18. Juli 2023

# ÜSTRA und GVH informieren Kundinnen und Kunden sowie Mitarbeitende: Polizei findet Daten nach Hackerangriff

ÜSTRA
Hannoversche Verkehrsbetriebe Aktiengesellschaft
Herr Heiko Rehberg
Pressesprecher
Am Hohen Ufer 6
30159 Hannover
Germany
Telefon:
+49 511 1668 3040
E-Mail:
presse@uestra.de
uestra.de

regiobus Hannover GmbH
Herr Tolga Otkun
Pressesprecher
Georgstraße 54
30159 Hannover
Telefon:
+49 511 36888 769
Mobil:
+49 162 2844666
E-Mail:
Tolga.Otkun@regiobus.de

Im Zusammenhang mit dem Hackerangriff auf die IT-Systeme der ÜSTRA am 31. März 2023 ist es zu einer unbefugten Offenlegung von Daten gekommen. Nachdem forensische Untersuchungen zunächst keine Hinweise auf einen Datenabfluss ergeben hatten, wurde die ÜSTRA nunmehr von der Polizeidirektion Hannover darüber informiert, dass dem Unternehmen zuzuordnende Daten im sogenannten Darknet aufgetaucht sind.

Die ÜSTRA hat diese Erkenntnis umgehend der Landesbeauftragten für den Datenschutz gemeldet und steht mit der Datenschutzbehörde sowie der Polizeidirektion und deren Abteilung für Cyberkriminalität seit dem Angriff im intensiven Austausch. Ziel ist es, die Auswirkungen zu minimieren.

Bislang gibt es noch keine Erkenntnisse darüber, ob Kundendaten wie zum Beispiel aus dem Bereich Abonnement-Verwaltung im Großraum-Verkehr Hannover (GVH), der von der ÜSTRA administriert wird, betroffen sind. Die vorliegenden Informationen werden derzeit gesichert und die abgeflossenen Daten in Bezug auf sensible personenbezogene Inhalte analysiert. Es wird allerdings noch einige Tage dauern, bis sich ein genaueres Bild abzeichnet. Dennoch informiert die ÜSTRA bereits jetzt alle Kundinnen und Kunden, die im März 2023 ein GVH Abo besaßen, sowie alle Mitarbeitenden ausführlich über den Vorfall und mögliche Risiken. Außerdem wurde eine extra Mailadresse für Fragen von Kundinnen und Kunden eingerichtet.

Die ÜSTRA war am 31. März 2023 Opfer eines Cyberangriffs geworden, bei dem mit einer sogenannten Ransomware Dateien auf Servern und Endgeräten verschlüsselt wurden. Als KRITIS (Kritische Infrastruktur)-zertifiziertes Unternehmen erfüllt die ÜSTRA besonders hohe IT-Sicherheitsstandards mit zahlreichen technischen und organisatorischen Maßnahmen. Entsprechend konnten in der Vergangenheit derartige Virenangriffe erfolgreich abgewehrt werden. Tatsächlich wurde die Ausbreitung auf einen erheblichen Teil der Systeme auch am 31. März verhindert. Beispielsweise konnte der gesamte

Betriebsbereich geschützt werden, Busse und Stadtbahnen der ÜSTRA fuhren die gesamte Zeit ohne größere Beeinträchtigungen für die Fahrgäste. Weil es sich jedoch laut Forensik-Experten um eine besonders aggressive und professionelle Schadsoftware handelt, die von den gängigen Virenscannern nicht erkannt werden konnte, waren die Folgen für die ÜSTRA dennoch beträchtlich.

Die ÜSTRA hatte unmittelbar nach dem Bemerken der Cyberattacke vielfältige technische und organisatorische Gegenmaßnahmen eingeleitet und arbeitet mit der Unterstützung externer Experten für Cybersicherheit seitdem erfolgreich daran, die IT-Struktur neu aufzubauen und gleichzeitig Sicherheitsmaßnahmen weiterzuentwickeln, um Cyberangriffe in Zukunft noch besser abwehren zu können.