

Betrug durch angebliche Microsoft-Mitarbeitende

Thema: **Missbrauch und Betrug** Fallnummer: **2022/13**

Der Kunde erhielt einen Anruf von angeblichen Microsoft-Mitarbeitenden, welche vorgaben, Probleme auf seinem Computer bereinigen zu wollen. Er gab ihnen Zugriff auf diesen Computer und teilte ihnen danach seine Kreditkartendaten mit, um eine laut Aussage der Betrüger abgelaufene Microsoft-Lizenz zu erneuern. Tatsächlich verschafften sich die Betrüger Zugang zum E-Banking des Kunden, überwiesen von seinem Konto Geld auf seine Kreditkarte und tätigten mit dieser in der Folge Transaktionen im Umfang von gut 7000 CHF. Die Bank verweigerte ihm eine Entschädigung, worauf er den Fall dem Ombudsman vorlegte. Im Rahmen des Ombudsverfahrens zeigte sie sich schliesslich bereit, den Kunden aus Kulanzgründen mit 2000 CHF zu entschädigen. Der Kunde nahm das Angebot an.

Auch die dem vorliegenden Fall zugrundeliegende Betrugsmethode scheint leider nach wie vor verbreitet zu sein, wobei die Betrüger vor allem Kunden in fortgeschrittenem Alter damit angehen. Angebliche Microsoft-Mitarbeitende melden sich und behaupten, der Computer des Kunden habe zahlreiche Sicherheitsprobleme, welche dringend behoben werden müssten. Gutgläubige Kunden erlauben ihnen den Zugriff auf ihren Computer, welcher üblicherweise mit einem Programm für den Fernzugriff erfolgt. Den Betrügern gelingt es dann, in das E-Banking des Kunden einzusteigen und selbständig Transaktionen auszulösen.

Wie genau die Betrüger in diesem Fall zu den Zugangsdaten zum E-Banking gekommen waren, blieb offen. Die betrügerische Transaktion bestand darin, dass Geld auf das Kreditkartenkonto des Kunden überwiesen wurde. Nach Abschluss dieses Vorgangs behaupteten die Betrüger unverfroren, die Microsoft-Lizenz des Kunden sei abgelaufen, und er könne diese für günstige 12 CHF erneuern. Der Kunde gab ihnen dafür seine Kreditkartendaten bekannt. Mit diesen Daten tätigten die Betrüger Transaktionen im Gesamtbetrag von rund 7000 CHF, welche der Kunde gemäss der Bank mit den dafür auf sein Mobiltelefon gesandten Codes bestätigt hatte.

Nach einer gewissen Zeit kam dem Kunden der Vorgang verdächtig vor. Er schaltete seinen Computer aus und telefonierte der Bank. Seine Kreditkarte wurde unverzüglich gesperrt. Der knapp 80-jährige Kunde schämte sich dafür, dass ihm der Betrug nicht früher aufgefallen war, als er des erlittenen Schadens gewahr wurde.

Nach Durchsicht der Unterlagen und der massgebenden Vertragsbedingungen kontaktierte der Ombudsman die Bank, welche dem Kunden eine Entschädigung mehrmals verweigert hatte. Sie warb öffentlich damit, dass sie Kunden, welche Opfer von Cyberangriffen geworden sind, bis zum Betrag von 100 000 CHF entschädige, was in der Presse breit aufgenommen wurde. In der entsprechenden

Bestimmung für ihr digitales Leistungsangebot wird zugesichert, den Kunden das Guthaben zu ersetzen, welches ihnen mittels der rechtswidrigen Entwendung ihrer Identifikationsmittel bzw. Sicherheitselemente durch Dritte entzogen wurde, namentlich bei Phishing- oder Malware-Attacken, sofern die Kunden die Teilnahmebedingungen für das digitale Leistungsangebot in allen Teilen eingehalten hatten. Der Ombudsman bat die Bank, den Anwendungsbereich dieser Bestimmung zu erläutern und darzulegen, weshalb sie gestützt darauf dem Kunden im vorliegenden Fall keine Entschädigung leisten wolle.

Die Bank vertrat die Ansicht, es sei vorliegend fraglich, ob der Tatbestand von Phishing erfüllt sei, da der Angriff per Telefon erfolgte und der Kunde die notwendigen Daten bewusst und freiwillig Dritten zugänglich machte, welche er nicht kannte und die keinen Bezug zur Bank hatten. In den Teilnahmebedingungen verweise die Bank auf eine Website, in welcher verschiedene Sicherheitsfragen behandelt würden und unter anderem festgehalten sei, dass persönliche Daten, insbesondere Kontodaten, auf keinen Fall weitergegeben werden dürfen und die Bank ihre Kunden niemals kontaktiere, um Zugangsdaten abzufragen.

Im vorliegenden Fall sei jedoch weniger ausschlaggebend, ob der Tatbestand des Phishing vorliege. Selbst wenn dies der Fall wäre, habe der Kunde eine entscheidende Bedingung für das in der fraglichen Bestimmung festgehaltene Leistungsversprechen verletzt. Dieses gelte nämlich nur dann, wenn die Teilnahmebedingungen in allen Teilen eingehalten wurden, was vorliegend nicht der Fall gewesen sei. Die Bank bedaure den Vorfall und schätze den Kunden sehr. Sie sei deshalb bereit, diesem aus Kulanz 2000 CHF zukommen zu lassen.

Der Ombudsman erachtete diese Argumentation nicht als schlüssig. Es ist seiner Meinung nach anerkannt, dass Phishing auch per Telefon erfolgen kann. Ist das Phishing nach Bank- oder Kartendaten erfolgreich, beinhaltet es immer, dass Kunden diese «freiwillig» an unberechtigte Dritte weitergeben, welche die Daten in der Folge missbrauchen, da die Betrüger den Kunden einen legitimen Grund dafür vorgaukeln und in teilweise sehr raffinierter Art und Weise eine Scheinwelt aufbauen. Wenn nun die Teilnahmebedingungen vorsehen, dass das beworbene Leistungsversprechen nicht gilt, wenn eine solche Weitergabe erfolgt, so erscheint dessen Anwendungsbereich als nicht fassbar.

Da der Ombudsman aufgrund der gesamten Umstände des Falles weitere Vermittlungsbemühungen als aussichtslos erachtete, unterbreitete er dem Kunden das Vergleichsangebot im Rahmen eines erläuternden Bescheids trotzdem. Dieser entschloss sich zu dessen Annahme.