Empfehlungen von epicenter.works zur Behandlung des Data Breach von Klimabonus.gv.at

1. Reperatur der Lücke
2. Data Breach Notification
3. Offene Kommunikation des Falles
4. Etablierung eines Bug Bounty Programmes
5. Einrichten von schnellen und effektiven Kommunikationswegen für Sicherheitsvorfälle
6. Alternativer Weg den Service auf Klimabonus.at anzubieten

27. August 2024

1. Reperatur der Lücke

Dies scheint mit 22. August geschehen zu sein. Die gegenständliche API ist mit 22. August vom Netz gegangen und das Webformular am Abend des 21. August 2024.

2. Data Breach Notification

Erhebungen zur Bemessung des Schadens und relevanter Datenabflüsse sind vorzunehmen. Da beliebige Daten als Ausweis zur Abfrage von Daten oder Veränderung eines IBANs verwendet worden sein könnten, reicht eine simple Analyse der Logfiles nicht. Gemäß der Datenschutzpolicy der Website werden nicht die Ausweisbilder selbst gespeichert, sondern nur die davon mittels Texterkennung ausgelesenen Daten. Demzufolge bleibt nur eine heuristische Analyse der durch die API abgefragten und veränderten Daten zur Bemessung des Schadens.

Schaden kann durch den Abfluss von Daten oder das Ändern des IBANs aufgetreten sein. Der **Klimabonus von Dritten könnte abgeflossen sein**, weil IBAN Überweisungen nicht mehr den Namen des/der Kontoinhaber:in überprüfen.

Dabei ist zu berücksichtigen, dass die Informationspflicht nicht nur gegenüber der Datenschutzbehörde bestehen kann, sondern in Fällen eines erhöhten Risikos für den Betroffenen auch gegenüber dem Betroffenen selbst gemäß Artikel 34 DSGVO. Im letzteren Fall kann die Information, wenn sie mit einem unverhältnismäßigen Aufwand verbunden wäre (z.B. sehr große Zahl von Betroffenen), auch durch öffentliche Bekanntmachung oder eine ähnliche Maßnahme (z.B. öffentliche Bekanntmachung, Information in der Zeitung) erfolgen.

3. Offene Kommunikation des Falles

Transparent und korrekt mit so einem Vorfall umzugehen, bedeutet sich der öffentlichen Diskussion zu stellen. Bei einem korrekten Umgang mit dem Fall sollte dies zu einer positiven öffentlichen Meinung führen. Da die Gefahr für Betroffene inzwischen gebannt ist (siehe Punkt #1), wäre dem *responsible disclosure* Prinzip genüge getan und einer Veröffentlichung durch den Sicherheitsforscher oder epicenter.works stünde nichts mehr im Wege.

Eine transparente Kommunikation von Seiten des Ministeriums sollte auch die Verantwortlichkeiten des externen Dienstleisters aufzeigen, so dieser ursächlich mit dem Fall verbunden ist oder seinen Pflichten nicht nachgekommen ist.

4. Etablierung eines Bug Bounty Programmes

Essentiell in der Bewertung des Falles sind die daraus gezogenen Lehren. Zur **Rückgewinnung von Vertrauen** und um die künftige Meldekultur von Sicherheitslücken zu stärken, wird **stark die Errichtung eines Bug Bounty Programmes im BMK empfohlen**.[1]

Ein solches Program bietet symbolische Geldbeträge (wenige hundert Euro) für Sicherheitsforscher:innen, wenn diese Lücken verantwortungsvoll und vertraulich melden. Dadurch wird Schaden von staatlichen IT-Systemen und Betroffenen abgewendet und die Verantwortlichen sparen sich in Wirklichkeit die um ein vielfaches höheren Kosten derartiger Sicherheitsüberprüfungen in der Privatwirtschaft (penetration test, red teaming). Diese Programme sind Gang und Gäbe in der Privatwirtschaft und bei mehreren Regierungen weltweit.

Zuletzt wird damit auch ein geordneter Kanal und Gewissheit für die Sicherheitsforscher:innen geschaffen. Es gab in Österreich bereits Fälle, in denen es zu Anzeigen durch (Grün geführte) Ministerien gegen jene kam, die Sicherheitslücken verantwortungsvoll gemeldet haben. Der zuständige Minister musste sich im Nachgang entschuldigen.[2] Ein Bug Bounty Program hätte hier Abhilfe geschaffen.

5. Einrichten von schnellen und effektiven Kommunikationswegen für Sicherheitsvorfälle

Die erste Meldung erfolgte auf servicebuero@bmk.gv.at und es vergingen einige Tage, bevor sie bearbeitet wurde. Das deutet auf ein fehlendes Sicherheitsmanagement hin. Es sollten dedizierte Kommunikationskanäle für Sicherheitsvorfälle eingerichtet werden. Diese sollten auch über den gängigen Weg mittels einer Security.txt kommuniziert werden.[3]

6. Alternativer Weg den Service auf Klimabonus.at anzubieten

Die Authentifizierung mittels eines Ausweisbildes ist nicht als sicheres Verfahren einzustufen und kann angesichts der Dauer der Legislaturperiode bereits als aussichtslos erachtet werden. Ein besseres Verfahren bietet die ID Austria Authentifizierung. Ausschließlich auf ID Austria zu setzen würde jedoch Bevölkerungsschichten ausschließen und wäre nach EU-Recht illegal (siehe Artikel 5a(15) von Verordnung (EU) 2024/1183). Deshalb sollten jedenfalls weiterhin Alternativen angeboten werden. Dabei wäre auf die bestehende Hotline zu verweisen oder ein RSA Brief als analoge Authentifizierungsmethode zu prüfen.

Jedenfalls sollten die Daten einer Person künftig nur noch nach ausreichender Authentifizierung zur Verfügung gestellt werden.

1 https://de.wikipedia.org/wiki/Bug-Bounty-Programm
2 https://epicenter.works/content/kritische-sicherheitsluecken-aufgedeckt-ministerium-zeigt-ngo-an
3 https://securitytxt.org/