29.07.2020

Vorsicht bei Zahlungsaufträgen per E-Mail

Ein neues Urteil des Bundesgerichts gibt zu reden: Hacker plünderten das Konto eines Kunden, und seine Bank haftet nicht. Doch gegen solche Schadensfälle kann man sich schützen.

Der Schock war gross, als Jean-Claude Henchoz (*Name geändert*) das letzte Urteil las: Das Bundesgericht hatte entschieden, dass der Kunde einer Genfer Privatbank für den ihm durch Hacker zugefügten Schaden selber aufkommen muss. Dies, nachdem das Kantonsgericht in Vorinstanz die Bank noch dazu verpflichtet hatte, Henchoz einen Grossteil des Verlusts zu erstatten – mehrere Hunderttausend Euro.

Kriminelle hatten sich Zugang zum E-Mail-Konto des Bankkunden verschafft und darüber mehrere Zahlungsaufträge an seine Bank verschickt. Als Empfänger gaben die Betrüger von ihnen bestimmte ausländische Konten an. Das Problem: Laut Vertrag zwischen Bank und Kunde waren Zahlungsaufträge per E-Mail, Telefon und Fax zulässig, ein schriftlicher Auftrag nicht erforderlich. Die Hacker machten sich diesen Umstand für ihre Überweisungen zunutze.

Nachdem das Genfer Kantonsgericht befunden hatte, die Bank hätte die missbräuchlichen Zahlungen frühzeitig bemerken und stoppen müssen, sah das Bundesgericht keinen Fehler seitens der Bank, weil vertraglich geregelte Aufträge per E-Mail nicht automatisch als potentiell betrügerisch angesehen und entsprechend überprüft werden müssten. Das Risiko hinsichtlich der Identifikation und für Übermittlungsfehler trage der Kunde.

Beachten Sie nachfolgende Empfehlungen, um sich vor Verlusten durch missbräuchliche Zahlungsaufträge zu schützen:

- Erteilen Sie Zahlungsaufträge nach Möglichkeit ausschliesslich über das E-Banking bzw. die Mobile Banking App Ihrer Bank oder persönlich in Ihrer Bankfiliale und lassen Sie andere Kanäle wie E-Mail, Telefon und Fax für Zahlungszwecke vertraglich sperren.
- Falls Zahlungsaufträge per E-Mail unausweichlich sind, verwenden Sie dafür einen E-Mail-Anbieter, welcher Zwei-Faktor-Authentifizierung anbietet, und machen Sie von diesem Zusatzschutz Gebrauch.
- Verwenden Sie unterschiedliche, komplexe Passwörter (https://www.ebas.ch/4-schuetzen-der-online-zugaenge/) für alle Ihre E-Mail-Konten sowie fürs E-Banking, bewahren Sie diese sicher auf (z.B. in einem Passwort-Manager) und geben Sie diese niemals irgendjemandem bekannt.
- Richten Sie eine separate E-Mail-Adresse für die Kommunikation mit Ihrer Bank ein, verwenden Sie diese Adresse für keine anderen Zwecke und geben Sie sie niemandem ausser Ihrer Bank bekannt.
- Lassen Sie falls möglich bei Ihrer Bank eine Transaktionsautorisierung einrichten, damit alle Zahlungsaufträge ab einer bestimmten Höhe durch Sie explizit und über einen anderen Kanal (z.B. Telefon) freigegeben werden müssen, bevor diese ausgeführt werden.
- Überprüfen Sie regelmässig Ihre Kontoauszüge sowie online die letzten Buchungen und benachrichtigen Sie bei Unstimmigkeiten unverzüglich Ihre Bank.

Copyright © 2024 – Alle Rechte vorbehalten. Hochschule Luzern – Informatik

Copyright © 2024 – Alle Rechte vorbehalten. Hochschule Luzern – Informatik