Ausgleichskasse Swissmem

Informationsschreiben an Rentner, Direktleistungsbeziehende, Nicht- und Selbständigerwerbende

Informationsschreiben: Cyberangriff auf die Ausgleichskasse Swissmem

Sehr geehrte Damen und Herren

Wir wenden uns mit diesem Schreiben an Sie, um Sie über einen Sicherheitsvorfall bei der Ausgleichskasse (AK) Swissmem zu informieren. Sie sind oder waren seit 2020 Leistungsbezüger oder Beitragsbezahler bei der AK Swissmem.

Trotz umfassender Sicherheitsstandards wurde unsere Organisation Opfer eines sogenannten Cyberangriffs. Darunter versteht man den Versuch von Kriminellen, auf die Informationstechnologie-Systeme (IT) von Organisationen oder Firmen zuzugreifen, um auf Computern gespeicherte Daten zu entwenden, zu löschen oder zu verschlüsseln.

Als unsere Spezialisten am Wochenende des 4./5. Januar 2025 den Vorfall entdeckten, haben sie die Systeme sofort von der Aussenwelt getrennt. Nach einem Unterbruch laufen die vollständig neu aufgesetzten IT-Systeme seit Donnerstag, 9. Januar, wieder normal. **Die Auszahlung der Ihnen zustehenden aktuellen und zukünftigen Leistungen ist gesichert und erfolgt weiterhin in der üblichen Form.**

Umfassende Analyse- und Sicherheitsmassnahmen wurden mit Unterstützung durch externe Spezialisten umgehend eingeleitet. Die gesetzlich zuständigen Instanzen wie der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftrage (EDÖB), das Bundesamt für Sozialversicherungen (BSV) und das Bundesamt für Cybersicherheit (BACS) sind informiert und hinzugezogen worden. Die AK Swissmem hat den Angriff ausserdem der Kantonspolizei Zürich gemeldet und Strafanzeige erstattet.

Die bisherige Analyse ergab, dass beim Vorfall Daten der AK Swissmem verschlüsselt und gesperrt wurden. Wir konnten alle Daten wiederherstellen. Es gab keine Angriffe auf Bankkonten und es wurde kein Geld entwendet.

Leider steht mittlerweile hingegen fest, dass die Angreifer Daten entwendeten. Es könnte sich dabei um viele Arten von Daten handeln: Von Informationen zur Verwaltungstätigkeit der AK Swissmem bis zu Personendaten inkl. Angaben zu Leistungen oder Beiträgen. Es ist zum aktuellen Zeitpunkt nicht klar, um welche Daten es sich handelt. Deshalb ist eine Information, ob Daten von Ihnen persönlich überhaupt betroffen sind oder nicht, leider unmöglich. Bislang liegen keine Hinweise auf eine missbräuchliche Verwendung der Daten durch die Angreifer vor. Es wurden gemäss heutigem Wissensstand keine Daten veröffentlicht.

Dennoch raten wir Ihnen zu grosser Vorsicht: Seien Sie besonders wachsam gegenüber verdächtigen Postzuschriften, E-Mails, Nachrichten oder Telefonanrufen, die nach persönlichen Informationen fragen, oder Sie zu verdächtigen Handlungen auffordern. Geben Sie persönliche Daten oder Bankverbindungen auf keinen Fall unbedacht weiter. Konkrete Empfehlungen finden Sie auf der Rückseite.

Wir bedauern diesen Vorfall ausserordentlich und entschuldigen uns für daraus entstehende Unannehmlichkeiten und Probleme.

Pfingstweidstrasse 102
Postfach 42
8037 Zürich

www.ak-swissmem.ch

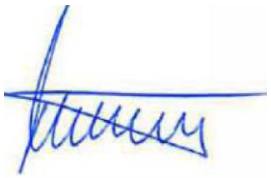
T 044 388 34 30

Zürcher Kantonalbank
IBAN CH45 0070 0110 0016 7770 7
Clearing 700

Ausgleichskasse Swissmem

Weitere Angaben zum Vorfall, insbesondere welche Daten betroffen sind, können wir leider nicht machen. Verbleibende Fragen zur Situation beantworten wir aber gerne bestmöglich über die Hotline unter 044 388 34 30; die zeitliche Verfügbarkeit erfahren Sie auf dieser Nummer. Den aktuellen Informationsstand finden Sie auch auf unserer Homepage www.ak-swissmem.ch.

Freundliche Grüsse
Ausgleichskasse Swissmem



Thomas Sommer
Präsident

Damian Keller
Geschäftsführer

Sicherheits- und Verhaltensempfehlungen:

- **Seien Sie besonders wachsam gegenüber verdächtigen Postzuschriften, E-Mails, Nachrichten oder Telefonanrufen, die nach persönlichen Informationen fragen, oder Sie zu verdächtigen Handlungen auffordern.**
- **Klicken Sie nicht auf Links in E-Mails oder SMS, welche Ihnen unaufgefordert zugesendet werden, oder bei welchen Sie ein ungutes Gefühl haben. Das gilt insbesondere dann, wenn in diesen Nachrichten zeitlicher Druck aufgebaut und/oder mit Konsequenzen gedroht wird.**
- **Lassen Sie sich nicht einschüchtern oder unter Druck setzen.**
- **Geben Sie niemals Passwörter oder PIN am Telefon oder per E-Mail bekannt.**
- **Geben Sie persönliche Daten oder Bankverbindungen auf keinen Fall unbedacht weiter.**
- **Gewähren Sie niemals fremden Personen Zugriff auf Ihren Computer, auch wenn Ihnen diese vertrauenswürdig erscheinen.**
- **Übergeben Sie niemals Bargeld oder andere Wertgegenstände an eine Ihnen unbekannte Person.**

Im Zweifelsfall hilft Ihnen das Bundesamt für Cybersicherheit (BACS) gerne bei der Beurteilung und mit Empfehlungen für das weitere Vorgehen: https://www.report.ncsc.admin.ch/de/.

Sind Sie betrogen worden und haben Sie einen finanziellen Verlust erlitten oder werden Sie bedroht respektive erpresst, dann bringen Sie den Fall bei der zuständigen Kantonspolizei zur Anzeige, in Notfällen auf 112 oder 117.