Mittwoch, den 6. August 2025

Wirtschaft

Mit gefälschter BIL-Webseite fast eine halbe Million Euro ergaunert

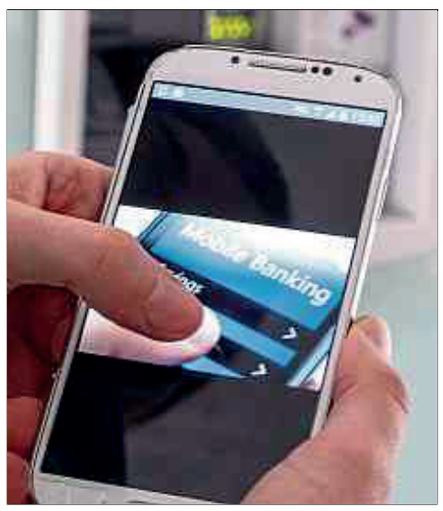
Hintergrund. Es war ein Klick auf der Fake-BIL-Seite zu viel: Fast 50 Personen haben sich in der gegründeten „Opfergruppe“ zusammengetan und legen ihre Schadensbilanz vor

Die Täter nutzten eine täuschend echte Nachbildung der BIL-Website, wobei viele Betroffene ihre Daten aufgrund einer vermeintlichen Fehlermeldung mehrfach eingaben. Foto: LW

Von Marco Meng und Ingo Zwank

Kriminelle haben in Luxemburg professionell gefälschte Bank-Webseiten genutzt, um Kunden der Banque Internationale à Luxembourg (BIL) zu betrügen. Opfer berichteten von erheblichen finanziellen Verlusten zwischen 6.500 und 9.900 Euro durch Überweisungen auf ausländische Konten. Die Täter nutzten eine täuschend echte Nachbildung der BIL-Website, wobei viele Betroffene ihre Daten aufgrund einer vermeintlichen Fehlermeldung mehrfach eingaben und so die Zwei-Faktor-Authentifizierung unwissentlich abschlossen. Die Polizei spricht von 20 Anzeigen.

Geschädigte kritisieren das mangelnde Engagement der Bank. Alice Pauly, eines der Opfer der Betrugsmasche, fühlt sich „regelrecht im Regen stehen gelassen“. Sie verlor 6.500 Euro und schloss sich mit weiteren BIL-Kunden, die durch die Fake-Seite einen Schaden erlitten, nun in einer Gruppe zusammen. „45 Leute sind es mittlerweile“, so Pauly gegenüber dem „Luxemburger Wort“. Und der ermittelte Schaden dieser Personen beläuft sich auf 481.070 Euro.



Die Beweislast, ob Kunden grob fahrlässig handelten, indem sie ihre Daten verrieten, liegt bei der Bank. Foto: Guy Jallay

Betrogene erhalten oft kein Geld zurück

Gerade bei solch betrügerischen Überweisungen bleiben Kunden laut der Europäischen Bankenaufsicht EBA besonders häufig auf dem Schaden sitzen. Für die Kunden der BIL somit keine ermunternden Aussichten.

Die Frage steht im Raum: Hat die Bank ihre Kunden rechtzeitig vor dieser falschen Webseite gewarnt? Anfang Juli veröffentlichte die Bank auf ihrer Webseite die Mitteilung, nicht über die Suchmaschine Google auf das BILnet-Onlinebanking zuzugreifen, sondern die Webadresse der Bank selbst im Browser einzugeben. Reicht das als Warnung aus? Generell ist bei „Phishing“ – dem Stehlen von Bankzugangsdaten – der Standpunkt der Banken: Die Kunden handelten „grob fahrlässig“, weil sie ihre Login- und PIN-Daten weitergaben. Doch ist es tatsächlich „grob fahrlässig“, wenn man etwa auf einer verblüffend echt aussehenden BIL-Webseite seine Daten eingibt, weil man sich in sein Konto einloggen möchte? Was, wenn die Kunden nicht einmal merkten, dass die Webseite gefälscht ist, sondern einfach dachten, es liege eine technische Störung vor, weswegen sie sich nicht einloggen konnten?

Allerdings haben die Opfer dann den Fehler begangen, versehentlich die Überweisung der Kriminellen, die sich mit den erbeuteten Daten Zugang zu den Konten verschafften, zu bestätigen, wie es auch die Polizei in geschilderten „Tathergang“ ausführt.

Was den vorliegenden Fall betrifft, „so finden wir trotz der Raffinesse des Vorgehens eine Reihe von Ähnlichkeiten mit anderen Betrugsfällen, auf die die Polizei, die Banken, die Presse, die ABBL und die CSSF in den letzten Jahren aufmerksam gemacht haben“, bestätigt der Bankenverband ABBL.

Solche Betrugsversuche über gefälschte Webseiten finden häufig am Wochenende oder außerhalb der Öffnungszeiten der Bank statt. „Die Überprüfung der URL hätte den Opfern wahrscheinlich geholfen, den Betrug zu erkennen“, so die ABBL gegenüber dem „Wort“. Auch seien die Opfer in Stresssituationen gebracht worden durch Absturz der Website und wurden (teils) aufgerufen, ihre LuxTrust-Zugangsdaten preiszugeben. „Keine Bank und keine Behörde würde dies tun“, so die ABBL.

In diesem speziellen Fall wäre es richtig gewesen, sich über die Mobile-Banking-App der Bank anzumelden oder die URL der Bank direkt in den Browser einzugeben, statt eine Suchmaschine oder eine vermeintliche Werbeanzeige der BIL zu verwenden.

Raffiniertes Vorgehen

Manche Geschädigten berichten allerdings auch, sie hätten nirgends ihre PIN eingegeben und keine Banküberweisungen bestätigt. Experten bestreiten, dass das möglich ist. Eine Überweisung wird nur durchgeführt, wenn sie mit einem 2. Faktor bestätigt wird. Es soll aber Fälle geben, in denen sich Täter mit einem zweiten Handy und entsprechender zweiter Telefonnummer bei der Bank autorisierten, um Kontozugang zu erhalten.

Einen Rechtsstreit in einem solchen Fall gibt es aktuell in Deutschland, wo sich Täter vermutlich neue Zugangsdaten per Post von der Bank anforderten und offenbar die Briefe der Bank beim Kontobesitzer abfingen. So änderten sie dann Überweisungslimits und transferierten Geld nach Malta. Solche Fälle sind in Luxemburg aber bislang nicht bekannt, es sei denn, die Ermittlungen zu den Betrugsfällen bei der BIL ergeben nun etwas anderes. „Bislang wurde uns kein solcher Fall gemeldet“, heißt es dazu von der Bankenvereinigung ABBL.

Wenn es vor Gericht geht, liegt grundsätzlich die Beweislast, dass ein Kunde grob fahrlässig gehandelt hat, bei der Bank. Allerdings liegt es dann an der Einschätzung der Richter, wie sie es werten.

Sicherheit soll erhöht werden

Banken müssen künftig bei Überweisungen die genannte Kontonummer (IBAN) mit dem angegebenen Empfängernamen abgleichen und Warnungen mitteilen, wenn es Unstimmigkeiten gibt. In diesem Fall „steht es dem Nutzer frei, die Überweisung zu bestätigen, er übernimmt dann jedoch die volle Verantwortung im Falle eines Fehlers“, erklärt die ABBL.

Ab 2026 müssen zudem die europäischen Staaten die EUDI-Wallet bereitstellen, eine Art digitaler Personalausweis. Mit der staatlichen App für Smartphone oder andere Geräte kann man sich digital ausweisen, zum Beispiel bei Behördengängen, Verträgen oder auch Onlinebanking. Das schützt Daten vor Missbrauch und Tracking – und erschwert Phishing, weil man keine Passwörter oder PINs eintippen muss, die abgefangen werden könnten.

Phishing-Mails oder gefälschte Webseiten können keine gültige Wallet-Authentifizierung auslösen, denn diese erfolgt direkt und geschützt auf dem Endgerät des Nutzers, nicht über manipulierte Weblinks oder übertragene Transaktionsnummern (TAN). Ende 2027 müssen alle großen Plattformen, darunter auch Banken, die EUDI-Wallet als offizielles Identifikationsmittel akzeptieren.

IBAN-Lastschriftbetrug in Luxemburg noch selten

Ein „marginales Phänomen“, so die ABBL, ist in Luxemburg der Lastschriftbetrug. Hier stellen die Betrüger mithilfe der IBAN-Konten ihrer Opfer gefälschte Einzugsermächtigungen her. Auf der Grundlage dieses gefälschten Mandats senden sie dann einen Überweisungsantrag an die Bank, um Geld abzubuchen. Kriminelle nutzen dabei fehlende Kontrollen beim SEPA-Lastschriftverfahren zu Betrugszwecken aus.

Kommt es zur Tat, haben Banken eine Meldepflicht für verdächtige Transaktionen gegenüber der zentralen Meldestelle für Geldwäsche (CRF), denn Betrug ist eine Vortat der Geldwäsche.

Das Gute bei der Zahlungsmethode Lastschriftverfahren ist, dass man sich das Geld wieder zurückholen kann. SEPA-Lastschriften können innerhalb von acht Wochen zurückgeholt werden – bei betrügerischen Abbuchungen beträgt die Frist sogar 13 Monate. Auch kann man mittels mancher Banken-Apps eine Lastschrift sperren.

Eigene Kontrolle der Transaktionen

Banken und Verbraucherschützer raten daher, dass Kontoinhaber regelmäßig ihre Transaktionen kontrollieren sollen, um unrechtmäßige Kontoabbuchungen nicht zu spät oder gar nicht zu bemerken.

Um sich gegen Betrug zu schützen, ist Folgendes zu beachten:

- Keine sensiblen Vorgänge wie Onlinebanking über öffentliches WLAN durchführen.
- HTTPS-Verschlüsselung (Schloss-Symbol im Browser) bedeutet, dass die Verbindung sicher ist – nicht, dass die Seite vertrauenswürdig ist. Auch Phishing-Seiten nutzen HTTPS, da Zertifikate kostenlos erhältlich sind. Darauf weist BeeSecure hin. Tipp der Experten zur URL-Analyse: Man soll die URL von rechts nach links lesen, beginnend mit der Domain-Endung (.lu, .de, .com). Direkt davor steht der echte Name der Organisation. Der echte Domainname steht direkt vor der Endung. Alles weiter links (wie „www“, „login“ und ähnliches) kann frei gewählt und zur Täuschung genutzt werden.
- Am besten aber ist, die App zu benutzen oder die Webseite für das Onlinebanking zu speichern und nicht über eine Suchmaschine aufzurufen.
- Erhält man die Nachricht zum Bestätigen einer Überweisung: Stimmen Summe und Adressat?
- Banken fragen nie per Email, telefonisch oder per SMS nach Zugangsdaten oder PIN, auch nicht für „Aktualisierungen“ oder Ähnliches.
- Fällt Ihnen auf, dass etwas nicht stimmen kann, rufen Sie unverzüglich die 49 10 10 an, die rund um die Uhr sieben Tage die Woche erreichbar ist: Dort können Sie LuxTrust sperren und damit verhindern, dass Geld abgebucht wird.
- Die ABBL weist auf die Website cyberfraud.lu hin, die sie im Mai gemeinsam mit anderen Partnern im Rahmen der nationalen Präventionskampagne „Nicht klicken. Überprüfen. Melden.“ gestartet haben.