Offene Fragen zum Data Breach "Klimabonus"

29.08.2024

Bezugnehmend auf und ergänzend zum Dokument vom 27.08.2024 ergeben sich aus unserer Sicht noch folgende zusätzliche Empfehlungen zur Klärung noch offener Fragen bzw. zum korrekten und ethischen Umgang mit dem Vorfall.

Klärung wesentlicher Fragen vor Durchführung der Auszahlung (03.09.2024)

Wir empfehlen dringend, vor der Durchführung der Auszahlung eine unabhängige Überprüfung des Vorfalls (z. B. durch Interne Revision, externe Dienstleister o. Ä. Stelle mit entsprechendem Know-How und Unabhängigkeit) vorzunehmen, um sicherzustellen, dass weder ein materieller Schaden (wie insbesondere eine falsche Auszahlung des Klimabonus) noch ein immaterieller Schaden entstehen kann.

Basierend auf den uns sowie der Quelle vorliegenden Informationen ergeben sich derzeit folgende dringliche Fragestellungen, die vorab, vor Durchführung der Auszahlung des Klimabonus geklärt werden sollten:

1. Laut den Informationen unserer Quelle war es möglich, eine IBAN einzutragen, falls noch keine hinterlegt war. Wurde die Richtigkeit der eintragenden Person initial entsprechend überprüft (z. B. durch eine interne persönliche Kontrolle oder mittels ID-Austria)? Wenn ja, wie erfolgte die Prüfung
2. Wie konnte im Nachgang die Prüfung der Richtigkeit des IBANs erfolgen? Laut Datenschutzerklärung wurde kein Originalbild des Ausweises gespeichert, was eine nachträgliche Prüfung der Legitimität erschwert. Die Logfiles wurden nur für einen Monat gespeichert, während der API-Endpoint jedoch schon über einen längeren Zeitraum online verfügbar war.
3. Wann ist folgendes Formular online gegangen: https://www.klimabonus.gv.at/anfrage-rsa-abholung/. Weiters ab wann war die Abfrage für den Erhalt des Klimabonus auf der Startseite vorhanden?

Wir möchten darauf hinweisen, dass diese Fragestellungen auch für die Einschätzung einer möglichen Meldepflicht an die Betroffenen gemäß Art. 34 DSGVO von wesentlicher Bedeutung sind. Durch die Protokollierung der abgefragten Personen wäre eine direkte Information der Betroffenen möglich.

Darüber hinaus möchten wir betonen, dass unsere Detailfragen nur einen Ausschnitt der frei zugänglichen Informationen widerspiegeln. Es ist wahrscheinlich, dass bei Vorliegen sämtlicher Informationen weitere Fragen auftauchen werden. Daher raten wir dringend, eine unabhängige Prüfung so schnell wie möglich einzuleiten.

Weitere Fragen

Basierend auf den derzeitigen Informationen scheinen bei der Schnittstelle zwei wesentliche Versäumnisse vorzuliegen:

4. Das Verfahren ist an sich nicht geeignet, die Identität zweifelsfrei festzustellen. Gerade deshalb greift der Staat im Regelfall für Online-Zwecke auf eIDAS[1] kompatible Lösungen (ID-Austria) zurück. Es sollte geprüft werden, warum ein solch fehlerhafter Ansatz gewählt wurde.
5. Darüber hinaus war auch die gewählte Implementierung fehlerhaft. Es sollte untersucht werden, wie eine solche fehlerhafte Lösung eingeführt werden konnte (z. B. durch eine unzureichende Testphase für die OCR-Lösung).
6. Seit wann war das fehlerhafte Authentifizierungsverfahren online?
7. Gab es Abfragen zu mehreren Personen von der selben IP-Adresse?
8. Gab es Abfragen zu Personen des öffentlichen Interesses?
9. Gab es außergewöhnlich viele Abfragen in einem besonders kurzen Zeitraum?

Ethical Disclosure

Auf Grundlage der aktuellen Informationen halten wir ein "Ethical Disclosure" für unumgänglich. Wir möchten betonen, dass dies eine "Best Practice" in der IT-Sicherheit darstellt, die von vielen Staaten bewusst und offen praktiziert wird. Daher empfehlen wir weiterhin, nach Klärung der dringenden Fragestellungen und nach Umsetzung der notwendigen risikomindernden Maßnahmen, den Vorfall und die positive Bewältigung entsprechend öffentlich zu kommunizieren. Weiters sehen sich so auch Betroffene in der Lage zu überprüfen ob Zahlungen des Klimabonus korrekt eintreffen bzw. ob es sonstige Auffälligkeiten am Konto gibt. Daher stellt ein “Ethical Disclosure” letztendlich auch eine risiko-minimierende Maßnahme dar.

Eine Kommunikation des Vorfalls vor der Nationalratswahl erscheint uns unumgänglich. Sollte das BMK dies nicht tun, werden wir an die Öffentlichkeit gehen.

Mit besten Grüßen

epicenter.works – for digital rights

1 Verordnung (EU) 910/2014 bzw. Verordnung (EU) 2024/1183