

23. August 2019

Gefährliches Online-Banking via Smartphone

Circa 10.000 Attacken mit Schadprogrammen, sogenannter Finanz-Malware, wurden in der ersten Jahreshälfte dokumentiert. Dabei versuchen die Angreifer, Zugangsdaten zum Online-Banking, Konto- und Kreditkartennummern und inzwischen sogar Kryptowährungen wie Bitcoin abzugreifen. Die Angriffe richten sich auf Bankkunden aber auch auf die Banken selbst. In einem aktuellen Fall waren plötzlich die persönlichen Daten von rund 90.000 Mastercard-Kunden online zugänglich, u. a. die E-Mail-Adressen der Nutzer. Die werden von den Angreifern gerne genutzt, um gefälschte, für den Nutzer sehr gefährliche E-Mails zu verschicken, sogenannte Phishing-Mails.

Die Gefahr von Phishing-Mails

Solche Phishing-Mails wirken meistens täuschend echt. Ihr Ziel: Die Bankkunden sollen ihre Zugangsdaten bzw. PIN preisgeben. Dabei gelangen häufig schädliche E-Mail-Anhänge, z. B. vermeintliche Rechnungen, auf das Smartphone. Auch über eigens dafür programmierte, frei verfügbare Apps greifen die Cyberkriminellen inzwischen Daten der Smartphone-Nutzer ab. In der ersten Jahreshälfte 2019 gab es Berichten zufolge außerdem 339.000 Phishing-Versuche anhand gefälschter Webseiten, die aussehen wie die Startseiten großer Finanzinstitute.

Meistens betroffen: Android-Smartphones

Besonders häufig trifft es scheinbar Nutzer des Google-Betriebssystems Android. Das kann zum einen daran liegen, dass Android-Geräte einen großen Marktanteil besetzen, aber auch daran, dass das Android-Betriebssystem im Vergleich zur Apple-Software offener gestaltet ist. Externe Entwickler haben es leichter, eigene Apps zu programmieren und Android-Nutzern Anwendungen anzubieten, die nicht zum offiziellen App-Store gehören. Berichten zufolge hat Google kürzlich erst zahlreiche Apps mit Schadsoftware aus dem Verkehr gezogen.

Wichtige Sicherheitsmaßnahmen

Laut einer Umfrage des IT-Branchenverbands Bitkom aus dem Jahr 2018 nutzen lediglich 40 Prozent der Befragten ein Antivirenprogramm auf ihrem Smartphone. Und das obwohl damit immer häufiger Bankgeschäfte erledigt werden: Mehr als die Hälfte der Online-Banking-Nutzer wickelt Bankgeschäfte per Smartphone ab.

Um die Sicherheit beim Online-Banking via Smartphone zu erhöhen, sollten die Nutzer regelmäßig Sicherheitsupdates installieren, keine Software oder Anhänge von unbekanntem Quellen öffnen und einen Virenschutz installieren.

Smartphone-Nutzer sollten sich darüber hinaus vor öffentlichen WLAN-Netzwerken in Acht nehmen und diese keinesfalls fürs Online-Banking nutzen. Auch kostenlose Apps sind stets mit Vorsicht zu genießen, vor allem wenn sie Zugriff auf Daten erfordern, die nichts mit ihrem eigentlichen Zweck zu tun haben. Am besten nutzt man fürs Online-Banking die Zwei-Faktor-Authentifizierung. So bietet laut Experten der Tan-Generator als Ergänzung zur Banking-App die größte Sicherheit.

Sollten Sie aber dennoch das Opfer einer Cyber-Attacke werden, stehe ich Ihnen als Fachanwalt für Bank- und Kapitalmarktrecht zur Seite. Nutzen Sie die kostenlose Erstberatung, um Ihren Fall zu besprechen.



Guido Lenné

Rechtsanwalt aus der Anwaltskanzlei Lenné.

Rechtsanwalt Lenné ist auch Fachanwalt für Bank- und Kapitalmarktrecht.

Wir helfen Ihnen gerne! [Kontaktieren](#) Sie uns. Oder vereinbaren Sie [hier online einen Termin](#) für eine telefonische kostenfreie Erstberatung.