



Information über die Verletzung des Schutzes personenbezogener Daten gemäß Art. 34 DS-GVO

Sehr geehrte Kundin,
sehr geehrter Kunde,

wir bedauern sehr Ihnen mitteilen zu müssen, dass TWL Opfer eines Hackerangriffs wurde und personenbezogene Daten gestohlen wurden. Wir müssen derzeit leider davon ausgehen, dass alle unsere Kunden, Mitarbeiter und Geschäftspartner von dieser Straftat betroffen sind. Aufgrund der forensischen Untersuchungen, der Arbeiten an der Gefahrenabwehr und der Ermittlungen der Strafverfolgungsbehörden waren wir bis zum 11.05.2020 angehalten, keine Details zum Sicherheitsvorfall zu veröffentlichen. Deshalb können wir Sie leider erst jetzt umfassend zu den vergangenen Ereignissen informieren.

Nach aktuellem Stand der Ermittlungen ist Folgendes passiert:

- Am 20.04. haben wir entdeckt, dass Kriminelle Daten von unseren Systemen stehlen, und umgehend Maßnahmen eingeleitet, um den weiteren Datendiebstahl zu stoppen. Leider konnten trotzdem über 500 GB an Daten erfolgreich gestohlen werden.
- Inzwischen wissen wir, dass der Erstzugriff der Kriminellen Mitte Februar über eine infizierte E-Mail-Anlage erfolgte, die von den technischen Abwehrsystemen nicht erkannt wurde.
- In den darauffolgenden Wochen schafften es die Kriminellen trotz zahlreicher Sicherheitsvorkehrungen, sich unerkannt in unserem Netzwerk auszubreiten.
- Nach der Entdeckung des Angriffs haben wir sofort das zuständige Dezernat der Kriminalpolizei, das Dezernat Cybercrime des Landeskriminalamtes (LKA) Rheinland-Pfalz und das Bundesamt für Sicherheit in der Informationstechnik (BSI) eingeschaltet. Ermittlungen wurden aufgenommen und dauern noch an. Die zuständige Landesdatenschutzbehörde wurde von dem Vorfall in Kenntnis gesetzt. Ein externes Unternehmen für IT-Sicherheit wurde mit der forensischen Untersuchung und Abwehr des Vorfalls beauftragt. Eine Verschlüsselung der Systeme sowie ein Zugriff auf die Prozessleittechnik konnten erfolgreich verhindert werden. Die Versorgung der Stadt Ludwigshafen war und ist deshalb nicht gefährdet.
- Am 30.04. erfolgte dann die erste Kontaktaufnahme der Kriminellen zur Anbahnung einer Lösegeldforderung in einem zweistelligen Millionenbereich. Gedroht wurde mit der Veröffentlichung der gestohlenen Daten.
- Für uns ist es selbstverständlich, keine Geschäfte mit Kriminellen zu machen und nicht auf Lösegeldforderungen einzugehen, um weitere kriminelle Machenschaften nicht noch zu fördern. Dazu kommt, dass selbst die Zahlung eines Lösegelds erfahrungsgemäß nicht zu einem Stopp der Datenverbreitung im Internet geführt hätte.
- Seit dem 11.05. werden unsere Kunden von den Kriminellen per E-Mail angeschrieben, um weiteren Druck auf uns auszuüben. Parallel haben die Täter angefangen, die gestohlenen Daten im Darknet zu veröffentlichen.

Zu den im Darknet veröffentlichten Daten zählen nach aktuellem Stand personenbezogene Daten wie Name, Vorname und Anschrift, die E-Mail-Adresse oder Telefonnummer, sofern sie bei TWL hinterlegt ist, Angaben zum gewählten Tarif und, sollte TWL eine Einzugsermächtigung erteilt worden sein, die Bankverbindung. Wir gehen derzeit davon aus, dass alle unsere Kunden und Geschäftspartner betroffen sind, darunter leider auch Sie.



Auch wenn wir hierfür bisher keine konkreten Anhaltspunkte haben, möchten wir Sie darauf hinweisen, dass durch den Hackerangriff leider die Gefahr besteht, dass Kriminelle Ihre Daten für weitere Straftaten missbrauchen können. Dazu zählen zum Beispiel:

- Identitätsdiebstahl
- Phishing
- Versand von Viren und Trojanern per E-Mail.

Wir bitten Sie aus diesem Grund,

- ihre Konten regelmäßig zu prüfen und bei ungewöhnlichen Kontobewegungen unverzüglich Kontakt mit Ihrer Bank aufzunehmen,
- Passwörter, die in der Kommunikation mit TWL bspw. beim Zugang zum Kundenportal verwendet werden, zu ändern,
- verdächtige E-Mails von unbekanntem Absendern sofort zu löschen. Keinesfalls sollten Links oder Dateianhänge in solchen Mails geöffnet werden.

Wir werden ab dem 14.05.2020 auf unserer Webseite weitere konkrete Informationen zu Risiken und zum Umgang damit für Sie zur Verfügung stellen und fortlaufend aktualisieren.

Wir bedauern zutiefst, dass Sie von diesem Vorfall betroffen sind, und möchten uns in aller Form für die Unannehmlichkeiten, die Ihnen entstanden sind bzw. noch entstehen könnten, entschuldigen. Wir versichern Ihnen, dass uns der Ernst der Lage bewusst ist. Ihr Vertrauen als Kunde hat für uns oberste Priorität. Wir arbeiten deshalb mit Hochdruck an der Aufbereitung des Sicherheitsvorfalls.

Bereits im vergangenen Jahr haben wir als neue Vorstände die IT unmittelbar dem Vorstand zugeordnet und zum 1.7.19 einen neuen IT-Leiter eingestellt. Wir haben im Dezember 2019 tiefgehende Sicherheitsanalysen durchführen lassen, um Maßnahmen zur Steigerung unserer IT-Sicherheit zu identifizieren. Leider ist es den Cyberkriminellen gelungen, vor der vollständigen Umsetzung der erarbeiteten Maßnahmen in unsere IT-Systeme einzudringen. Wir arbeiten zusammen mit dem eingeschalteten externen Unternehmen für IT Sicherheit mit Hochdruck daran, zu verhindern, dass ein solcher Vorfall nochmals passieren kann.

Für Rückfragen stehen wir Ihnen unter folgenden Kontaktdaten gerne zur Verfügung: kundenservice@twl.de oder telefonisch unter 0800 1122700. Auf diesem Wege können Sie auch unseren Datenschutzbeauftragten erreichen. Wir bitten um Verständnis, dass es aufgrund der erwarteten Vielzahl an Anfragen zu Verzögerungen in der Bearbeitung kommen kann.

Freundliche Grüße

Technische Werke Ludwigshafen AG

Dieter Feid

Thomas Mösl