Fondshaus

# Gab es einen Cyberangriff auf Thomas Lloyd?

Kriminelle behaupten, mehrere Terabyte an Daten von dem Investmenthaus erbeutet zu haben. Thomas Lloyd widerspricht, obwohl die Hacker angebliche Beweise vorlegen.


Apple Karten Screenshot

**L. Nagel, M. Verfürden** Berlin, Düsseldorf

Öko-Investor Thomas Lloyd ist möglicherweise Opfer eines Cyberangriffs geworden. Wie die Hackergruppe „Cactus" am Dienstag im Darknet mitteilte, hat sie angeblich 2,4 Terabyte interner Daten erbeutet. Als Beleg veröffentlichten die Hacker mehrere Dokumente, darunter die angebliche Kopie des Reisepasses des Firmengründers und Vorstandsvorsitzenden Michael Sieg.

Der mutmaßliche Angriff war zunächst Journalisten des Schweizer Onlinemagazins „Inside IT" aufgefallen, mit denen das Handelsblatt gemeinsam recherchierte. Nach eigenen Angaben verwaltet Thomas Lloyd rund eine Milliarde Euro. 27.000 Anleger aus Deutschland haben in die geschlossenen Fonds des Öko-Investors 750 Millionen Euros investiert, die im niedersächsischen Örtchen Langen gemeldet sind.

Thomas Lloyd dementierte auf Anfrage des Handelsblatts einen Cyberangriff, wohl ohne die Angaben im Darknet selbst geprüft zu haben. Europachef Matthias Klein erklärte: „Einen Cyberangriff einer Hackergruppe mit dem Namen ‚Cactus' hat es nicht gegeben." Zugleich räumte er ein: „Welche angeblichen ‚Datenproben' im Darknet zu finden sind, entzieht sich unserer Kenntnis." Laut Klein sei ein Angriff auf Thomas Lloyd ohnehin ausgeschlossen: „Unsere Infrastruktur ist gegen Hackerangriffe jeglicher Art umfassend gesichert, sodass es keinen Anlass zur Befürchtung gibt, dass auf Anlegerdaten bei etwaigen Angriffen unbefugt zugegriffen werden könnte." Nach Kenntnis des Unternehmens seien keine Daten abgeflossen. Auch eine sogenannte Ransomware-Attacke schloss das Fondshaus aus: Die IT-Infrastruktur von Thomas Lloyd sei nicht von Hackern verschlüsselt worden. Thomas Lloyd werde nicht erpresst, es liege keine Lösegeldforderung vor. Ransomware-Attacken sind eine bekannte Masche der Cyberkriminalität. Die Hacker infizieren zunächst Firmencomputer mit Schadsoftware, laden heimlich die Daten herunter oder verschlüsseln anschließend die IT-Systeme. Im Anschluss erpressen die Hacker die Opfer – zuweilen sogar doppelt. Firmen müssen fürchten, dass vertrauliche Daten im Internet veröffentlicht werden und zugleich sind ihre Systeme empfindlich gestört. Die Angreifer bieten an, die Entschlüsselung zu ermöglichen, wenn sie Lösegeld gezahlt bekommen.

Thomas Lloyd

**Firmensitz in München (oben); CFO Vivien Maclachlan, CPO Miriam Plater, und CEO Michael Sieg:** Keine Daten seien abgeflossen.

Sollte sich keine Einigung erzielen lassen, droht die „Cactus"-Gruppe damit, die Daten zu veröffentlichen. „Journalisten, Forscher usw. werden Ihre Dokumente durchforsten und Unstimmigkeiten oder Unregelmäßigkeiten finden." Die Gruppe hat in ihrem Darknet-Blog „Regeln" für die Opfer veröffentlicht. Diese erhielten drei Tage Zeit, „um uns zu kontaktieren". Ziel sei eine „Vereinbarung", dann würden verschlüsselte Dateien angeblich wiederhergestellt und exfiltrierte Daten sicher gelöscht. Und: „Wir akzeptieren nur Zahlungen in Kryptowährung." Das soll in der Regel möglichst Anonymität gewährleisten.

Um den angeblich erfolgreichen Angriff auf Thomas Lloyd zu belegen, veröffentlichten die Hacker einen Verzeichnisbaum der angeblichen gestohlenen Dokumente im Darknet. Darin sind rund 32.000 Ordner mit Namen aufgelistet. Viele Bezeichnungen legen nahe, dass sie Dokumente

> Journalisten, Forscher usw. werden Ihre Dokumente durchforsten und Unstimmigkeiten oder Unregelmäßigkeiten finden.
>
> **Hackergruppe „Cactus"**

mit Kundeninformationen enthalten – sollten sie echt sein. Andere Ordner tragen die Namen von aktuellen oder ehemaligen Mitarbeiterinnen und Mitarbeitern. Zum Teil enthalten sie Unterordner mit Stichworten wie „Unfall" oder „Schwangerschaft". Andere Ordnernamen passen zu bekannten Geschäften von Thomas Lloyd.

So tauchen die CTI-Fonds in Langen namentlich auf und auch den aktuellen Wirtschaftsprüfern der Kanzlei Forvis Mazars sind Ordner gewidmet. Mehrere Ordner tragen das Label der deutschen Finanzaufsicht Bafin. Presseanfragen des Handelsblatts an Thomas Lloyd sind in Dateinamen jenen Monaten zugeordnet, in denen sie tatsächlich verschickt wurden.

### Partner: Vertrag sei authentisch

Ein kleines Datenpaket haben die Hacker im Darknet bereits veröffentlicht. Darin sind angebliche Personaldokumente von mehreren Mitarbeitern enthalten, ebenso wie mutmaßliche Verträge mit Geschäftspartnern. Sollten die Dokumente gefälscht sein, hätte sich jemand sehr viel Mühe gemacht. Herunterladen lässt sich unter anderem ein angeblicher Vertrag mit einem deutschen Energieversorger. Ein Sprecher des Unternehmens bestätigte dem Handelsblatt, dass der Vertrag authentisch ist. Die Kopie des Reisepasses von Firmenchef Sieg wiederum enthält dieselbe Passnummer, mit der er eine Firma in Singapur im Handelsregister angemeldet hat. Auch sein Geburtstag stimmt.

Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Ransomware-Gruppe „Cactus" mindestens seit März 2023 aktiv. Sie verschlüssele Opfersysteme und drohe mit der Veröffentlichung von gestohlenen Daten auf ihrer Seite, erklärte die Behörde. Dem BSI