SCHADEN.NEWS

18.02.2026

„ACHTUNG, WIR WURDEN GEHACKT“: K&L-BETRIEBE IM VISIER VON CYBERKRIMINELLEN

In den vergangenen Tagen sind mehrere Werkstätten Opfer von Cyberkriminalität geworden. Einer von ihnen ist Tino Freuer, Inhaber des Karosserie- und Lackiercenters Münsterland. „Es war genau 9.03 Uhr vergangenen Donnerstag (12. Februar), als mein Handy zu klingeln begann und für den Rest des Tages nicht mehr stillstand. Ich wurde von mehreren Kunden und Geschäftspartnern informiert, dass eine dubiose Mail von unserem Betriebsaccount bei ihnen eingegangen war“, berichtet er im schaden.news-Gespräch. Der Betreff der Mail: Nur eine Nummer. Der Inhalt: Ein vermeintlich eingebautes Dokument, das nur per Klick angesehen werden könne. Dieser Klick hatte offenbar große Folgen: „In meinem Gesendet-Ordner lagen auf einmal 40.000 solcher Mails“, berichtet Tino Freuer. Kurz darauf geisterten gleich gestaltete E-Mails mit dem Absender verschiedener anderer K&L-Betriebe durch die Branche. Offenbar hatten sie wohl den Inhalt einer infizierten Mail geöffnet und die Software dadurch weiterverbreitet. Auch Mailaccounts von Schadensteuerern und Kfz-Versicherern sollen mehreren K&L-Betrieben zufolge betroffen gewesen sein.

ALLIANZ RISIKO BAROMETER: CYBERATTACKEN AUF PLATZ 1 BEI KMU

In der Tat sind Cyberangriffe auf kleine und mittelständische Unternehmen nach wie vor die größte Gefahr für Betriebe. Laut dem Allianz Risiko Barometer führen Cyberattacken in Deutschland die Liste der Gefahren sogar an. Das ergab eine weltweite Befragung des Versicherers. Demnach stehen zum fünften Mal in Folge Cyberrisiken an der Spitze der globalen Risikoliste, gefolgt von Risiken im Zusammenhang mit KI.

BUNDESAMT GIBT HILFESTELLUNG BEI IT-SICHERHEITSVORFÄLLEN

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt gerade kleine und mittelständische Unternehmen davor, das Thema Cybersicherheit zu unterschätzen. „Nicht selten führen diese (Cyberattacken) zu immensen Schäden und schwächen die Unternehmensreputation. Oftmals werden Daten von Kunden und Kooperationspartnern sowie andere sensible Daten abgegriffen, verändert, gelöscht, verschlüsselt und/oder auf inkriminierten Internetseiten veröffentlicht“, erklärt das Bundesamt auf seiner Website. Um Betriebe zu unterstützen, hat das BSI umfangreiche Leitfäden für KMU zur Verfügung gestellt und gibt auch Hilfestellung im Falle eines IT-Sicherheitsvorfalls.

„SOFORT ALLE BANKEN VOR UNGEWÖHNLICHEN ABBUCHUNGEN GEWARNT“

Betriebsinhaber Tino Freuer aus Greven hat sofort reagiert, nachdem ihm die Cyberattacke bekannt wurde: „Gemeinsam mit meinem IT-Team haben wir alle internen Zugänge erneuert. Zusätzlich hab ich bei unseren Banken angerufen und sie vor ungewöhnlichen Abbuchungen gewarnt.“ Denn was genau die Spam-Mail erreichen wollte, ist bisher nicht bekannt. Der Betriebsinhaber veröffentlichte noch am gleichen Tag eine Story auf Social Media, um auch andere Werkstätten davor zu warnen, auf den Link in der Mail zu klicken und somit zu einer Weiterverbreitung der sogenannten Ransomware beizutragen: „Achtung, wir wurden gehackt. Wenn ihr Mails mit Anhängen von uns bekommen solltet, gebt auf keinen Fall Logindaten oder ähnliches preis!“ Zudem hat der Geschäftsführer noch einmal in Sicherheits-Software investiert. „Wir sind vorbereitet, damit uns so eine Cyberattacke nicht nochmal trifft. Und wir haben dazugelernt", betont Tino Freuer und rät anderen Betrieben, ihre IT-Sicherheit unter die Lupe zu nehmen und sich abzusichern. Er weiß: „Auch wenn es viel Geld kostet: Im Mittelstand kommen Betriebe nicht mehr um eine professionelle IT-Betreuung herum. Das kann man nicht mehr allein stemmen. Und die Investition kann ein Unternehmen wie unseres letztendlich vor großen finanziellen Schäden bewahren.“

Ina Otto