Betreff: Benachrichtigung über eine Datenpanne nach Art. 34 Datenschutz-Grundverordnung (DSG-VO)

Sehr geehrte Damen und Herren,

Am 29. März haben wir festgestellt, dass die IT-Systeme der Chemischen Fabrik Wocklum Gebr. Hertin GmbH & Co. KG von einem IT-Sicherheitsvorfall betroffen waren. Heute können wir bestätigen, dass es sich dabei um einen kriminellen Ransomware-Angriff handelt. Nachfolgend möchten wir Ihnen daher weitere Informationen zu einer möglichen Kompromittierung Ihrer personenbezogenen Daten geben.

Der aktuelle Stand der Untersuchungen ergibt, dass die Hacker sich unbefugten Zugriff auf interne Unternehmensinformationen und auch auf personenbezogene Daten verschafft und diese verschlüsselt haben.
Am 21. April 2022 haben die Angreifer diverse Daten im Darknet veröffentlicht. Es besteht gegebenenfalls das Risiko, das vertrauliche Daten auch weiterhin zum Kauf angeboten werden, auch wenn das Ziel dieser kriminellen Handlungen wohl vorrangig die Störung des Geschäftsbetriebes was

Der Aufforderung der Täter (Hacker) nach Zahlung von Lösegeld haben wir nach wirtschaftlichen und möglichen Schadensrisiken nicht entsprochen und werden dies auch zukünftig nicht tun.

Als wir von dem Vorfall erfuhren, haben wir umgehend alle Server vom Netz genommen, um unsere Systeme zu sichern und weiteren unbefugten Zugriff zu verhindern. Wir haben spezialisierte Forensiker:innen und Cybersicherheitsexpert:innen damit beauftragt, den Vorfall zu untersuchen, Daten von Backups wiederherzustellen und die Sicherheit unserer Systeme weiter zu erhöhen. Darüber hinaus haben wir unsere Mitarbeiter:innen sensibilisiert und werden Schulungen im Bereich Cybersicherheit weiter ausbauen.

Im Sinne der Transparenz und im Einklang mit Art. 34 der Datenschutz-Grundverordnung möchten wir Sie hiermit informieren, dass auch Ihre personenbezogenen Daten in unseren Systemen gespeichert sind und somit von dem Vorfall betroffen sein könnten

Da wir leider nicht ausschließen können, dass auch Ihre Daten kompromittiert wurden, und es deshalb möglich ist, dass für Sie ein Risiko des Identitätsdiebstahls, des Betruges, des finanziellen Verlustes, des Verlustes der Kontrolle über Ihre personenbezogenen Daten oder gesellschaftlicher Nachteile besteht, empfehlen wir Ihnen zum Schutz Ihrer personenbezogenen Daten die Überprüfung der folgenden Maßnahmen:

1. Die Änderung von Passwörtern
2. Ein internes Sensibilisierungsprogramm für Mitarbeiter:innen

3. Ihre Banken über das mögliche Risiko zu informieren und Ihre Bank- und andere Finanzkonten auf mögliche unbefugte Aktivitäten zu überwachen
4. Ihre elektronische Kommunikation auf verdächtige Nachrichten zu überprüfen

Mit den sofort eingeleiteten Maßnahmen konnten wir das Schadenspotential geringhalten und unsere Lieferfähigkeit zu einem Großteil sicherstellen. Unsere wesentlichen Systeme, das Warenwirtschaftssystem, die Logistiksteuerung, die Schnittstellen zu unseren Banken und viele sicherheitsrelevante Systeme konnten kurzfristig binnen weniger Tage bereits wieder gestartet werden. Auch haben wir Fortschritte in der Sicherung unserer Systeme und Ihrer Daten erzielen können und werden sehr zeitnah unsere Systeme vollständig wieder hergestellt haben. Für etwaige Lieferverzögerungen möchten wir uns entschuldigen, auch für den Fall, dass Sie Rechnungen oder Auftragsbestätigungen oder sonstige automatisierte Dokumente doppelt erhalten haben. Für Fragen diesbezüglich möchten wir Sie bitte, sich mit Ihrem Ansprechpartner im Hause in Verbindung zu setzten.

Bei datenschutzrechtlichen Fragen erreichen Sie unseren Datenschutzbeauftragten unter folgenden Kontaktdaten:

Riske IT GmbH
Herr Pascal Riske
Keldenicher Straße 23
50389 Wesseling
Web: www.riske-it.de
E-Mail: datenschutz@riske-it.de

Bitte haben Sie Verständnis dafür, dass wir angesichts der Komplexität der Untersuchungen zum jetzigen Zeitpunkt keine weiteren Informationen über den Vorfall teilen können. Sollten wir weitere relevante Erkenntnisse gewinnen, werden wir erneut informieren.

Wir bedauern diesen Vorfall und alle Unannehmlichkeiten, die Ihnen möglicherweise dadurch entstehen könnten. Seien Sie vergewissert, dass die Sicherheit unserer Systeme und Ihrer Daten für uns oberste Priorität hat.