Stand 07.05.2021

Handlungsempfehlungen im Zusammenhang mit der aktuell andauernden SMS-Betrugswelle

Herausgeber: Seitz & Co. Industrieservice GmbH. Quellen: online Recherche, Expertengespräche. (www.seitz-co.de/Downloads/Handlungsempfehlung-SMS-Betrug.pdf).

Es werden vermeintliche SMS Benachrichtigungen im Namen von Paketlieferanten aber auch im Namen von anderen Privatunternehmen vermehrt versendet. Diese haben unterschiedliche Aufbauweisen, Signaturen und Rufnummern und haben meistens, aber nicht immer, einen Link zur Nachverfolgung einer Paketlieferung beigefügt.

Vermeintliche Absender können namentlich auch aus dem Bekannten und Freundeskreisen sein, sowie auch die Absenderrufnummern. Die Anrede erfolgt direkt oder indirekt.

Empfehlung der Vorgehensweiße bei SMS Empfang (und E-Mail)

Erhalten Sie eine Nachricht von einer unbekannten Nummer oder eine unerwartete Nachricht oder eine Nachricht mit unseriösen Aufbau, ist diese umgehend zu löschen und nicht zu öffnen.

Die Natur einer Nachricht lässt sich meistens bereits in den ersten Zeilen erkennen. Im Zweifelsfall den Absender über eine bereits bekannte oder eigen recherchierte Rufnummer kontaktieren und nachfragen.

Klicken Sie nie direkt auf einen beigefügten Link. Kann die Nachricht korrekt sein, sollte der Link kopiert werden und in einer online Suchmaschine, modifiziert mit z.B. einen zusätzlichen Buchstaben *G* vorweg, eingegeben werden. Sind Sicherheitsrisiken zu der zielführenden Webseite bekannt, erscheinen meistens hierzu entsprechende Ergebnisse in der Suche. Alternativ kann der Link auch auf Webseiten von führenden Antivirenherstellern eingebeben werden, diese bieten eine Prüfung auf schädliche Links an. (Zwecks Datenschutz sollte hier keine Prüfung von Links mit personenbezogenen Daten oder von Cloud-share Speichern o.ä. eingegeben werden)

Vorbeugemaßnahmen

- **Keine Nutzung von Lieferbestätigung via SMS** (besser via Mail);
- SMS – Whitelisting auf dem Gerät einrichten (nur SMS von Telefonbuchkontakten werden zugestellt);
- SMS Funktion (beim Provider) deaktivieren;
- **Sperrung von Mehrwertdiensten und Drittanbieter** (Provider);
- Bekanntmachung der Gefahren im Bekannten- und Freundeskreis;
- **Deaktivieren von Sideload** (Installation von Apps aus unbekannten Quellen);
- Keinen Internetbrowser auf dem Gerät installieren.

Risiken

- Je nach Einstellung eines Smartphones können Nachrichten bereits beim Eintreffen automatisch geöffnet werden, in diesem Szenario kann man sich, je nach Version und Sicherheitsstand des Betriebssystems, vor einer Infektion nicht mehr schützen;
- Je nach Einstellung eines Smartphones werden Nachrichten auf dem Sperrbildschirm angezeigt. Wird diese ausversehen angeklickt oder anstatt nach links, nach rechts gewischt ((je nach Konfiguration wird zur einen Seite die Nachricht geöffnet oder geschlossen/gelöscht) z.B. kann das Smartphone die Wischgeste fehlinterpretieren, wenn sich Schmutz oder Flüssigkeit auf dem Bildschirm oder der Hand befindet) kann eine Infizierung des Gerätes erfolgen, wenn die Sicherheitsfunktionen des Betriebssystems dies nicht mehr verhindern kann;
- Es sind Malwarevarianten bekannt, welche unter bestimmten Bedingungen bereits beim Öffnen der SMS das Gerät infizieren können;
- Wurde die Fake-SMS geöffnet (und der Link angeklickt), wird eine Spyware auf das Smartphone geladen. Diese baut nach aktuellem Stand eine Verbindung zu einem Control-Server in Asien auf, welcher dann weitere Schadsoftware auf das Gerät laden kann;
- Die Absichten der Angriffe sind
    - das Abgreifen von persönlichen Daten für gewerbsmäßigen Datenhandel wie z.B. (bei Hacking) von Socialmedia Anbietern und Betreibung von Profiling;
    - Kosten verursachen durch SMS Versand an Sonderrufnummern und Mehrwertdienste oder ausländische Rufnummern;
    - Nutzung des Gerätes in einem Bot Netz zum Weiterverbreiten von Schadsoftware;
    - Kompromittieren von Transaktionsdaten zum Erschleichen eines Kontozugangs.

Indizien einer Infektion

- Die Telefonie und Internetfunktion wurde durch den Provider deaktiviert;
- Sie erhalten Anrufe von fremden Personen (die ggf. von ihrer Rufnummer ein SMS zu einer Paketzustellung erhalten haben);
- Es sind unbekannte Apps installiert (z.B. DHL.apk);
- Im Downloadordner befinden sich Installationsdateien (.apk).

Maßnahmen nach einer Infektion

- Gerät in den Flugmodus;
- Gerät ausschalten und nur noch im abgesicherten Modus starten;
- Beweissicherung (Bilder von SMS / App / Anrufverlauf)
- Datensicherung einzelner Daten (Bilder, Chatverlauf, Kontakte). Kein volles Backup, da ansonsten der Virus mitgesichert wird;
- **Gerät auf Werkseinstellungen zurücksetzen** und somit alle Daten löschen, da sich die Schadsoftware im Kernel eingenistet hat;
    - Ist für die Rücksetzung des Gerätes eine Verbindung mit dem Internet notwendig, sollte vorher manuell die Schadsoftware von dem Gerät deinstalliert werden.
- Alle gespeicherten und somit potenziell gefährdete Kontakte auf dem Gerät umgehend informieren;
- **Zugangsdaten zu allen Konten und Diensten ändern und neu einrichten**;
- **Kennwortänderung auch bei Webanmeldungen (Mailaccount / Online-Banking / etc…)**
- Strafanzeige erstellen (Zwecks Kostenerstattung bei hohen Mobilfunkabrechnungen);
- Datenpanne bei der zuständigen Datenschutzbehörde melden (Meldepflicht).