

Cyberangriff auf die Rechenzentrumsstandorte des ZAST-Portals

Stand: 27.07.2023

Der Rechenzentrumsbetreiber für das ZAST-Portal wurde im Mai 2023 Ziel eines Cyberangriffs.

Der externe Dienstleister verfügt im Raum München über drei Rechenzentrumsstandorte, die im Mai Ziel einer Cyberattacke wurden. Der Großteil der gehosteten Systeme wurde mittels eines Verschlüsselungstrojaners vollständig verschlüsselt (Server, Systeme und Daten). Neben zahlreichen anderen Kunden war auch das ZAST-Portal von dieser Cyberattacke betroffen. Die ZAST-internen Abrechnungs- und Kommunikationssysteme sind nicht von der Attacke betroffen gewesen.

Bei den verschlüsselten personenbezogenen Daten im ZAST-Portal handelt es sich um Daten des Bayerischen Rettungsdienstes (Personal, Fahrzeugbesatzung), dessen Patientinnen und Patienten sowie involvierte Ärztinnen und Ärzte. Neben Personenstammdaten wurden Krankenversicherungsdaten und Einsatzdaten verschlüsselt.

Gemäß den externen Experten für Cybersicherheit beim Rechenzentrumsbetreiber sowie dem Landeskriminalamt konnte kein nennenswerter Abfluss von Kundendaten bzw. von personenbezogenen Daten festgestellt werden. Die Auswertungen der gesamten Netzwerkprotokolle lassen nicht erkennen, dass über den technischen Austausch von Daten hinaus, die im Zuge des Angriffs und der Angriffsvorbereitung erfolgt sind, entsprechende Daten übermittelt worden sind.

Der Angriff hat in datenschutzrechtlicher Hinsicht zweifellos die Verfügbarkeit personenbezogener Daten verletzt. Die Integrität der Daten und deren Vertraulichkeit ist nach heutigem Stand der Ermittlungen aber nicht betroffen gewesen.

Eine Meldung an das Bayerische Landesamt für Datenschutzaufsicht, an das BSI sowie an die Ermittlungsbehörden wurden durch den Rechenzentrumsbetreiber abgesetzt.

Wir informierten den Bayerischen Landesbeauftragten für den Datenschutz gemäß den Vorgaben der DSGVO.

Bereits am 22. Mai 2023 haben wir begonnen, ein neues Portal aufzubauen, welches am 09. Juni 2023 erfolgreich in Betrieb genommen werden konnte. Die Systeme wurden beim Rechenzentrumsbetreiber auf einem aktuellen sicherheitstechnischen Niveau aufgebaut. Stammdaten, die nicht in den Systemen der ZAST GmbH verfügbar sind und somit nicht wiederhergestellt werden konnten, wurden neu angelegt.

Ende Juni 2023 gelang es den externen Experten für Cybersicherheit die verschlüsselten Systeme im Rechenzentrum zu entschlüsseln und diese nach einer Sicherheitsanalyse den Kunden wieder zur Verfügung zu stellen. Daraufhin haben wir begonnen, die historischen Daten aus dem Altsystem in das neue Portal zu migrieren.