Von: xxx
Gesendet: Sonntag, 3. April 2022 13:46
An: xxx
Cc: xxx
Betreff: Erhebliches Sicherheitsrisiko im Log-In Verfahren der PAYBACK GmbH

Sehr geehrter Herr Dr. Selk,

ich habe auf meine an sie gerichtete Anfrage vom 13.03.2022 leider nur eine unpassende Antwort des Payback Kundenservice speziell zu meinem persönliches Payback Kundenkonto erhalten. Meine Anfrage bezog sich **NICHT** auf mein persönliches Payback Kundenkonto. Ich persönlich bin nicht von der PAYBACK Sicherheitslücke betroffen. Wie der Payback Kundenservice richtig erkannt hat, habe ich selbstverständlich bereits die optionalen zusätzlichen Sicherheitsfunktionen (individuelles Passwort und 2-Faktor-Zertifizierung) persönlich eingerichtet.

Und genau diese Legitimierungs-Optionen sollen zur Kundensicherheit standardmäßig das unsichere Log-In Verfahren vollständig ablösen. Denn das weiterhin in alten Konten aktive unsichere Identifizierungsverfahren mit Kundennummer, Postleitzahl und Geburtstag ist die Schwachstelle im Payback Verfahren über das seit Jahren die Punktekonten von tausenden Kunden geplündert wurden. Ich verfolge das Thema bereits seit einigen Jahren. Als Reaktion auf meinen Blogeintrag aus dem Jahr 2016 (https://www.amexio.de/blog/tausende-payback-konten-von-betruegern-gepluendert/) erhielt ich im Laufe der Zeit von vielen Geschädigten Zuschriften. In nahezu allen Fällen ließ sich rekonstruieren, dass Sie nicht Opfer einer Phishing-Attacke geworden sind. Anfangs prüfte Payback noch individuell, und erstattete ggf. Paybackpunkte, wenn kein Verschulden des Kunden vorlag. Mittlerweile wurde diese Praxis eingestellt und dem Kunden grds. unterstellt, er wäre gehackt worden. Die seit Jahren bekannte Schwachstelle im Log-In Verfahren wird weiter einfach geleugnet. Ich unterstelle, dass Payback das Einfallstor seit Jahren bekannt ist, weil schon im Jahr 2016 Payback in vielen Fällen bei leergeräumten Konten das Geburtsdatum im Anschluss aus Sicherheitsgründen aus dem Kundenkonto entfernt hat.

Wenn Payback schon kein Interesse an der Behebung der Schwachstelle zeigt, dann hätte ich von Ihnen als externen Datenschutzbeauftragten erwartet, dass das Thema ernsthaft geprüft und mit der Geschäftsführung die vorhandenen Optionen zur Gefahrenreduzierung aktiv angegangen werden.

Es ist mir völlig unverständlich, warum Payback kein eigenes Interesse daran hat die Sicherheitslücke zu schließen, nachdem jetzt effektive alternative Identifizierungsverfahren implementiert worden sind und eine Umstellung grds. ohne größere Probleme möglich wäre. Die Angst davor, dass einige Kunden ein sicheres aber nicht ganz so komfortables Log-In Verfahren ablehnen könnten, darf nicht der Grund dafür sein, eine Sicherheitslücke bewusst nicht endgültig zu schließen.

Und genau aus diesem Grund ist die Aussage von Payback: *„**PAYBACK ist sicher, PAYBACK hat keine Sicherheitslücke**“* nicht korrekt! Ich fordere daher nochmals die vollständige Abschaltung des unsicheren Log-In Verfahrens.