

Hackerangriff zwingt Recyclingfirma Eu-Rec in Insolvenz - Was nun?

Hackerangriff zwingt das Recyclingunternehmen Eu-Rec in Hermeskeil zur Insolvenz. Vorstand strebt nachhaltige Sanierung an.



Hermeskeil, Rheinland-Pfalz, Deutschland - Die Eu-Rec GmbH, ein Recyclingunternehmen mit Sitz in Hermeskeil, Rheinland-Pfalz, hat Insolvenz angemeldet. Der Grund für diesen dramatischen Schritt ist ein schwerer Hackerangriff, der die digitale Infrastruktur des Unternehmens stark beschädigte und die Betriebsabläufe erheblich störte. Seit über 30 Jahren engagiert sich Eu-Rec in der umweltschonenden Wiederverwertung von Wertstoffen und beschäftigte zuletzt mehr als 50 Mitarbeiter, wie [t-online.de](https://www.t-online.de) berichtet. Der Insolvenzantrag wurde beim Amtsgericht Trier gestellt. Trotz der schwierigen Lage ist die Geschäftsführung optimistisch und plant, gemeinsam mit dem vorläufigen Insolvenzverwalter, Rechtsanwalt Ingo Grünewald, eine tragfähige Lösung zu

erarbeiten.

Bereits vor dem Hackerangriff befand sich die Eu-Rec GmbH in einer angespannten wirtschaftlichen Situation. Hohe Energiepreise und schwankende Auftragseingänge belasteten das Unternehmen zusätzlich. Die Entscheidung zur Stellung des Insolvenzantrags fiel der Familie Streit, die das Unternehmen leitet, nicht leicht, wird jedoch als Möglichkeit gesehen, die Unternehmensstrukturen zu überprüfen und zu optimieren. Mitarbeiter werden über die Situation informiert, und ihre Löhne sind durch das Insolvenzgeld gesichert, was **merkur.de** hervorhebt. Der Geschäftsbetrieb der Eu-Rec GmbH soll trotz der Insolvenz in vollem Umfang fortgeführt werden, denn die Führungskräfte sind überzeugt, dass das Geschäftsmodell Potenzial im Bereich der nachhaltigen Kreislaufwirtschaft hat.

Cyberangriffe und ihre Folgen

Der Vorfall ist Teil einer besorgniserregenden Entwicklung: Cyberangriffe auf deutsche Unternehmen nehmen zu. Eine aktuelle Studie zeigt, dass 53 Prozent der betroffenen Unternehmen Opfer von Phishing waren und 42 Prozent Angriffe auf ihre Cloud-Services erlebten. Auch Angriffe auf Mailserver und Webserver sind häufig. Die in der **KPMG** veröffentlichten Daten verdeutlichen, dass Dienstleister oft als Einfallstor für diese Angriffe genutzt werden. Bei 54 Prozent der Unternehmen, die angegriffen wurden, erfolgten die Attacken über die Infrastruktur von Dienstleistern.

Die Schäden, die durch solche Cyberangriffe entstehen, können für Unternehmen existenzbedrohend sein. Datenlecks und der Diebstahl sensibler Informationen stellen signifikante Risiken dar. Die häufigsten Ziele sind Kundendaten, Bank- und Finanzdaten sowie Personaldaten. Diese Entwicklungen kaschieren die Herausforderungen, vor denen moderne Unternehmen stehen, und werfen ein Schlaglicht auf die Notwendigkeit, die digitale Sicherheit zu stärken.

Details	
Vorfall	Insolvenz,Cyberkriminalität
Ursache	Hackerangriff
Ort	Hermeskeil, Rheinland-Pfalz, Deutschland
Quellen	<ul style="list-style-type: none">• www.t-online.de• www.merkur.de• kpmg.com

Besuchen Sie uns auf: n-ag.de