Liebe Kundin, lieber Kunde

OneLog – das Login-Tool der Schweizer Medien- und Verlagshäuser und ein Gemeinschaftsunternehmen von CH Media, NZZ, Ringier und TX Group – ist wieder verfügbar.

Die Nutzerinnen und Nutzer werden bei der OneLog-Anmeldung auf den Webseiten der jeweiligen Marken (z.B. bei Blick) im Login-Prozess automatisch aufgefordert, ein neues Passwort zu setzen. Anschliessend erhält die Nutzerin oder der Nutzer von OneLog eine E-Mail zum Password-Reset.

Vorsicht vor Phishing: Ohne ein vorheriges aktives Anstossen des Logins durch die Nutzerin oder den Nutzer versendet OneLog keine derartige Aufforderung per E-Mail. Dies gilt auch für die einzelnen Medienmarken und andere Partner (z.B. JobCloud), die OneLog einsetzen.

Wie immer sollen Nutzerinnen und Nutzer für jede Anwendung und jeden Dienst ein einmaliges, starkes Passwort wählen. Nur so bleibt die Sicherheit anderer Konten auch dann gewährleistet, wenn ein einzelnes Passwort kompromittiert wird – wofür bei OneLog weiterhin keine Hinweise vorliegen. OneLog geht vielmehr von einem Cyber-Sabotageakt aus; die Ermittlungen zum Cyber-Sabotageakt werden derweil unter Einbezug der zuständigen Behörden weitergeführt.

Bei Fragen zum Datenschutz kann man sich an die Datenschutzstelle von OneLog unter datenschutz@onelog.ch wenden.

OneLog setzt alles daran, seinen Nutzerinnen und Nutzern eine stabile und vertrauenswürdige Umgebung zu gewährleisten und bedauert die entstandenen Unannehmlichkeiten.

Updates

Medienmitteilung vom 23.12.2024

Q&A

Die wichtigsten Punkte

- **Art des Angriffs:**
  OneLog geht von einem Sabotageangriff aus, nicht von einem Diebstahl oder unerlaubten Aneignung (Exfiltration) von Daten.
- **Persönliche Daten:**
  Es gibt derzeit keine Hinweise darauf, dass persönliche Daten, einschliesslich persönlicher Informationen oder Passwörter, gestohlen wurden. OneLog verwaltet keine sensiblen Daten wie Kreditkartendaten oder Informationen aus Lebensläufen.
- **Plattform-Funktionalität:**
  Der Sabotage-Angriff hat die Funktionalität der Plattform beeinträchtigt, was zu einer vorübergehenden Unterbrechung der Anmelde- und Registrierungsdienste führte. Seit dem 4.11.2024 sind die OneLog Systeme wieder verfügbar.

Unsere Empfehlungen

- Auch wenn aktuell keine Hinweise vorliegen, dass Passwörter von Benutzerinnen und Benutzern von OneLog kompromittiert wurden, empfiehlt OneLog, vorsorglich das bei OneLog verwendete Passwort zu ändern, insbesondere wenn dasselbe Passwort auch auf anderen Plattformen verwendet wird.
- Vorsicht vor Phishing-Versuchen (z.B. Trittbrettfahrern): OneLog versendet keine Mails zur Passwortänderung ohne vorheriges aktives Anstossen des Logins durch den Nutzer.
- OneLog versendet ausschliesslich und nur nach vorherigem aktivem Anstossen durch den Nutzer/-in ein Passwort-Rücksetzungsmail. Insofern der Nutzer/-in ein solche Aufforderung unerwünscht erhält, ist dies ein Phishing-Versuch. Ein nicht angefordertes Mail sollte umgehend gelöscht werden.
- Partner von OneLog (z.B. Blick, Handelszeitung und Beobachter) haben ihre User/-innen teilweise auch direkt über die

Wiederverfügbarkeit von OneLog und über den weiteren Prozess informiert.
- Nutzer/-innen wenden sich bei Fragen zum Thema Datenschutz an die Datenschutzstelle von OneLog unter datenschutz@onelog.ch bzw. an die Datenschutzstellen der jeweiligen Medien- und Partnermarken.

Zum Vorfall

- OneLog geht derzeit davon aus, dass es sich um einen Sabotageakt handelt. Es gibt derzeit keine Hinweise darauf, dass persönliche Daten, einschliesslich persönlicher Informationen oder Passwörter, gestohlen wurden.
- OneLog hatte keine sensiblen Daten wie Kreditkartendaten oder Informationen aus Lebensläufen. Es waren auch keine Daten aus den Abo- oder Bezahlsystemen in die Systeme von OneLog repliziert worden. Was OneLog verwaltet sind Login-Daten (wobei Passwörter nur als Hashwert mit besonderem Schutz gespeichert sind), Logs und je nach Partner noch (in der Minderheit) Zusatzdaten wie z.B. ein bei der Registrierung erfasstes Geburtsdatum oder eine Adresse für eine Teilnahme an einem Wettbewerb.
- OneLog hatte vor dem Hintergrund laufender Ermittlungen regelmässig informiert und dabei sehr genau abgewogen, welche Informationen öffentlich geteilt werden. Dies war - und ist weiterhin - notwendig, um der vermeintlichen Täterschaft keine wertvollen Details aus der Ermittlungsarbeit zu liefern oder Trittbrettfahrer (z.B. für Phishing-Angriffe) mit Informationen zu versorgen. Aus diesem Grund können z.B. auch keine detaillierten Angaben zum verwendeten Verschlüsselungs-Algorithmus für die Daten und Passwörter gemacht werden oder welche Erkenntnisse sich aus den Logs ergeben. Die Wiederherstellung des OneLog Services und die Integrität der Ermittlungen haben jeweils oberste Priorität.
- Wie es seit der Gründung von OneLog der Fall ist, steht OneLog auch jetzt mit dem EDÖB in Kontakt (nebst den Strafverfolgungs- und weiteren Behörden).

- Partner von OneLog wie z.B. Blick, Handelszeitung und Beobachter haben Ihre User/-innen selbst direkt informiert, dass der OneLog Service wieder verfügbar ist und welche Massnahmen die User gebeten werden, aktiv anzustossen müssen, um ein neues Passwort zu setzen. Das funktionierte bisher gut . Eine direkte E-Mail an alle bei OneLog registrierte Personen wurde unter anderem nicht vorgenommen, weil eine solche Massenmail zu einer teilweisen Blockierung der Absenderadresse geführt hätte und in der Folge Passwortrücksetzungen dort nicht mehr funktioniert hätten. Darum entschied sich OneLog dagegen.
- OneLog setzt umfangreiche Sicherheitsmassnahmen ein, um den Schutz der Nutzerdaten zu gewährleisten. Dazu gehören moderne Methoden wie Datenverschlüsselung, Multifaktor-Authentifikation, regelmässige Backups und Audit-Trails, die sicherstellen, dass alle Aktivitäten nachvollziehbar protokolliert werden. Zudem gibt es Vorgaben zur Passwortkomplexität und ein kontinuierliches Monitoring, das auch Audits durch unabhängige Dritte umfasst.
- Um die Sicherheit weiter zu stärken, betreibt OneLog ein BugBounty-Programm, das externe Sicherheitsexperten dazu einlädt, potenzielle Schwachstellen frühzeitig zu identifizieren und zu melden.
- Trotz dieser Massnahmen bleibt in der digitalen Welt immer ein Restrisiko bestehen, da sich Cyberbedrohungen und Angriffstechniken ständig weiterentwickeln und kein System absolut unverwundbar ist. Im Fall von OneLog wird von einem Cyber-Sabotageakt ausgegangen mit dem vermuteten Ziel, absichtlich Schaden an der digitalen Infrastruktur zu verursachen, die die Funktionsfähigkeit des Login-Tools beeinträchtigen sollte. Ohne hier in die Details zu gehen entspricht der Fall nach den bisherigen Erkenntnissen nicht dem klassischen Muster der sonst bekannten Ransomware-Attacken.