23.02.2022

Kriminelle wollen an Ihre SIM-Karte und dann an Ihr Bankkonto

Hacker stehlen oder kopieren SIM-Karten und missbrauchen sie, um sich Zugang zu Apps und Bankdaten zu verschaffen. Der Angriff beginnt meistens mit einer Phishing-Nachricht.

68 Millionen US-Dollar haben Betrüger in den USA mit dem sogenannten SIM-Swapping ergaunert. Dabei entwenden oder kopieren die Kriminellen die SIM-Karte ihrer Opfer und verwenden sie, um sich Zugang zu Apps und Bankdaten zu erschleichen (Quelle: Heise Security, 20 Minuten).

Auch in der Schweiz sind Fälle von SIM-Swapping bekannt, wenn auch vergleichsweise wenige. Der initiale Angriff geschieht in den meisten Fällen mittels Phishing (https://www.ebas.ch/phishing) -Mails, -SMS- oder Messenger-Nachrichten, welche einen Link auf eine gefälschte Website enthalten, die vom Angreifer betrieben wird. Dort soll der unwissende Anwender seine Mobilfunk-Angaben und/oder Zugangsdaten zu einem bestimmten Online-Dienst oder E-Banking angeben. Teilweise werden Zugangsdaten auch über Datenlecks im grossen Stil (z.B. im Darknet angeboten) gekauft.

Da E-Banking-Portale und andere Online-Dienste immer häufiger Zwei- oder Mehr-Faktor-Authentifikation (2FA, MFA) einsetzen, benötigt ein Angreifer einerseits Benutzername oder Vertragsnummer und Passwort sowie anderseits eine gestohlene oder beim Mobilfunkanbieter nachbestellte SIM-Karte, um den zweiten Sicherheitsfaktor abfangen und verwenden zu können. Die gestohlenen oder anderweitig erworbenen Daten und SIM-Karten werden von den Betrügern dann verwendet, um sich unrechtmässig Zutritt zum jeweiligen E-Banking-Portal oder Online-Dienst zu verschaffen.

Schützen Sie sich, indem Sie...

- nie einen Link verwenden, der per E-Mail, SMS oder Messenger-Dienst zugeschickt oder per QR-Code eingescannt wurde, um sich bei einem Finanzinstitut oder Online-Dienst anzumelden.
- nie Formulare ausfüllen, die per E-Mail zugestellt wurden und zur Eingabe von Anmeldeinformationen auffordern.
- Anhänge von E-Mails und Kurznachrichtendiensten mit grosser Vorsicht behandeln.
- in Telefongesprächen nie vertrauliche Informationen, wie z.B. Passwörter, preisgeben.
- die Adresse zur Anmeldeseite Ihres Online-Dienstleisters oder Finanzinstituts immer manuell in die Adresszeile Ihres Browsers eingeben.
- beim Aufruf der Anmeldeseite die SSL-Verbindung (https://, Schlosssymbol) überprüfen und sich durch die Kontrolle der Internetadresse in der Adresszeile Ihres Browsers vergewissern, dass Sie sich am richtigen Ziel befinden.
- ihr Mobilgerät nicht aus den Augen lassen und Gerät sowie SIM-Karte bei Verlust oder Diebstahl sofort sperren lassen.
- sich bei Unsicherheit oder Unklarheit an das Finanzinstitut wenden.

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik