Betrügerische SMS-Nachrichten im Umlauf

Daten von über 500 Millionen Facebook-Nutzern, die aus einem Datenleck im Jahr 2019 stammen, sind kürzlich wieder im Internet aufgetaucht. Die Daten umfassen neben Namen auch Handynummern, Orte, sowie teilweise Geburtsdaten und Mail-Adressen. Wie sich gerade auch auf meinem Handy zeigt, erhalten betroffene Nutzer aus Deutschland vermehrt SMS-Nachrichten mit gefährlichem Inhalt.
Derzeit handelt es sich oft um gefälschte Paketbenachrichtigungen, die den Handybesitzer auffordern, auf einen Link zu tippen, um zu sehen, wo sich eine angebliche Paketlieferung befindet.

Die Nachrichten, die ich bisher erhalten habe, sind nicht besonders gut gemacht. Erstens sieht man im Absender die Nummer im Klartext und nicht etwa Hinweise auf Paketdienstleister wie DHL oder DPD, außerdem sind die Links oft auf den ersten Blick verdächtig, weil sie auf unübliche Webseiten verweisen. Wer nur schnell drüber liest, kann sich schnell täuschen lassen und erkennt die Fälschung nicht rechtzeitig. Wer so eine SMS erhält, sollte auf keinen Fall den enthaltenden Link antippen und schon gar nicht Bezahldaten oder Passwörter auf danach geöffneten Webseiten eintippen.

Was genau passiert, wenn man doch auf den Link geklickt hat, kann man pauschal nicht sagen. Die Palette an Möglichkeiten ist umfangreich:

- Man kann in einer Abofalle landen.
- Die eingegebenen Zugangsdaten werden eingefangen und von Betrügern verwendet.
- Es wird eine Schadsoftware installiert, die genau die gleichen SMS-Nachrichten an andere Handybesitzer sendet. Hierzu sind Fälle bekannt, in denen über 1000 SMS-Nachrichten unbemerkt versendet wurden. Bei vielen Tarifen kostet jede SMS 0,19€, da verbreitet sich also nicht nur eine gefährliche SMS, sie kostet den Betroffenen auch noch viel Geld.
- Es werden plötzlich Apps installiert, die man gar nicht haben wollte.
  Solange man sie nicht bemerkt,
  - spionieren sie z.B. alles aus, was auf dem Handy eingegeben wird oder
  - die Bilder werden heruntergeladen und auf gefälschten Facebook-Profilen verwendet
  - oder man wird abgehört oder
  - der Aufenthaltsort des Handys wird ständig an die Betrüger übertragen.

Die Abos kann man kündigen, Kreditkarten sperren, die Apps wird man aber oft nicht so einfach los oder man sieht sie erst gar nicht.
In so einem Fall kann man nicht mehr davon ausgehen, das eigene Handy noch sicher benutzen zu können. Unbekannte App-Symbole oder plötzlich auftauchende Werbeanzeigen, die man nicht einfach wegklicken kann, sind dafür bedenkliche Anzeichen.

Die Lösung wäre das Zurückspielen einer Sicherheitskopie des Handys, die so gut wie niemand hat (ich übrigens auch nicht). Also bleibt meistens nur, das Handy in den Lieferzustand zurück zu versetzen und alles neu einzurichten. Dabei geht natürlich einiges an Fotos und netten WhatsApp-Nachrichten verloren, aber die hier geschilderten Alternativen sind schlimmer.

Sozialverband Deutschland
Ortsverband Wathlingen
E-Mail: sovd-wathlingen@t-online.de