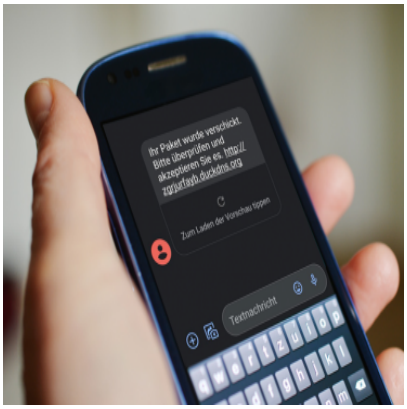

Eine neue Welle massenhafter BetrugsfÃ¤lle: Smishing (SMS-Phishing)

Seit Ostern werden vermehrt SMS (Short Messages) auf Handys geschickt, in der Sie aufgefordert werden, Ã¼ber einen Link Ihre Paketzustellung zu prÃ¼fen bzw. abzurufen.

Die Nachricht erscheint zunÃ¤chst harmlos, da sie Ã¼ber eine Ã¼bliche Mobilnummer versendet wird (0157, 0179, 0177, 0178, 01511 etc.) und vermeintlich von bekannten Dienstleistern wie DHL, UPS oder Fedex stammt, die auch regulÃ¤r auf diesem Wege Nachrichten zu dem aktuellen Versandstatus mitteilen. Erschwerend kommt hinzu, dass der Handynutzer sogar mit Namen angesprochen wird.

Ã?ber den angegebenen Link wird jedoch eine App angeboten, die nach der Installation vertrauliche DatensÃ¤tze an BetrÃ¼ger Ã¼bermittelt, dabei aber durchaus echt erscheint. Auf diesem Wege werden beispielsweise GesprÃ¤chs- und Nachrichteninhalte sowie Login- und Bankdaten abgezogen.

Wurde die Flubot-App erstmal installiert, kann sie nicht so leicht gelÃ¶scht werden. Betroffenen wird empfohlen, das GerÃ¤t auf Flugmodus zu schalten, anschlieÃ?end persÃ¶nliche / relevante Daten zu sichern und danach auf die Werkseinstellungen zurÃ¼ckzusetzen. Sicherheitshalber ist das Bankkonto auf nicht autorisierte Abbuchungen zu prÃ¼fen. Das BSI rÃ¤t zudem, den Mobilfunkanbieter zu benachrichtigen und den Fall bei der Polizei anzuzeigen.

Insbesondere aufgrund der Pandemie werden zurzeit unzÃ¤hlige Artikel versandt, was den BetrÃ¼gern in die HÃ¤nde spielt. Die Kunden mÃ¶chten ihre Sendungen schnell erhalten und geraten oft aufgrund der glaubwÃ¼rdig aussehenden Darstellungen von Icons und SchriftzÃ¼gen schnell in die Falle.

Gestohlene DatensÃ¤tze werden im Internet illegal zum Verkauf angeboten und kÃ¶nnen somit von verschiedenen TÃ¤tern fÃ¼r diverse Zwecke missbraucht werden.

Falls Sie eine verdÃ¤chtige SMS erhalten, sollten Sie diese nicht Ã¶ffnen, sondern umgehend lÃ¶schen. Hinweise auf gefÃ¤lschte Benachrichtigung sind z. B. â??Letzte MÃ¶glichkeit Ihr Paket abzuholenâ?? oder â??Ihr Paket wurde verschickt Bitte Ã¼berprÃ¼fen und akzeptieren Sie es!â??, oder auch ungewÃ¶hnliche Endungen des Links wie tinyurl.com, duckdns.org oder shorturl.at. Zahlungsaufforderungen sind fÃ¼r Sendungsnachverfolgungsnachrichten generell unÃ¼blich.

Titelbild:
www.pixabay.com â?? Freie kommerzielle Nutzung

Uwe Gerstenberg
04/16/2021