Von: xxx
Gesendet: Sonntag, 13. März 2022 18:38
An: xxx
Cc: xxx
Betreff: Erhebliches Sicherheitsrisiko im Log-In Verfahren der PAYBACK GmbH
Priorität: Hoch

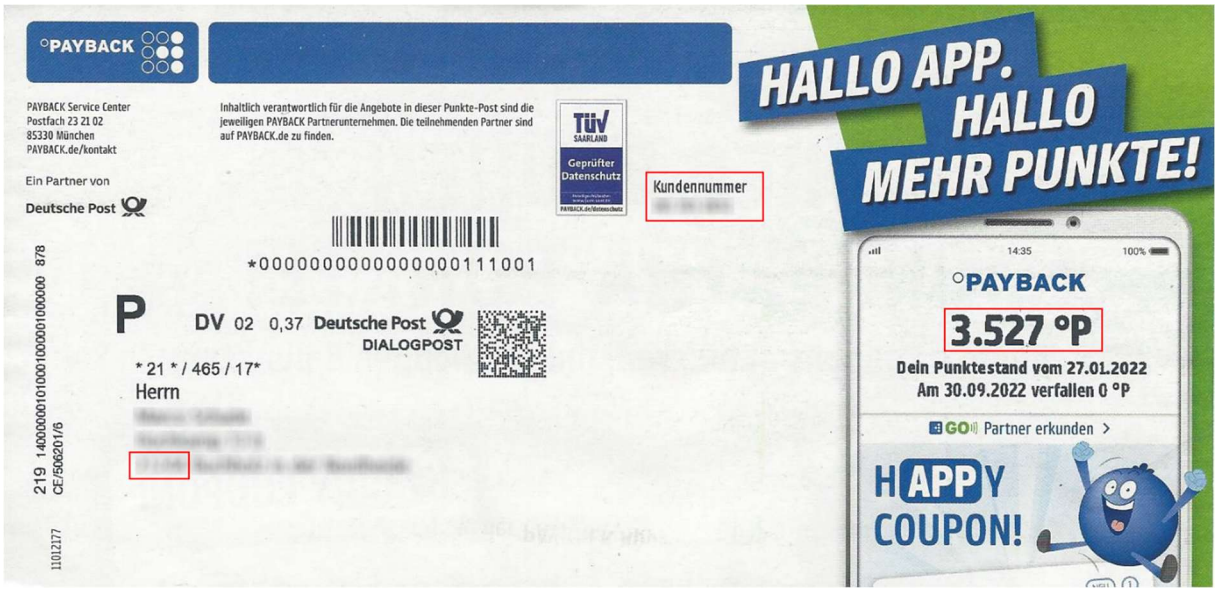
Sehr geehrter Herr Dr. Selk,

ich wende mich heute an Sie um die seit Jahren vorhandenen Sicherheitsrisiken im PAYBACK Log-In Verfahren auf der Webseite und an den Payback-Terminals bei Payback-Partnern zu beanstanden. Die weiterhin angebotene Möglichkeit sich über Kundennummer, Postleitzahl und Passwort einloggen zu können ist nicht sicher. Ich hatte in der Vergangenheit Payback bereits über dieses Risiko in Kenntnis gesetzt, und um Stellungnahme gebeten. Eine Antwort habe ich bis heute jedoch nicht erhalten.

Payback schreibt zu dieser Thematik aktuell in Ihrer App: *„Die Log-In Methode in den Filialen mancher Partner z.B. mit Kundennummer, PIN / Postleitzahl und Geburtsdatum ist nicht die Schwachstelle. Um alle diese Parameter zu bekommen, müsste zuvor das E-Mail Konto gehackt worden sein. Hier in Emails dann weitere Infos zu PLZ und Geburtsdatum gefunden, oder eine Geldbörse entwendet oder ein Phishingversuch erfolgreich gewesen sein. Das Risiko, dass Täter alle diese Parameter haben, ist als gering einzuschätzen. Wie gesagt sehen wir, dass die richtige und schon einige Schritte vor dem Einloggen bei Payback gestohlene Kombination Email-Adresse und Passwort zu Anwendung kommt.“*

Payback behauptet somit, dass diese Informationen nur durch gehackte E-Mail Konten in die Hände von Betrügern kommen können und schiebt die Verantwortung für derartige Vorfälle komplett in die Verantwortung der Kunden. Diese Aussage entspricht nicht den Tatsachen. Für Betrüger gibt es gleich zwei realistische Angriffsziele, die einzig in der Verantwortung von Payback und ihrer Partner-Firmen liegen und entsprechend eine Sicherheitslücke darstellen, die umgehend geschlossen werden muss.

- Betrüger greifen Kundendaten bei Payback-Partnerfirmen ab. Hier liegen dann ggf. alle für den Log-In relevanten Informationen vor. Bei Onlineshops sind neben der Anschrift (mit PLZ!) und dem Geburtsdatum des Kunden bei Payback-Partnern ebenfalls die Payback-Kundennummer gespeichert. Für Hacker-Angriffe bei den Partner-Unternehmen trägt der Payback-Kunde keine Verantwortung.
- Noch einfacher können die erforderlichen Daten über die Postausendungen von Payback ermittelt werden. Diese Werbebriefe versendet Payback mehrfach im Jahr per Post. Im Anschreiben sind neben der Anschrift (mit PLZ!) auch die vollständige Kundennummer und der aktuelle Punktestand enthalten. Über das Altpapier kann so, zusätzlich ermittelt werden, welche Konten besonders lukrative Ziele sind. Das fehlende Geburtsdatum kann in vielen Fällen sehr einfach durch den Kauf von Datensätzen bei Adresshändlern (z.B. aus Gewinnspielteilnahmen) erhoben werden. Darüber hinaus gibt es auch verschiedene andere Möglichkeiten an das Geburtsdatum zu kommen (z.B. Karrierenetzwerke, Facebook, Datenbestände von gehackten Unternehmen im Darknet, gezielte Anrufe bei potenziellen Betrugsopfern, sofern ein Eintrag im Telefonbuch vorliegt). Entsprechend stellen weggeworfene Werbesendung ein erhebliches Sicherheitsrisiko dar.



In der Vergangenheit hatte Payback aufwändig geprüft, ob ein Verschulden des Kunden vorliegt und ggf. die Payback-Punkte erstattet, sofern dies nicht der Fall war. Anschließend wurde von Payback regelmäßig das Geburtsdatum entfernt und der Log-In musste auf die sichere Variante mit Passwort umgestellt werden. Ich gehe daher davon aus, dass Payback längst Kenntnis darüber hat, dass der Log-In mit Kundennummer, Postleitzahl und Geburtsdatum der Hauptangriffspunkt ist und ein erhebliches Sicherheitsrisiko darstellt.

Ich bitte Sie daher dieses Risiko zu bewerten und bei der PAYBACK Geschäftsführung zu platzieren. Ich fordere Payback aus den vorgenannten Gründen auf, dass unsichere Verfahren online und bei den Payback-Terminals umgehend abzuschalten. Außerdem ist es nicht erforderlich bei Werbebriefen die Kundennummer anzugeben. Solange das unsichere Log-In Verfahren weiter möglich ist, sollte deshalb auch die Kundennummer in Anschreiben entfernt werden.