Von:
Gesendet: Freitag, 20. Mai 2022 14:53
An: REFERAT15@bfdi.bund.de

Betreff: 220520_Sachstandsinformation - Meldung eines Datenschutzvorfalls, AZ: 1400.06.004023.2022

Stabsstelle Datenschutz: Az.: 1400.06.004023.2022

Sehr geehrte Damen und Herren,
sehr geehrter Herr

unter Bezug auf den Ihnen bereits am Mittwoch gemeldeten Vorfall möchten wir gerne Transparenz schaffen und über den aktuellen Sachstand informieren. Die Ursache liegt in einem menschlichen Versagen im Rahmen einer fehlerhaften Softwareversorgung. Das Online-Portal der BA steht 7*24 Std. den Kundinnen und Kunden zur Verfügung. Auf der hochmodernen Online-Container Plattform müssen im Zyklus von spätestens zwei Wochen die aktualisierten Base Images (OS-Patches = Betriebssystem-Patches) auf die Produktionsumgebung ausgeliefert werden. Dies ist eine Vorgabe der IT-Sicherheit und erfolgt im Normalfall automatisiert durch die jeweiligen sog. Build-Pipelines („ vorgegebene automatische Ausrollverfahren").

Aufgrund einer festgestellten Inkompatibilität der vorliegenden OS-Patches mit der bestehenden Software musste hierbei eine Datei der Build-Pipeline (sog. Dockerfile) für alle Umgebungen angepasst werden. Dabei wurde für das Dockerfile für die Produktionsumgebung irrtümlich auf den Entwicklungsstand der Software referenziert und ausgerollt. Das Ausrollen – also die fehlerhaft Aktualisierung - erfolgte um 8.00 Uhr morgens, nach Feststellung und Analyse des Fehlers wurde das Onlineportal um 9.35 heruntergefahren und der Fehler korrigiert.

Mögliche Konsequenz: Damit es dann zur Situation kommen konnte, dass man Daten eines anderen Nutzers einsehen konnte, mussten mindestens zwei Nutzer nahezu gleichzeitig (Millisekunden-Bereich) auf der gleichen Container-Instanz (Systemumgebung) angemeldet werden. Dann konnte es passieren, dass der zweite Nutzer das noch vorhandene Account-Objekt („Anmeldedaten") des ersten Nutzers überschreibt (mit seinen Account-Daten) und der erste Nutzer, wenn sein Passwortcheck bereits erfolgreich durchgeführt wurde, die Daten des zweiten Nutzers bekommen hat. Je nach zeitlicher Abfolge (im Sekundenbereich) der Anmeldungen kam es aber auch zu Fehlermeldungen bei der Anmeldung oder „Passwort- falsch"-Meldungen und keiner Anmeldung.

Der Vorgang ist technisch höchst komplex. Eine Vereinfachung könnte die Darstellung unpräzise werden lassen.

Wichtig: Der Fehler, dass Benutzer die Benutzerdaten eines anderen angemeldeten Benutzers sehen konnten, trat nur auf wenn beide Benutzer auch in derselben Container-Instanz angemeldet waren. In der Online-Produktionsumgebung der BA arbeiten 8 Container-Instanzen gleichzeitig um möglichst performant die Online-Leistungen zur Verfügung zu stellen – damit reduziert sich der Kreis der Betroffenen – nach Auskunft der IT – von ca. 27.000 Anmeldungen in dem betroffenen Zeitraum (18.05.22 von 8:00 – 9:35) **auf max. 3577** (entspricht der Anzahl Fehlermeldungen in den internen Logs) betroffene Anmeldungen.

Höchstwahrscheinlich ist die Anzahl der Betroffenen jedoch erheblich geringer, da „nahezu gleichzeitige Anmeldungen" von Benutzern sehr viel seltener sind.

Die genaue Zahl und auch die Namen der Betroffenen können aufgrund der temporären Systemspeicher in den Containern leider nicht mehr festgestellt werden.

Vor dem Hintergrund, dass Maßnahmen datenschutzrechtlicher Natur auch verhältnismäßig zu der technisch festgestellten wahrscheinlichen Anzahl der Betroffenen sein müssen, halten wir eine Information an alle Kundinnen und Kunden der BA für unangemessen. Der Fehler wurde durch menschliches Versagen verursacht und eine Verunsicherung der Kunden hinsichtlich der Systeme der BA ist wegen des Vermittlungsauftrages kontraproduktiv. Den in der Stabsstelle Datenschutz bekannt gewordenen Fällen ist zudem gemein, dass die Kundinnen und Kunden – die Zugriff auf fremde Daten hatten – neben der berechtigten Kritik sehr verantwortungsbewusst sind. Vor diesem Hintergrund erscheint zumindest unwahrscheinlich, dass ein hohes Risiko für Rechte und Freiheiten der betroffenen Personen anhält.

Beschwerdeführer werden selbstverständlich nach Art. 34 DSGVO informiert.

Maßnahmen zum Wiederholungsausschluss dieses Fehler sind in der IT bereits umgesetzt:

- Erstellen und Anwendung eines (Regressions-)Testfalls für die aufgetretene Konstellation
- Noch stärkere Trennung von Code- und Konfigurations- und Build-Artefakten in den Pipelines
- Vier Augen Prinzip bei Änderungen der Produktions-Deployments ist zukünftig zwingend vorgegeben um die automatischen Pipelines zusätzlich abzusichern.

Geplant ist zudem ein interner "Security-Reifegrad-Audit".

Der IT-Bereich, der Presse-Bereich und die Stabsstelle Datenschutz stehen in engem Austausch. Soweit sich in der Angelegenheit Neuigkeiten ergeben, informieren proaktiv. Eine Information für die Kundinnen und Kunden ist hier zu finden.

Für Fragen stehe ich gern zur Verfügung.

Mit freundlichen Grüßen
im Auftrag

Stabsstelle Datenschutz

Bundesagentur für Arbeit
Zentrale
Regensburger Straße 104
90478 Nürnberg