Aktuelle Phishingmasche bei VR-Banken: Vermeintliche "Microsoft-Mitarbeiter" kontaktieren Kunden

Innerhalb weniger Tage wurde uns von mehreren Banken gemeldet, dass Bankkunden von angeblichen Microsoft-Mitarbeitern kontaktiert wurden. In diesem Zusammenhang gab es auch Betrugsversuche im Online-Banking.

Die Vorgehensweise unterscheidet sich von Fall zu Fall, teilweise liegen uns entsprechende Informationen nicht vor:

- In einem der Fälle rief ein angeblicher Mitarbeiter von Microsoft unterschiedliche Kunden einer Bank an und forderte diese auf, sofort ein "Sicherheitsupdate" auf dem Computer durchzuführen. Anschließend wurde den Kunden beim Einloggen ins Online-Banking die bekannte Phishingmethode "Rücküberweisung" eingeblendet.

- In einem weiteren Fall griff der angebliche Microsoft-Mitarbeiter direkt per Fernzugriff auf den Rechner des Kunden zu (der Kunde hat diesem Zugriff auf den Rechner aktiv zugestimmt). Hierbei wurde ebenfalls eine missbräuchliche Überweisung durchgeführt. Der Anruf erfolgte nach unseren Informationen aus den USA, die Überweisung des Betrags auf ein Konto in Indien wurde als "Service-Auftrag" angestoßen. Eine erfolgreiche Überweisung wurde jedoch durch den Kunden bei der Bank gestoppt.

Gemeinsam ist den Fällen der direkte telefonische Kontakt zu den Kunden sowie der Vorwand, dass sich ein Mitarbeiter von Microsoft melde. Die Betrüger verleiten die Kunden anschließend zu Aktionen, welche missbräuchliche Abbuchungen oder Überweisungen von Konten der Kunden ermöglichen.

Es ist damit zu rechnen, dass weitere, diesem Vorgehen ähnelnde Maschen auftreten. In der Vergangenheit haben sich Betrüger, die Kunden telefonisch kontaktiert haben, auch z. B. bereits als Bankmitarbeiter ausgegeben.

Vergleichbare Anrufe, auch im Namen anderer Firmen, gab und gibt es immer wieder. Meist ist das Ziel, einen Rechner zu kompromittieren, d. h. Malware zu installieren (vgl. z. B. die Meldung "Abzock-Anrufer geben sich als Microsoft-Techniker aus" aus dem Jahr 2012 bei heise online).

Quelle: intern