Arbeitsübersetzung (BMF-Sprachendienst)

German Translation (Work Translation)

Bekämpfung der Finanzmittelbeschaffung durch Ransomware: mögliche Risikoindikatoren

Die im Folgenden aufgeführten möglichen Risikoindikatoren wurden anhand der Erfahrungen und Daten von Staaten aus dem gesamten globalen FATF-Netzwerk zusammengestellt. Sie sollen die Aufdeckung verdächtiger Transaktionen im Zusammenhang mit Erpressersoftware („Ransomware“) verbessern. Die Aufstellung gliedert sich nach unterschiedlichen Perspektiven auf den Prozess der Leistung von Ransomware-Zahlungen.

Vor Anwendung der Risikoindikatoren sollten die nachstehenden Hinweise zum Umgang damit sowie der FATF-Bericht zur Bekämpfung der Finanzmittelbeschaffung durch Ransomware von 2023 gelesen werden.

Bekämpfung der Finanzmittelbeschaffung durch Ransomware

Der Bericht enthält eine Analyse der Methoden von Kriminellen bei der Durchführung von Ransomware-Angriffen und dem Waschen von Lösegeld.

Besonders betont wird darin, dass die Behörden, um erfolgreich gegen das Waschen von Lösegeld vorgehen zu können, auf die vorhandenen Verfahren der internationalen Zusammenarbeit zurückgreifen und diese nutzen müssen. Zudem müssen sie die Kenntnisse erwerben und die Instrumente entwickeln, die zur schnellen Erfassung wesentlicher Informationen, zur Verfolgung der nahezu in Echtzeit stattfindenden virtuellen Transaktionen und zur Abschöpfung von Kryptowerten vor ihrem Verschwinden benötigt werden.

https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/countering-ransomware-financing.html

Das Vorliegen eines einzelnen Indikators in Bezug auf einen Kunden oder eine Transaktion rechtfertigt für sich genommen möglicherweise noch keinen Verdacht

auf eine Ransomware-Straftat und stellt auch nicht zwangsläufig ein eindeutiges Anzeichen für eine entsprechende Aktivität dar. Es kann gegebenenfalls jedoch Anlass für eine engere Überwachung und nähere Untersuchung sein.

Die Indikatorenliste ergänzt die Indikatoren, die in der FATF-Publikation zu Warnsignalen bei Kryptowerten[1] aufgeführt sind, und ist sowohl für Behörden als auch für die Privatwirtschaft relevant. In Letzterer können die Indikatoren für Kryptowertedienstleister, Banken sowie andere Finanz- und Zahlungsinstitute von Interesse sein.

[1] Siehe *FATF Virtual Assets Red Flag Indicators of Money Laundering and Terrorism Financing* (September 2020) unter www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf.

Woran können Banken/andere Finanz- und Zahlungsinstitute Zahlungen von Ransomware-Opfern erkennen?

- abgehende Überweisungen an Firmen, die Beratung zu Cybersicherheit oder Hilfe bei Sicherheitsvorfällen anbieten und sich auf Ransomware-Angriffe spezialisiert haben
- ungewöhnliche eingehende Überweisungen von Versicherungen, die sich auf Schäden durch Ransomware-Angriffe spezialisiert haben
- Kundenmitteilungen über Ransomware-Angriffe oder -Zahlungen
- öffentlich zugängliche Informationen über Ransomware-Angriffe auf Kunden
- zahlreiche Transaktionen von ein und demselben Bankkonto auf mehrere Konten bei einem Kryptowertedienstleister
- Verwendungszweck enthält Wörter wie „Lösegeld“ oder Namen von Ransomware-Gruppierungen
- Zahlungen an Kryptowertedienstleister in Hochrisikoländern (siehe Kasten)

Woran können Kryptowertedienstleister Zahlungen von Ransomware-Opfern erkennen?

- Kaufanfrage für Kryptowerte durch eine Firma, die Hilfe bei Sicherheitsvorfällen anbietet, oder eine Versicherung im Auftrag eines Dritten
- Kunde gibt gegenüber dem Kryptowertedienstleister an, dass Kryptowerte zum Zweck einer Ransomware-Zahlung erworben werden
- Nutzer, der in der Vergangenheit keine Kryptowertetransaktionen durchgeführt hat, überweist Gelder außerhalb der üblichen Geschäftspraxis
- Kunde erhöht sein Kontolimit und tätigt eine Überweisung an einen Dritten
- Kunde scheint mit Sorge oder Ungeduld auf die Dauer der Zahlungsdurchführung zu reagieren
- Käufe oder Überweisungen anonymitätsfördernder Kryptowährungen
- Zahlungen an Kryptowertedienstleister in Hochrisikoländern
- Neukunde erwirbt Kryptowerte und überweist seinen gesamten Kontosaldo an eine einzige Adresse

Woran können Kryptowertedienstleister Eingänge von Ransomware-Zahlungen/Konten von Ransomware-Kriminellen erkennen?

- Kunde handelt nach einer ersten umfangreichen Kryptowerteüberweisung kaum noch oder gar nicht mehr mit digitalen Währungen
- Blockchain-Analyse zu Wallet-Adressen ergibt Verbindungen zu Ransomware
- sofortige Abhebung nach Umwandlung von Geld in Kryptowerte
- Überweisung von Kryptowerten an Wallets mit Ransomware-Bezug
- Nutzung eines Kryptowertedienstleisters in einem Hochrisikoland
- Überweisung von Kryptowerten an einen Kryptomixer
- Nutzung eines verschlüsselten Netzwerks
- Verifizierungsinformationen liegen in Form eines Fotos von Daten auf einem Computermonitor vor oder haben einen Dateinamen, der „WhatsApp image“ o. Ä. enthält
- Syntax eines Kunden passt nicht zu seinen demografischen Merkmalen
- laut Kundenangaben verfügt ein Kunde über einen E-Mail-Account bei einem Anbieter mit hohem Datenschutzstandard, z. B. Proton Mail oder Tutanota
- uneinheitliche Identifizierungsangaben oder Versuch, unter falscher Identität ein Konto zu eröffnen
- mehrere Konten mit denselben Kontaktdaten; Nutzung ein und derselben Adresse unter verschiedenen Namen
- Kunde scheint ein VPN zu nutzen
- Transaktionen mit anonymitätsfördernden Kryptowährungen

Kasten: Staaten mit erhöhtem Geldwäscherisiko

Zwar gibt es keine allgemeingültige Definition oder Methode zur Feststellung, ob in einem Land ein erhöhtes Geldwäsche-/Terrorismusfinanzierungsrisiko besteht, doch die Betrachtung länderspezifischer Risiken in Verbindung mit anderen Risikofaktoren kann hilfreiche Informationen für die genauere Ermittlung möglicher GW-/TF-Risiken liefern. Zu den Indikatoren für ein erhöhtes Risiko zählen a) Länder oder Regionen, die glaubwürdigen Quellen zufolge terroristische Aktivitäten finanzieren oder unterstützen oder in denen gelistete terroristische Vereinigungen aktiv sind, b) Länder, in denen glaubwürdigen Quellen zufolge in erheblichem Umfang organisierte Kriminalität, Korruption oder andere kriminelle Aktivitäten stattfinden, da sie z. B. Quellen- oder Transitländer für illegales Rauschgift, Menschenhandel, Schmuggel oder illegales Glücksspiel sind, c) Länder, gegen die von internationalen Organisationen wie den Vereinten Nationen Sanktionen, Embargos oder ähnliche Maßnahmen verhängt wurden, sowie d) Länder, in denen glaubwürdigen Quellen zufolge in den Bereichen Regierung, Strafverfolgung und Regulierungsvorschriften Schwachstellen vorhanden sind, darunter Länder, in denen der FATF zufolge nur ein schwaches System zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung existiert, insbesondere in Bezug auf Kryptowertedienstleister, und Kryptowertedienstleister und andere Verpflichtete bei Geschäftsbeziehungen und Transaktionen besonders vorsichtig sein sollten.

Quelle: FATF (2021) *Updated Guidance for a Risk-Based Approach: Virtual Assets and VASPs*, Tz. 154