GERMAN WEBSITE NOTICE

17 November 2026

BENACHRICHTUNG ÜBER EINE VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

WAS IST PASSIERT?

Am 25. Juli 2026 stellte WireCo World Group Inc. und ihre Tochtergesellschaften („WireCo", „wir" oder „uns") unbefugte Aktivitäten auf seinen internen IT-Systemen fest. Wie sich später herausstellte, handelte es sich dabei um einen Cyberangriff, der von einem bekannten und versierten Angreifer durchgeführt wurde. Nach Entdeckung des Vorfalls haben wir die betroffenen Systeme isoliert und auf Anweisung unserer Rechtsberater externe Cybersicherheitsexperten hinzugezogen, um eine umfassende Überprüfung unseres internen Netzwerks durchzuführen und uns bei der Untersuchung, Eindämmung und Behebung des Vorfalls zu unterstützen. Die unbefugten Aktivitäten scheinen zwischen dem 9. Juli 2026 und dem 25. Juli 2026 stattgefunden zu haben.

Nachdem wir unsere internen IT-Systeme gesichert hatten, stellten wir fest, dass der Angreifer auf bestimmte Daten zugegriffen und diese exfiltriert hatte. Diese Daten enthielten personenbezogene Informationen. Seit wir den Angriff entdeckt haben, arbeiten wir ununterbrochen daran, die betroffenen Daten zu überprüfen, um personenbezogene Daten zu identifizieren. Die Durchführung dieses Vorgangs hat einige Zeit in Anspruch genommen.

WELCHE PERSONENBEZOGENEN DATEN SIND BETROFFEN?

Wir informieren Sie darüber, dass der Vorfall personenbezogene Daten betrifft, die WireCo über Sie gespeichert hat, darunter möglicherweise:

- Vollständige Namen und Kontaktdaten (Wohnadressen, Telefonnummern, E-Mail-Adressen),
- Nationale Identifikationsnummer/n, nationale Versicherungsnummer/n oder Sozialversicherungsnummer/n,
- Ausweiskopien oder Kopien von anderen von einer Behörde ausgestellten Ausweisdokumenten,
- Geburtsdatum,
- Bankkonto und Kreditkarteninformationen.

Falls Sie Mitarbeiter sind oder waren oder anderweitig für WireCo arbeiten oder gearbeitet haben, können die personenbezogenen Daten außerdem Folgendes umfassen:

- Unterlagen über das Beschäftigungsverhältnis, einschließlich Leistungsbeurteilungen, disziplinarische Unterlagen sowie Angaben zur Gewerkschaftszugehörigkeit und zum Vorstrafen,
- Abwesenheits- und gesundheitsbezogene Daten (z. B. Unterlagen über Krankheiten und arbeitsmedizinische Informationen) und/oder
- Angaben zu nächsten Angehörigen und Notfallkontakten.

WELCHE FOLGEN SIND ZU ERWARTEN?

Angesichts der Art der betroffenen Daten könnten Sie den folgenden Risiken ausgesetzt sein:

- Identitätsdiebstahl oder Identitätsbetrug,
- Phishing-Versuche (betrügerische E-Mails oder Nachrichten, die darauf abzielen, weitere personenbezogene Daten zu erlangen),
- Finanzbetrug, insbesondere im Falle eines Missbrauchs von Bankdaten, nationalen Versicherungsnummern oder Sozialversicherungsnummern und/oder
- Unerwünschte Kontaktaufnahmen oder Social-Engineering-Versuche.

Wir möchten Sie offen über diese Risiken informieren, damit Sie geeignete Maßnahmen zu Ihrem Schutz ergreifen können.

WAS WIR UNTERNEHMEN

Bereits vor dem Vorfall verfügten wir über ein mehrschichtiges Cybersicherheitsprogramm, das administrative, technische und organisatorische Sicherheitsmaßnahmen umfasste. Diese Maßnahmen dienten dazu, die Wahrscheinlichkeit und die Auswirkungen von Cyberbedrohungen zu verringern und die Vertraulichkeit, Integrität und Verfügbarkeit unserer Informationssysteme und Daten zu schützen.

Seit dem 25. Juli 2026 haben wir verschiedene Maßnahmen ergriffen, um unser Cybersicherheitsprogramm weiter zu stärken und auf den Vorfall zu reagieren. Im Einzelnen:

- Wir haben die betroffenen Systeme isoliert und gesichert, um weiteren unbefugten Zugriff zu verhindern.
- Wir haben führende Cybersicherheitsspezialisten mit der Durchführung einer forensischen Untersuchung beauftragt.
- Wir haben nationale und lokale Datenschutzbehörden benachrichtigt.
- Wir haben verschlüsselte Systeme aus sicheren Backups wiederhergestellt.
- Wir haben verbesserte Sicherheitskontrollen eingeführt, darunter zusätzliche Überwachungsmaßnahmen und Zugriffsbeschränkungen für unsere IT-Systeme.
- Wir haben eine umfassende Überprüfung unserer Informationssicherheitsmaßnahmen eingeleitet, um eine Wiederholung eines solchen Vorfalls zu verhindern.

Außerdem haben wir einen externen Dienstleister damit beauftragt, das Dark Web zu überwachen, um festzustellen, ob Daten aus unseren Systemen dort veröffentlicht wurden. Obwohl der Angreifer einen Link zu den betroffenen Dateien veröffentlicht hat, liegen uns bislang keine Hinweise darauf vor, dass personenbezogene Daten verkauft oder zum Verkauf angeboten wurden und es gibt auch keine Anzeichen für einen weiteren Missbrauch dieser Daten.

WireCo hat seine derzeitigen Mitarbeiter über den Vorfall informiert. Von einer kleinen Anzahl ehemaliger Mitarbeiter, Kunden, Lieferanten und externer Besucher liegen uns jedoch keine

Kontaktdaten vor. WireCo veröffentlicht daher diese öffentliche Bekanntmachung, um diejenigen Personen zu informieren, die WireCo nicht direkt kontaktieren kann.

WAS SIE TUN KÖNNEN

Obwohl uns keine tatsächlichen oder versuchten Betrugsfälle aufgrund des Missbrauchs personenbezogener Daten oder finanziellen Schäden für betroffene Personen infolge dieses Vorfalls bekannt sind, empfehlen wir Ihnen, die folgenden Vorsichtsmaßnahmen zu ergreifen:

- **Überwachen Sie Ihre Bankkonten**– achten Sie auf ungewöhnliche oder nicht autorisierte Transaktionen und melden Sie diese unverzüglich Ihrer Bank.
- **Seien Sie wachsam gegenüber Phishing** – seien Sie vorsichtig bei unerwarteten E-Mails, Textnachrichten oder Telefonanrufen, in denen nach persönlichen Daten gefragt wird, auch wenn diese scheinbar von einer vertrauenswürdigen Quelle stammen.
- **Ändern Sie Ihre Passwörter** – aktualisieren Sie die Passwörter für Ihre privaten Konten, insbesondere wenn Sie dort Passwörter wiederverwendet haben, die denen ähneln, die Sie für Ihre Arbeitssysteme verwenden.

Wie immer empfehlen wir Ihnen, wachsam gegenüber Identitätsdiebstahl und Betrug zu bleiben und Ihre Kontoauszüge zu überprüfen.

IHRE RECHTE

Datenschutzgesetze gewähren Ihnen bestimmte Rechte hinsichtlich der Verarbeitung Ihrer personenbezogenen Daten. Die möglicherweise geltenden Rechte variieren je nach Rechtsordnung und können unter bestimmten Umständen das Recht auf Auskunft, Berichtigung und Löschung umfassen. Wenn Sie eines dieser Rechte ausüben möchten, reichen Sie bitte einen schriftlichen Antrag über die unten angegebenen Kontaktdaten ein.

WEITERE INFORMATIONEN

Wir wissen, dass Sie uns wichtige Informationen anvertrauen, und möchten Ihnen versichern, dass wir diesen Vorfall sowie die Sicherheit und den Schutz Ihrer personenbezogenen Daten ernst nehmen.

Wir bedauern diesen Vorfall aufrichtig. Sollten Sie Fragen oder Bedenken haben, wenden Sie sich bitte an Daniel Burch unter DanBurch@WireCo.com.

Informationen zum Verantwortlichen

Land	Verantwortlicher
Deutschland	WireCo Germany GmbH **Address:** Casarstraße 1 66459 Kirkel-Limbach Germany