Nutzer.**

SMISHING steht für die Kombination aus SMS und Phishing, also gefakte SMS-Benachrichtigungen. Dahinter stecken Betrüger, die versuchen, Schadsoftware (Phishing-Programme) auf Handys zu installieren und Daten abzugreifen.

Das Wichtigste vorab: Egal, ob Sie tatsächlich ein Paket erwarten oder nicht - klicken Sie NICHT auf den Link in diesen SMS.

- **Android-Nutzer** werden über den Link vor allem zum Download der (schädlichen) FluBot-App aufgefordert, perfekt getarnt als eine für die Paketverfolgung angeblich notwendige App von bekannten Logistikunternehmen wie FedEx oder DHL.

- **Auf einem iPhone** kann sich die Schadsoftware FluBot in der Regel nicht einnisten. Klicken Apple iOS-Nutzer auf den Link, landen sie in der Regel auf Werbe- oder Phishing-Seiten, auf denen sie dann sensible Informationen preisgeben sollen.

Hinter FluBot steckt ein (Bank-)Trojaner, der versucht, Zugangsdaten abzufischen und an Login-Daten und Tan-Nummern zu kommen. Die App ist in der Lage, das Aufrufen von Apps und Browserdaten zu verfolgen und Gesprächsdaten und SMS zu protokollieren. Zudem kann FluBot die vollständige Kontrolle über das betroffene Smartphone übernehmen.

Ist eine Schadsoftware erst einmal auf Ihrem Handy installiert, greifen Cyberkriminelle im Hintergrund Ihre persönlichen Daten ab. Zudem verbreitet sich die Schadsoftware durch ein Schneeballsystem über Ihre eigene Nummer weiter an sämtliche Kontakte auf dem Handy.

Der Wortlaut der Paketbenachrichtigung-SMS ist häufig:

- Ihr Paket wurde verschickt. Bitte überprüfen und akzeptieren Sie es: (Link)
- Ihre Bestellung ist unterwegs. Klicken Sie auf folgenden Link, um die Sendungsverfolgung zu öffnen.
- Hallo Name (xxx) Ihr Paket ist da. Letzte Chance es abzuholen. (Link)
- Hallo, ihr Paket steht noch aus. Bestätigen Sie ihre Angabe hier (Link)
- Ihre Bestellung bei Amazon Prime Now trifft bald bei Ihnen ein. Sendung jetzt nachverfolgen (Link)
- Ihre Sendung geht soeben in Zustellung, verfolgen Sie ihre Sendung unter (Link)

Meist ist diese SMS sehr schlicht gehalten. Besonders trickreich: Die Absendernummern wirken eher harmlos (beginnen beispielsweise mit 0176, 0160 oder 0179) und werden mit Rufnummern von gängigen deutschen Mobilfunknummern gesendet.

Was Sie tun sollten:

- Klicken Sie den Link in der SMS NICHT an!
- Blockieren Sie die Rufnummer des Absenders.
- Sollte Ihnen der Absender oder die Absenderin bekannt sein, können Sie ihn oder sie anrufen und nach der Richtigkeit der SMS fragen bzw. auf das Versenden der (ungewollten) SMS aufmerksam machen.
- Installieren Sie keine Apps aus unbekannten Quellen auf dem Handy. Gerade bei Android-Geräten ist es generell möglich, Apps zu installieren, die nicht im Play Store zu finden sind. Diese Einstellung sollten Sie deaktivieren: Suchen sie dafür unter „Einstellungen“ nach „unbekannte Apps installieren“ oder „Apps aus unbekannten Quellen“ und entfernen Sie dort die entsprechenden Berechtigungen.
- Lassen Sie am besten bei Ihrem Mobilfunkanbieter eine Drittanbietersperre aktivieren. Diese Sperren können kostenlos gebucht werden.
- Die Installation eines Antivirenprogrammes kann ebenfalls hilfreich sein.
- Löschen Sie die SMS (zur Sicherheit vorher einen Screenshot für Beweiszwecke anfertigen).
- IPhone-Besitzern wird zu einem Update des Betriebssystems auf mindestens Version iOS 14.4.2 geraten.
- Android erhält Sicherheitsupdates für die Systeme 8.1, 9, 10 und 11.
- Grundsätzlich hilft eine regelmäßige Datensicherung auf Ihrem Handy, Daten - zum Beispiel nach Zurücksetzen des Handys auf Werkseinstellung – wiederherzustellen.

Was Sie tun sollten, wenn Sie den Link schon angeklickt haben und die Schadsoftware bereits installiert ist:

- Stellen Sie das Smartphone in den Flugmodus (oder schalten Sie es aus).
- Informieren Sie Ihren Mobilfunkprovider und lassen Sie eine Drittanbietersperre einrichten.
- Prüfen Sie über Ihr Benutzerkonto oder Ihr Bankkonto, ob bereits Kosten entstanden sind.
- Erstatten Sie Strafanzeige bei der Polizei. Dazu das Smartphone und auch Screenshots mitbringen.
- Starten Sie das Smartphone nur im abgesicherten Modus und prüfen Sie, welche Apps zuletzt oder nicht bewusst installiert wurden. Entfernen Sie diese Apps und starten Sie das Smartphone neu.
- Setzen Sie Ihr Smartphone auf Werkseinstellungen zurück (nachdem Sie Anzeige erstattet haben). Sichern Sie vorher alle wichtigen Daten wie Fotos, Dokumente usw. lokal (zum Beispiel über eine USB-Verbindung). Denn mit dem Zurücksetzen auf die Werkseinstellungen gehen alle gespeicherten und installierten Daten verloren. Dieser Schritt ist allerdings notwendig, um die über die aktuellen SMS-Spam-Nachrichten verteilten Android-Schadprogramme vollständig zu entfernen

Sie haben noch Fragen oder sind betroffen? Unsere Sicherheitsexperten helfen Ihnen gerne