Gysin Katja EDÖB

Von:	Lobsiger Adrian EDÖB
Gesendet:	Donnerstag, 31. Oktober 2024 12:02
An:	_EDÖB Sekretariat
Cc:	Sidler Andreas EDÖB; Castiglione Alexandra EDÖB; Henguely Florence EDÖB; _EDÖB-KOM
Betreff:	Vischer AG. 20241031. OneLog

Eingang

Von: [redacted]
Datum: 31. Oktober 2024 um 10:05:58 GMT
An: Lobsiger Adrian EDÖB [redacted]
Betreff: OneLog

EDÖB - PFPDT
IFPDT - FDPIC
act. [redacted]

Lieber Adrian

Die OneLog AG (**OneLog**) hat uns in der Dir bekannten Data-Breach-Angelegenheit mit der Unterstützung und Vertretung mandatiert. Eine erste Information erfolgte über [redacted], und in der Folge lief einiges zur Aufarbeitung des Zwischenfalls. Dies beinhaltete auch eine erste Einschätzung des Risikos der einzelnen betroffenen Personen, welches als nicht hoch eingestuft wurde.

Aus diesem Grund erfolgte auch keine formelle Meldung an Dich, da eine solche über Euer Meldeformular nur möglich ist, wenn der Verantwortliche offiziell mitteilt, dass er von einem hohen Risiko für die betroffenen Personen ausgeht. Da OneLog bisher nicht davon ausgegangen ist und weiterhin nicht davon ausgeht, dass ein solches vorliegt, meldete sie konsequenterweise nicht. Es wäre nicht richtig gewesen. Ich hoffe, Du kannst das nachvollziehen.

OneLog kann aber gut nachvollziehen, dass Du gerne weitere Angaben zum Zwischenfall haben möchtest, und es liegt Ihr (und den beteiligten Partnern) daran, Dich hier zu informieren. Darum vertraulich meine E-Mail mit folgenden Informationen zum gegenwärtigen Stand der Dinge:

- Am 23. Oktober 2024 um 21:35 Uhr UTC erfolgte ein Zugriff auf von OneLog bei AWS betriebene Cloud-Instanz. Der unbekannten Täterschaft gelang es trotz Sicherungen (inklusive MFA) an die Zugangsdaten für die Root-Accounts zu gelangen und diese erfolgreich zu benutzen, um über die Management-Konsole mehr oder weniger sämtliche Daten in den verschiedenen Instanzen, inklusive der dort befindlichen Backups zu löschen (nicht jedoch alle Logs).
- Betroffen waren bei OneLog (als Verantwortliche) folgende Personendaten: E-Mail, UserID und ein Passwort-Hash (mit Salt; das Passwort muss aus mindestens acht Zeichen, einer Zahl sowie Gross- und Kleinbuchstaben bestehen) sowie bei einem geringeren Teil noch Anrede, Vorname und Nachname. Ferner waren auf dem System natürlich auch Benutzer- und Systemlogs. Gewisse Brands nutzen OneLog zusätzlich zur Speicherung weiterer Daten wie Geburtsjahr, Adresse, Mobile-Nummer und Nickname, in welchen Fällen OneLog als Auftragsbearbeiterin fungiert. OneLog hatte Datensätze von 3.5 Mio. Benutzerinnen und Benutzern.
- Die Daten werden nun anhand anderer Kopien wiederhergestellt, aber das wird noch einige Tage dauern. Vorher ist ein Passwort-Reset nicht nötig und möglich.
- OneLog geht davon aus, dass die Verfügbarkeit der Daten vorübergehend betroffen gewesen sein wird; ob auch die Vertraulichkeit betroffen war, wird sich zeigen müssen. Die Daten waren at-rest verschlüsselt (d.h. zusätzlich zum Passwort-Hash). Ob die Daten im Rahmen des Zugriffs entschlüsselt wurden oder bei den gegebenen Einstellungen überhaupt werden konnten über die Management-Konsole, ist noch nicht klar. Der

Zugriff dauerte gemäss ersten Hinweisen jedoch nur relativ kurze Zeit und fokussierte auf die Löschung von Daten und Verändern von Parametern, um den Wiederanlauf zu erschweren.

- Es wurde mit einem erfahrenen Unternehmen sofort eine forensische Untersuchung eingeleitet, auch um festzustellen, ob es um "blosse" Sabotage geht, oder auch Anhaltspunkte über einen möglichen Datenabfluss bestehen. Aktuell gibt es für letzteres keine Anhaltspunkte (die Experten gingen gegenüber OneLog von einer Wahrscheinlichkeit von 70% aus, dass es zu keinem Datenabfluss gekommen ist). Somit deuten die bisherigen Hinweise im Moment dahingehend, dass es sich um einen Sabotageakt handelte. Bekennerhinweise oder Erpresserforderungen gab es bisher keine. Es findet ein laufendes Darknet-Monitoring statt, wo ebenfalls bisher keine Hinweise auf den Vorfall aufgetaucht sind, auch nicht von etwaigen Trittbrettfahrern, wie sie manchmal vorkommen.
- Die Polizei wurde eingeschaltet, bisher ohne Ergebnisse.
- Unabhängig von der Wiederherstellung des Service können die Dienstleistungen der diversen Partner weiter genutzt werden (die Paywalls wurden deaktiviert). Wir haben vernommen, dass sich Personen bei Euch beschwert haben, dass sie keinen Zugang zu ihren CVs mehr haben. Dies betrifft die Anwendung JobCloud und spezifisch die Funktion, dass Benutzerinnen und Benutzer bei einer Bewerbung ihren hinterlegten CV vom System automatisch abfüllen lassen können. Dies geht derzeit nicht. Ansonsten kann JobCloud genutzt werden (auch Bewerbungen sind möglich). JobCloud stellt OneLog notabene keine Kunden-, Profil- oder Lebenslaufdaten seiner Benutzerinnen und Benutzer zur Verfügung. So bald OneLog ihre Funktion wieder aufnimmt, stehen die Funktionalitäten und Daten den Benutzerinnen und Benutzer von JobCloud wie gewohnt zur Verfügung.

Bitte beachte, dass die vorstehenden Angaben lediglich derzeit vorhandene Informationen wiedergeben. Es können sich jederzeit neue Erkenntnisse ergeben; die Experten arbeiten noch. Die Aufarbeitung des Vorfalls wird selbstverständlich auch eine Überprüfung der Informationssicherheit beinhalten, damit sich ein solcher Vorfall nicht wiederholt.

OneLog will die betroffenen Personen informieren, hat aber die besondere Herausforderung, dass es ihr technisch nur möglich ist, eine relativ geringe Anzahl von E-Mail am Tag zu versenden, wobei das Kontingent auch E-Mails für Passwort-Rücksetzungen umfasst, die dann weiterhin möglich bleiben müssen. Würde sie die 3.5 Mio. Kunden per E-Mail informieren, würde dies tägliche Versendungen über eine Zeitdauer von zwei Monaten bedeuten bis alle erreicht wären. Solange will OneLog nicht warten. Daher wird via Medien-Mitteilung bzw. über die Plattformen der OneLog-Partner informiert werden, wie dies Art. 24 Abs. 5 Bst. c DSG im Fall einer Meldepflicht auch vorsieht. Die Information soll insbesondere beinhalten, was die betroffenen Personen müssen, um ihr Login zu reaktivieren, da ein neues Passwort gesetzt werden muss. Es wird auch darauf hingewiesen, dass dasselbe Passwort nicht für mehrere Dienste eingesetzt werden sollte. Ferner wird kurz informiert, um welche Art der Verletzung es geht, welche Massnahmen getroffen wurden, und wohin sie sich mit Fragen wenden können.

OneLog geht jedoch aufgrund der Passwort-Komplexitätsvorgaben derzeit nicht davon aus, dass das Passwort innert sich lohnender Zeit geknackt werden kann, selbst wenn die verschlüsselten Daten entschlüsselt und exfiltriert worden wären, wofür es derzeit keinen Hinweis gibt. Bei OneLog könnten diese Passwörter ohnehin nicht mehr benutzt werden, da alle Benutzer ein neues Passwort setzen müssen. Das primäre Risiko sieht Onelog darüberhinaus derzeit in der unzulässigen Verwendung der E-Mail-Adresse, namentlich durch Zusendung von mehr Spam. Dagegen kann eine betroffene Person ohnehin keine Massnahme treffen, und dies stellt zwar eine Unannehmlichkeit dar, aber rechtlich kein hohes Risiko. OneLog sieht in Bezug auf die von ihr verantworteten Daten aufgrund der Umstände derzeit auch kein hohes Risiko in Bezug auf Phishing, Identitätsdiebstahl oder Betrug. Daher ist sie im Rahmen ihrer Risikobeurteilung zum Schluss gelangt, dass für die einzelnen betroffenen Personen kein hohes Risiko vorliegt.

Ich hoffe, dass diese vertraulichen Informationen Euch für den Moment weiterhelfen. An der öffentlichen Kommunikation wird – in Abstimmung mit den Partnern – derzeit gearbeitet und mit einer ersten kurzen weiteren öffentlichen Kommunikation ist heute zu rechnen, später gefolgt von weiteren (dann, wenn die Benutzer ihr Login tatsächlich wieder benutzen können).

In Bezug auf die betroffenen Daten, die OneLog für einzelne Partner als Auftragsbearbeiterin bearbeitet hat, werden die betreffenden Partner soweit erforderlich direkt auf Dich zu kommen; die technischen Hintergründe sind dieselben. Solltest Du dies wünschen, können wir dies gerne weitermelden.

Für weitere Fragen stehen wir gerne zur Verfügung. Ich bin bereits in verschiedenen anderen Meetings besetzt, aber wir können gerne heute Abend sprechen, wenn Du dies möchtest. Schreibe mir doch einfach kurz.

Gruss,

David

VISCHER AG

[redacted]