> *Die in Luxemburg ansässigen Zahlungsdienstleister würden ihre Kunden niemals per E-Mail auffordern, ihre Zugangsdaten preiszugeben.*
>
> **Commission de Surveillance du Secteur Financier**

Wer auf den Betrug hereinfiel, erlebte eine böse Überraschung. Foto: Gerry Huberty

Post muss Phishing-Opfern das Geld nicht zurückerstatten

Im Juli wurden Eboo-Nutzern die Konten von Internetkriminellen leergeräumt

Von Marco Meng

Einige Nutzer von Eboo-Konten der Post Luxembourg Opfer waren im Sommer Ziel von Internetkriminellen. Sie wurden auf eine falsche Webseite gelockt, die das E-Banking der Bank imitierte, um auf diesem Weg an die LuxTrust-Logins zu gelangen („Phishing"). Kurz darauf war das Konto leergeräumt.

Im konkreten Fall erhielten die Opfer gefälschte Mails mit vermeintlichem Absender Post oder LuxTrust. Darin wurden sie aufgefordert, einen Link zu drücken, um das Konto mit einer Payconiq-App zu verknüpfen. Die Post weist darauf hin, dass sie keine E-Mails mit solchen Aufforderungen verschickt, und unterstreicht, es habe auch im Fall von Eboo-Phishing keinen allgemeinen Fehler im Sicherheitssystem des Online-Bankings von Post Finance gegeben.

Das Unternehmen macht keine Angaben zur Anzahl der betroffenen Kunden oder zu den entwendeten Beträgen. Auch nicht dazu, ob sie den Kunden das Geld aus Kulanzgründen erstattete. Versuche der Opfer, das Geld von der belgischen Bank, an die das Geld von den Tätern überwiesen wurde, zurückzuerhalten, schlugen fehl.

Keine PIN eingegeben?

Ein Betroffener, dem bislang kein Geld erstattet wurden, sieht bei PostFinance insofern eine „gewisse Mitverantwortung", als von den 4.000 Euro, die ihm gestohlen wurde, 2.000 Euro Dispokredit sind. Er habe aber nie einen Dispokredit nachgefragt, sondern der sei ihm automatisch vom Kreditinstitut eingerichtet worden. Nun haben die Täter nicht nur sein Guthaben abgeräumt, sondern auch sein Konto bis zum Limit „überzogen". Außerdem habe er eine Dreiviertelstunde versucht, über die Post-Hotline eine Person anzurufen, die Auskunft über die E-Mail geben konnte. Eine PIN habe er nicht eingegeben, und es sei ihm deswegen schleierhaft, wie das Phishing funktionieren konnte. Vonseiten der Polizei und der Post heißt es hingegen, die PIN muss auf der falschen Webseite eingegeben worden sein.

„Wir erhalten und bearbeiten kontinuierlich Klagen und Meldungen über Phishing-Vorfälle", sagt Pascal Enzinger, Leiter der Abteilung für Internetkriminalität bei der Luxemburger Police. „Unseren Erfahrungen nach werden die Betroffenen auf eine dem originalen Webauftritt-der Bank nachempfundene Webseite geleitet", sagt der Oberkommissar. „Für alle uns bekannten unberechtigten Zugriffe und Überweisungen nutzten die Täter immer die gephishten Zugangsdaten inklusive Token Pin. Gegenteilige Vorfälle sind uns nicht bekannt."

Die Finanzaufsichtsbehörde CSSF hat auf Ebene des Online-Banking Angebots der Post „Eboo" keine Sicherheitsmängel oder Schwachstellen festgestellt. „Der Vorfall ist darauf zurückzuführen, dass Kunden der Post ihre Zugangsdaten auf einer gefälschten Internetseite eingegeben und die Betrüger so Zugriff auf die Konten der Kunden erhalten haben", so die CSSF. Es bestehe also weiterhin ein Sensibilisierungsbedarf auf Seiten der Kunden, um solche Vorkommnisse in Zukunft zu verhindern.

Vor Eingabe ihrer Daten sollten sich die Kunden stets vergewissern, dass sie sich auf der echten Internetseite ihres Dienstleisters befinden. „Die in Luxemburg ansässigen Zahlungsdienstleister würden ihre Kunden niemals per E-Mail auffordern, ihre Zugangsdaten preiszugeben" so die CSSF.

Gemäß den Vorschriften des Gesetzes vom 10. November 2009 über Zahlungsdienstleistungen ist ein Zahlungsdienstleister grundsätzlich dazu verpflichtet, den Kunden im Falle der Ausführung eines nicht autorisierten Zahlungsvorgangs schadlos zu halten, also den abgebuchten Betrag zu erstatten. Dies gilt jedoch nicht, sofern ein vorsätzliches oder grob fahrlässiges Verhalten des Kunden zur Ausführung des Zahlungsvorgangs geführt hat. Es obliegt also der Post, ob sie den Kunden den erlittenen Schaden aus Kulanzgründen ausgleicht.

Sollten sich die Parteien über das Bestehen einer solchen Entschädigungspflicht nicht einig sein, so steht es dem Kunden frei, die CSSF einzuschalten und eine Beschwerde gegen den Zahlungsdienstleister einzulegen. Ansonsten steht ihm der Rechtsweg offen.

Jeder kann Opfer werden

Mit Phishing sind Banken und ihre Kunden jeden Tag konfrontiert. Und wie der Bankenverband ABBL mitteilt, gehen die Täter dabei längst nicht mehr plump vor. Im Sommer war eine Masche beispielsweise: man erhielt per SMS oder Email die Mitteilung eines großen Onlineunternehmens für Reisebuchungen, der „der Bezahlvorgang ist nicht erfolgreich gewesen". Man müsse die Zahlung der Urlaubsbuchung erneut bestätigen. Wer dann den Link klickte und auf der echt aussehenden, aber gefälschten Webseite des Buchungsdienstes seine Daten zum Bezahlen „bestätigte", von dessen Bankkonto hatten sich kurz darauf Kriminelle bedient.

Oder die Betrüger forderten die Kunden dazu auf, die Zahlungsinformationen zu bestätigen, Grund sei ein Update der Buchungs-App. Über einen blauen Button sollen Kunden sich einloggen. Tun sie das nicht, werde das Kundenkonto innerhalb von zwei Tagen geschlossen, die gebuchte Reise verfalle. Wird man derart unter Druck gesetzt, innerhalb kurzer Zeit einen Link zu klicken, sei das ein Hinweis darauf, dass es sich um eine Betrugsmasche handelt, warnt die ABBL.

Im August (letzte veröffentlichte Daten) wurden dem Computer Incident Response Center Luxembourg (CIRCL) 80 Phishing-Versuche gemeldet.