

Update zum Cyberangriff

Cyberangriff auf Softwarelieferanten: Was wir wissen und was nicht

Guten Tag

Wir informieren Sie erneut über den Cyberangriff auf unseren Softwarelieferanten PK Softech AG. Inzwischen wissen wir mehr darüber, was passiert ist. Gleichzeitig sind noch wichtige Fragen offen. Wir möchten Ihnen aufzeigen, was wir heute wissen, was noch abgeklärt wird und was das für Sie bedeutet.

Aktuelle Informationen finden Sie auch auf unserer Ereignisseite: [Cyberangriff auf Softwarelieferanten | PUBLICA](#)

Warum erhalten Sie diese Nachricht von uk@publica.ch?

Die E-Mail-Adresse uk@publica.ch wird von unserem Team Unternehmenskommunikation betreut. Über diese Adresse informieren wir Sie zum Cyberangriff.

Sind Ihre persönlichen Daten betroffen?

Das können wir Ihnen leider noch nicht sagen. Wir wissen derzeit noch nicht gesichert, welche Daten tatsächlich abgeflossen sind, von welchen Personen sie stammen und wie viele Personen betroffen sind. Die Spezialistinnen und Spezialisten sind an der Auswertung dieser Datensätze. Das ist komplex und benötigt Zeit.

Möglicherweise betroffen sind Daten von versicherten, rentenbeziehenden und ehemals versicherten Personen von Publica. Dazu gehören unter anderem Namen, Adressen, Geburtsdaten, AHV-Nummern, Telefonnummern, E-Mail-Adressen sowie Angaben zur beruflichen Vorsorge. Bei rentenbeziehenden Personen können auch die IBAN betroffen sein.

Die Untersuchungen dazu laufen. Sobald wir feststellen können, welche Personen betroffen sind, informieren wir diese direkt.

Sind Ihr Vorsorgeguthaben und Ihre Rente sicher?

Ja. Die Systeme von Publica sind vom Cyberangriff nicht betroffen. Der Betrieb läuft normal weiter. Ihr Vorsorgeguthaben ist sicher und die Renten werden wie gewohnt ausbezahlt.

Was ist passiert?

Ende September 2026 wurde unser Softwarelieferant Opfer eines sogenannten Ransomware-Angriffs. Der Angriff erfolgte beim Softwarelieferanten und richtete sich nicht direkt gegen Publica. Vom Cybervorfall sind zudem weitere Pensionskassen betroffen.

Was ist ein Ransomware-Angriff?

Bei einem Ransomware-Angriff dringen Cyberkriminelle mithilfe von Schadsoftware

in ein Computersystem ein, beispielsweise durch gefälschte E-Mails oder Sicherheitslücken. Sie verschlüsseln Daten und machen sie dadurch unzugänglich. Anschliessend fordern sie Lösegeld, um die Daten wieder freizugeben und drohen beispielsweise damit, gestohlene Daten zu veröffentlichen. Selbst wenn das Lösegeld bezahlt wird, gibt es keine Garantie, dass die Daten wiederhergestellt werden.

Nicht jeder Angriff läuft gleich ab. Manchmal werden Daten verschlüsselt, manchmal gestohlen und manchmal geschieht beides.

Die Hackergruppe Akira wird mit dem Angriff in Verbindung gebracht. Das Bundesamt für Cybersicherheit (BACS) informiert über die Vorgehensweise dieser Gruppe: [Cyberkriminalität: Hackergruppe AKIRA intensiviert ihre Aktivitäten](#)

Wie war es beim Softwarelieferanten?

Es laufen nach wie vor Abklärungen und es hat auch ermittlungstaktische Gründe, dass Publica nicht alle Informationen veröffentlichen kann. Aber grundsätzlich müssen wir davon ausgehen, dass beim Softwarelieferanten Daten abgeflossen sind. Ob und in welchem Umfang Personendaten von Publica darunter sind, wird weiterhin untersucht. Es ist auch möglich, dass wir nie Gewissheit erhalten werden, ob Personendaten von versicherten und rentenbeziehenden Personen abgeflossen sind.

Darum seien Sie weiterhin skeptisch und nehmen Sie die Schutzmassnahmen ernst.

Warum hatte der Softwarelieferant Personendaten?

PK Softech AG entwickelt die Software für unsere Vorsorgeverwaltung. Diese wird regelmässig weiterentwickelt und aktualisiert.

Vor der Einführung geplanter Weiterentwicklungen und neuer Softwareversionen, sogenannter Releases, werden Tests durchgeführt. Damit wird überprüft, ob die Anwendungen und die unterschiedlichen Vorsorgefälle sowie Sonderkonstellationen korrekt funktionieren. Für diese Tests waren beim Softwarelieferanten auch Daten vorhanden.

Die Löschung von Altdaten auf der Testumgebung wurde uns vom Softwarelieferanten bestätigt.

Welche Daten möglicherweise abgeflossen sind, ist Teil der laufenden Abklärungen.

Sind bereits Daten im Darkweb aufgetaucht?

Aktuell haben wir keine Hinweise darauf, dass Daten von Publica im Darkweb veröffentlicht wurden.

Das bedeutet allerdings nicht, dass wir einen Datenabfluss ausschliessen können. Die Situation wird weiterhin beobachtet. Sobald wir neue Informationen dazu haben, informieren wir Sie.

Wurde Lösegeld gefordert oder werden Personen erpresst?

Bei Ransomware-Angriffen versuchen Kriminelle häufig, Lösegeld zu erpressen. Uns ist nicht bekannt, ob im Zusammenhang mit diesem Angriff Lösegeldforderungen gestellt wurden oder ob Organisationen oder einzelne Personen erpresst werden. Diese Fragen sind Gegenstand der laufenden Ermittlungen der Bundesanwaltschaft.

Haben verdächtige E-Mails oder Anrufe mit dem Cyberangriff zu tun?

Uns erreichen Fragen, ob verdächtige E-Mails, SMS oder Anrufe mit dem Cyberangriff zusammenhängen.

Ein solcher Zusammenhang ist nicht zwingend gegeben. Denn Kriminelle gelangen auf unterschiedlichen Wegen an Kontaktdaten. Sie nutzen beispielsweise öffentlich zugängliche Informationen, Daten aus früheren Datenlecks oder verschicken betrügerische Nachrichten an zahlreiche Empfänger.

Wenn Sie eine verdächtige Nachricht erhalten, bedeutet dies also nicht automatisch, dass Ihre Daten beim aktuellen Cyberangriff abgeflossen sind. Umgekehrt können wir einen Zusammenhang derzeit auch nicht ausschliessen.

Wie können Sie sich schützen?

Bitte bleiben Sie aufmerksam, insbesondere bei unerwarteten E-Mails, SMS und Anrufen. Kriminelle können persönliche Angaben nutzen, um Vertrauen zu erwecken.

- Geben Sie keine Passwörter oder Zugangsdaten weiter.
- Klicken Sie nicht auf verdächtige Links und öffnen Sie keine unerwarteten Anhänge.
- Seien Sie vorsichtig, wenn jemand persönliche Daten oder Bankinformationen verlangt.
- Lassen Sie sich nicht unter Druck setzen. Fragen Sie im Zweifelsfall direkt bei der betreffenden Organisation nach. Verwenden Sie dafür die Ihnen bekannten Kontaktangaben. Sensibilisieren Sie auch Familienangehörige und Bekannte über diese Risiken.
- Weitere Informationen zu aktuellen Betrugsmaschen und zum richtigen Verhalten finden Sie beim [Bundesamt für Cybersicherheit](#).

Was unternimmt Publica?

Wir nehmen den möglichen Abfluss von Personendaten sehr ernst. Gemeinsam mit den zuständigen Bundesstellen arbeiten wir daran, den Vorfall aufzuklären.

Am 15. Oktober 2026 haben wir bei der Bundesanwaltschaft Strafanzeige eingereicht.

Wir haben in den letzten Jahren unser Informationssicherheitsmanagementsystem verstärkt und einzelne Massnahmen zum besseren Schutz von Daten umgesetzt. Auch im Zusammenhang mit dem aktuellen Vorfall überprüfen wir die bestehenden Sicherheitsmassnahmen.

Für uns steht im Vordergrund, den Vorfall aufzuklären und die potenziell betroffenen Personen bestmöglich zu schützen und zu informieren.

Wie geht es weiter?

Wir verstehen, dass die offenen Fragen verunsichern. Vielleicht ärgert es Sie auch, dass Sie noch immer nicht wissen, ob Ihre persönlichen Daten betroffen sind. Das können wir gut nachvollziehen.

Die Abklärungen sind umfangreich und benötigen Zeit. Wir möchten Sie möglichst umfassend informieren. Gleichzeitig ist es uns wichtig, nur gesicherte Erkenntnisse weiterzugeben.

Sobald wir mehr wissen, informieren wir Sie wieder. Sollten wir feststellen, dass Ihre persönlichen Daten betroffen sind, informieren wir Sie direkt.

Den aktuellen Stand und Antworten auf häufige Fragen finden Sie jederzeit [auf unserer Ereignisseite](#).

Freundliche Grüsse

Pensionskasse des Bundes Publica



Pensionskasse des Bundes Publica
Eigerstrasse 57, CH-3007 Bern



[Impressum](#) [Datenschutz](#)

Sie erhalten diesen Newsletter, weil wir Ihnen gegenüber eine gesetzliche Informationspflicht haben. Eine Abmeldung ist nicht möglich.
Versendet mit mailXpert