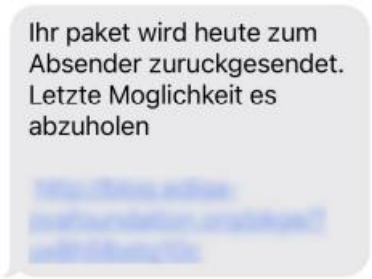
ALLES ZUM SMISHING

Seit Monaten erhalten Nutzerinnen und Nutzer von Smartphones und Handys SMS-Nachrichten, die zum Klicken eines Links auffordern. Es handelt sich dabei um das sogenannte „Smishing“ – eine Wortschöpfung aus den Begriffen SMS (Kurznachrichten) und Phishing (Diebstahl von Zugangsdaten über gefälschte Nachrichten oder E-Mails).

Im Frühjahr 2021 gaben die Täter häufig vor, dass die Empfängerinnen und Empfänger der SMS bald ein Paket erhalten oder eine Sendung zurück an die Absenderin beziehungsweise den Absender gehen soll. In einigen der SMS-Texte ist sogar eine persönliche Anrede zu beobachten.



Android-Nutzerinnen und -Nutzer bekommen über den Link in der SMS-Nachricht den Download einer App angeboten. Diese löst allerdings keines der vorgetäuschten Probleme, sondern späht lokale Adressdaten aus, verbreitet weitere schadhafte SMS-Nachrichten und führt Phishing-Angriffe durch. Dabei tarnen die Kriminellen die Schadsoftware z. B. als eine für die Paketverfolgung angeblich notwendige App von bekannten Logistikunternehmen wie FedEx oder DHL. Apple iOS-Anwenderinnen und -Anwender landen in der Regel auf Werbe- oder Phishing-Seiten.

Seit Herbst 2021 greifen die Täter seltener auf gefälschte Paketbenachrichtigungen zurück. Stattdessen teilen sie den Empfängerinnen und Empfängern der SMS zum Beispiel mit, dass eine Sprachnachricht (engl. „Voicemail“) vorläge oder das Smartphone mit einem Schadprogramm infiziert sei. Hinter dem Link aus der Mitteilung befindet sich dann eine Anleitung zum Download der Sprachnachricht bzw. eines angeblichen Sicherheitsupdates. Erst wer diese Dateien herunterlädt, installiert die Schadsoftware der Betrüger.

Daneben fallen Smishing-SMS auf, in denen den Empfängerinnen und Empfängern vorgetäuscht wird, dass ihre privaten Fotos geleakt wurden, weil sich eine Schadsoftware auf dem Handy befinden soll. Damit üben die Täter Druck aus und versuchen so, die Smartphone-Nutzerinnen und -Nutzer ebenfalls dazu zu bewegen, ein vermeintliches Sicherheitsupdate zu installieren. Auch in diesem Fall führt der Download zur Infektion des Systems.

Zwar haben die deutschen Provider Filtermaßnahmen ergriffen, um den Versand von Smishing-SMS zu unterbinden, jedoch können diese keinen vollständigen Schutz bieten, da die Täter ständig gegensteuern. So wird seit kurzem beobachtet, dass die Nachrichten manchmal absichtliche Buchstabendreher, Schreibfehler oder zufällige Zeichenketten enthalten, um die Spam-Filter der Mobilfunkbetreiber zu umgehen.

All diese SMS-Nachrichten haben gemein, dass Sie einen Link enthalten. Dieser Link leitet direkt zu Schadsoftware oder zu Phishing-Seiten, auf denen Sie dann sensible Informationen preisgeben sollen. Sofern Sie noch NICHT auf den Link geklickt haben, rät das BSI:

- Klicken Sie nicht auf den Link und löschen Sie die Nachricht umgehend nach Erhalt. Sollte Ihnen der Absender oder die Absenderin bekannt sein, rufen Sie ihn oder sie zum Beispiel an und fragen Sie nach der Richtigkeit der SMS.

- Sperren Sie über Ihr Betriebssystem die Absenderin beziehungsweise den Absender der Nachricht.
- Laden Sie Apps nur aus den bekannten Stores herunter und nicht aus externen Quellen. Deaktivieren Sie unter Android die Installation von Apps aus unbekannten Quellen. Suchen Sie dafür in den Einstellungen nach „Apps aus unbekannten Quellen“ oder „Unbekannte Apps installieren“ und entfernen Sie dort den Haken.
- Egal ob Android oder iOS: **Aktualisieren Sie Ihr Gerät!** IOS liegt momentan in der Version 15.0.2 vor. Android erhält Sicherheitsupdates für die Systeme 8.1, 9, 10 und 11. **Tipps für einen wirksamen Basisschutz** finden Sie auf unseren weiteren Webseiten.
- Sie können bei Ihrem Mobilfunkanbieter die Drittanbietersperre aktivieren lassen. Dadurch lassen sich versehentliche Kosten oder eventuelle Kosten durch Schadsoftware weitestgehend vermeiden. Hinweise zur Umsetzung erhalten Sie über die Informationsangebote beziehungsweise Service-Portale ihres Mobilfunkproviders.

Sollten Sie schon einen Link angeklickt oder sogar schon Software installiert haben, empfiehlt das BSI darüber hinaus:

- Nehmen Sie Ihr Gerät aus dem Mobilfunknetz, indem Sie den Flugmodus aktivieren. Damit unterbinden Sie weiteren SMS-Versand und eine eventuelle Kommunikation von Android-Schadsoftware mit anderen Geräten.
- Informieren Sie Ihren Mobilfunkprovider über Ihren Fall.
- Prüfen Sie beispielsweise Ihr Bankkonto oder Ihren Zahlungsdienstleister auf Abbuchungen, die Sie nicht beabsichtigt haben.
- Auch in diesem Fall ist es ratsam, eine Drittanbietersperre einrichten zu lassen. Hier hilft Ihr Mobilfunkanbieter weiter.
- Erstatten Sie Strafanzeige bei der örtlichen Polizeidienststelle. Nehmen Sie dazu Ihr Smartphone zur Beweissicherung mit.
- 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). 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.