Sicherheitsvorfall beim SolNet Webmail – Stellungnahme vom 4. November 2026

Der Vorfall betrifft SolNet Kunden, welche den Webmail-Dienst (Roundcube) genutzt haben. Es liegen keine Hinweise auf eine unbefugte Übernahme von E-Mail-Konten vor.

Am 1. November wurden wir auf den Vorfall aufmerksam und haben umgehend das Bundesamt für Cybersicherheit (BACS) informiert. Der Fall wurde im Weekly Cybersecurity Report des Bundes publiziert und von Inside IT aufgegriffen.

Nachfolgend finden Sie die Antworten auf die offenen Fragen.

Was ist passiert und welche Daten sind betroffen?

Wir konnten bestätigen, dass veröffentlichte Beispieldaten aus Protokolldateien unseres Webmail-Dienstes stammen. Diese enthalten unter anderem E-Mail-Adressen, Empfänger, Betreffzeilen und Verbindungsdaten. In den untersuchten Protokolldaten waren Passwörter ausschliesslich maskiert dargestellt. Es wurden keine Passwörter im Klartext festgestellt.

Wer sich tatsächlich Zugang zu diesen Daten verschafft hat und wer sie derzeit besitzt, wissen wir nicht. Die im Forum genannten Mengenangaben können wir nicht bestätigen.

Unsere Untersuchung hat unberechtigte Zugriffe auf Protokolldateien unseres Webmail-Dienstes aufgrund einer Lücke bestätigt. Die betroffenen Versandprotokolle umfassen den Zeitraum vom 13. bis 31. Oktober 2026.

War die bekannte PHP-Schwachstelle die Ursache?

Nein. Die betreffende PHP-Schwachstelle wurde am 21. Oktober 2026 bekannt und auf unserem Server noch am selben Tag durch ein Sicherheitsupdate behoben. Unsere Untersuchung hat bestätigt, dass diese Schwachstelle beim vorliegenden Vorfall nicht ausgenutzt wurde.

Wurden betroffene Kunden informiert?

Ja. Die identifizierten betroffenen SolNet Kunden wurden am 2. November 2026 direkt durch mich als CEO informiert. Zusätzlich haben wir auf unserer Status-Website (https://www.solnet.ch/pages/tt-detail.php?id=2826) laufend über den Vorfall berichtet.

Vorsorglich haben wir den Kunden empfohlen, ihr E-Mail-Passwort im SolNet Kundencenter zu ändern und bei verdächtigen E-Mails besonders aufmerksam zu sein. Zusätzlich empfehlen wir die Aktivierung der Multifaktor-Authentifizierung.

Welche Massnahmen wurden eingeleitet?

Wir haben den Vorfall umgehend dem Bundesamt für Cybersicherheit (BACS) gemeldet und nach Identifikation der Quelle den betroffenen Webmail-Server vorsorglich ausser Betrieb genommen.

Die Webmail-Umgebung wurde neu aufgebaut und externen Sicherheitsprüfungen unterzogen. Seit dem 2. November 2026 ist der Webmail-Dienst wieder in Betrieb und wird laufend überwacht.

Besteht für uns weiterer Handlungsbedarf?

Wir empfehlen, auch bei E-Mails von bekannten Absendern auf verdächtige Inhalte zu achten. Zudem empfehlen wir jedem Unternehmen, sich beim Cyber Security Hub des Bundes anzumelden, um aktuelle Informationen und Warnungen zur Cybersicherheit zu erhalten.

Sollten sich neue Erkenntnisse ergeben, die weitere Kunden betreffen, werden wir diese direkt informieren.

Ich bedauere diesen Vorfall zutiefst. Die Sicherheit und der Schutz der Daten unserer Kunden haben für mich höchste Priorität.

Freundliche Grüsse

Erich Hohermuth
CEO
SolNet / BSE Software GmbH