Schweizerische Eidgenossenschaft
Confederation suisse
Confederazione Svizzera
Confederaziun svizra

**Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter**
**EDÖB**

Informationstechnologien, Geschäfte
Informationstechnologien



# 20241114 Protokoll TelKo zum Fall Onelog

Aktenzeichen: 215.0765267

| | | | |
|---|---|---|---|
| Teilnehmende | lic. iur. David Rosenthal, Vischer AG Rechtsvertretung Onelog AG, Rignier AG<br>Silvano Oeschger, CEO, Onelog AG<br>[redacted], Group Chief Information Security Officer, Ringier AG<br>[redacted] DPO, Onelog AG<br><br>Alexandra Castiglione, EDÖB<br>Fritz von Allmen, EDÖB<br>Marco Beck, EDÖB | | |
| Datum | Donnerstag, 14. November 2024 10:30 | Aktennotiz | ☐ |
| Version | 0.30 | Beratung | ☐ |
| Autoren | Marco Beck EDÖB<br>Fritz von Allmen EDÖB<br>Alexandra Castiglione EDÖB | Medienanfrage | ☐ |
| Klassifizierung | INTERN | Auskunftsgesuch | ☐ |
| Status | In Arbeit | Besprechungsnotizen | ☒ |
| Link GEVER | | Sitzungsprotokoll | ☐ |

[redacted]

## Inhaltsverzeichnis



## Änderungsverzeichnis

| Datum | Version | Änderung | Autor |
|---|---|---|---|
| 13.11.2024 | 0.10 | AVOR für TelKo | Marco Beck |
| 14.11.2024 | 0.20 | Erste Version nach der TelKo | Marco Beck |
| 26.05.2025 | 0.30 | Berichtigung nach Art. 41 DSG | Katja Gysin |
| | | | |

# 1 «Drehbuch» für die TelKo

## 1.1 Neuigkeiten

| Fragestellungen | Antworten |
|---|---|
| Gibt es weitere Entwicklungen seit der Information des EDÖB vom 31. Oktober und vom 4. November und 8. November? | Keine neuen Entwicklungen seit der letzten Information an den EDÖB.<br><br>OneLog hat auch eine «vorsorgliche» Meldung bei der EU gemacht. Dies weil 2 Firmen (aus der TX-Group) die OneLog nutzen ihren Geschäftssitz in der EU haben.<br>Die Meldestellen haben die Information zur Kenntnis genommen.<br>Die Luxemburgische Behörde hat jedoch nachgefragt, wieso OneLog diese Meldung gemacht hat, da sie dies nicht nachvollziehen können. |
| Welche Arbeiten laufen momentan noch? | Die Ermittlungen sind immer noch am Laufen.<br><br>Alle betroffenen Systeme sind online und funktionieren wieder.<br><br>Es gibt jedoch einzelne User, die mit dem Login Probleme haben. Diese werden via Support unterstützt. |
| Welche Arbeiten sind geplant? | Es soll sichergestellt werden, dass ein solcher Vorfall nicht wieder vorkommen kann.<br><br>Es gibt keine Timeline für etwelche weitere Arbeiten. |
| Sind aktuell noch Abklärungen im Gange?<br><br>Wenn ja welche? | Ja, unter anderem bei der Polizei, dem BACS und bei den involvierten Forensikern. |
| Was ist der Stand der forensischen Untersuchung und welche neuen Erkenntnisse haben sich daraus ergeben? | Untersuchung ist noch am Laufen.<br><br>Bis jetzt sind keine Trittbrettfahrer festgestellt worden.<br><br>Auch wurden keine Forderungen gegenüber OneLog gestellt.<br><br>Es ist jedoch nicht mit raschen Ergebnissen zu rechnen. |

| Fragestellungen | Antworten |
|---|---|
| Wurde Anzeige erstattet?<br><br>Falls ja: gibt es bereits polizeiliche Erkenntnisse? | Ja, bei der Polizei (Annahme: KaPo ZH) |
| Aus Ihren Mails entnehmen wir, dass folgende Datenkategorien betroffen waren:<br><br>- E-Mail<br>- UserID<br>- Passwort-Hash<br>Sowie je nach Medienunternehmen:<br>• *Geburtsjahr*<br>• *Adresse*<br>• *Mobile-Nummer*<br>• *Nickname*<br>• *Nationalität*<br>• *Universität*<br>• *Geburtsdatum*<br>• *Personalausweis-/Steuer-/AHV-Daten (jobs.ch)*<br><br>Ist diese Aufzählung vollständig oder fehlt noch etwas?<br><br>Welche Datenkategorien fehlen evtl. noch? | Die drei Datenkategorien (E-Mail, UserID und Passwort-Hash) werden durch OneLog AG erhoben. Die restlichen Datenkategorien werden im Namen der angeschlossenen Medien-Firmen erhoben und OneLog AG ist hier der Auftragsverarbeiter. Diese Daten werden nur für einzelne Firmen erhoben und die Daten ihnen weitergegeben.<br><br>Die UserID ist nicht die OneID. Die UserID ist nur für das SSO Portal von OneLog. Die UserID wird aus einem Random-Wert gebildet.<br><br>Es sind aktuell keine weiteren Datenkategorien betroffen.<br><br>Die OneLog SSO-Plattform und die OneID sind zwei komplett unabhängige Produkte der OneLog AG. Von der Löschung der Daten ist nur die OneLog SSO-Plattform betroffen. |

## 1.2 Ablauf und Details zur Cyber-Attacke

| Fragestellungen | Antworten |
|---|---|
| Ist der Angreifer bekannt?<br><br>Wurde Anzeige erstellt? | Nein, Ermittlungen sind noch am Laufen. Jedoch schätzen sie die Chancen, dass der/die Angreifer Identifiziert werden, als sehr klein ein.<br><br>Anzeige wurde bei der Polizei gemacht. |
| Wie war es möglich den Root Account AWS zu hacken?<br><br>Erklärung, wie die MFA bypassed wurde?<br><br>Phishing? | [redacted] |
| Wie viele Instanzen?<br>Welcher Plan / Service liegt den Instanzen zugrunde?<br>Analyse von Monatsrechnung / Volumes? | Es war die ganze SSO-Plattform betroffen. |
| Malware detektiert? | Gemäss Logs wurden keine weiteren Aktivitäten festgestellt bzw. es wurden keine Anzeichen für Malware Installationen festgestellt. |
| Wie wurde geprüft, ob Daten abgeflossen sind?<br><br>Analyse von Netzwerktraffic?<br><br>AWS Cloudtrail / Server Access Logs | Die relativ kurze Zeit der Intervention deutet auf keinen Datenabfluss hin. Zudem wurden in den Logs keine Hinweise auf einen Datenabfluss gefunden.<br><br>Die Login-Daten wurden zwar alle gelöscht, jedoch waren die Log-Dateien noch vorhanden. |

Die Informationen dieses Teils sind strittig bzw. Gegenstand eines gerichtlichen Verfahrens.

| Fragestellungen | Antworten |
|---|---|
| Gibt es Szenarien, die sie ausschliessen können?<br>Z.B. Angriff von Geheimdiensten, Datenlöschung nur um Spuren eines gezielten Angriffs zu verwischen, Backdoors eingerichtet? | -- |
| Wie gelang es die gelöschten Daten wiederherzustellen? | Die Login-Daten werden zu den Medien-Partner repliziert, jedoch ohne Passwort-Hash. Mit diesen replizierten Daten konnten die SSO-Daten wieder hergestellt werden.<br><br>Es ist noch geplant, dass auch die Zusatzdaten bei OneLog wieder hergestellt werden. Dies ist jedoch eine Entscheidung der einzelnen Medien-Partner. |
| Weitere Details aus dem forensischen Bericht? | Die Login-Daten wurden zwar alle gelöscht, jedoch waren die Log-Dateien nicht davon betroffen. Mit diesen Log-Daten werden noch weiter analysiert. |

### 1.3 Betroffene Daten und Zwecke

| Fragestellungen | Antworten |
|---|---|
| Wie ist die Auftellung zwischen OneLog und den Publishern punkto Verantwortlichkeit / Auftragsbearbeitung?<br><br>Für welche Daten ist OneLog selbst Verantwortlicher? | Für das OneLog SSO-Portal bzw. deren Login-Daten hat die OneLog AG die volle Verantwortung.<br><br>Für die Zusatzdaten auf dem SSO-Portal ist die OneLog AG in der Rolle des Auftragsbearbeiters.<br><br>Sie betonen nochmals, dass OneLog SSO und OneID zwei unabhängige Produkte der OneLog AG sind und NUR die OneLog SSO-Daten sind von diesem Vorfall betroffen. |
| Sind Profilingdaten* von dem Ereignis betroffen?<br><br>Wo liegt die Data Management Plattform (DMP)?<br><br>Wurden die Nutzerprofile gelöscht und müssen somit neu aufgebaut werden?<br><br>(*Erstellung und Verwendung von Profilen für personalisierte Werbung) | [redacted] Die Informationen dieses Teils sind strittig bzw. Gegenstand eines gerichtlichen Verfahrens. |
| Inwiefern kann ausgeschlossen werden, dass Daten von Betroffenen kompromittiert wurden, welche nicht OneLog genutzt haben? | -- |
| Gestützt auf welche Anhaltspunkte wurde das Risiko für die Betroffenen als nicht hoch eingestuft?<br><br>Hat sich an dieser Einschätzung aufgrund der gewonnenen Erkenntnisse etwas geändert?<br><br>Wie wurde der Umstand gewichtet, dass 3,5 Mio Nutzer betroffen sind? | Ihre Einschätzung kommt davon, dass nur das Login vom Vorfall betroffen war.<br><br>Bis auf die nicht Verfügbarkeit der Kommentar-Funktion, gab es aus Sicht von OneLog AG keine Einschränkungen für die User.<br><br>Denn die Paywall war deaktiviert, es gab kein Login, bei welchem das Passwort hätte missbraucht werden können und mit Spam und Phishing müssen die User so oder so rechnen. |

### 1.4 Weiteres Vorgehen:

Das gelieferte FAQ-Dokument kann den Personen weitergegeben werden, die sich beim EDÖB melden.

Herr Rosenthal weist noch darauf hin, dass sie uns in diesem Gespräch Informationen weitergegeben haben, die von ihnen nicht veröffentlicht werden.

Sie werden den EDÖB gerne bei weiteren Erkenntnissen wieder informieren.

### 1.5 Weiterführend:

#### 1.5.1 Mögliche Angriffsvektoren gegen AWS S3:

Die folgenden Fragen wurden nicht gestellt, wurden bereits beantwortet oder sind auf Grund der bisherigen Antworten obsolet. Sie verbleiben jedoch zur Vollständigkeit im Dokument.

| Fragestellungen | Antworten |
|---|---|
| Public Bucket Exposure (S3 Enumeration) | |
| Credential Leak (Suspicious Bucket Deletion Activity) | |
| Privilege Escalation | |
| Ransomware Attack | |
| Data Exfiltration | |
| Exploiting Misconfigured Bucket Policies (z.B. Replication Policy Misuse) | |

#### 1.5.2 Untersuchungen:

Die folgenden Fragen wurden nicht gestellt, wurden bereits beantwortet oder sind auf Grund der bisherigen Antworten obsolet. Sie verbleiben jedoch zur Vollständigkeit im Dokument.

| Fragestellungen | Antworten |
|---|---|
| S3 Enumeration | |
| Suspicious Bucket Deletion Activity | |
| Data Exfiltration / Bucket Replication | |