



26.07.2023

## **KFZ-VERSICHERER VON CYBER-ANGRIFFEN BETROFFEN**

Die Information erreichte die Partnerwerkstätten der HDI-Versicherung in der vergangenen Woche. In einer Mail vom 20. Juli 2023, die der Redaktion vorliegt, erklärt Matthias Metzdorf, Leiter Schaden-Service des SSV Schadenschutzverbandes: „Am 17.07.2023 wurde HDI seitens des externen IT-Dienstleisters SoftProject GmbH informiert, dass dieser Opfer eines Cyber-Angriffs geworden sei. SoftProject ist für einzelne HDI Gesellschaften in der Koordination der Schadenbearbeitung tätig und bildet eine Schnittstelle zu mehreren Schaden-Dienstleistern und Partnerwerkstätten in Deutschland.“ Auf Anfrage von schaden.news beim Kfz-Versicherer in Hannover wurde der Angriff bestätigt, der nach wie vor die Schadenregulierung der HDI Versicherung stark einschränkt.

### **SYSTEME HERUNTERGEFAHREN UND ERMITTLER EINGESCHALTET**

Auch der Dienstleister SoftProject bestätigte der Redaktion die Cyber-Attacke auf das Rechenzentrum. „Nach vorliegenden Erkenntnissen wurde ein Teil der Applikationslandschaft der SoftProject GmbH verschlüsselt. Die bisherigen forensischen Prüfungen haben keine Hinweise auf einen Datenabfluss ergeben“, heißt es in einem Statement. Nach Angaben von HDI hat der Versicherer seine Systeme direkt nach Bekanntwerden des Vorgangs heruntergefahren und die zuständigen Ermittlungsbehörden eingeschaltet. Derzeit würden dazu die technischen Untersuchungen laufen. Auch die Hannoveraner hatten wohl Glück im Unglück: „Anzeichen dafür, dass beim Dienstleister gespeicherte Daten von HDI entwendet wurden, bestehen bisher nicht.“ Der HDI habe unverzüglich sämtliche Schnittstellen zu dem externen Dienstleister gesperrt und den Datentransfer gestoppt. „Zudem haben wir umfangreiche Analysen unserer Systeme durchgeführt. Die IT-Systeme von HDI sind nach derzeitigem Stand nicht betroffen.“

## **WERKSTATTPORTAL NICHT NUTZBAR**

Gegenüber schaden.news räumte der Kfz-Versicherer aber ein, dass es Infolge des gestoppten Datentransfers für Kunden, Anspruchsteller und Partner von HDI momentan zu Verzögerungen bei der Schadenmeldung und in der Abwicklung von Schadenfällen kommen kann. Das Werkstattportal ist nicht nutzbar. „Die Kommunikation mit Partnerwerkstätten und anderen Schaden-Dienstleistern wird in der Zwischenzeit über alternative Kommunikationsstrecken (z.B. GDV, E-Mail oder Fax) abgewickelt.“ Matthias Metzdorf hatte die Partnerwerkstätten darauf hingewiesen, dass Reparaturaufträge und -freigaben nur über diese Wege kommuniziert würden.

## **DATENKLAU BEI DER BAYERN VERSICHERUNG UND PROVINZIAL RHEINLAND**

Ebenfalls im Juli wurde bereits ein Cyber-Angriff bei einer Tochter der Bayerischen Versicherungskammer bekannt. Anders als bei der HDI Versicherung wurden hier laut Medienberichten personenbezogenen Daten von mehr als 17.000 Kunden von der Bayern Versicherung gestohlen. Auch hier wurde die Versicherung nicht direkt, sondern der IT-Dienstleister Majorel Group Luxembourg S.A. angegriffen. Weltweit nutzen nach Unternehmensangaben mehr als 70 Versicherer das webbasierte Schadenmanagement, die Vertriebsunterstützung oder Schadenregulierung. Darunter auch die Provinzial Rheinland, die ebenfalls von der Attacke betroffen ist. In diesem Fall handelt es sich jedoch nicht um die Geschäftsbereiche Kraftfahrt-Schaden, sondern um die Sparte Lebensversicherungen.

Christian Simmert