SmartRiskSolutions
Risk & Crisis Management Consultancy

Hinweis zum Einsatz von Kryptowährungen bei Lösegeldzahlungen

OFAC

Hinweis zum Einsatz von Kryptowährungen bei Lösegeldzahlungen

Bei Cybererpressungen und Produkterpressungen sind Lösegeldforderungen zur Zahlung in Bitcoin die Regel. Auch bei klassischen Erpressungen fordert die Täterschaft häufig die Zahlung mittels konvertierbarer Kryptowährung. Bei Entführungen sind Lösegeldzahlungen in Kryptowährungen nach wie vor die Ausnahme.

Doch Gesetze und Vorschriften, insbesondere der USA, stellen an die Personen und Organisationen, die Lösegeld mittels Kryptowährung zahlen bzw. beim Zahlungsprozess unterstützen, hohe Complianceanforderungen.

Am 01. Oktober 2020 veröffentlichten das Office of Foreign Assets Control (OFAC) und das Financial Crimes Enforcement Network (FinCEN) zwei “Advisories” zu Lösegeldzahlungen bei Ransomwarefällen.

Hintergrund

Im Juli 2020 zahlte laut Medienberichten das Unternehmen Garmin nach einer Ransomware-Attacke (Verschlüsselungstrojaner) ein hohes Lösegeld in Form von Bitcoin. Dieser Vorgang erregte den Argwohn amerikanischer Aufsichtsbehörden, denn die scheinbar verwendete Ransomware „WastedLocker“ wird der russischen Hackergruppe „Evil Corp“ zugeschrieben. Diese steht auf US-Sanktionslisten. Sollte das Unternehmen tatsächlich gezahlt haben, drohen millionenschwere Geldbußen – Verstöße gegen Sanktionsbestimmungen können aber auch zu Haftstrafen führen.

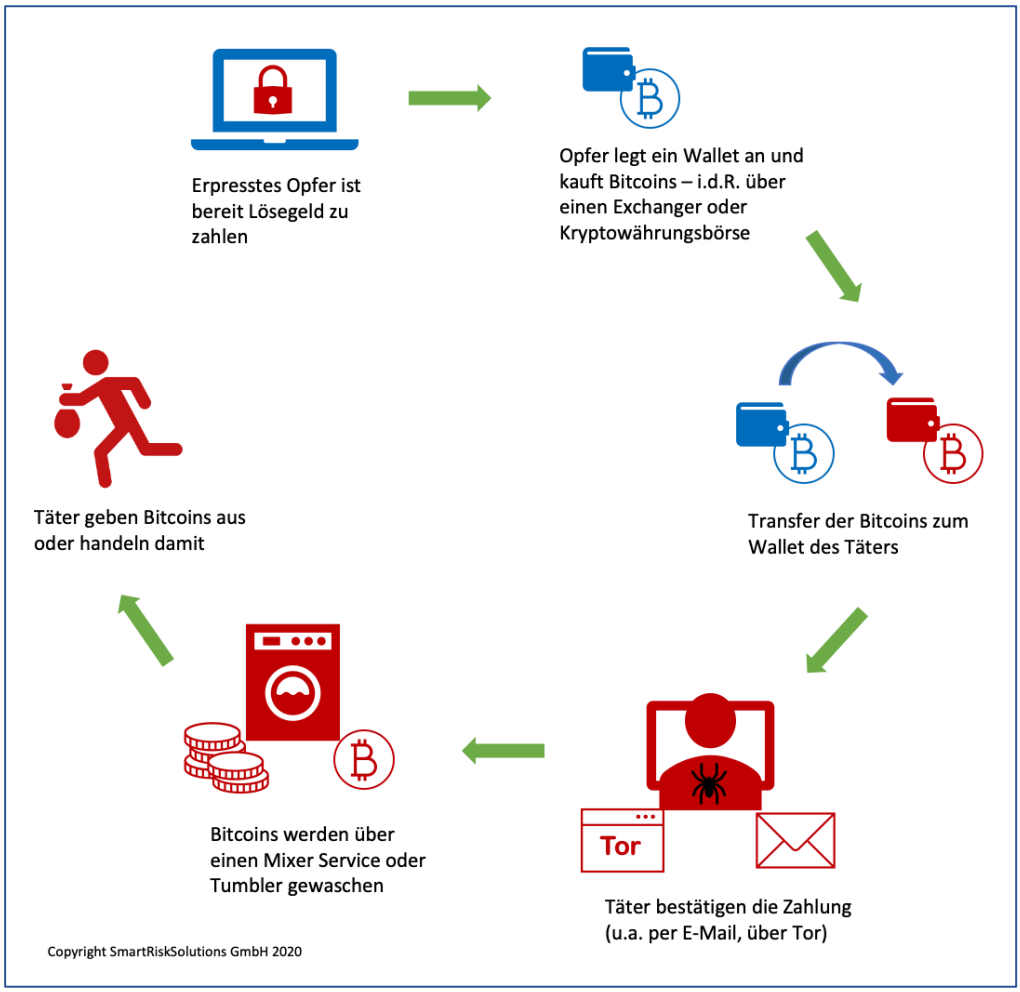
Vor diesem Hintergrund ist die nun sehr deutliche schriftliche Warnung und Erinnerung der US-Behörden zu verstehen, die Sanktionsvorschriften bei Lösegeldzahlungen einzuhalten. Das Office of Foreign Assets Control (OFAC) ist für die Überwachung und Durchsetzung von Sanktionen zuständig. Das Financial Crimes Enforcement Network (FinCEN) ist in erster Linie mit der Bekämpfung der Geldwäsche durch Finanz- und Geldinstitute betraut.

Finanztransaktionen im Hinblick auf US-Sanktionen

Unabhängig davon, ob es sich um digitale oder Fiat-Währungen (Euro, US-Dollar ...) handelt, sind bei Finanztransaktionen die national und international gültigen Gesetze zu beachten. Neben Sanktionsklauseln sind dies u.a. Geldwäschegesetze und Anti-Terror-Gesetze.

Auch wenn die schriftlichen Warnungen in diesen „Advisories“ Bezug zu Ransomware nehmen, sollte nicht außer Acht gelassen werden, dass sich die US-Regelungen auf jegliche Finanztrankaktionen mit direktem oder indirektem Bezug zu Personen, Ländern und Landesregionen beziehen, gegen die Sanktionen verhängt wurden. Die Vorschriften betreffen sowohl geschäftliche Aktivitäten als auch Lösegeldzahlungen im Rahmen von Erpressungen und Entführungen. Bereits 2018 setzte OFAC erstmals Bitcoin-Adressen auf Sanktionslisten.

Vereinfachte Darstellung zum Ablauf von Lösegeldzahlungen mittels Bitcoin (BTC)



An wen sich die beiden neuen „Ratgeber“ richten

Die Hinweisdokumente von OFAC und FinCEN zu Ransomwarezahlungen beziehen sich auf Unternehmen und Personen, die Opfer von Ransomware (Verschlüsselungstrojaner) wurden sowie Dienstleister, die Betroffene bei der Abwicklung der Lösegeldzahlung unterstützen. Dies sind insbesondere Banken, Money Service Business (MSB) Anbieter, Kreditkartenfirmen, IT-Forensikfirmen, Krisenberatungsunternehmen sowie Versicherer.

Grundsätzlich ist OFAC auf dem Gebiet der USA und für Personen, Unternehmen und Organisationen der USA zuständig. Doch das US-Finanzministerium mit den beiden Organisationen OFAC und FinCEN beansprucht gelegentlich auch eine extraterritoriale Zuständigkeit für sich.

Auswirkungen für nicht-amerikanische Unternehmen und Personen

Wir raten dringend davon ab, als nicht-amerikanisches Unternehmen die US-Vorschriften auf die leichte Schulter zu nehmen. „Hoffen, dass es gut geht“ und OFAC den Vorgang nicht mitbekommen wird, ist eine sehr risikoreiche Strategie – und fatal, wenn ein Erpressungsfall später medial bekannt wird.

Es gibt genügend Beispiele aus der Vergangenheit, die zeigen, dass OFAC auch gegen nicht-US Firmen und Personen entschieden vorgeht, wenn OFAC Kenntnis von Geschäftsaktivitäten mit sanktionierten Personen, Organisationen und Staaten erlangt.

Bei den Sanktionsvorschriften des US-Finanzministeriums ist eine extraterritoriale Wirkung zu befürchten. Das bedeutet, dass auch für nicht-amerikanische Firmen und Personen Sanktionen drohen. Insbesondere dann, wenn US-Amerikaner oder US-Firmen dazu verleitet werden, gegen US-Sanktionen zu verstoßen. Man spricht hier seitens der Amerikaner vom sogenannten Nexus.

Problematisch ist auch, dass die OFAC für nicht-amerikanische Unternehmen eine „Black-Box“ und nicht sehr transparent in ihrem Handeln ist. Die amerikanische Rechtslage ist komplex und die umfangreichen Bestimmungen und vagen Ausführungen erschweren eine Beurteilung. Kompetente Rechtsberatung ist hier erforderlich.

Hinzu kommen auch möglicherweise wirtschaftspolitische Interessen der USA, wenn das betroffene Unternehmen in einem starken Wettbewerb zu einem US-Unternehmen steht. Dann könnten die OFAC-Nachforschungen deutlich intensiver ausfallen.

Schwierige Lage für betroffene Unternehmen

Wenn Unternehmen Opfer einer Ransomware-Attacke werden und die Täter direkt oder indirekt mit sanktionsbehafteten Personen, Organisationen oder Staaten in Verbindung stehen, dürfen diese Zahlungen nicht ausgeführt werden.

Eine Ausnahmegenehmigung von den Sanktionsbestimmungen kann bei der OFAC beantragt werden. Die Chancen auf eine Erlaubnis sind sehr gering und es ist ein sehr langwieriger Prozess. Zeit steht bei einer Ransomware-Attacke nur sehr bedingt zur Verfügung, denn der Ausfall der IT kostet Unternehmen mit jedem Tag hohe Summen und kann existenzgefährdend sein.

Rechtlich ist die Folge, dass ein Unternehmen bei einem möglichen Sanktionsverstoß keine Lösegeldzahlung durchführen darf – auch wenn dies existenzgefährdend ist. Entschließt sich ein Unternehmen oder eine Person dennoch zur Zahlung an einen sanktionierten Empfänger, wird die OFAC bei der Prüfung des Falles auch strafmindernde Kriterien bei der Bewertung hinzuziehen. Dies sollte man bei der Schadensminimierung beachten. Diese Kriterien sind u.a.:

- Die Polizei frühzeitig informieren
- Den Behörden Daten übergeben, die für die Ermittlungen hilfreich sind

Einen Weg, den Täter wählen könnten, wäre noch besser zu verschleiern, um wen es sich beim Angreifer handelt. Aus Tätersicht wird es möglicherweise interessanter sein, sich zukünftig stärker auf nicht-amerikanische Opfer zu konzentrieren – was möglicherweise auch eine der Absichten von OFAC ist. Der Täterschaft ist auch bewusst, dass Behörden immer wieder erfolgreich bei der Aufdeckung von Bitcoin-Empfängern sind. Daher bieten einige Erpresser inzwischen Rabatte, wenn das Opfer die Zahlung nicht mittels Bitcoin, sondern mit noch schwerer als Bitcoin verfolgbarer „Anonymity-Enhanced Cryptocurrencies (AECs)“ vornimmt.

Da Erpresser „treue Kunden“ sind, besteht bei Zahlungen an sanktionierte Empfänger ein weiteres Erpressungsrisiko, dem sich Betroffene aussetzen.

Risikominimierung aus Compliancesicht

Eine Überprüfung der Empfänger von Geldzahlungen ist nicht nur bei Cybererpressungen, sondern auch bei klassischen Erpressungen und Produkterpressungen sowie bei Zahlungen von Lösegeldern an Entführern erforderlich. Ob die Überprüfung verwertbare Informationen liefert, ist eine andere Frage.

Selbst bei Zahlung an einen sanktionierten Empfänger aus Unwissenheit liegt ein Verstoß gegen US-Sanktionsbestimmungen vor, die zumindest zivilrechtliche Geldzahlungen nach sich ziehen kann. Daher empfehlen wir zur Risikominimierung grundsätzlich folgendes:

- Intensives Due Diligence zu den Empfängern bzw. Kryptowährungs-Adressen
- Versuchen zu ermitteln, wer hinter der Ransomware Attacke oder der Art der verwendeten Ransomware steht
- Frühzeitige Einbindung von international erfahrenen Fachanwälten
- Detaillierte Falldokumentation, insbesondere zum Due Diligence Prozess und vorhandenem Compliancesystem
- Im Falle einer Lösegeldzahlung mit virtueller Währung idealerweise einen beim US-Finanzministerium registrierten Money Service Business (MSB) Anbieter für die Transaktion des Lösegeldes nutzen.
- Sicherstellen, dass die an der Transaktion beteiligten Organisationen (Bank, Money Service Business) einen Bericht an FinCEN senden – sogenannter „Suspicious Activity Report“ (SAR), insbesondere wenn das betroffene Unternehmen oder unterstützende Dienstleister einen US-Bezug haben.
- Die Kooperation bzw. Informationsweitergabe zum Fall an Behörden wirken sich strafmildernd aus.

Über uns

Die SmartRiskSolutions GmbH ist auf die Themen Reisesicherheit, Krisenmanagement, Ermittlungen, Due Diligence sowie dem Schutz von Vermögensinhabern spezialisiert.

SmartRiskSolutions wird von erfahrenen Beratern geleitet, mit langjähriger Erfahrung bei Sicherheitsbehörden und in der Privatwirtschaft.

Für Versicherer sind wir als Krisenberater weltweit regelmäßig u.a. bei Fällen von Entführungen, Erpressungen, Cybererpressungen und bei böswilliger Produktmanipulation tätig.

Kontakt

Gerne erläutern wir Ihnen in einem persönlichen Gespräch, wie wir Sie unterstützen können.

SmartRiskSolutions GmbH
Nördliche Münchner Straße 14a
82031 Grünwald
Tel. +49 89 1250 3247-0
info@smartrisksolutions.de
www.smartrisksolutions.de