Vorsicht vor Quishing: Neue Betrugsmasche mit gefälschten QR-Codes

Immer mehr Deutsche fallen auf gefälschte Briefe herein, die mittels QR-Codes sensible Daten stehlen wollen. Experten warnen vor der neuen Betrugsmasche „Quishing“.

In Deutschland sind immer mehr Menschen mit einer neuen Betrugsmasche konfrontiert, die über gefälschte Briefe verbreitet wird. Unternehmer Mirko Lange aus Bayern machte kürzlich eine erschreckende Entdeckung. Er erhielt einen professionell wirkenden Brief von der Commerzbank, der ihn aufforderte, sein Photo-TAN-Verfahren zu aktualisieren. Der Inhalt schien überzeugend, doch Lange war kein Kunde der Bank, was ihm stutzig machte.

Der Brief, der bei ihm in München ankam, war so gut gemacht, dass es ihm schwerfiel, die Fälschung auf Anhieb zu erkennen. „Auf den ersten Blick gab es keine Auffälligkeiten“, erläutert Lange. Er stellte jedoch fest, dass der Absender, der offiziell der Commerzbank zu sein schien, nicht korrekt war. Diese Erfahrungen verdeutlichen, dass die Betrüger immer raffinierter werden und es für den Durchschnittsbürger oft kaum möglich ist, gefälschte Dokumente als solche zu identifizieren.

Was ist „Quishing“? Eine neue Gefahrenquelle

Die Methode, die Lange erlebte, wird als „Quishing“ bezeichnet. Bei diesem Ansatz versuchen Kriminelle, sensible Daten über QR-

Codes zu erlangen, die in gefälschten Briefen platziert sind. Das Landeskriminalamt Nordrhein-Westfalen (LKA NRW) warnt vor dieser Bedrohung und betont, dass die Täter versuchen, die betroffenen Personen dazu zu bringen, persönliche Bankinformationen preiszugeben.

Das bayerische LKA ist sich der Situation ebenfalls bewusst und steht im Austausch mit seinen nordrhein-westfälischen Kollegen. Lange hat die Warnungen weitergegeben und auf seiner LinkedIn-Seite über die erschreckenden Details und die Professionalität der Betrüger berichtet. „Das war für mich unvorstellbar, ich hätte niemals mit einer Phishing-Attacke per Brief gerechnet“, führte er an. Dies zeigt, wie wichtig es ist, wachsam zu sein, besonders in einer Zeit, in der Betrüger ihre Methoden ständig weiterentwickeln.

Schutzmaßnahmen gegen „Quishing“

Die Sicherheitsbehörden geben einige grundlegende Ratschläge, wie man sich gegen solcherlei Betrugsversuche schützen kann. Bürger sollten kritisch sein und den Absender im Zweifel direkt kontaktieren, um sich über die Echtheit eines Schreibens zu vergewissern. Bei QR-Codes sollte man vorsichtig sein und diese nur scannen, wenn man sicher ist, dass die Quelle vertrauenswürdig ist. Damit werden persönliche Daten besser geschützt.

Ein weiteres wichtiges Sicherheitsmerkmal ist die Anwendung einer Multi-Faktor-Authentifizierung beim Online-Banking. Diese Maßnahme ist besonders empfehlenswert, um Account-Daten abzusichern. Die Commerzbank selbst bestätigt, dass sie von diesen Phishing-Versuchen Kenntnis hat und Maßnahmen ergreift, um die Nutzung durch die Täter zu verhindern.

Der Sicherheitsexperte Olaf Classen weist darauf hin, dass die Gefahr noch weitreichender ist, als viele es vermuten. Seine Erkenntnisse über gefälschte QR-Codes an E-Auto-Ladesäulen verdeutlichen, dass die Betrüger in vielen alltäglichen

Situationen tätig sein können. QR-Codes sind mittlerweile überall zu finden, sei es in Geschäften oder bei Einsätzen wie Parkautomaten. Das Risiko, in eine Falle zu tappen, wird durch die Unsichtbarkeit des Betrugs erhöht.

Classen merkt an, dass viele Menschen noch ahnungslos gegenüber diesen neuen Techniken sind. Die nahezu perfekte Ausführung der Fälschungen lässt die meisten Betroffenen unvorbereitet und dadurch verwundbar zurück. Wenn Betrugsversuche über E-Mail oft erkannt werden, stellen solche Briefsendungen eine neue Herausforderung dar, die die Sicherheitslage nachhaltig beeinflussen könnte.

Diese Vorfälle sind ein klares Signal, dass die Verbraucher verstärkt auf technische und organisatorische Sicherheitsvorkehrungen achten müssen, um sich vor diesem wachsenden Problem zu schützen. Umso wichtiger ist es, Bewusstsein für solche Verfahren zu schaffen und über sie zu informieren.

Details