Arbeitsübersetzung (BMF-Sprachendienst)

German Translation (Work Translation)

FATF-Bericht

Bekämpfung der Finanzmittelbeschaffung durch Ransomware

März 2023

Inhaltsverzeichnis

Siehe auch

Bekämpfung der Finanzmittelbeschaffung durch Ransomware: mögliche Risikoindikatoren

Diese Aufstellung möglicher Risikoindikatoren ergänzt den vorliegenden FATF-Bericht „Bekämpfung der Finanzmittelbeschaffung durch Ransomware“ und kann dem öffentlichen und privaten Sektor als Hilfestellung bei der Identifizierung verdächtiger Aktivitäten im Zusammenhang mit Ransomware dienen.

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

Abkürzungsverzeichnis

AML/CFT	Anti-money laundering/Countering the financing of terrorism (Bekämpfung der Geldwäsche und Terrorismusfinanzierung)
CERT	Computer Emergency Response Team
DeFi	Decentralised finance
FIU	Financial Intelligence Unit
IP	Internet protocol
ÖPP	Öffentlich-private Partnerschaft
RaaS	Ransomware as a Service
VACG	Virtual Asset Contact Group
VPN	Virtual private network

Zusammenfassung

Das Volumen der Geldflüsse im Zusammenhang mit Ransomware-Angriffen hat in den letzten Jahren weltweit dramatisch zugenommen. Branchenschätzungen zufolge haben sich die Lösegeldzahlungen 2020 und 2021 im Vergleich zu 2019 vervierfacht. Dank neuer Methoden sind Ransomware-Angriffe profitabler und erfolgreicher geworden. Dazu gehören Angriffe auf hochwertige Unternehmen sowie das sogenannte Ransomware as a Service (RaaS), bei dem Kriminelle benutzerfreundliche Softwarepakete an Affiliates verkaufen. Die Folgen eines Ransomware-Angriffs können verheerend sein und die nationale Sicherheit bedrohen, u. a. durch die Beschädigung und Störung kritischer Infrastrukturen und Dienste.

Ziel der FATF ist es, mit diesem Bericht das Verständnis für die weltweiten Geldflüsse im Zusammenhang mit Ransomware zu verbessern und bewährte Verfahren zur Bekämpfung dieser Bedrohung aufzuzeigen. Der Bericht enthält außerdem eine Liste möglicher Risikoindikatoren, die den Behörden und dem Privatsektor helfen werden, diese Geldflüsse aufzudecken. Die Feststellungen in diesem Bericht stützen sich auf Erfahrungen und Fachwissen aus dem gesamten öffentlichen und privaten Sektor, einschließlich Beiträgen und Fallbeispielen aus über 40 Ländern des globalen FATF-Netzwerks.

Ein Ransomware-Angriff ist eine Form von Erpressung und sollte nach den FATF-Standards als Geldwäschevortat unter Strafe gestellt werden. In diesem Bericht wird festgestellt, dass Lösegeldzahlungen und das anschließende Waschen der Gewinne fast ausschließlich über Kryptowerte abgewickelt werden. Kriminelle nutzen die Internationalität von Kryptowerten aus, um große grenzüberschreitende Transaktionen nahezu in Echtzeit durchzuführen, bisweilen ohne Beteiligung traditioneller Finanzinstitute und damit ohne entsprechende Mechanismen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (AML/CFT). Mithilfe anonymitätsfördernder Technologien, Verfahren und Token bei der Geldwäsche, wie z. B. Kryptowährungen und Mixer mit erhöhter Anonymität, können Kriminelle ihre Transaktionen noch stärker verschleiern.

Die fast ausschließliche Verwendung von Kryptowerten zur Geldwäsche im Zusammenhang mit Ransomware unterstreicht die Notwendigkeit einer beschleunigten Umsetzung der FATF-Empfehlung 15, in der die Länder aufgefordert werden, Maßnahmen zur Verringerung der mit Kryptowerten verbundenen Risiken zu ergreifen und den Sektor der Kryptowertedienstleister zu regulieren. Diese Maßnahmen sind von entscheidender Bedeutung, um zu verhindern, dass Kriminelle Kryptowertedienstleister in Ländern mit schwachen oder fehlenden AML-/CFT-Kontrollen in Anspruch nehmen können.

Darüber hinaus wurde festgestellt, dass Ransomware-Angriffe in der Regel selten gemeldet werden, sei es aufgrund von Schwierigkeiten bei der Aufdeckung durch den Privatsektor, negativen Auswirkungen auf das Geschäft des Opfers oder aus Angst vor Vergeltungsmaßnahmen seitens der Kriminellen, wenn ein Opfer einen Angriff meldet. Dies erklärt zum Teil auch die mangelnde Erfahrung mit Geldwäscheermittlungen im Zusammenhang mit Ransomware. Die Länder müssen weiter daran arbeiten, mehr Aufdeckungsquellen zu erschließen und die Erfassung der Fälle zu verbessern. Die Behörden müssen schnell handeln, um wichtige Informationen zu erhalten, und sollten über die notwendigen Instrumente und Fähigkeiten verfügen, um Kryptowerte wirksam nachverfolgen und abschöpfen zu können.

Ransomware betrifft eine Vielzahl von Bereichen und an den Ermittlungen können neben den traditionellen AML-/CFT-Behörden auch andere Akteure beteiligt sein, darunter Cybersicherheits- und Datenschutzbehörden. Aus diesem Grund setzt die wirksame Bekämpfung von Ransomware und der damit verbundenen Geldwäsche einen multidisziplinären Ansatz voraus. Da Kryptowerte von Natur aus dezentral und grenzüberschreitend sind, ist die Schaffung bzw. Nutzung bestehender internationaler Kooperationsmechanismen für eine erfolgreiche Bekämpfung der Geldwäsche im Zusammenhang mit Ransomware unerlässlich.

Um die globalen Maßnahmen gegen Ransomware-Angriffe und die damit verbundene Geldwäsche zu verstärken, schlägt die FATF folgende Maßnahmen vor.

Vorgeschlagene Maßnahmen

Die für diese Studie gesammelten Informationen enthalten praktische Beispiele für Maßnahmen, die Länder ergreifen können, um ihre Fähigkeiten zur Bekämpfung illegaler Geldflüsse im Zusammenhang mit Ransomware-Angriffen zu verbessern. In diesem Abschnitt werden diese bewährten Verfahren zusammengefasst und Vorschläge gemacht, wie die Länder Geldwäsche im Zusammenhang mit Ransomware-Angriffen effektiver unterbinden können.

Umsetzung einschlägiger FATF-Standards (auch zu Kryptowertedienstleistern) und verstärkte Aufdeckung

- Die Länder sollten ihre Bemühungen zur Einhaltung der einschlägigen FATF-Standards betreffend Kryptowertedienstleister beschleunigen, indem sie Empfehlung 15 (einschließlich der Travel Rule[1]) so bald wie möglich umsetzen. Damit wird sichergestellt, dass Kryptowertedienstleister die erforderlichen AML-/CFT-Pflichten zur Erfassung wichtiger Finanzinformationen und Meldung verdächtiger Transaktionen erfüllen.
- Die Länder sollten sicherstellen, dass Ransomware-Angriffe im Einklang mit FATF-Empfehlung 3 als Geldwäschevortat (z. B. als Form von Erpressung) unter Strafe gestellt werden.
- Die Länder sollten die Aufdeckung von Ransomware-Angriffen verbessern, indem sie
  - Verpflichtete bei der Aufdeckung von Ransomware-Angriffen und der damit verbundenen Geldwäsche sowie der Meldung verdächtiger Transaktionen unterstützen, u. a. durch die Weitergabe von Informationen zu neuen Entwicklungen, von Leitfäden zur Aufdeckung und von Warnindikatoren (wie diejenigen aus der FATF-Publikation „Bekämpfung der

[1] Die Travel Rule ist eine zentrale AML-/CFT-Vorschrift, nach der Kryptowertedienstleister Informationen über die Auftraggeber und Begünstigten von Kryptowertetransfers erheben, aufbewahren und übermitteln müssen. So können Finanzinstitute und Kryptowertedienstleister Sanktionslisten abgleichen und verdächtige Transaktionen aufspüren.

Finanzmittelbeschaffung durch Ransomware: mögliche Risikoindikatoren“[2]).

- die Betroffenen ermutigen, Vorfälle freiwillig zu melden, u. a. durch die Bekanntmachung von Unterstützungsangeboten und die Schaffung sicherer Meldekanäle.

- Die Länder sollten außerdem die Schaffung von Kommunikationsmöglichkeiten mit nicht traditionellen Akteuren, die keinen AML-/CFT-Pflichten unterliegen (z. B. Cyberversicherer oder Vorfallmanagementfirmen), in Betracht ziehen.

Unterstützung von Finanzermittlungen und Vermögensabschöpfung

- Die zuständigen Behörden sollten herkömmliche Methoden der Strafverfolgung sowie kryptowertespezifische Methoden anwenden und ggf. anpassen, um Geldwäscheermittlungen im Zusammenhang mit Ransomware-Angriffen durchzuführen. Die zuständigen Behörden sollten über die spezifischen Fähigkeiten und Fachkenntnisse verfügen, die für erfolgreiche Finanzermittlungen im Zusammenhang mit Ransomware-Angriffen erforderlich sind. Dazu zählen die Entwicklung von, der Zugriff auf und Schulungen zu Blockchain-Analyse- und Überwachungstools.

- Die Länder sollten sicherstellen, dass die Strafverfolgungsbehörden dauerhaft über die erforderlichen Fähigkeiten und Befugnisse verfügen, um Vermögenswerte, insbesondere Kryptowerte, rasch und wirksam sicherstellen und einziehen zu können. Sie sollten gewährleisten, dass spezielle Mechanismen zur ordnungsgemäßen Verwaltung von sichergestellten Kryptowerten vorhanden sind.

Ein multidisziplinärer Ansatz zur Bekämpfung von Ransomware-Angriffen

- Die Länder sollten sicherstellen, dass die von Ransomware-Angriffen ausgehenden Geldwäscherisiken in ihren nationalen Risikoanalysen ermittelt und analysiert werden. Aufgrund der dezentralen Struktur von Kryptowerten und Ransomware-Banden gilt dies auch für Länder mit Kryptowertesektoren, für die Ransomware-Angriffe derzeit keine nationale Bedrohung darstellen. Die im Rahmen der Risikoanalyse gewonnenen Erkenntnisse können wiederum in nationale Cyberstrategien einfließen, da sie einen ganzheitlichen, nationalen Überblick über die Ransomware-Risiken ermöglichen.

- Die Länder sollten zwischen den zuständigen Behörden Koordinierungsmechanismen entwickeln, und zwar von den Strafverfolgungs-, AML-/CFT- und Cyberkriminalitätsbehörden

[2] Verfügbar unter: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/countering-ransomware-financing.html

bis hin zu nicht traditionellen Partnern wie Cybersicherheits- oder Datenschutzbehörden. Dies fördert den Austausch von Informationen und Erkenntnissen und schafft eine nützliche Plattform für den wechselseitigen Austausch von Fachwissen.

Förderung von Partnerschaften mit dem Privatsektor

- Die Länder sollten Mechanismen zur Förderung der öffentlich-privaten Zusammenarbeit einrichten. In diese Kooperationsmechanismen sollten ggf. auch Kryptowertedienstleister und andere nicht traditionelle Partner eingebunden werden. Auf diese Weise können nützliche Plattformen zur Sensibilisierung, zum Austausch von Fachwissen und Erkenntnissen sowie zur Unterstützung der Strafverfolgungsziele geschaffen werden.

Verbesserung der internationalen Zusammenarbeit

- Die Länder sollten bilaterale, regionale und multilaterale Mechanismen schaffen und sich aktiv daran beteiligen, z. B. durch Verbindungsbüros oder die Einrichtung rund um die Uhr besetzter Kontaktstellen, um eine zügige internationale Zusammenarbeit und einen schnellen Informationsaustausch zu ermöglichen. Dies wird zur raschen grenzüberschreitenden Rückverfolgung von Geldern und wirksamen Vermögensabschöpfung beitragen und den Behörden dabei helfen, grenzüberschreitende Netzwerke, die Ransomware-Angriffe verüben und dabei Geldwäsche begehen, erfolgreich zu zerschlagen.

Einführung

Schwerpunkt und Anwendungsbereich

1. Ransomware ist eine Art Schadsoftware („Malware"), die von Kriminellen entwickelt und/oder verwendet wird, um den Zugriff auf Daten, Systeme oder Netzwerke zu blockieren und im Gegenzug ein Lösegeld zu fordern. Zu den üblichen Methoden eines Ransomware-Angriffs gehören die Verschlüsselung oder der Diebstahl von Daten sowie die Störung des Betriebs der Betroffenen. Bei Ransomware-Angriffen kommt häufig mehr als eine Methode zum Einsatz und es wird unter Umständen angedroht, die Daten der Betroffenen zu veröffentlichen.[3]

2. Anzahl und Ausmaß von Ransomware-Angriffen haben in den letzten Jahren deutlich zugenommen.[4] Ransomware-Angriffe dienen in erster Linie der Gewinnerzielung, und die Zunahme der Angriffe hat dementsprechend zu einem Anstieg der Ransomware-Erlöse und der damit verbundenen Geldwäsche geführt. Branchenschätzungen zufolge haben sich Ransomware-Zahlungen in den Jahren 2020 und 2021 im Vergleich zu 2019 mindestens vervierfacht.[5] Wenngleich aktuelle Branchenschätzungen auf einen Abwärtstrend für 2022 hindeuten (möglicherweise aufgrund der Zahlungsverweigerung der Betroffenen), ist der Wert der von Cyberkriminellen erbeuteten Kryptowerte weiterhin deutlich höher als vor 2019.[6] Die tatsächliche Anzahl der Angriffe und die damit verbundenen Verluste dürften deutlich höher liegen, da Ransomware-Angriffe häufig nicht gemeldet werden.

3. Ransomware-Angriffe haben Regierungen, öffentlichen Einrichtungen, Unternehmen und Privatpersonen erheblichen Schaden zugefügt und in einigen Fällen die Gesundheitsversorgung beeinträchtigt und die nationale Sicherheit bedroht, indem u. a. die Abschaltung kritischer Infrastrukturen und Dienste erforderlich war oder vertrauliche Daten kompromittiert wurden.[7] Dabei haben Cyberkriminelle Methoden entwickelt, um ihre Gewinne und Erfolgschancen durch Ransomware-Angriffe zu erhöhen. Dementsprechend dürfte die Bedrohung durch illegale Geldflüsse im Zusammenhang mit Ransomware-Angriffen weiter zunehmen.

4. Kriminelle fordern nahezu ausschließlich, dass die Lösegeldzahlung in Kryptowährung erfolgt. Die Betroffenen bzw. für sie handelnde Dritte nutzen für

---

3 FBI "Scams and Safety: Ransomware" (abgerufen im September 2022), verfügbar unter: www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware; Australian Cyber Security Centre "Ransomware" (abgerufen im September 2022), verfügbar unter: www.cyber.gov.au/ransomware.

4. ENISA Threat Landscape 2022 (Oktober 2022), verfügbar unter www.enisa.europa.eu/publications/enisa-threat-landscape-2022

5 Chainalysis, "Chainalysis Crypto Crime Report 2022" (Februar 2022), verfügbar unter: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

6 Chainalysis, "Ransomware Revenue Down As More Victims Refuse to Pay" (Januar 2023), verfügbar unter: https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/

7 Angriffe auf Krankenhäuser haben beispielsweise die Versorgung der Patienten gefährdet und Angriffe auf Polizeidienststellen die Sicherheit beeinträchtigt.

die Zahlung von Lösegeld häufig Kryptowertedienstleister[8]. Cyberkriminelle nutzen Kryptowertedienstleister auch, um illegale Gelder zu waschen und ihre Gewinne in Fiatgeld umzutauschen, das leichter für den Kauf von Waren und Dienstleistungen eingesetzt werden kann und ein stabileres Wertaufbewahrungsmittel darstellt.

5. 2018 hat die FATF Kryptowerte und Kryptowertedienstleister in ihre Empfehlungen aufgenommen. Seitdem hat die FATF verschiedene Leitfäden herausgegeben, einschließlich Warnindikatoren für Geldwäsche und Terrorismusfinanzierung, die den Ländern und dem Privatsektor helfen sollen, die Risiken in diesem Sektor zu überwachen und zu mindern.[9] Auch wenn Ransomware-Angriffe in diesen Dokumenten eine gewisse Rolle spielten, hat sich die FATF in dem vorliegenden Bericht erstmalig konkret mit Geldwäschetrends und -methoden in Verbindung mit Ransomware-Angriffen auseinandergesetzt.

6. Unter dem Vorsitz Singapurs nutzt die FATF dessen Erfahrungen mit Finanzermittlungen im Zusammenhang mit Kryptowerten, um Herausforderungen zu identifizieren und bewährte Verfahren zur Bekämpfung der Finanzmittelbeschaffung durch Ransomware und der damit verbundenen Geldwäsche weiterzugeben. Dieser Bericht befasst sich mit der Frage, wie Zahlungen im Zusammenhang mit Ransomware-Angriffen erkannt und gemeldet werden können, wie Geldflüsse im Zusammenhang mit Ransomware-Angriffen verhindert, aufgedeckt und untersucht werden können und wie die entsprechenden Gewinne gewaschen werden. Er befasst sich nicht mit dem Einsatz von Ransomware zur Terrorismusfinanzierung, da in den für diesen Bericht vorgelegten Informationen und Fallbeispielen kein nennenswerter oder auffälliger Einsatz von Ransomware für diesen Zweck festgestellt wurde.

7. Da ein Ransomware-Angriff eine Form der Erpressung darstellt, wird in den FATF-Empfehlungen gefordert, dass alle Länder Geldwäsche im Zusammenhang mit Ransomware-Angriffen als Straftat einstufen (Empfehlung 3). Gemäß den FATF-Empfehlungen sollten die Länder Maßnahmen ergreifen, um ihre Geldwäscherisiken zu identifizieren, zu analysieren und zu mindern (Empfehlungen 1-2). Sie sollten sicherstellen, dass der Privatsektor, einschließlich Kryptowertedienstleister, angemessene Präventionsmaßnahmen ergreift, wie z. B. die Meldung verdächtiger Transaktionen (Empfehlungen 9-23). Darüber hinaus sollten sie sicherstellen, dass die Strafverfolgungsbehörden Gewinne aus Straftaten identifizieren, zurückverfolgen und einziehen (Empfehlungen 4 und 29-31) und sie sollten bei der Verfolgung von Geldwäsche

---

[8] Kryptowertedienstleister bedeutet jede natürliche oder juristische Person, die nicht anderweitig unter die Empfehlungen fällt und als Unternehmen eine oder mehrere der folgenden Tätigkeiten für oder im Namen einer anderen natürlichen oder juristischen Person durchführt: Umtausch zwischen Kryptowährung und Fiatgeld, Umtausch zwischen einer oder mehreren Formen von Kryptowerten, Übertragung von Kryptowerten, Verwahrung und/oder Verwaltung von Kryptowerten oder von Instrumenten, die die Kontrolle über Kryptowerte ermöglichen, und Beteiligung an und Erbringung von Finanzdienstleistungen im Zusammenhang mit dem Angebot und/oder dem Verkauf von Kryptowerten durch einen Emittenten.

[9] Siehe FATF (Juni 2022) *Targeted Update on Implementation of the FATF Standards on Virtual Assets And Virtual Asset Service Providers* (September 2020) *Virtual Assets Red Flag Indicators* und (August 2019) *Confidential FATF Guidance on Financial Investigations Involving Virtual Assets.*

und Vortaten sowie der daraus resultierenden Gewinne auf internationaler Ebene zusammenarbeiten (Empfehlungen 36-40).

8. Ransomware-Angriffe sind nur eine von vielen Formen der Cyberkriminalität. Die Informationen in diesem Bericht konzentrieren sich auf Ransomware und treffen möglicherweise nicht auf andere Formen der Cyberkriminalität zu, wie z. B. Malware, Phishing, die Kompromittierung geschäftlicher E-Mails oder die Kompromittierung und den Verkauf von Finanzdaten.

Ziele und Gliederung

9. In Teil I dieses Berichts wird erläutert, wie Cyberkriminelle ihre Gewinne aus Straftaten erlangen, waschen und sich auszahlen lassen. Ziel ist es, weltweit das Bewusstsein für das Ausmaß der globalen Bedrohung durch Ransomware-Angriffe zu schärfen und das Verständnis dafür zu verbessern, wie Lösegeldzahlungen bei Ransomware-Angriffen funktionieren und wie die Gewinne aus diesen Angriffen zu den Cyberkriminellen gelangen.

10. In Teil II werden Herausforderungen und bewährte Verfahren für die Aufdeckung, Ermittlung und Unterbindung von Geldflüssen im Zusammenhang mit Ransomware-Angriffen dargestellt.

11. Dieser Bericht soll die **operativen Behörden** bei der Erstellung qualitativ hochwertiger Finanzinformationen, der Durchführung von Finanzermittlungen sowie der Aufdeckung, Rückverfolgung und Sicherstellung von Gewinnen aus Straftaten unterstützen. **Nationale Regulierungsbehörden** und **politische Entscheidungsträger** können die Informationen aus diesem Bericht zur Ermittlung von Schwachstellen und Risikominderung nutzen. Gleichzeitig soll der Bericht **Finanzinstituten**, **Kryptowertedienstleistern** und dem **Nichtfinanzsektor** bei der Entwicklung und Umsetzung von Kontrollen zur Aufdeckung, Meldung und Verhinderung illegaler Geldbewegungen im Zusammenhang mit Ransomware-Angriffen helfen.

Vorgehensweise

12. Dieses Projekt wurde unter der Federführung von Experten aus Israel und den USA umgesetzt. Darüber hinaus haben die folgenden Länder und Gremien als Teil des Projektteams zu dem Bericht beigetragen: Australien, Deutschland, die Europäische Kommission, Frankreich, Japan, Kanada, Luxemburg, Mexiko, die Philippinen, die Schweiz, Singapur, Südafrika, Spanien, die Türkei, das Vereinigte Königreich, die Asia Pacific Group on Money Laundering und die Egmont Group of Financial Intelligence Units (Egmont-Gruppe).

13. Die Erkenntnisse in diesem Bericht beruhen auf:

- einer Sichtung der vorhandenen Fachliteratur und frei zugänglichen Materialien zu diesem Thema,
- einer Anfrage an das globale FATF-Netzwerk aus über 200 Ländern mit der Bitte um Informationen über die Risikowahrnehmung der Länder, nationalen Gesetze und Befugnisse, Herausforderungen und bewährten Verfahren sowie Fallbeispiele im Zusammenhang mit Ransomware-Angriffen. Insgesamt erhielt das Projektteam Beiträge von über 40 Delegationen.

- Gespräche innerhalb der Virtual Asset Contact Group (VACG) der FATF.[10]
- gezielten Gesprächen mit dem Privatsektor über die VACG.

[10] Im Juni 2019 beschloss die Policy Development Group, die Virtual Asset Contact Group ins Leben zu rufen, um dem Privatsektor die FATF-Standards zu vermitteln und sicherzustellen, dass die Branche zügig technologische Lösung für deren Umsetzung entwickelt.

Teil I: Geldflüsse aus Ransomware-Angriffen

Umfang der Geldflüsse

14. Der Umfang der Ransomware-Angriffe und der damit verbundenen Geldflüsse hat weltweit dramatisch zugenommen. In vielen Ländern wurde in den letzten Jahren ein Anstieg der Häufigkeit von Ransomware-Angriffen beobachtet – je nach Land oder Region zwischen 10 und mehreren hundert Prozent. Gleichzeitig ist die Zahl der Meldungen von Opfern und die Zahl der verdächtigen Transaktionen im Zusammenhang mit Ransomware-Angriffen in verschiedenen Ländern gestiegen. In einem Land gingen im ersten Halbjahr 2021 Verdachtsmeldungen zu Transaktionen im Zusammenhang mit Ransomware-Angriffen mit einem Volumen von 590 Mio. USD (552 Mio. EUR) ein. Dies entspricht einem Anstieg von 42 % im Vergleich zum Jahr 2020, in dem das Volumen noch bei 416 Mio. USD (389 Mio. EUR) lag. [11] Aus aktuellen Jahresberichten der Strafverfolgungsbehörden geht eine erhebliche Zunahme der Ransomware-Aktivitäten[12] hervor und Schätzungen der Branche zeigen ein ähnliches Wachstum in Bezug auf die Anzahl der Angriffe und der aktiven Ransomware-Stämme. 2021 lag die geschätzte Zahl der Ransomware-Angriffe bei etwa 623,3 Mio. und hat sich damit gegenüber 2020 (304,6 Mio.) mehr als verdoppelt.[13] Auch die geschätzte Zahl der aktiven Ransomware-Stämme soll sich gegenüber 2019 verdoppelt haben.[14]

15. Obwohl einige Länder nur eine niedrige Zahl von Ransomware-Angriffen gemeldet haben, geht aus den für diesen Bericht erhobenen Informationen trotzdem hervor, dass Ransomware-Angriffe nach wie vor zu selten gemeldet werden, auch wenn die Zahl der Verdachtsmeldungen und der Meldungen von Opfern in einigen Ländern gestiegen ist. Daher können die Gesamtzahl der Vorfälle und die Höhe der gezahlten Lösegelder nur schwer geschätzt werden. Die für diesen Bericht vorgelegten Fallbeispiele zeigen, dass Ransomware-Angriffe für Industrie- und Entwicklungsländer – unabhängig von der Region – ein Risiko darstellen können.

16. In mehreren Ländern wurde festgestellt, dass die Zunahme von Ransomware-Angriffen und der damit verbundenen Geldflüsse mit der Entwicklung von Technologien durch Cyberkriminelle zusammenhängt, wie z. B. **Big Game Hunting** (Erpressung umsatzstarker Unternehmen), **Ransomware as a Service** (RaaS, ein Angebot von Schadsoftware, die gegen Bezahlung genutzt werden kann) oder **Doppel-/Dreifach-/Mehrfach-Erpressungstaktiken**, um die Wirksamkeit der Angriffe und die daraus resultierenden Gewinne zu maximieren (siehe Kasten 1).

---

11 FINCEN, "Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021" (Juni 2021), verfügbar unter: www.fincen.gov/sites/default/files/2021-10/Financial Trend Analysis Ransomware 508 FINAL.pdf

12 FBI, "Internet Crime Report 2021" (abgerufen am1. Dezember 2022), verfügbar unter: www.ic3.gov/Home/AnnualReports; EUROPOL, "Internet Organised Crime Threat Assessment (IOCTA) 2021" (abgerufen am1. Dezember 2022), verfügbar unter: www.europol.europa.eu/publications-events/main-reports/iocta-report

13 SonicWall, "2022 SonicWall Cyber Threat Report" (2022), verfügbar unter: www.infopoint-security.de/media/2022-sonicwall-cyber-threat-report.pdf

14 Chainalysis, "Chainalysis Crypto Crime Report 2022" (Februar 2022), verfügbar unter: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

Kasten 1. Entwicklung von Ransomware-Technologien

Beim **Big Game Hunting** nehmen Cyberkriminelle große, umsatzstarke Unternehmen oder bekannte Einrichtungen ins Visier, von denen sie annehmen, dass sie eher zur Zahlung eines Lösegelds bereit sind, um ihre Geschäftstätigkeit wieder aufnehmen zu können oder um öffentliche Aufmerksamkeit zu vermeiden. Cyberkriminelle wählen außerdem gezielt Unternehmen aus, die mit Just-in-time-Lieferketten arbeiten und bei denen die Kosten für Ausfallzeiten höher sein dürften, sowie kritische Infrastrukturen und Organisationen mit vertraulichen oder wertvollen Informationen. Die Angreifer gehen wahrscheinlich davon aus, dass diese Organisationen im Gegensatz zu anderen Betroffenen eher zur Zahlung eines Lösegelds bereit sind.

RaaS bezeichnet ein betrügerisches Geschäftsmodell, bei dem Cyberkriminelle im Dark Web Softwaresysteme für Ransomware-Angriffe anbieten oder Teile eines Angriffs auslagern, darunter z. B. die Verbreitung von Schadsoftware, die Erstkompromittierung des Netzwerks eines Opfers, der Diebstahl der Daten oder die Lösegeldverhandlungen für Affiliates gegen eine Gebühr und/oder einen Anteil am Lösegeld. Kriminelle können außerdem gestohlene Zugangsdaten erwerben, um auf die Systeme der Opfer zuzugreifen und Ransomware zu verbreiten, und sie können sich Informationen über bestimmte Branchen in bestimmten Ländern beschaffen, um die Auswahl ihrer Ziele und die Wirksamkeit ihrer Angriffe zu optimieren. Das RaaS-Modell hat die Kosten für Ransomware-Angriffe gesenkt und erfordert weniger Fachwissen, was die Einstiegshürden senkt und es auch weniger erfahrenen Kriminellen ermöglicht, Ransomware-Angriffe zu verüben.

Double Extortion bezeichnet ein Modell, bei dem Ransomware-Angreifer die Daten eines Opfers stehlen, bevor sie sie verschlüsseln, und dann mit der Veröffentlichung der gestohlenen Daten drohen, wenn die Lösegeldforderungen nicht erfüllt werden. Somit kommt zu der Bedrohung durch das kompromittierte System noch die Bedrohung durch die Veröffentlichung der Daten hinzu. Durch diese Taktik wird zusätzlicher Druck auf die Opfer ausgeübt, der Lösegeldforderung nachzukommen, selbst wenn sie ihre Geschäftstätigkeit wiederherstellen können.

Triple Extortion bezeichnet ein Modell, bei dem die Ransomware-Angreifer nicht nur von den eigentlichen Opfern des Angriffs Geld verlangen, sondern auch von denen, die durch die Offenlegung der erbeuteten Daten, z. B. geschützte Gesundheitsdaten,

personenbezogene Informationen, Kontodaten und geistiges Eigentum, Schaden erleiden könnten.

Multiple Extortion bezeichnet ein Modell, bei dem mehr als zwei Erpressungsmethoden zum Einsatz kommen. Dabei werden neben dem Double-Extortion-Modell mit Datenverschlüsselung und -exfiltration weitere Druckmittel eingesetzt, wie z. B. Distributed Denial of Service (DDoS), Kontaktaufnahme mit Kunden der Betroffenen, Leerverkäufe von Aktien der Betroffenen oder Störung von Infrastruktursystemen.

17. Öffentlichen Informationen zufolge richtete sich über die Hälfte aller gemeldeten Ransomware-Angriffe gegen Einrichtungen der Regierung bzw. des öffentlichen Sektors, des Gesundheitswesen sowie der Industriegüter- und Dienstleistungsbranche [15, 16]. Dies ist zum Teil auf das Big Game Hunting zurückzuführen, das die hohen Zahlungen und den allgemeinen Anstieg der Ransomware-Zahlungen erklären dürfte. In den letzten Jahren haben Cyberkriminelle zudem Energieversorgungsunternehmen, Finanzinstitute, Kommunikationsunternehmen und Bildungseinrichtungen ins Visier genommen. Wenngleich Cyberkriminelle sich beim Big Game Hunting auf Großunternehmen konzentrieren, werden auch mittlere und kleine Unternehmen und Branchen häufig Opfer von Ransomware-Angriffen. Tatsächlich zielen die meisten Ransomware-Angriffe weiterhin auf kleine und mittlere Unternehmen ab. Diese kleineren Ziele haben möglicherweise ein günstigeres Risiko-Gewinn-Verhältnis als Großangriffe gegen größere Unternehmen. Im zweiten Quartal 2020 richteten sich fast 55 % aller Angriffe gegen Unternehmen mit weniger als 100 Beschäftigten und etwa 75 % der Angriffe gegen Unternehmen mit einem Umsatz von weniger als 50 Mio. USD (47 Mio. EUR).[17]

18. Die Lösegeldsummen reichen von Hunderten von Dollar oder Euro an Kryptowerten bei kleinen Angriffen auf Einzelpersonen bis hin zu Millionen von Dollar oder Euro bei Angriffen auf Großunternehmen, insbesondere kritische Infrastrukturen oder Organisationen mit sensiblen oder wertvollen Informationen. Die Erfahrungen der Länder zeigen, dass auch die von den Tätern geforderten Lösegelder in den letzten Jahren gestiegen sind. Im Jahr 2021 betrug die durchschnittliche Lösegeldzahlung etwa 800.000 USD (748.000 EUR) in Kryptowährung und war damit fast fünfmal so hoch wie im Jahr 2020.[15] Dieser Anstieg dürfte auf die oben beschriebenen Big-Game-Hunting-Methoden zurückzuführen sein. In einigen Fällen betrugen die Lösegeldsummen mehrere

---

15 Sophos, "The State of Ransomware in State and Local Government" (September 2022), verfügbar unter: https://assets.sophos.com/X24WTUEQ/at/rbjqpp5wwm6v5h3wj9v3733/sophos-state-of-ransomware-government-2022-wp.pdf.

16 Digital Shadows, "Ransomware: Analyzing The Data From 2020" (Januar2021), verfügbar unter: www.digitalshadows.com/blog-and-research/ransomware-analyzing-the-data-from-2020/.

17 Coveware, "Q2 Quarterly Report" (August 2020), verfügbar unter: www.coveware.com/blog/q2-2020-ransomware-marketplace-report.

zehn Millionen Dollar oder Euro in Kryptowährung. So wurde laut Presseberichten eine Versicherungsgesellschaft mit Sitz in den USA 2021 Opfer eines Ransomware-Angriffs durch „Phoenix CryptoLocker" (Berichten zufolge der drittgrößte RaaS-Anbieter nach Umsätzen hinter Conti und DarkSide)[18] und zahlte 40 Mio. USD (37 Mio. EUR), um die Kontrolle über ihr Netzwerk wiederzuerlangen.[19]

Merkmale und geografische Trends

19. Ransomware ist grundsätzlich ein internationales Phänomen, was zum Teil auf die inhärenten Eigenschaften von Cyberkriminalität und Kryptowerten zurückzuführen ist. Die Informationen aus dem globalen FATF-Netzwerk sowie aus Fallbeispielen und Branchendaten deuten auf bestimmte Merkmale und geografische Trends bei Ransomware-Angriffen hin. So wurden zahlreiche Ransomware-Netzwerke mit Ländern mit erhöhten Geldwäscherisiken in Verbindung gebracht (siehe Kasten 2). Diese Länder werden von Ransomware-Kriminellen häufig zur Ein- oder Auszahlung ihrer Gewinne genutzt. In anderen Fällen wurden Ransomware-Angriffe von diesen Ländern aus verübt oder indirekt von ihnen unterstützt.[20]

Kasten 2. Länder 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 illegale Drogen, 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 Schwachstellen bei der Governance, Strafverfolgung und Regulierung bestehen, darunter Länder, in denen die FATF ein schwaches AML-/CFT-System festgestellt hat, insbesondere in Bezug auf Kryptowertedienstleister, und in denen Kryptowertedienstleister und

18 Chainalysis, "Chainalysis Crypto Crime Report 2022" (Februar 2022), verfügbar unter: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

19 Mehrotra, Kartikay and Turton, William, "CNA Financial Paid $40 Million in Ransom After March Cyberattack," Bloomberg, 20 May 2021 (abgerufen am 1 Dezember 2022), verfügbar unter: www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

20 See Alert (AA22-187A) from the U.S. Cybersecurity & Infrastructure Security Agency (Juli 2022), verfügbar unter: www.cisa.gov/uscert/ncas/alerts/aa22-187a.

andere Verpflichtete bei ihren Geschäftsbeziehungen und Transaktionen besondere Vorsicht walten lassen sollten.

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

20. Das Ausmaß der Ransomware-Angriffe ist regional unterschiedlich. Branchenberichte aus dem Jahr 2022 zeigen, dass der Nahe Osten und Afrika am wenigsten von Ransomware-Angriffen betroffen waren (4 %), gefolgt von Lateinamerika (6 %), dem asiatisch-pazifischen Raum (10 %), Europa (28 %) und Nordamerika (52 %).[21] Die unterschiedlichen Größenordnungen in den verschiedenen Regionen wirken sich auch auf die Wahrnehmung des von Ransomware-Angriffen ausgehenden Risikos aus. Informationen des globalen FATF-Netzwerks zeigen, dass die Länder, in denen verstärkt umsatzstarke Unternehmen erpresst werden und die Lösegelder entsprechend hoch sind, das Geldwäscherisiko im Zusammenhang mit Ransomware-Angriffen eher hoch einschätzen.

21. Viele große Ransomware-Banden nutzen eine RaaS-Variante, sogenannte Affiliate-Modelle, bei denen sie Teile eines Ransomware-Angriffs gegen eine Gebühr und/oder einen Anteil am Lösegeld auslagern. In solchen Fällen sind die an einem Ransomware-Angriff beteiligten Täter häufig geografisch weit verstreut, und es kann schwierig sein, sie zu identifizieren und zu lokalisieren. Wie das folgende Fallbeispiel EMOTET zeigt, können Cyberkriminelle bei Ransomware-Angriffen aus verschiedenen Ländern zusammenarbeiten oder gemeinsame Infrastrukturen nutzen. Aufgrund der Vielzahl beteiligter Täter aus verschiedenen Ländern können die Geldflüsse der wichtigsten Ransomware-Angreifer nur schwer nachverfolgt werden.

Kasten 3. Fallbeispiel EMOTET[1]

EMOTET war eine der größten Malware-Kampagnen der letzten Jahre. Sie wurde 2014 zuerst als Bankingtrojaner[2] entdeckt und hat sich anschließend zu einem der wichtigsten Tools für andere Malware und Ransomware weiterentwickelt. Als EMOTET 2021 zerschlagen wurde, war das Netzwerk für 70 % der weltweiten Malware-Angriffe verantwortlich, u. a. durch die Ransomware-Varianten RYUK und DoppelPaymer, die Unternehmen im Vereinigten Königreich erheblichen wirtschaftlichen Schaden zugefügt hatten. Ermöglicht wurde die Zerschlagung durch enge Zusammenarbeit der Strafverfolgungsbehörden Deutschlands, Frankreichs, Kanadas, Lettlands, der Niederlande, der Ukraine, des Vereinigten Königreichs und der Vereinigten Staaten sowie durch die von Europol und Eurojust koordinierten internationalen Aktivitäten. Durch diese partnerschaftliche Kooperation konnten die nationalen Strafverfolgungsbehörden Daten aufspüren und analysieren und auf diese Weise Zahlungen und Registrierungsdaten Kriminellen zuordnen,

[21] Group-IB, "Ransomware Uncovered Report. Group-IB" (Mai 2022), verfügbar unter: https://spiresolutions.com/wp-content/uploads/2021/07/ransomware_uncovered_2020.pdf.

die EMOTET genutzt haben. Dieser Fall veranschaulicht das Ausmaß und die Beschaffenheit von Cyberkriminalität und zeigt, wie wichtig die internationale Zusammenarbeit zur Eindämmung dieser Bedrohung ist.

Quelle: Vereinigtes Königreich

Anmerkungen:
1. Siehe auch Pressemitteilung von Europol zu EMOTET, verfügbar unter: www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
2. Ein Bankingtrojaner ist eine Schadsoftware, mit der Zugangsdaten von Bankkunden gestohlen oder sich Zugang zu deren Finanzinformationen verschafft werden sollen.

22. Aufgrund des grenzüberschreitenden Charakters von Kryptowerten, die fast immer für Ransomware-Zahlungen verwendet werden, erfolgt auch das Waschen von Ransomware-Zahlungen grenzüberschreitend. Die Nutzer von Kryptowerten können Peer-to-Peer-Transaktionen durchführen, d. h. sie überweisen direkt untereinander nur mit ihrem privaten Schlüssel und einer Internetverbindung – unabhängig von geografischen Grenzen und ohne Beteiligung von Instituten mit AML-/CFT-Pflichten. Cyberkriminelle mit Internetzugang können diese Eigenschaften von Kryptowerten ausnutzen, um umfangreiche grenzüberschreitende Transaktionen nahezu in Echtzeit durchzuführen, ohne dass traditionelle Finanzinstitute mit einschlägigen AML-/CFT-Maßnahmen beteiligt sind. Sie können außerdem auf Kryptowertedienstleister weltweit zurückgreifen, die ihren Sitz in Ländern ohne oder mit nur schwachen AML-/CFT-Kontrollen haben und die von Cyberkriminellen genutzt werden, um ihre illegalen Gewinne in Fiatgeld auszahlen zu lassen.

Kasten 4. Was sind Kryptowerte?

Ein Kryptowert ist ein Wert in digitaler Form, der digital gehandelt oder übertragen und für Zahlungs- oder Anlagezwecke genutzt werden kann. Nicht darunter fallen digitale Darstellungsformen von Fiat-Währungen, Wertpapieren und anderen finanziellen Vermögenswerten, die bereits anderweitig in den FATF-Empfehlungen abgedeckt sind.

Die am häufigsten verwendeten Kryptowerte sind Tauschmittel, bei denen die Generierung oder die Aufzeichnung der Eigentumsverhältnisse durch eine auf Kryptografie basierende Distributed-Ledger-Technologie wie z. B. eine Blockchain erfolgt. Wie im Folgenden erläutert wird, laufen viele beliebte Kryptowerte auf öffentlichen Blockchains, auf denen pseudonyme Transaktionsdaten einsehbar sind.

Quelle: FATF

Gängige Methoden und Trends

23. Erfolgreiche Finanzermittlungen nach einem Ransomware-Angriff erfordern ein fundiertes Verständnis der zur Geldwäsche verwendeten Methoden. Da

Ransomware-Angriffe häufig nicht gemeldet werden, wurden in diesem Bericht Informationen aus einer Vielzahl offener Quellen sowie Erfahrungen aus verschiedenen Ländern zusammengetragen, um besser zu verstehen, wie Lösegeldzahlungen geleistet, gewaschen, entgegengenommen und in einigen Fällen in Fiatgeld getauscht werden.

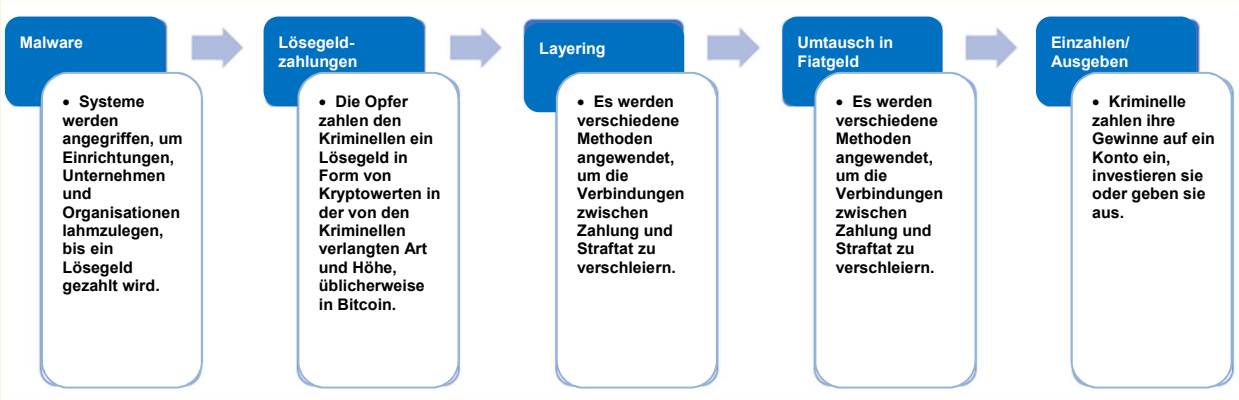
24. Bei einem Ransomware-Angriff fließen die Gelder oft über verschiedene traditionelle Finanzinstitute sowie über Kryptowertedienstleister. Andere Dritte, wie Cyberversicherungs-, Vorfallmanagement- oder Cybersicherheitsfirmen, können ebenfalls an der Reaktion auf einen Ransomware-Angriff beteiligt sein, einschließlich bei Zahlung des Lösegelds im Namen der Opfer.

25. Während Kryptowerte die bevorzugte Methode für Lösegeldzahlungen sind, fließen die Gelder bei einem Ransomware-Angriff insgesamt über mehrere traditionelle Finanzinstitute sowie Kryptowertedienstleister und andere Dritte.

Tabelle 1. Potenziell an Geldflüssen aus Ransomware-Angriffen beteiligte Branchen

Finanzinstitute	Finanzinstitute fungieren in der Regel als Intermediäre, die von den Opfern eines Ransomware-Angriffs (oder von in deren Namen handelnden Dritten) genutzt werden, um Gelder an einen Kryptowertedienstleiter für den Kauf von Kryptowerten zu überweisen.
Kryptowertedienstleister	Opfer von Ransomware-Angriffen (oder in deren Namen handelnden Dritte) nehmen Kryptowertedienstleister in Anspruch, um die von den Ransomware-Angreifern geforderte Art und Menge an Kryptowerten zu kaufen und zu überweisen.
Versicherungsfirmen	Versicherungsfirmen können Lösegeld als Teil einer Cyberversicherung abdecken und in einigen Fällen auch bezahlen.
Vorfallmanagementfirmen (Incident Response Companies)	Vorfallmanagementfirmen, die von Opfern eines Ransomware-Angriffs engagiert werden, verhandeln in vielen Fällen mit den Angreifern über das Lösegeld. Als Teil ihrer Dienstleistungen kaufen diese Firmen von Kryptowertedienstleistern die für das Lösegeld benötigten Kryptowerte und überweisen sie im Namen des Opfers an die Angreifer.
Cybersicherheitsfirmen	Firmen, die für den Schutz der Daten, Systeme, Netzwerke und angeschlossenen Geräte ihres Kunden vor unbefugtem und illegalem Zugriff verantwortlich sind.

Kasten 5. Typische Geldflüsse im Zusammenhang mit Ransomware-Zahlungen:



Wenn ein Opfer eine Lösegeldforderung erhält, überweist das Opfer oder ein für das Opfer handelnder Dritter in der Regel per elektronischer Zahlungsanweisung, Kreditkarte oder über ein automatisiertes Clearinghaus Geld an einen Kryptowertedienstleister, um die vom Ransomware-Angreifer geforderte Art und Menge an Kryptowerten zu kaufen. Dritte, die im Namen des Opfers handeln, sind beispielsweise Vorfallmanagement- oder Cyberversicherungsfirmen.

Anschließend sendet das Opfer oder der Dritte das Lösegeld, häufig von einer Wallet bei einem Kryptowertedienstleister, an die Kryptoadresse des Täters. Dabei handelt es sich in der Regel um eine selbstverwaltete („unhosted“) Wallet (d. h. eine auch als „non-custodial wallet“ bezeichnete Soft- oder Hardware, die es dem Nutzer ermöglicht, Kryptowerte unabhängig von einem Dritten, wie z. B. einem Kryptowertedienstleister, zu verwahren, zu speichern oder zu übertragen, die von einem Cyberkriminellen oder einem Finanzagenten kontrolliert wird, oder um eine Wallet, die von einem Kryptowertedienstleister mit Sitz außerhalb des Landes verwaltet wird, in dem der Cyberangriff stattfindet, wobei dieses andere Land meistens nicht mit den Strafverfolgungsbehörden oder FIUs kooperiert.

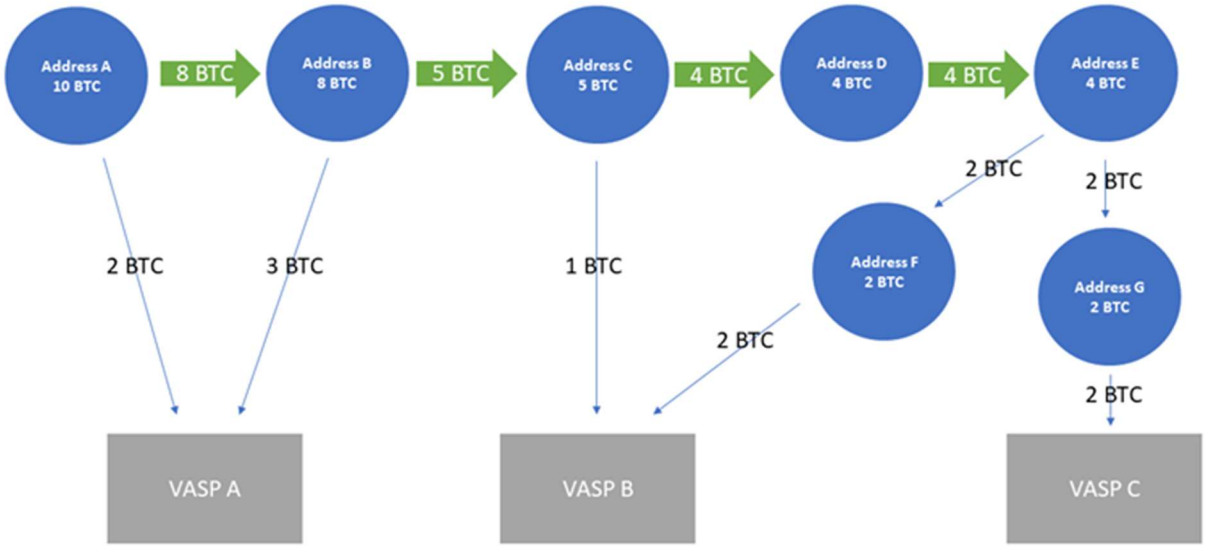
In vielen Fällen wird der Cyberkriminelle anschließend verschiedene Verschleierungsmethoden anwenden (die weiter unten ausführlicher beschrieben werden). Schließlich nutzen Cyberkriminelle häufig Kryptowertedienstleister im Ausland, um Kryptowerte in Fiatgeld umzutauschen, oder sie belassen Gelder für längere Zeit in selbstverwalteten Wallets oder nutzen Kryptowerte zur Bezahlung von an den Angriffen beteiligten Dritten.

26. Cyberkriminelle verwenden häufig auch Technologien, Methoden und Token zur Erhöhung der Anonymität bei der Geldwäsche, darunter eine oder mehrere der nachfolgend beschriebenen Methoden. Dabei gehen sie beim Waschen ihrer Gewinne nicht immer mit denselben Methoden oder in derselben Reihenfolge vor.

- Ransomware-Angreifer verlangen häufig, dass die Zahlungen der Opfer in Kryptowährung an von ihnen kontrollierte Wallet-Adressen gesendet werden, und geben dabei häufig für jeden Angriff **verschiedene Wallet-Adressen** an.
- Nachdem ein Angreifer Geld erhalten hat, kann er mehrere Zwischenadressen verwenden, um die Kryptowerte über eine Reihe von Transaktionen mit

kleineren Beträgen nacheinander von einer Wallet-Adresse zur nächsten zu verschieben. Die Gelder werden oft an Wallet-Adressen bei verschiedenen Kryptowertedienstleistern übertragen. Diese Transaktionsmuster werden als **Peel Chains** bezeichnet und werden nicht nur für die Verschleierung von Kryptowertetransfers genutzt.[22] Sie können auch von Kriminellen genutzt werden, um große Mengen an Kryptowerten über eine Reihe kleinerer Transaktionen zu waschen und so die Rückverfolgungschancen zu verringern. Die Spur der Kryptowerte kann insbesondere dann verwischt werden, wenn die Transaktionen sehr schnell und kurz hintereinander durchgeführt werden.

Abbildung 1. Peel Chains



- Cyberkriminelle waschen Kryptowerte häufig auch mithilfe von **Mixern oder Tumblern** (z. B. Wasabi), bei denen verschiedene Methoden zur Verschleierung der Verbindung zwischen den Absender- und Empfängeradressen der Kryptowerte zum Einsatz kommen, sei es anstelle oder zusätzlich zur Verschiebung der Kryptowerte über Peel Chains. In einigen Fällen nutzen Cyberkriminelle auch sogenannte CoinJoin-Transaktionen, bei denen mehrere Absender und Empfänger ihre Zahlungen zu einer einzigen aggregierten Transaktion zusammenfassen. Dazu bedarf es eines spezialisierten Dienstleisters wie JoinMarket, der interessierte Nutzer zusammenbringt und sie bei der Durchführung einer solchen Transaktion unterstützt.
- Ransomware-Angreifer nutzen außerdem **Kryptowährungen mit erhöhter Anonymität** (auch **Privacy Coins** genannt), wenngleich die meisten ihre Zahlungen in Bitcoin verlangen. Aus Erfahrungen der Länder und Branchenberichten geht hervor, dass diese anonymen Kryptowährungen für Zahlungen an Ransomware-Angreifer genutzt werden, da bei ihnen die Wallet des Absenders und Empfängers verschleiert werden kann. Hierbei kann

[22] Peel Chains werden häufig beobachtet und können aufgrund des Designs von Krypto-Wallets auch natürlich auftreten.

beispielsweise eine Kombination aus anonymitätssteigernden Technologien wie Mixer, Ringsignaturen, Schattenadressen und vertrauliche Ringtransaktionen zum Einsatz kommen, die allesamt die Wallet des Absenders und Empfängers verschleiern können. Immer mehr Ransomware-Angreifer verlangen Zahlungen ausschließlich in Monero, auch wenn Bitcoin die am häufigsten verwendete Kryptowährung bei Ransomware-Angriffen ist (99 %).[23] In einigen Ländern wurden Fälle festgestellt, bei denen die Angreifer Zahlungen sowohl in Bitcoin als auch in Monero akzeptierten. Für Zahlungen in Bitcoin verlangten sie jedoch eine Zusatzgebühr in Höhe von 10-20 % des geforderten Lösegelds, da diese Transaktionen leichter nachverfolgt werden können. Kriminelle zahlen also zusätzliche Gebühren für die Nutzung anonymitätsfördernder Technologien, wie z. B. Mixing-Dienste, um den Behörden die Nachverfolgung und Zuordnung von Transaktionen zu erschweren.

- Mehrere Länder haben auch festgestellt, dass Cyberkriminelle Lösegeldzahlungen häufig über Kryptowertedienstleister oder DeFi-Protokolle von Bitcoin in andere Kryptowerte umwandeln.[24, 25] Dieses Vorgehen wird gerne als **Chain-Hopping** bezeichnet, d. h. der Wechsel von einem Kryptowährung zu einer anderen Blockchain, oft schnell hintereinander und mit dem Ziel, die Rückverfolgbarkeit dieser Transaktionen zu verhindern. Aus einem Land wurde berichtet, dass Cyberkriminelle zunehmend DeFi-Protokolle nutzen, um zu sogenannten Stablecoins[26] zu wechseln, bevor sie das Geld in Fiat-Währung umtauschen. DeFi-Plattformen sind für Kriminelle attraktiv, da viele von ihnen keine AML-/CFT-Kontrollen durchführen, obwohl sie je nach Ausgestaltung ihres Geschäftsmodells den entsprechenden Pflichten unterliegen. In einem Land wurde berichtet, dass Cyberkriminelle DeFi-Protokolle und Mixer systematisch zur Geldwäsche einsetzen, in einigen Fällen mehrmals hintereinander.
- Bei der Geldwäsche nutzen Cyberkriminelle häufig zentralisierte Kryptowertedienstleister, darunter außerbörsliche Händler, um ihre Gewinne

---

23 Coveware, "Q3 Ransomware Marketplace Report" (November 2019), verfügbar unter: www.coveware.com/blog/q3-ransomware-marketplace-report.

24 Der Begriff „Decentralised Finance" (DeFi) wird verwendet, wenn dezentralisierte oder verteilte Anwendungen, die über eine Blockchain auf der Basis von Smart Contracts ausgeführt werden, Finanzdienstleistungen anbieten, die mit denen von Kryptowertedienstleistern vergleichbar sind. Eine DeFi-Anwendung (d. h. ein Softwareprogramm) ist nach den FATF-Standards kein Kryptowertedienstleister, da die Standards nicht für die zugrunde liegende Software oder Technologie gelten. Die Ersteller, Eigentümer, Betreiber oder andere Personen, die die Kontrolle oder einen hinreichenden Einfluss auf die DeFi-Anwendungen ausüben, können jedoch unter die FATF-Definition eines Kryptowertedienstleisters fallen, wenn sie entsprechende Dienstleistungen anbieten oder aktiv ermöglichen.

25 DeFi-Protokolle, insbesondere Cross Chain Bridges, werden nicht nur zum Waschen von Ransomware-Zahlungen verwendet, sondern werden zunehmend von Cyberkriminellen genutzt, um Sicherheitslücken auszunutzen und Kryptowerte zu stehlen.

26 Anmerkung zur Terminologie: Nach Auffassung der FATF ist der Begriff „Stablecoin" keine eindeutige rechtliche oder technische Kategorie, sondern in erster Linie ein von den Anbietern selbst verwendeter Marketingbegriff. Um diesem Claim nicht unfreiwillig Vorschub zu leisten, werden diese Kryptowährungen im vorliegenden Bericht als „sogenannte Stablecoins" bezeichnet.

auszahlen zu lassen. Cyberkriminelle senden Kryptowerte häufig an einen Kryptowertedienstleister in einem Hochrisikoland oder einem Land mit schwachen bzw. fehlenden AML-/CFT-Kontrollen, um sie in Fiatgeld umzutauschen. Kriminelle in Hochrisikoländern können hierfür auf lokale zentralisierte Kryptowertedienstleister zurückgreifen, wie im Falle der in den USA gelisteten Kryptowertedienstleister Suex,[27] Chatex,[28] Garantex[29] und Bitzlato Limited (siehe Kasten 6).[30] Mehrere Länder berichteten, dass sich die Auszahlungsstellen hauptsächlich in städtischen, zentralen Lagen befinden. In einigen Fällen nutzten Cyberkriminelle verschiedener Banden denselben Kryptowertedienstleister, um ihre Kryptowerte zu erhalten oder zu waschen.

- Sind mehrere Parteien an einem Angriff beteiligt, müssen Cyberkriminelle in der Regel ihre Partner und die Betreiber der genutzten Infrastruktur bezahlen. Kriminelle Infrastrukturbetreiber sind zunehmend bereit, Zahlungen in Kryptowerten zu akzeptieren, die von Cyberkriminellen mit den aus ihren Angriffen erzielten Gewinnen geleistet werden. Blockchain-Analyse-Firmen haben in vielen Fällen die direkte Weiterleitung von Ransomware-Zahlungen an Kryptoadressen mit Verbindung zu kriminellen Betreibern von „Infrastructure-as-a-Service“ festgestellt.

Kasten 6. Bitzlato Limited[1]

Im Januar 2023 wurde bei einer länderübergreifenden Operation festgestellt, dass die in Russland sehr aktive Kryptobörse Bitzlato Limited eine entscheidende Rolle bei der Geldwäsche konvertierbarer virtueller Währungen gespielt hatte. Die Operation wurde von den französischen und US-amerikanischen Behörden geleitet und von Europol unterstützt. Behörden aus Belgien, den Niederlanden, Portugal, Spanien und Zypern waren ebenfalls beteiligt. Bitzlato wurde verdächtigt, an mehreren illegalen Transaktionen mitgewirkt zu haben, unter anderem für Cyberkriminelle wie der Ransomware-as-a-Service-Bande Conti, die Verbindungen zu Russland hat. Laut US-Justizministerium hat Bitzlato mehr als 15 Mio. USD an Ransomware-Gewinnen erzielt. Parallel dazu erließ die US-amerikanische FIU (Financial Enforcement Network) eine Verfügung, in der die Plattform als „erhebliches Geldwäscheproblem“ eingestuft wurde.

Diese Ermittlungen ermöglichten die Zerschlagung der Börsenplattform, einschließlich der Sicherstellung digitaler Infrastruktur und inkriminierter Vermögenswerte in Krypto-Wallets in

27 Siehe Pressemitteilung des US-Finanzministeriums, verfügbar unter: https://home.treasury.gov/news/press-releases/jy0364

28 Siehe Pressemitteilung des US-Finanzministeriums, verfügbar unter: https://home.treasury.gov/news/press-releases/jy0471

29 Siehe Pressemitteilung des US-Finanzministeriums, verfügbar unter: https://home.treasury.gov/news/press-releases/jy0701

30 Siehe Pressemitteilung des US-Finanzministeriums, verfügbar unter: www.justice.gov/opa/pr/founder-and-majority-owner-cryptocurrency-exchange-charged-processing-over-700-million

Frankreich in Höhe von 18 Mio. EUR, sowie die Verhaftung von Schlüsselpersonen in verschiedenen Ländern.

Bitzlato hatte damit geworben, von seinen Nutzern nur eine minimale Identifikation zu verlangen. Aufgrund dieser mangelhaften KYC-Verfahren soll Bitzlato zu einem Hort für Gewinne aus Straftaten und Gelder für kriminelle Aktivitäten geworden sein.

Quelle: Frankreich und USA

1. Siehe auch Pressemitteilung der französischen Nationalgendarmerie, verfügbar unter: www.gendarmerie.interieur.gouv.fr/gendinfo/enquetes/2023/demantelement-d-une-plateforme-de-cryptomonnaies-servant-au-blanchiment; sowie Pressemitteilung von Europol, verfügbar unter: www.europol.europa.eu/media-press/newsroom/news/bitzlato-senior-management-arrested

27. In einigen Ländern wurde auch festgestellt, dass Cyberkriminelle **Finanzagenten** mit Konten bei Kryptowertedienstleistern einsetzen, um über „Off-Ramps“, d. h. Dienste oder Plattformen, die den Umtausch von Kryptowerten in Fiatgeld ermöglichen, ihre Gewinne wieder zurück in Fiatgeld umzutauschen. Diese Konten können mit einer gestohlenen oder gefälschten Identität erstellt werden oder es kann sich um ein rechtmäßiges Konto handeln, dessen Inhaber ein Komplize ist. Bei Finanzagenten handelt es sich in der Regel um unverbundene Dritte in der letzten Phase des Geldwäscheprozesses, die für einen Teil des Geldflusses im Geldwäscheprozess verantwortlich sind. Da sie nicht mit der kriminellen Organisation in Verbindung stehen und nur kleinere Beträge transferieren, sind sie schwerer zu identifizieren.

Kasten 7. Beispiel für die Anwerbung von Finanzagenten

Cyberkriminelle werben Finanzagenten an und statten sie mit mobilen Endgeräten aus. In den meisten Fällen haben diese Finanzagenten keine Internetpräsenz und sind kaum mit dem Internet vertraut. Anschließend werden bei anonymen E-Mail-Anbietern außerhalb des Landes E-Mail-Konten eingerichtet, was die Identifizierung der Kontonutzer erschwert. Die Finanzagenten nutzen für das Onboarding ein sogenannten „Handlern“ bereitgestelltes mobiles Endgerät, um ein Konto bei einem Finanzinstitut oder einem Kryptowertedienstleister einzurichten. Nach dem erfolgreichen Onboarding geben die Finanzagenten das Gerät an den „Handler“ zurück. Diese nutzen dann das Gerät für Online-Transaktionen im Namen des Finanzagenten. In einigen Fällen nutzen die Kriminellen VPN-Dienste (Virtual Private Network), die die IP-Adresse des verwendeten Geräts verschleiern. Auf diese Weise bleibt der tatsächliche geografische Standort des Kriminellen, der die Transaktionen durchführt, verborgen.

Quelle: Südafrika

Teil II: Herausforderungen und bewährte Verfahren bei der Bekämpfung von Geldwäsche durch Ransomware-Angriffe

Rechtlicher Rahmen

28. Ein solider rechtlicher Rahmen dient den zuständigen Behörden als Grundlage für die Entwicklung wirksamer Strategien zur Risikominderung bei Ransomware-Angriffen. In diesem Abschnitt wird die Relevanz der FATF-Standards für i) die Strafbarkeit von Ransomware-Angriffen im Zusammenhang mit Geldwäsche und ii) die Anwendung von Präventionsmaßnahmen in den einschlägigen regulierten Sektoren analysiert.

Ransomware-Angriffe als Geldwäschevortat

29. Obwohl die meisten Länder keine spezifischen strafrechtlichen Vorschriften für Ransomware-Angriffe haben, können sie in der Regel Ransomware-Angriffe dennoch als Vortat strafrechtlich verfolgen.[31]

30. Aus den Beiträgen der Projektteilnehmer geht hervor, dass die Länder die Vortat eines Ransomware-Angriffs meistens als Erpressungsdelikt oder – noch häufiger – als Cyberstraftat, z. B. Datenbeschädigung oder Eindringen in bzw. Beschädigung von Computerprogrammen und -systemen, verfolgen. Nach FATF-Empfehlung 3 sollten die Länder Geldwäsche im Zusammenhang mit Erpressungsdelikten unter Strafe stellen. Bei Erpressungsdelikten liegt der Vorteil darin, dass sie technologieneutral sind, sodass damit Ransomware-Angriffe unabhängig von der verwendeten Methode oder Form erfasst werden können. Die Länder, in denen Ransomware-Angriffe als Erpressungsdelikte verfolgt werden, sollten sicherstellen, dass ihre Gesetze auf dem neuesten Stand sind, damit die zuständigen Behörden illegale Kryptogeldflüsse wirksam untersuchen und abschöpfen können (siehe Abschnitt 6).

31. Im Gegensatz zur Erpressung wurden Cyberstraftaten von der FATF nicht in ihre Mindestliste der Vortaten aufgenommen.[32] In der Praxis scheint dies jedoch nicht zu Lücken bei der Verfolgung von Geldwäsche im Zusammenhang mit Ransomware-Aktivitäten geführt zu haben. Eine Stichprobe unter einigen Ländern ergab, dass diejenigen, die Ransomware-Angriffe als Cyberstraftat verfolgen, diese als Vortat einstufen (entweder in einem Vortatenkatalog oder über einen „All-Crime-Ansatz“). Im Rahmen dieser Studie berichtete kein Land über Probleme bei der Verfolgung von Geldwäsche im Zusammenhang mit Ransomware. Die Länder sollten jedoch sicherstellen, dass sie durch ihre Wahl des Vortatbestands nicht daran gehindert werden, Geldwäsche im Zusammenhang mit Ransomware strafrechtlich zu verfolgen.

Anwendung von Präventionsmaßnahmen auf relevante Akteure

32. Gemäß den FATF-Standards sollten die Länder insbesondere auch mit Bezug auf Finanzinstitute, den Finanzsektor und Kryptowertedienstleister, Maßnahmen zur Verhinderung von Geldwäsche umsetzen. Diese Maßnahmen sollen

---

31 Die meisten Länder gaben an, dass sie Lösegeldzahlungen von Opfern an die Ransomware-Angreifer nicht unter Strafe stellen, obwohl einige Länder den Angriffsopfern dringend davon abraten, ein Lösegeld zu zahlen.

32 Siehe festgelegte Straftatkategorien im Glossar der FATF-Empfehlungen

sicherstellen, dass diese Verpflichteten ihre Geldwäscherisiken kennen und mindern, angemessene Kontrollen durchführen, einschließlich der Identifizierung ihrer Kunden, und verdächtige Transaktionen gemäß den FATF-Empfehlungen 9 bis 23 erkennen und melden.

33. Angesichts des Zusammenspiels von Ransomware und Kryptowerten war die 2018 vorgenommene Änderung der FATF-Standards zur Ausdehnung dieser Maßnahmen auf Kryptowertedienstleister ein wichtiger Schritt zur Verbesserung der globalen AML-/CFT-Vorschriften zur Bekämpfung von Ransomware-Risiken. Bis Januar 2023[33] hatten jedoch 63 (73 %) der 86 Länder, deren Einhaltung der überarbeiteten Standards (Empfehlung 15) geprüft wurde, diese Anforderungen nur teilweise oder gar nicht erfüllt.[34] Nur bei einem der 86 Länder ergab die Prüfung, dass die Anforderungen vollständig erfüllt wurden.

34. Angesichts der Vielzahl der im Hinblick auf die Umsetzung der Empfehlung 15 geprüften Länder dürften diese Zahlen für die Situation im gesamten globalen FATF-Netzwerk weitgehend repräsentativ sein. Diese Einschätzung wird auch durch die Ergebnisse einer FATF-Umfrage vom März 2022 gestützt, die ergab, dass 2022 weniger als die Hälfte der Befragten über ein Lizenzierungs- oder Registrierungssystem für Kryptowerte und Kryptowertedienstleister verfügten. Daher ist es wahrscheinlich, dass es in den meisten Ländern bei der Erfüllung der AML-/CFT-Pflichten durch Kryptowertedienstleister Lücken gibt, insbesondere auch bei der Identifizierung von Kunden oder der Meldung verdächtiger Transaktionen. In Anbetracht des grenzüberschreitenden Charakters von Kryptowerten ist es wichtig, dass die Länder im gesamten globalen Netzwerk die Einhaltung von Empfehlung 15 (einschließlich Travel Rule) vorantreiben.

Vorgeschlagene Maßnahmen

- Die Länder sollten ihre Bemühungen zur Einhaltung der einschlägigen FATF-Standards in Bezug auf den Sektor für Kryptowertedienstleister verstärken, indem sie die Empfehlung 15 (einschließlich Travel Rule) so bald wie möglich umsetzen. Damit wird sichergestellt, dass Kryptowertedienstleister die erforderlichen AML-/CFT-Pflichten zur Erfassung wichtiger Finanzinformationen und Meldung verdächtiger Transaktionen erfüllen.
- Die Länder sollten sicherstellen, dass Ransomware-Angriffe gemäß FATF-Empfehlung 3 als Geldwäschevortat (z. B. als Form der Erpressung) unter Strafe gestellt werden.

[33] Siehe konsolidierte Prüfungsergebnisse, verfügbar unter: www.fatf-gafi.org/en/publications/Mutualevaluations/Assessment-ratings.html. Hinweis: Nicht alle Länder waren Gegenstand der Prüfung im Hinblick auf die überarbeitete Methodik zu Empfehlung 15.

[34] Diese Analyse basiert auf den Länderprüfungen und den Folgeberichten der Länder, die im Hinblick auf die überarbeitete Methodik zu Empfehlung 15 geprüft wurden.

Aufdeckung und Meldung

35. Aufgrund der geografischen Verteilung der Cyberkriminellen, ihres Einsatzes von Geldwäschemethoden und der derzeitigen Merkmale von Ransomware-Angriffen (wie in Teil I erörtert) ist es schwierig, das Ausmaß der durch dieses Phänomen verursachten Geldflüsse abzuschätzen. In den meisten Ländern werden Ransomware-Angriffe immer noch zu selten gemeldet, sodass es schwierig ist, sich ein vollständiges Bild von den finanziellen Gewinnen und Geldströmen im Zusammenhang mit Ransomware zu verschaffen.

36. Solide Verfahren für die Aufdeckung und Meldung bilden die Grundlage für erfolgreiche Finanzermittlungen (siehe Abschnitt 6). Die Erfahrungen der Länder und die eingereichten Fallbeispiele zeigen, dass Geldflüsse im Zusammenhang mit Ransomware hauptsächlich über zwei Wege aufgedeckt werden: Verdachtsmeldungen und Meldungen von Betroffenen. In diesem Abschnitt werden Herausforderungen und bewährte Verfahren in Bezug auf den Umfang der Meldepflichten, die Identifizierung verdächtiger Transaktionen, die Ermutigung von Betroffenen zur Meldung von Angriffen und andere Quellen zur Aufdeckung von Ransomware-Angriffen erörtert.

Umfang der Meldepflichten

37. Die zuständigen Behörden nutzen Verdachtsmeldungen in der Regel zur Aufdeckung von Ransomware-Angriffen und als Informationsquelle bei Ermittlungen. Die überwiegende Mehrheit der Verdachtsmeldungen im Zusammenhang mit Ransomware stammt bisher von Kryptowertedienstleistern und Banken.

38. Einige wenige Länder haben Branchen, die in der Regel keinen AML-/CFT-Pflichten unterliegen, als zusätzliche potenzielle Quelle für die Aufdeckung illegaler Gewinne aus Ransomware-Angriffen identifiziert. Diese nicht traditionellen Branchen zu ermutigen oder zu verpflichten, verdächtige Transaktionen zu melden, kann insbesondere dann sinnvoll sein, wenn diese Branchen direkt an der Abwicklung von Ransomware-Angriffen im Auftrag von Kunden beteiligt sind.

39. So verfügt die Versicherungsbranche im weiteren Sinne, d. h. insbesondere mit Ransomware und Cyberversicherungen befasste Unternehmen, möglicherweise über unmittelbare Informationen zu Ransomware-Angriffen gegen Kunden mit einer Cyberversicherung, die Erstattungsansprüche geltend machen. Diese Unternehmen fallen nicht unter die FATF-Definition des Begriffs „Finanzinstitut“, der den Abschluss und die Vermittlung von Lebensversicherungen und anderen fondsgebundenen Versicherungen umfasst. Einige Länder haben mit der Versicherungsbranche Kontakt aufgenommen, um die Meldung von Ransomware-Angriffen zu fördern oder vorzuschreiben, was sich bereits positiv auf die Meldung von Ransomware-Angriffen ausgewirkt hat.

Kasten 8. Erhöhung der Meldungen von Ransomware-Angriffen durch gezielte Ansprache der Versicherungsbranche

Die Nicht-Lebensversicherungsbranche unterliegt in Frankreich AML-/CFT-Pflichten. Im Jahr 2021 wurde die Branche über spezielle Arbeitsgruppen bestehend aus Vertretern des öffentlichen und privaten Sektors angesprochen. Ziel dieser Arbeitsgruppen war es, die Versicherbarkeit von Cyberrisiken zu analysieren und die Widerstandsfähigkeit von Unternehmen gegen Cyberangriffe zu stärken. Ein wichtiges Ergebnis dieser Arbeitsgruppen war ein veröffentlichter Bericht[1], der sich u. a. mit den Entwicklungen der Geldwäscherisiken im Zusammenhang mit Ransomware sowie mit den AML-/CFT-Pflichten und bewährten Verfahren im Zusammenhang mit der Zahlung und Erstattung von Lösegeld befasst.

Auch die zuständige Aufsichtsbehörde ACPR hat die Versicherungsunternehmen u. a. bei Vor-Ort-Prüfungen genauer unter die Lupe genommen. Die ACPR erinnerte daraufhin die Verpflichteten an ihre AML-/CFT-Pflichten im Zusammenhang mit der Erbringung solcher Dienstleistungen, einschließlich der Notwendigkeit, alle relevanten Finanzinformationen zu überwachen und einzuholen (insbesondere zur Rückverfolgung von Zahlungen).

Seitdem hat TRACFIN einen Anstieg der Verdachtsmeldungen aus der Versicherungsbranche im Zusammenhang mit Ransomware-Zahlungen beobachtet: von 28 in 2020 und 19 in 2019 auf 66 in 2021. Der Anstieg im Jahr 2021 ist zum Teil auf ein einzelnes Versicherungsunternehmen zurückzuführen und ist noch nicht signifikant genug, um daraus Schlussfolgerungen ziehen zu können.

Quelle: Frankreich

1. Verfügbar auf Französisch unter www.banque-france.fr/sites/default/files/rapport_45_f.pdf

40. Vorfallmanagementfirmen haben ebenfalls Zugang zu sachdienlichen Informationen im Zusammenhang mit Ransomware-Angriffen und -Zahlungen. Diese Unternehmen, wie z. B. Unternehmen für Digitale Forensik und Reaktion auf Zwischenfälle sowie Anwaltskanzleien, helfen Opfern dabei, angemessen auf Ransomware-Angriffe zu reagieren. Sie können bei Ransomware-Zahlungen an Cyberkriminelle Unterstützung leisten, indem sie die Höhe des Lösegelds aushandeln, das Fiatgeld der Kunden in Kryptowerte umwandeln und die Gelder auf von den Kriminellen kontrollierte Konten überweisen. Wenn die Branche zur Meldung von Ransomware-Angriffen ermutigt bzw. verpflichtet wird, können Ransomware-Angriffe rechtzeitig erkannt und gemeldet werden, zumal die Kunden diese Unternehmen wahrscheinlich als Erste über einen Angriff informieren (teilweise vor den Strafverfolgungsbehörden). Je nach Geschäftsmodell und Dienstleistungsangebot können diese Unternehmen auch unter die Definition von „Kryptowertedienstleister“ fallen (und folglich den AML-/CFT-Pflichten und der Verpflichtung zur Abgabe von Verdachtsmeldungen unterliegen), sofern sie als Unternehmen für oder im

Namen einer anderen natürlichen oder juristischen Person tätig sind und Kryptowerte gegen andere Kryptowerte oder Fiatgeld tauschen sowie Kryptowerte übertragen, verwahren oder verwalten.

Kasten 9. Regulierung von DFIR-Unternehmen

Unternehmen für Digitale Forensik und Reaktion auf Zwischenfälle (kurz DFIR) sowie Cyberversicherungsunternehmen können Opfer von Ransomware-Angriffen im Rahmen der Erbringung ihrer Dienstleistungen unterstützen, indem sie Ransomware-Zahlungen veranlassen. In den Jahren 2020 und 2021 stellte FinCEN (die US-amerikanische FIU) in Leitfäden[1] klar, dass diese Tätigkeit je nach Sachverhalt eine Geldübermittlung darstellen könnte. Unternehmen, die Geldüberweisungen vornehmen, müssen sich als Gelddienstleister registrieren lassen und unterliegen AML-/CFT-Pflichten. In den Leitfäden wurden auch finanzielle Warnindikatoren sowie Ransomware-Angriffe und damit verbundene Zahlungen an DFIR- und Cyberversicherungsunternehmen zur Identifizierung verdächtiger Aktivitäten und Einreichung von Verdachtsmeldungen genannt.

Im ersten Halbjahr 2021 entfielen rund 63 % der Verdachtsmeldungen im Zusammenhang mit Ransomware auf Meldungen von in den USA ansässigen DFIR-Unternehmen.[2] Darüber hinaus stieg die Gesamtzahl der 2021 bei der FinCEN eingegangenen Meldungen im Zusammenhang mit Ransomware um 188 %. Diese Meldungen ermöglichten es FinCEN, Muster und Trends zu erkennen und zu analysieren, um die gesamtstaatlichen Maßnahmen zur Prävention und Bekämpfung von Ransomware-Angriffen zu unterstützen. So ergab die FinCEN-Analyse für das gesamte Jahr 2021, dass Ransomware weiterhin eine erhebliche Bedrohung für kritische Infrastruktursektoren, Unternehmen und die Öffentlichkeit in den USA darstellt. Darüber hinaus zeigte die Analyse, dass Ransomware-Varianten aus Russland für den Großteil der gemeldeten Ransomware-Aktivitäten verantwortlich waren und 69 % des Werts der Ransomware-Vorfälle und 75 % der Ransomware-bezogenen Vorfälle im zweiten Halbjahr 2021 ausmachten.[3]

Quelle: USA

Fußnoten

1. Verfügbar auf Französisch unter www.banque-france.fr/sites/default/files/rapport_45_f.pdf
2. Siehe FinCENs Financial Trend Analysis, verfügbar unter: www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf
3. Siehe FinCENs Financial Trend Analysis, verfügbar unter: www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf

41. Die obigen Ausführungen verdeutlichen, wie nützlich es ist, je nach Risiko und Kontext auch diverse nicht traditionelle Unternehmen zur Meldung zu ermutigen oder zu verpflichten. Auf diese Weise können verdächtige Aktivitäten aus verschiedenen Perspektiven gemeldet und erfasst werden, sodass die Behörden besser in die Lage versetzt werden, durch die Zusammenführung von

Informationen aus verschiedenen Sektoren Vorfälle aufzudecken, die sonst unerkannt geblieben wären.

Maßnahmen zur verstärkten Aufdeckung verdächtiger Transaktionen

42. Die Länder sind sich der Tatsache bewusst, dass verdächtige Aktivitäten im Zusammenhang mit Ransomware in allen Sektoren allgemein nicht ausreichend gemeldet werden. Ihre Aufdeckung kann durch die geografisch dezentrale Struktur der Ransomware-Banden, die Vielzahl der beteiligten Kriminellen sowie den Einsatz verschiedener Geldwäschemethoden erschwert werden. Ein Sektor allein kann die Gesamtsituation oftmals nicht überblicken.

43. Um die Häufigkeit und Qualität von Verdachtsmeldungen durch die Verpflichteten sowie die Aufdeckung insgesamt zu verbessern, nutzen die Länder verschiedene Methoden wie z. B. den Dialog mit dem Privatsektor sowie die Entwicklung und Weitergabe von Warnindikatoren und speziellen Leitfäden, die die Aufdeckung erleichtern sollen (siehe auch Abschnitt 8.3).

Kasten 10. Ransomware-Leitfaden der israelischen Behörde zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (IMPA)

Die israelische FIU (IMPA) hat eine strategische Analyse einschlägiger Verdachtsmeldungen durchgeführt, um die Merkmale von Lösegeldzahlungen bei Ransomware-Angriffen zu ermitteln. Dazu gehörten Angaben zur Häufigkeit und Art der angegriffenen Unternehmen, Höhe der gezahlten Beträge, Art der verwendeten Kryptowerte sowie Beteiligung Dritter. Dies führte zur Herausgabe eines Leitfadens zum Thema Ransomware, der Warnsignale und Fallbeispiele enthält. Er wurde auf der IMPA-Website[1] veröffentlicht, an alle einschlägigen Verpflichteten verteilt und in einer offiziellen Pressemitteilung bekannt gegeben.

Die bei der Analyse gewonnenen Erkenntnisse wurden außerdem auf diversen öffentlichen Foren und Fachkonferenzen vorgestellt. Die Veröffentlichung beförderte u. a. den Dialog mit dem israelischen mit israelischen Vorfallmanagementfirmen und ebnete so den Weg für eine weitere Vertiefung der Beziehungen und die Erörterung von Möglichkeiten der Zusammenarbeit und des Informationsaustauschs in der Zukunft.

Quelle: Israel

1. Nur auf Hebräisch verfügbar unter: www.gov.il/BlobFolder/dynamiccollectorresultitem/red-flags-typology-ransomware-impa-140222/he/professional-docs_red_flags_typology_ransomware_impa_140222.pdf

44. Wenn Kryptowertedienstleister Verdachtsmeldungen im Zusammenhang mit Ransomware erstatten, beruhen diese in den meisten Fällen auf dem Verdacht, dass Kryptowerte für Lösegeldzahlungen erworben wurden. Als nützliche Indikatoren dienen den Kryptowertedienstleistern dabei u. a. von Opfern ihnen gegenüber gemachte Aussagen, von einer bekannten Vorfallmanagementfirma getätigte Käufe sowie Zahlungen, die direkt oder indirekt mit einer Kryptoadresse verbunden sind, die vermutlich durch eine Blockchain-Analyse

als für Ransomware anfällig identifiziert wurde. Da Kryptowertedienstleister bei vielen Lösegeldzahlungen unmittelbar als Intermediär auftreten, sind sie eine wichtige Quelle für Verdachtsmeldungen zu illegalen Geldflüssen im Zusammenhang mit Ransomware. Eine Auflistung einschlägiger Risikoindikatoren für Kryptowertedienstleister findet sich in der FATF-Publikation „Bekämpfung der Finanzmittelbeschaffung durch Ransomware: mögliche Risikoindikatoren".

Kasten 11. Beteiligung einer Vorfallmanagementfirma

Die IMPA erhielt über einen israelischen Kryptowertedienstleister eine Verdachtsmeldung zu einer Vorfallmanagementfirma, die Kryptowerte (im damaligen Wert von mehreren Zehntausend Dollar) erwarb, um damit im Auftrag eines nicht benannten Angriffsopfers eine Lösegeldzahlung zu leisten. Der Verdachtsmeldung zufolge wurde unabhängig davon beim selben israelischen Kryptowertedienstleister von einem Vertreter des mutmaßlichen Angriffsopfers weitere Kryptowährung gekauft.

Finanzermittlungen der IMPA ergaben, dass die Wallet-Adresse, an die der Großteil der Gelder überwiesen wurde, in Verbindung zu anderen Ransomware-Angriffen stand und von anderen Adressen Gelder erhalten hatte. Die akkumulierten Gelder wurden dann an einen in einem Hochrisikoland ansässigen Kryptowertedienstleister überwiesen. Des Weiteren wurden die unabhängig von der Firma gekauften Gelder über mehrere Adressen weitergeleitet, wobei ein Großteil letztendlich über einen Mixer geschleust wurde. Ein entsprechender Analysebericht wurde zur weiteren Ermittlung an die zuständigen Strafverfolgungsbehörden weitergegeben.

Quelle: Israel

45. Im Gegensatz zu Kryptowertedienstleistern können Banken oder andere Finanz- und Zahlungsinstitute möglicherweise erkennen, wenn ein Angriffsopfer im Zusammenhang mit einer Lösegeldzahlung Fiatgeld an einen Kryptowertedienstleister oder einen in seinem Auftrag handelnden Dritten überweist, und eine entsprechende Verdachtsmeldung erstatten. Häufig haben sie jedoch keinen direkten Einblick in Lösegeldzahlungen oder die damit verbundene Geldwäsche, da die meisten Zahlungen in Kryptowährung und nicht mit Fiatgeld getätigt werden. Daher haben Finanz- und Zahlungsinstitute in der Regel nur sehr wenig Informationen zu Kryptoadressen oder zur Mittelherkunft, was den Einsatz von Blockchain-Analysetools erschwert. Angesichts dieser Hindernisse benötigen sie daher in vielen Fällen Proxy-Indikatoren, um potenzielle Ransomware-Zahlungen erkennen zu können. Ausgehend von Fallbeispielen gehören zu den üblichen Indikatoren ungewöhnliche Überweisungen an Kryptowertedienstleister (v. a. wenn das Unternehmen normalerweise nicht mit Kryptowerten handelt), der Kauf von Kryptowerten durch Cybersicherheits-, Versicherungs- und Vorfallmanagementfirmen, eigene Angaben des Kunden, dass die Banküberweisung zur Lösegeldzahlung verwendet wird, sowie öffentlich zugängliche Informationen zu Ransomware-Angriffen (Pressemitteilungen, Vorfallsberichte usw.). Eine ausführliche Liste einschlägiger Risikoindikatoren findet sich in der FATF-Publikation

„Bekämpfung der Finanzmittelbeschaffung durch Ransomware: mögliche Risikoindikatoren“.

Meldung von Vorfällen durch die Betroffenen

46. Aufgrund der geringen Anzahl von Meldungen zu Ransomware-Zahlungen in den meisten Ländern sind Verdachtsmeldungen weiterhin ein unzureichendes Instrument, um das volle Ausmaß von Ransomware-Angriffen und der damit verbundenen Geldwäsche aufzudecken und zu verstehen und als Hilfe bei Ermittlungen zu dienen. Daher sind auch die Meldungen der Angriffsopfer eine wichtige Informationsquelle für die Aufdeckung und Ermittlung von mit Ransomware verbundenen Geldflüssen. Eine zeitnahe Meldung durch die Betroffenen ist wichtig, damit die Strafverfolgungsbehörden schnell handeln und die Geldflüsse rückverfolgen können, und erhöht die Wahrscheinlichkeit einer erfolgreichen Strafverfolgung.

47. Die Vorfallmeldepflichten sind von Land zu Land unterschiedlich und hängen vom jeweiligen Rechtsrahmen ab. In den meisten Fällen ist die Meldung von Vorfällen freiwillig. Wenn Opfer einen Angriff melden, wenden sie sich in der Regel an die Polizei, Cybersicherheitsbehörden bzw. spezielle Meldestellen für Cyberangriffe oder an die örtlichen Computer Emergency Response Teams (CERT).

48. Jedoch ist auch hier das Meldeaufkommen gering, da nicht alle Angriffe von den Betroffenen gemeldet werden. Es gibt diverse Gründe, weshalb die Opfer aus Angst vor möglichen Konflikten mit ihren eigenen Geschäftsinteressen vor einer freiwilligen Meldung von Ransomware-Angriffen zurückschrecken. Dazu gehören die Sorge um Reputationsschäden, der Wunsch nach schneller Wiederherstellung des Normalbetriebs oder auch die Angst vor Vergeltungsmaßnahmen seitens der Cyber-Kriminellen. Bei Ransomware-Angriffen geht es von Natur aus um den unerlaubten Zugriff auf personenbezogene und sensible Kundendaten. Das Eingeständnis von Sicherheits- oder Datenlücken gegenüber den Strafverfolgungsbehörden oder der Öffentlichkeit wird als geschäftsschädigend empfunden und kann möglicherweise zu Zivilklagen führen. Außerdem können Kriminelle den Opfern auch mit der Veröffentlichung ihrer Daten drohen, wenn diese die Strafverfolgungsbehörden informieren.

49. Des Weiteren haben die Opfer nach erfolgter Lösegeldzahlung ggf. keinen Anreiz, den Vorfall freiwillig zu melden. Wenn die Opfer eine Cyberversicherung haben, sehen sie eventuell keinen finanziellen Grund, den Vorfall zu melden, da die Versicherung die Kosten der Lösegeldzahlung möglicherweise übernimmt. In einigen Ländern melden sich die Opfer nach einer Lösegeldzahlung auch nicht, weil sie befürchten, gegen nationale Vorschriften zu verstoßen (z. B. bei Zahlungen an sanktionierte Unternehmen) oder als Komplize einer kriminellen Vereinigung zu gelten.

50. Um Angriffsopfer zur Meldung zu ermutigen, wenden die Länder verschiedene Methoden an. So haben einige Länder Strategien entwickelt oder Maßnahmen wie z. B. öffentliche Aufklärungskampagnen umgesetzt, um das Bewusstsein für Ransomware-Angriffe zu schärfen und deren Meldung zu ermutigen. Diese Strategien und Maßnahmen beziehen in der Regel den Privatsektor mit ein und sollen zeigen, wie die Behörden dabei helfen können, den durch Ransomware-Angriffe verursachten Schaden zu reduzieren. Dazu gehören die Rückgabe der

Vermögenswerte an die Geschädigten sowie die Weitergabe von Entschlüsselungsschlüsseln zur Datenwiederherstellung, sofern vorhanden.

Kasten 12. „No more Ransom"-Website[1]

Die Website „No more Ransom" ist eine Initiative der National High Tech Crime Unit der niederländischen Polizei, des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität von Europol und zweier Privatunternehmen und soll Ransomware-Opfern dabei helfen, ihre verschlüsselten Daten ohne Lösegeldzahlung an die Kriminellen wiederzuerlangen. Die Website enthält ein Verzeichnis von Schlüsseln und Anwendungen, mit denen durch verschiedene Arten von Ransomware gesperrte Daten entschlüsselt werden können. So können Betroffene wieder auf ihre verschlüsselten Dateien oder gesperrten Systeme zugreifen, ohne Lösegeld zahlen zu müssen.

Die Initiative vereint diverse Partner aus dem öffentlichen und privaten Sektor verschiedener Länder, einschließlich Strafverfolgungsbehörden und IT-Sicherheitsfirmen. Sie soll Nutzer darüber aufklären, wie Ransomware funktioniert und welche Gegenmaßnahmen getroffen werden können, um eine Infektion wirksam zu verhindern. Außerdem ermutigt die Website die Opfer, kein Lösegeld zu zahlen, und enthält Links, über die Betroffene auf die Meldewebsite ihres jeweiligen Landes weitergeleitet werden, damit sie den Vorfall anzeigen können.

Quelle: No More Ransom

1. Näheres hierzu siehe: www.nomoreransom.org/en/index.html

51. Um der Sorge um das mit einer Meldung verbundene Reputationsrisiko zu begegnen, haben einige Länder versucht, für Unternehmen, die Opfer eines Ransomware-Angriffs wurden, ein sicheres Umfeld zu schaffen, damit sie sich ohne Angst vor Reputationsschäden melden können, z. B. über regelmäßige Austauschformate und Teilnahme an Unternehmenstagungen. Eine weitere bewährte Praxis ist die Einrichtung von „One-Stop"-Internetportalen, die den Opfern als zentrale Anlaufstelle für die Meldung von Vorfällen dienen und gleichzeitig fachkundige Beratung und Abhilfemaßnahmen anbieten. Wenngleich es hierbei in erster Linie um die Aufdeckung des Ransomware-Angriffs an sich geht, enthalten die Meldungen der Opfer auch Informationen, die für Finanzermittlungen – einschließlich Aufklärung der entsprechenden Geldflüsse und Geldwäsche – von entscheidender Bedeutung sind.

Kasten 13. Kanadisches Centre for Cyber Security

Das kanadische Centre for Cyber Security (Cyber Centre) wurde als zentrale Initiative im Rahmen der kanadischen nationalen Cybersicherheitsstrategie 2018 ins Leben gerufen. Das Cyber Centre dient als zentrale Anlaufstelle für fachkundige Beratung, Hilfe, Dienstleistungen und Unterstützung im Bereich der Cybersicherheit für Behörden, Eigentümer und Betreiber kritischer Infrastrukturen, den Privatsektor und die kanadische Öffentlichkeit. Sein Angebot richtet sich an Privatpersonen und Unternehmen und umfasst Handreichungen zur Prävention von und Wiederherstellung nach Ransomware-Angriffen

sowie Berichte zur Bedrohungslage. Das Cyber Centre sammelt Meldungen von Cyber-Vorfällen staatlicher und privater Akteure, sowohl auf nationaler als auch auf internationaler Ebene. Die Meldungen können online, per E-Mail oder telefonisch erstattet werden. Das Centre empfiehlt den Betroffenen auch, bei der Polizei Anzeige zu erstatten, wenn sie den Cyber-Vorfall als unmittelbare Gefahr für Leib und Leben oder als Straftat einschätzen.

Quelle: Kanada

52. Einige Länder haben für bestimmte Branchen oder Vorfälle eine Meldepflicht eingeführt. Das betrifft z. B. Angriffe auf kritische Infrastrukturen (wie Energie, Kommunikation, Gesundheit usw.) oder Daten-Leaks. In vielen Ländern gilt dies auch für Verpflichtete des Finanzsektors (z. B. Banken), die nach den einschlägigen Rechtsvorschriften signifikante Vorfälle an die zuständigen Behörden (z. B. Aufsichtsinstanzen) melden müssen. Auch Datenschutzvorschriften können eine Meldeempfehlung bzw. -pflicht für Datenschutzverletzungen im Zusammenhang mit personenbezogenen Daten enthalten, was zu einer zeitnahen Aufdeckung beitragen kann. Um die Aufdeckung illegaler Geldflüsse zu verbessern, hat es sich bewährt, bei diesen Meldungen relevante Finanzinformationen (z. B. Wallet-Adresse, Art der Kryptowährung) zu erfassen.

Sonstige Aufdeckungsquellen

53. Wie oben ausgeführt, können der Austausch und die Zusammenarbeit mit Akteuren außerhalb des Finanz-, Nichtfinanz- und Kryptowertesektors, insbesondere mit Internet-Providern und dem Cybersicherheitssektor, eine wertvolle Informationsquelle sein. Allerdings unterliegen diese Sektoren nicht unbedingt AML-/CFT-Anforderungen wie z. B. der Pflicht zur Verdachtsmeldung. In einigen Fällen kann auch ein Interessenkonflikt vorliegen (z. B. bei den für die Opfer tätigen Cybersicherheitsfirmen), der einem proaktiven Meldeverhalten entgegenstehen könnte. In diesen Fällen können die Informationen ggf. über informelle Mechanismen wie öffentlich-private Partnerschaften mit Beteiligung der entsprechenden Firmen oder einen direkten Austausch beschafft werden.

Kasten 14. Kooperation mit einer Cybersicherheitsfirma

Nach einem Angriff durch eine Ransomware-Bande beauftragte die betroffene Firma eine Cybersicherheitsfirma. Das Lösegeld sollte in Bitcoin oder Monero gezahlt werden. Die betroffene Firma zahlte das Lösegeld an die kriminelle Bande über die Cybersicherheitsfirma.

Diese informierte anschließend die Strafverfolgungsbehörde über den Vorgang, sodass die Behörden die illegalen Geldflüsse rückverfolgen konnten. Die Strafverfolgungsbehörde arbeitet regelmäßig mit Cybersicherheitsfirmen zusammen. Bei dieser Zusammenarbeit soll möglichst wenig in die Wiederherstellungsdienste der Firmen für ihre Kunden eingegriffen und gleichzeitig sichergestellt werden, dass zentrale Informationen wie IP- und Krypto-Adressen für strafrechtliche Ermittlungen bereitgestellt werden.

Im konkreten Fall stellte die Strafverfolgungsbehörde den Einsatz von Anonymisierungsmethoden wie die Zwischenschaltung von Mixern sowie die Verwendung diverser selbstverwalteter (unhosted) Wallet-Adressen fest. Zum Zeitpunkt der Ermittlungen wurde ein Großteil der Gelder in selbstverwalteten Wallets gehalten/verwahrt und konnte daher nicht weiter rückverfolgt werden. Ein Großteil der Gelder soll über zwei Kryptowertedienstleister im Ausland geschleust worden sein.

Quelle: Schweiz

54. Die zuständigen Behörden können Ransomware-Angriffe und -Zahlungen auch über eigenständige Finanzermittlungen aufdecken, indem sie bekanntermaßen mit Ransomware verbundene Wallets einer Blockchain-Analyse unterziehen. Dazu gehört auch die Überwachung gemeldeter Angriffe, Blogs und von Blockchain-Analysefirmen zur Verfügung gestellte Open-Source-Analysen sowie die proaktive Kontaktaufnahme mit potenziellen Opfern.

55. Diese Maßnahmen können zusätzliche Hinweise auf frühere Ransomware-Angriffe liefern. Außerdem können so Erkenntnisse über das Ausmaß einzelner Ransomware-Angriffe gewonnen werden, aber auch über Trends, Typologien und die von Kriminellen zum Waschen, Erhalten und Einsatz ihrer illegalen Gewinne verwendete Infrastruktur.

Kasten 15. Analyse öffentlich zugänglicher Quellen zur Identifizierung von RaaS-Kriminellen

Die türkische FIU erhielt von einem Kryptowertedienstleister eine Verdachtsmeldung zu einer Krypto-Wallet-Adresse, die mit einer von dem Kryptowertedienstleister als „Name 1“ bezeichneten Person verbunden war. Eine Internetrecherche des Namens förderte eine Website mit demselben Namen zutage. Weitere Ermittlungen ergaben, dass die Website mit dem Darknet verbundene Aktivitäten durchführte und als Zwischenhändler für den Verkauf von Ransomware und anderer Schadsoftware fungierte.

Bei der weiteren Recherche über öffentlich zugängliche Quellen wurde Folgendes festgestellt:

- Die an der Transaktion beteiligte und in der Verdachtsmeldung genannte Person verwendete einen anderen Namen („Name 2“). So konnte der wahre Name der Person („Person X“) identifiziert werden. Diese Person hatte bereits zuvor die Aufmerksamkeit des für Cyberkriminalität zuständigen Polizeidezernats auf sich gezogen.
- Die verdächtige Person X bot u. a. folgende Dienstleistungen und Produkte an: unbefugter Zugang, Zugang zu vertraulichen Informationen, gefälschte Identitätsdaten, Hacking von Social-Media-Konten, Verkauf von Hacklinks und Phishing-Seiten.
- Die Bezahlung für diese illegalen Produkte/Dienstleistungen erfolgte mit Bitcoin oder anderer virtueller Währung.

Die türkische FIU ersuchte den mit der in der Verdachtsmeldung genannten Person verbundenen Kryptowertedienstleister um weitere Informationen, insbesondere Krypto-Wallet-Adressen,

Finanztransaktionen (sowohl mit Kryptowährung als auch Fiatgeld) und sonstige personenbezogene Daten. Aufgrund des Verdachts, dass es sich bei der in der Verdachtsmeldung genannten Person um einen Zwischenhändler beim Verkauf von Ransomware und anderer Schadsoftware handelt, wurde ein Analysebericht erstellt und an die für Cyberkriminalität zuständigen Stellen der türkischen Polizei übermittelt. Die Ermittlungen laufen noch.

Quelle: Türkei

56. Länder können auch durch den Informationsaustausch mit anderen Ländern auf Ransomware-Angriffe und Lösegeldzahlungen aufmerksam gemacht werden. Durch internationale Zusammenarbeit, Rechtshilfe und informellen Informationsaustausch mit ausländischen Behörden können Informationen zu Geldflüssen mit Bezug zu ausländischen Angriffen/Opfern gewonnen werden, die über inländische Krypto-Börsen verschleiert wurden.

Vorgeschlagene Maßnahmen

- Die Länder sollten die Verpflichteten bei der Aufdeckung von Ransomware-Angriffen und der damit verbundenen Geldwäsche sowie der Meldung verdächtiger Transaktionen unterstützen, indem sie ihnen u. a. Informationen über neue Entwicklungen, Leitfäden zur Aufdeckung sowie Warnindikatoren (wie diejenigen aus der FATF-Publikation „Bekämpfung der Finanzmittelbeschaffung durch Ransomware: mögliche Risikoindikatoren“) zur Verfügung stellen.
- Die Länder sollten die Opfer ermutigen, Vorfälle freiwillig zu melden, indem sie z. B. auf bestehende Unterstützungsangebote hinweisen und sichere Meldekanäle schaffen.
- Die Länder sollten außerdem auch die Schaffung von Kommunikationsmöglichkeiten mit nicht traditionellen Akteuren, die keinen AML-/CFT-Pflichten unterliegen (z. B. Cyberversicherer oder Vorfallmanagementfirmen) in Betracht ziehen.

Finanzermittlungsstrategien

57. Nahezu alle Ransomware-Angriffe dienen der Gewinnerzielung. Den meisten Ländern ist bewusst, dass Ermittlungen im Zusammenhang mit Ransomware eine bedeutende finanzielle Komponente aufweisen. Fallbeispiele zeigen, dass die Rückverfolgung der eingesetzten Kryptowerte ein zentraler Bestandteil dieser Ermittlungen ist. Die Länder, die Ermittlungen zu Ransomware-Angriffen durchgeführt haben, berichten in der Regel auch von parallelen Finanzermittlungen zur Rückverfolgung der Lösegeldzahlungen.

58. Es fehlt weltweit an Erfahrungen mit Geldwäscheermittlungen im Zusammenhang mit Ransomware. Nur wenige Länder haben in Ransomware-Fällen bislang Anklage wegen Geldwäsche erhoben. Dies kann zum Teil auf die in Abschnitt 5 erörterten Schwierigkeiten bei der Aufdeckung und Meldung zurückzuführen sein.

59. Im folgenden Abschnitt werden die spezifischen Herausforderungen und bewährten Praktiken erfolgreicher Finanzermittlungen bei Ransomware-Vorfällen und damit verbundener Geldwäsche unter folgenden Aspekten erörtert: (i) Kooperation mit den Betroffenen zur Informationsbeschaffung, (ii) Ermittlungsmethoden und -mechanismen sowie (ii) Vermögensabschöpfung.

Schnelles Handeln und Kooperation mit den Betroffenen zur Informationsbeschaffung

60. Aufgrund der Beschaffenheit von Cyberstraftaten wie Ransomware-Angriffen hängt eine erfolgreiche Strafverfolgung von der Fähigkeit ab, schnell zu handeln und wichtige Informationen über den Angriff und die Zahlung zu beschaffen. Dazu gehören Kryptoadressen, Gesamtbetrag der Lösegeldzahlung und Art der dafür verwendeten Kryptowährung, jeweiliges Überweisungsdatum, Art der beteiligten Dienste, Identität des Opfers, Kommunikation zwischen dem Opfer und den Ransomware-Kriminellen sowie Informationen zu sämtlichen an der Lösegeldzahlung beteiligten Dritten.

61. In vielen Fällen setzt die Beschaffung dieser Informationen die Kooperation der Opfer oder der an dem Vorfallmanagement und/oder Lösegeldzahlungsprozess beteiligten Dritten voraus. Wie oben erörtert, halten sich die Opfer jedoch möglicherweise mit der Meldung von Vorfällen an die Strafverfolgungsbehörden zurück (siehe Abschnitt 5.3). Eventuell zögern die Opfer auch, mit den Strafverfolgungsbehörden zu kooperieren, weil sie einen Interessenskonflikt sehen; sie wollen oft so schnell wie möglich wieder ihren Geschäftsbetrieb aufnehmen und zahlen daher vielleicht lieber das Lösegeld. Möglicherweise haben sie auch Angst vor Vergeltungsmaßnahmen der Kriminellen, wenn sie die Strafverfolgungsbehörden einschalten. Die Strafverfolgungsbehörden wiederum benötigen möglicherweise Zeit, um forensische Beweise zu sichern, kontrollierte Operationen vorzubereiten und andere Ermittlungsschritte zu unternehmen, was die Wiederaufnahme des Geschäftsbetriebs verzögern kann.

62. Verspätete oder unvollständige Meldungen und mangelnde Kooperation seitens der Betroffenen können die Qualität der für erfolgreiche und weitere Ermittlungen erforderlichen Informationen beeinträchtigen. Wenn die Betroffenen keine klaren Vorgaben haben, wie sie nach einem Angriff und/oder einer Lösegeldzahlung verfahren sollen, können die vorhandenen Beweise mangels Datenspeicherung kompromittiert werden. Die in Abschnitt 5.3 dargestellten bewährten Praktiken wie z. B. Aufklärungskampagnen oder andere Bemühungen zur Kooperation mit den Betroffenen können zur Bewältigung dieser Herausforderungen beitragen.

63. Einige Länder haben auch die Notwendigkeit eines Informationsaustauschs zwischen den Ermittlern der Cyber-Vortat und den Geldwäscheermittlern hervorgehoben. Im Laufe der forensischen Beweiserhebung für die Vortatermittlungen bei Ransomware-Angriffen sammeln die Strafverfolgungsbehörden automatisch Informationen, die für die Geldwäscheermittlungen relevant sind. Mithilfe dieser Informationen können die Strafverfolgungsbehörden Verbindungen zwischen verschiedenen Gruppen und Affiliates von Ransomware-Angreifern herstellen; außerdem erhalten sie ggf. weiterführende Hinweise für umfassendere Finanzermittlungen. Wie die verschiedenen inländischen zuständigen Behörden wirksam zusammenarbeiten können, wird in Abschnitt 8.2 beschrieben.

Kasten 16. Beweiserhebung während Vortatermittlungen als wichtige Quelle für Finanzermittlungen

Forensische Beweise: Dazu gehören Angriffsvektoren (d. h. wie sich Kriminelle unerlaubten Zugang verschaffen), Informationen zum Ransomware-Stamm, IP-Adressen, verwendete Namen bzw. Decknamen und die Geräte der Angreifer. Diese Informationen können direkt von den Opfern, den Internet-Providern, Cybersicherheits- und Vorfallmanagementfirmen oder mittels IT-Forensik eingeholt werden.

Beweise direkt vom Privatsektor: Zu den relevanten Firmen gehören die Eigentümer der Technologie oder Infrastruktur, die bei einem Ransomware-Angriff kompromittiert wurde. Die Ermittler können Kundeninformationen von E-Mail- oder Social-Media-Unternehmen einholen, bei denen der Täter möglicherweise Konten für die Kommunikation mit dem Opfer unterhielt.

Öffentlich zugängliche Informationen: Eine Analyse öffentlich zugänglicher Informationen, einschließlich sozialer Medien, Online-Foren, Darknet-Plattformen sowie der Kommunikation von Ransomware-Kriminellen, kann zur Identifizierung potenzieller Täter beitragen.

Ermittlungsmethoden und -mechanismen

Relevanz herkömmlicher Ermittlungsmethoden

64. Die von Ransomware-Kriminellen zur Verschleierung ihrer Standorte, Identitäten und Geldflüsse verwendeten Technologien können die Ermittlungen behindern. Besondere Herausforderungen ergeben sich aus der Nutzung von VPNs, des „Onion Router“[35] oder von verschlüsselten E-Mails, die ein höheres Maß an Datenschutz und Sicherheit, aber auch anonyme Aktivitäten beim Datenverkehr im Netz ermöglichen. Die rasante Entwicklung dieser Technologien kann diese Problematik noch verschärfen.

65. In FATF-Empfehlung 31 sind die grundlegenden Befugnisse beschrieben, mit denen die Strafverfolgungsbehörden zur Durchführung wirksamer Finanzermittlungen ausgestattet sein müssen. Die herkömmlichen Ermittlungsmethoden sind mit Blick auf die aktuellen Herausforderungen weiterhin relevant, da sie die Beschaffung und Analyse wichtiger Informationen zu den mit Ransomware verbundenen Geldflüssen ermöglichen. Dazu gehören Überwachungsmaßnahmen, das Abfangen bzw. Abhören von Kommunikation sowie verdeckte Maßnahmen. Bei Finanzermittlungen im Zusammenhang mit Kryptowerten müssen diese herkömmlichen Methoden jedoch angepasst werden. So können z. B. folgende Maßnahmen ergriffen werden, um erfolgreiche Ermittlungsergebnisse zu erzielen:

- *Überwachung*: Ermittlung der von Tatverdächtigen genutzten elektronischen Gerätetypen, um eine etwaige Verwendung von Krypto-Wallets und ihre bevorzugten elektronischen Kommunikationsmittel festzustellen.

[35] Auch als TOR bekannt. Hierbei handelt es sich um eine Open-Source-Software, mit der Nutzer anonym im Internet surfen können.

- *Abfangen bzw. Abhören von Kommunikation und verdeckte Maßnahmen* Erkenntnisgewinnung über die Aktivitäten der Zielperson und die Arbeitsweise einer kriminellen Vereinigung, Ermittlung von mit der Zielperson in Verbindung stehenden Personen, relevanten Finanzdaten und Vermögenswerten sowie Infiltrierung krimineller Communities (z. B. Darknet-Foren), um die Anonymität der Täter und Begünstigten aufzuheben.

- *Herausgabeanordnungen:* Beschaffung von Informationen bei Kryptowertedienstleistern oder anderen an Lösegeldzahlungen beteiligten Finanzinstituten usw.

66. Beim Einsatz dieser Instrumente im Rahmen von Finanzermittlungen können auch über Verdachtsmeldungen bzw. Vorfallsmeldungen der Betroffenen gewonnene Informationen herangezogen werden (siehe Abschnitt 5). Die Strafverfolgungsbehörden können relevante Finanzinstitute und Kryptowertedienstleister ggf. über Verdachtsmeldungen und Blockchain-Analysen (siehe Abschnitt 6.2.2) identifizieren, um von ihnen mittels Herausgabeanordnung notwendige Beweise einzuholen. Kryptowertedienstleister können bei Finanzermittlungen im Zusammenhang mit Ransomware nützliche Informationen zur Identifizierung bereitstellen, sprich Basisdaten und Angaben zum wirtschaftlich Berechtigten sowie Transaktionsdaten (z. B. Nutzeridentität und damit verbundene Informationen, IP-Adressen, Kreditkarten oder Bankkonten usw.).

67. Wie in Abschnitt 3 erörtert, wurde bei einigen Ransomware-Netzwerken auch eine Verbindung zu Hochrisikoländern festgestellt, in denen Kryptowertedienstleister nur schwachen bzw. gar keinen AML-/CFT-Anforderungen unterliegen oder diese oftmals nicht erfüllen. Wenn Gelder über diese Kryptowertedienstleister fließen oder dort gehalten werden, kann dies die Ermittlungen erschweren. In diesen Fällen erheben die Kryptowertedienstleister möglicherweise nicht die einschlägigen Informationen oder reagieren nicht auf Anfragen der Strafverfolgungsbehörden.

68. Die Ermittler stehen vor ähnlichen Herausforderungen, wenn Kriminelle selbstverwaltete Wallets nutzen. Dabei erhalten die Nutzer die Kontrolle über Kryptowerte ohne Beteiligung eines Kryptowertedienstleisters, was die Verhinderung und Aufdeckung von Geldwäscheaktivitäten erschwert. Die fehlende Verbindung zu einem Drittunternehmen (das nach den FATF-Standards registriert/zugelassen sein sollte) macht es für die Behörden schwerer, den Inhaber einer Wallet zu identifizieren, da sie nicht bei Dritten Informationen einholen können.

69. Aufgrund der begrenzten Umsetzung der FATF Travel Rule durch Kryptowertedienstleister können Cyberkriminelle ebenfalls leichter unentdeckt bleiben und Ermittlungen behindert werden. Nach der Travel Rule müssen Kryptowertedienstleister und andere an der Übertragung von Kryptowerten beteiligte Finanzinstitute bei jeder Übertragung Informationen zum Sender (Auftraggeber) und Empfänger (Begünstigten) erheben und übermitteln. Dies erhöht die Transparenz der Transaktionen im Sinne der Missbrauchsverhinderung und ermöglicht den Strafverfolgungsbehörden den Zugriff auf Informationen zur Identifizierung der an einer bestimmten Transaktion beteiligten Parteien. In einem FATF-Bericht aus 2022 wurde allerdings festgestellt, dass nur ein Drittel der darin abgedeckten Länder Rechtsvorschriften zur Umsetzung der Travel Rule für Kryptowertedienstleister erlassen haben und sogar noch weniger die entsprechenden Anforderungen

tatsächlich durchsetzen. [36] Diese Regulierungslücke führt dazu, dass den Strafverfolgungsbehörden in Ländern ohne Travel Rule weniger Informationen der Kryptowertedienstleister zur Verfügung stehen. Dies bedeutet auch, dass Kryptowertedienstleister in Ländern mit Travel Rule, die Transaktionen mit Kryptowertedienstleistern aus Ländern ohne Travel Rule durchführen, vermutlich ebenfalls keine entsprechenden Informationen erhalten, sodass selbst in den Ländern, die die Travel Rule umsetzen, den Ermittlungsbehörden ebenfalls weniger Informationen zur Verfügung stehen.

Kasten 17. Herkömmliche Finanzermittlungsmethoden gegen eine Ransomware-Bande

Eine von einem Ransomware-Angriff betroffene italienische Firma erstattete Anzeige bei der Polizei, nachdem sie das Lösegeld mit Bitcoin gezahlt und ihre von dem Angriff infizierten Daten erfolgreich entsperrt hatte. Die Zahlung war über einen in der Lösegeldforderung genannten Kryptowertedienstleister getätigt worden.

Die polizeilichen Ermittlungen ergaben, dass die Website des Kryptowertedienstleisters offiziell in Italien registriert war. Anschließend wurde eine italienische Person identifiziert, die die Bitcoin-Geldflüsse im Zusammenhang mit der Lösegeldzahlung ermöglicht hatte. Daraufhin durchsuchte die Polizei die Wohnung dieser Person und beschlagnahmte dabei Zahlungskarten, Mobiltelefone sowie Hardware in Form von Festplatten, USB-Sticks und Tablets. Über eine Telefonüberwachung und Auswertung der ausgetauschten Handynachrichten konnte eine Gruppe weiterer italienischer Personen (die „Bande“) identifiziert werden, die ebenfalls an Bitcoin-Geldtransfers im Zusammenhang mit Ransomware beteiligt waren. Die Finanzermittlungen ergaben, dass die von den Ransomware-Opfern überwiesenen Fiatgelder von der Bande auf ausländische Bankkonten ausländischer Kryptowertedienstleister (auch in Hochrisikoländern) überwiesen wurden.

Infolge der Finanzermittlungen sowie der forensischen Auswertung der Mobiltelefone und Hardware stellten die Behörden fest, dass die Bande Ransomware verbreitete und bei jedem Angriff mehrere Hundert Euro Lösegeld forderte. Die Gruppe wurde wegen Erpressung in Verbindung mit Ransomware und anschließender Geldwäsche angeklagt, wobei die mittels verschiedener Opfern erzielten Gewinne auf insgesamt ca. 300.000 EUR geschätzt wurden. Die Ermittlungen laufen noch.

Quelle: Italien

Kryptospezifische Methoden

70. Zusätzlich zu den herkömmlichen Methoden sollten die Strafverfolgungsbehörden bei Finanzermittlungen im Zusammenhang mit Ransomware auch kryptospezifische Methoden anwenden. Die meisten Kryptowerte werden auf einer öffentlichen Blockchain laufen über eine

[36] FATF (Juni 2022) *Targeted Update on Implementation of the FATF Standards on Virtual Assets And Virtual Asset Service Providers.* Dieser Bericht deckt nur die Länder ab, deren Prüfungs-/Follow-up-Berichte zwischen Juni 2021 und Mai 2022 veröffentlicht wurden.

öffentliche Blockchain, die als einsehbare Datenbank fungiert, über die pseudonyme Daten zu Krypto-Transaktionen mithilfe frei verfügbarer oder kostenpflichtiger Blockchain-Analysetools (siehe Abschnitt 7) rückverfolgt werden können. In Kombination mit den herkömmlichen Ermittlungsmethoden ermöglicht es die Blockchain-Analyse Ermittlern, ggf. die zur Identifizierung der Ransomware-Kriminellen und ihrer Affiliates notwendigen Informationen zu beschaffen und die Bewegungen der inkriminierten Gelder rückzuverfolgen.

71. Zur Rückverfolgung dieser Gelder mithilfe einer Blockchain-Analyse muss in der Regel zunächst die erste Wallet-Adresse identifiziert werden, weshalb als erster wichtiger Schritt Informationen zur Lösegeldzahlung aufzudecken und zu erheben sind. Sobald die ursprüngliche Wallet-Adresse bekannt ist, können die Ermittler u. a. die dortigen Zahlungsein- und -ausgänge feststellen. Welche Informationen verfügbar sind, kann allerdings vom verwendeten Dienst abhängen. Wenngleich die öffentliche Blockchain nützliche Informationen für Finanzermittlungen enthält, finden einige Krypto-Transaktionen auch außerhalb der Blockchain statt. Bestimmte Blockchain-Analysetools stützen sich außerdem auf Clustering-Algorithmen und andere Techniken, um Wallet-Adressen oder Transaktionen, die mit kriminellen Handlungen wie Ransomware in Verbindung gebracht werden können, entsprechend zu gruppieren.

72. Des Weiteren können die über Blockchain-Analysen gewonnenen Informationen auch beim Einsatz herkömmlicher Ermittlungsmethoden zum Tragen kommen. So könnte die Blockchain-Analyse z. B. zur Identifizierung eines Kryptowertedienstleisters beitragen, der eine Wallet-Adresse hostet, die Zahlungsein- und -ausgänge von Ransomware-Kriminellen aufweist, was die Strafverfolgungsbehörden dazu veranlassen könnte, bei dem betreffenden Kryptowertedienstleister mittels Zwangsmaßnahmen Informationen über die Wallet-Adresse einzuholen.

Kasten 18. Aufdeckung bislang unbekannter Opfer infolge von Ermittlungen zu bekannten Ransomware-Wallets

Es wurde online eine Blockchain-Bedrohungsanalyse im Zusammenhang mit einer Bitcoin-Adresse durchgeführt, an die zwischen dem 12. Mai 2017 und dem 27. Mai 2021 etwa 20 Bitcoin gesendet worden waren. Es wurde festgestellt, dass die betreffende Bitcoin-Adresse unmittelbar mit Ransomware-Angriffen auf mehrere südafrikanischen Unternehmen und Behörden in Verbindung stand. Die Analyse ergab, dass im Februar 2018 0,06 Bitcoin von einer separaten lokalen Bitcoin-Adresse eines südafrikanischen Kryptowertedienstleisters an die o. g. Adresse transferiert wurden.

Nach Einholung von Teilnehmerdaten bei diesem Kryptowertedienstleister konnte ein weiteres Opfer identifiziert werden, das zugab, einen finanziellen Schaden erlitten zu haben. Die betroffene Person wollte den Vorfall aus Angst vor einer öffentlichen Blamage wegen mangelhafter Sicherung von Kundendaten nicht melden. Der Fall wurde von der südafrikanischen FIU an die örtlichen Ermittlungsbehörden abgegeben. Da das identifizierte Opfer keine

Strafanzeige erstatten wollte, wurde der Fall von den örtlichen Strafverfolgungsbehörden zurückgezogen und eingestellt.

Quelle: Südafrika

73. Die von Ransomware-Kriminellen verwendeten anonymitätsfördernden Geldwäschemethoden (siehe Abschnitt 3) stellen die Strafverfolgungsbehörden ebenfalls vor Herausforderungen bei der Rückverfolgung und Zuordnung von Transaktionen mittels Blockchain-Analyse, wenngleich einige Blockchain-Analyse-Firmen technische Möglichkeiten zur Überwindung dieser Schwierigkeiten entwickelt haben. Im Falle von Affiliate-Modellen oder RaaS-Anbietern sowie zwischengeschalteten Finanzagenten gestalten sich Finanzermittlungen im Zusammenhang mit Ransomware noch komplexer. Da die Zahlungen nicht immer zum Opfer zurückverfolgt werden können, ist es schwierig, die für die erste Krypto-Zahlung verwendete Adresse zu ermitteln, die in der Regel als Anhaltspunkt für die Blockchain-Analyse dient.

74. Neben der Blockchain-Analyse zur Rückverfolgung der Lösegeldzahlung und der anschließenden Geldwäsche sollten die Ermittler auch vorherige Transaktionen im Zusammenhang mit einer Ransomware-Bande nachverfolgen. Mit diesem zusätzlichen Schritt können die Strafverfolgungsbehörden ggf. potenzielle Trends und Typologien und/oder weitere Straftaten erkennen.

75. Als bewährte Praxis haben die Strafverfolgungsbehörden einiger Länder Datenbanken mit wichtigen Informationen zu an Ransomware-Fällen beteiligten Finanzagenten oder Wallet-Adressen eingerichtet. Diese Datenbanken enthalten in der Regel Informationen zu Vorfällen, zur Identität von Finanzagenten, zur Schadenshöhe und zu den Ransomware-Kriminellen (z. B. Kontonummern, Wallet-Adressen, Nutzernamen). Die Datenbanken helfen bei der Identifizierung und Rückverfolgung von Ransomware-Zahlungen und der damit verbundenen Geldwäsche, da über den Datenpool frühere Ermittlungshinweise (einschließlich Zahlungsdaten) mit aktuellen und künftigen Vorfällen abgeglichen werden können. Auf diese Weise können die Strafverfolgungsbehörden die gesamte Dimension eines Geldwäschenetzwerks erfassen, das sich oftmals über verschiedene Verpflichtete und Sektoren erstreckt.

Vermögensabschöpfung

76. Neben besseren Aufdeckungs- und Finanzermittlungskapazitäten benötigen die Strafverfolgungsbehörden auch die gesetzlichen Befugnisse und Kapazitäten, um Kryptowerte sicherstellen und einziehen zu können. Transaktionen mit Kryptowerten erfolgen nahezu in Echtzeit. Das bedeutet, dass die zuständigen Behörden, sobald sie von einem Ransomware-Angriff bzw. einer Lösegeldzahlung erfahren, in der Lage bzw. befugt sein müssen, die Zahlung schnell – d. h. idealerweise innerhalb weniger Stunden – rückzuverfolgen und zügig einzufrieren, um ein Verschwinden der Gelder zu vermeiden. Gemäß FATF-Empfehlung 4 sollten die entsprechenden Befugnisse bereits in vielen Ländern – in unterschiedlicher Form – vorhanden sein.

77. Mehrere Länder haben auch die Nützlichkeit alternativer Instrumente zur Sicherung von Straftaterträgen (z. B. Aufschubbefugnisse der FIU) hervorgehoben, die im Umgang mit in Verdachtsmeldungen identifizierten inkriminierten Geldern eingesetzt werden können. Um mit dem dynamischen Charakter von Kryptowerten Schritt zu halten, müssen ggf. auch die bestehenden

Gesetze, Vorschriften, Strategien und Maßnahmen zur Vermögensabschöpfung aktualisiert werden.

Kasten 19. Colonial Pipeline

Im Juni 2021 gab das US-Justizministerium die Beschlagnahme von 63,7 Bitcoin im Wert von ca. 2,3 Mio. USD bekannt. Bei diesen Geldern handelte es sich mutmaßlich um den Erlös aus einer Lösegeldzahlung vom 8. Mai 2021 an Mitglieder einer als DarkSide bekannten Bande, die das Pipelinesystem Colonial Pipeline angegriffen und damit kritische Infrastruktur außer Betrieb gesetzt hatte. Der Beschlagnahmebeschluss wurde von einem Richter in Kalifornien am selben Tag genehmigt.

Colonial Pipeline wurde am oder um den 7. Mai 2021 Opfer eines medial stark beachteten Ransomware-Angriffs, der dazu führte, dass das Unternehmen Teile seiner Infrastruktur außer Betrieb nehmen musste. Colonial Pipeline meldete dem FBI, dass es nach einem Angriff auf sein Computernetzwerk durch eine Organisation namens DarkSide eine Lösegeldforderung in Höhe von ca. 75 Bitcoin erhalten und bezahlt habe. Wie in der eidesstattlichen Erklärung vermutet, konnten die Strafverfolgungsbehörden durch Überprüfung des öffentlichen Bitcoin-Ledgers mehrere Bitcoin-Transfers zurückverfolgen und feststellen, dass etwa 63,7 Bitcoin, die aus der Lösegeldzahlung des Opfers stammten, an eine bestimmte Adresse überwiesen worden waren. Bei diesen Bitcoins handelt es sich um Erlöse aus einem Computereinbruch sowie um mit Geldwäsche verbundene Vermögenswerte, die nach den einschlägigen straf- und zivilrechtlichen Einziehungsvorschriften beschlagnahmt werden können.

Quelle: USA

Vorgeschlagene Maßnahmen

Die zuständigen Behörden sollten bei Geldwäscheermittlungen im Zusammenhang mit Ransomware-Angriffen sowohl herkömmliche Strafverfolgungsmethoden als auch auf Kryptowerte zugeschnittene Methoden anwenden und entsprechend anpassen.

Die Länder sollten sicherstellen, dass die Strafverfolgungsbehörden dauerhaft über die erforderlichen Fähigkeiten und Befugnisse verfügen, um Vermögenswerte, insbesondere Kryptowerte, zügig und wirksam sicherstellen und einziehen zu können.

Fähigkeiten und Fachkenntnisse

78. Wie in Abschnitt 6.2 erörtert, sind herkömmliche Strafverfolgungsmethoden für Geldwäscheermittlungen im Zusammenhang mit Ransomware zwar weiterhin unerlässlich, dennoch setzen erfolgreiche Geldwäscheermittlungen bis hin zur Anklage und Vermögensabschöpfung bei Kryptowerten auch spezifisches

technisches Fachwissen voraus. Dazu gehört auch technologisches und rechtliches Wissen über die Kryptolandschaft.

79. Darüber hinaus sollten Ermittlungsteams, die mit Geldwäschefällen oder der Vermögensabschöpfung im Zusammenhang mit Ransomware befasst sind, auch Mitarbeiter mit technischen Kenntnissen in den Bereichen Cybersicherheit, Computerforensik, Online-Intelligence und Open-Source-Plattformen umfassen. Dabei sollte der Schwerpunkt auf der Internetrecherche liegen, um öffentlich verfügbare Finanzinformationen zu Transaktionen mit Kryptowerten zu sammeln, einschließlich Informationen, die aus Blockchain-Analysen, der Durchsuchung von Websites, sozialen Medien, Online-Foren, Darknet und Darknet-Plattformen sowie aus Online-Missbrauchsmeldungen gewonnen werden können.

80. Insbesondere im Zusammenhang mit Kryptowerten brauchen die zuständigen Behörden ggf. neue Fähigkeiten und Fachkenntnisse, um Informationen auswerten und beschaffen zu können. Dabei müssen sie sich insbesondere mit den Möglichkeiten der Blockchain-Analyse/Überwachung vertraut machen, wie etwa der Anwendung von Blockchain-Analysetools, einschließlich kostenloser Software zur Ansicht der öffentlichen Blockchain, sowie mit Analysemethoden zur Rückverfolgung von Geldern. Verschiedene Tools bieten zudem unterschiedliche und sich ergänzende Möglichkeiten (Analyse verschiedener Arten von Kryptowerten, Analyse von Chain Hopping, Open-Source-Intelligence usw.).

81. Für die Entwicklung der verschiedenen Instrumente und ihren Einsatz bei Ermittlungen sind spezielle Schulungen und Fachkenntnisse erforderlich und einige Länder haben bereits Wege zur Einbindung von Spezialisten in entsprechende Ermittlungen gefunden (siehe Abschnitt 8.2). Die erforderlichen Ressourcen können durchaus kostspielig sein und einige Länder haben eventuell nicht die zur Entwicklung dieser Fähigkeiten benötigten Mittel, was die Behörden bei ihren Geldwäscheermittlungen im Zusammenhang mit Ransomware behindern kann.

82. Wenn internes Fachwissen nicht verfügbar oder unzureichend ist, können die Behörden ggf. auch von privaten Unternehmen entwickelte Tools einsetzen. Mithilfe der von Drittanbietern bereitgestellten Tools können die Behörden dann Krypto-Transaktionen auf allen großen und den meisten kleineren Krypto-Blockchains identifizieren, nachverfolgen und zuordnen. Derzeit unterstützen diese Tools Hunderte von Token und verwenden Methoden wie Clustering-Algorithmen, Web Scraping und die Überwachung von Betrugsdatenbanken, die es den Ermittlern ermöglichen, eine Vielzahl von Transaktionen mit realen Personen und Unternehmen zu verknüpfen und entsprechend zuzuordnen. Die Tools generieren Transaktionsdiagramme und ermöglichen eine Netzwerkanalyse, mit deren Hilfe die Behörden komplexe Zusammenhänge verstehen und dann im Rahmen der Strafverfolgung und Vermögensabschöpfung vor Gericht präsentieren können. Diese Tools können den Behörden auch dabei helfen, die Kryptowertedienstleister zu identifizieren, die zur Geldwäsche oder zum Umtausch inkriminierter Gelder in Fiatgeld genutzt wurden und über ermittlungsrelevante Informationen verfügen könnten.

83. Mit Blick auf die Vermögensabschöpfung setzt die Sicherstellung und Verwaltung von Kryptowerten zusätzliches technisches und rechtliches Wissen voraus. Die Behörden müssen hierfür geeignete Maßnahmen ergreifen und

Verfahren einführen, um eine ordnungsgemäße Sicherstellung und Verwahrung zu gewährleisten. Dabei hat sich bewährt, spezielle Mechanismen für die Sicherstellung, Einziehung und Verwertung von Kryptowerten einzurichten. Dazu gehören ordnungsgemäße Sicherstellungsverfahren, die Verwaltung von Seed-Phrases[37] und sog. Cold-Storage der sichergestellten Kryptowerte (d. h. ihre Speicherung offline in einer selbstverwalteten Wallet) sowie ein geeigneter Umgang mit Verwahrketten.

Vorgeschlagene Maßnahmen

- Die zuständigen Behörden sollten über die für erfolgreiche Finanzermittlungen im Zusammenhang mit Ransomware-Angriffen notwendigen speziellen Fähigkeiten und Fachkenntnisse verfügen. Dazu zählen die Entwicklung und der Zugriff auf Blockchain-Analyse- und Überwachungstools sowie entsprechende Schulungsmaßnahmen.
- Die Länder sollten spezielle Mechanismen zum ordnungsgemäßen Umgang mit sichergestellten Kryptowerten vorsehen.

Nationale Maßnahmen und Koordinierung

Nationale Risikoanalyse und Strategie

84. Nach FATF-Empfehlung 1 sollen die Länder ihre Geldwäscherisiken ermitteln und bewerten und zur Minderung dieser Risiken einen risikobasierten Ansatz verfolgen. Dieser Ansatz sollte auch als Grundlage für eine effiziente Ressourcenzuteilung innerhalb ihres AML-/CFT-Systems dienen.

85. Das Thema Ransomware wird oftmals aus der Perspektive der Cybersicherheit betrachtet. So haben einige Länder nationale Strategien zur Cybersicherheit oder -kriminalität verabschiedet, die die innerstaatliche Koordinierung fördern und ein politisches Bekenntnis zur aktiven Bekämpfung von Ransomware und den damit verbundenen illegalen Geldflüssen beinhalten. An diesen nationalen Strategien sind in der Regel verschiedene Behörden[38] beteiligt und teilweise auch die für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung zuständigen Ressorts wie Justiz, Finanzen und Inneres sowie der Privatsektor. Es gilt jedoch zu berücksichtigen, dass viele dieser Strategien nicht unbedingt auf die Risiken illegaler Geldflüsse ausgerichtet sind, die im Rahmen einer Risikobewertung eingehend analysiert werden sollten.

[37] Eine Reihe von Wörtern, die von einer Wallet-Anwendung nach dem Zufallsprinzip generiert und in einer bestimmten Reihenfolge aufgelistet werden und mit denen der Zugang zu einem oder mehreren privaten Schlüsseln (wieder) hergestellt werden kann, indem ein zusätzlicher Schutz (z. B. Passwort) umgangen wird.

[38] Dazu gehören die für Strafverfolgung, Verteidigung, Sicherheit und IT zuständigen Behörden, da Ransomware eine Bedrohung der nationalen Sicherheit darstellt.

Kasten 20. Spaniens nationale Cybersicherheitsstrategie

Mit seiner (zuletzt 2019 aktualisierten) nationalen Cybersicherheitsstrategie will Spanien seine Fähigkeiten zur Bekämpfung von Cyberbedrohungen stärken. In der Strategie werden Prioritäten, Ziele und geeignete Maßnahmen aufgestellt, mit denen ein hohes Sicherheitsniveau für Netzwerke und IT-Systeme erzielt und aufrechterhalten werden soll. Einige der wichtigsten Handlungsstränge der Strategie zielen darauf ab, die Fähigkeiten zur Bekämpfung von Cyberbedrohungen zu verbessern und die Kapazitäten zur Ermittlung und Verfolgung von Cyberkriminalität zu stärken.

Die Strategie sieht vor, die justizielle und polizeiliche Zusammenarbeit durch die Bereitstellung ausreichender Ressourcen für die zuständigen Behörden und spezielle Ausbildungsmaßnahmen zu stärken. In diesem Zusammenhang wurde auch ein institutioneller Rahmen für die Cybersicherheit geschaffen, zu dem der nationale Cybersicherheitsrat gehört. Dieser dem spanischen Premierminister unterstellte Rat soll die nationale Sicherheitspolitik im Bereich Cybersicherheit koordinieren sowie die Koordinierung und Zusammenarbeit zwischen den öffentlichen Stellen[1] und dem Privatsektor[2] fördern, was für einen multidisziplinären Ansatz wesentlich ist.

Quelle: Spanien

Fußnoten
1. Außen-, Justiz-, Verteidigungs-, Innen- und Finanzministerium, Präsidialamt, nationaler Geheimdienst, nationaler Sicherheitsstab und andere.
2. Zu den Experten des Privatsektors gehören Vertreter von Berufsverbänden, Unternehmen sowie der Wissenschaft.

86. Die Länder sollten die von Ransomware ausgehende Bedrohung auch im Rahmen ihrer nach FATF-Empfehlung 1 erstellten nationalen Risikoanalyse berücksichtigen. Diese Analyse bildet die Grundlage für die Entwicklung von Maßnahmen zur Risikominderung, zu denen auch die Umsetzung der in diesem Bericht enthaltenen Handlungsempfehlungen gehört. Wenn Länder die Geldwäscherisiken im Zusammenhang mit Ransomware verstehen, können sie ausgehend von einem risikobasierten Ansatz die erforderlichen Ressourcen zuteilen, u. a. für die Entwicklung technischer Fähigkeiten und Fachkenntnisse im Kryptobereich sowie die Beschaffung von Blockchain-Analysetools für die zuständigen AML-/CFT-Behörden.

87. Auch Länder, in denen Ransomware und die damit verbundene Geldwäsche derzeit keine signifikante inländische Bedrohung darstellen, sollten – insbesondere aufgrund der einzigartigen Beziehung zwischen Ransomware und Kryptowerten – die von Ransomware ausgehenden Risiken einer illegalen Finanzmittelbeschaffung berücksichtigen. Dabei sollten sie nicht nur die Gefahr von Ransomware-Angriffen auf inländische Opfer berücksichtigen, sondern auch die Möglichkeit, dass in ihrem Land Ransomware-Kriminelle ansässig sind oder Kryptowertedienstleister zum Waschen oder Auszahlen von Ransomware-Erlösen genutzt werden. So arbeiten etliche Kryptowertedienstleister mit einer über mehrere Länder verteilten Struktur, indem sie sich in einem Land registrieren, in einem anderen Land Mitarbeiter beschäftigen und die technische Infrastruktur oder private Schlüssel in verschiedenen Ländern hosten. Das bedeutet, dass die betroffenen Länder – insbesondere über Kryptowertedienstleister – dennoch illegalen Geldbewegungen im Zusammenhang mit Ransomware ausgesetzt sein können.

Kasten 21. Berücksichtigung von Ransomware in der nationalen Risikoanalyse

Die USA haben im März 2022 ihre dritte Nationale Geldwäsche-Risikoanalyse (NMLRA) veröffentlicht, in der die größten GW-/TF-Risiken beleuchtet wurden, wobei auch Cyberkriminalität und Anfälligkeiten im Zusammenhang mit Kryptowerten berücksichtigt wurden. Dabei wurde festgestellt, dass die Zahl der Cybervorfälle seit 2018 erheblich zugenommen hat und Ransomware eine besonders bedrohliche Form der illegalen Finanzmittelbeschaffung darstellt. Der NMLRA zufolge haben auch die Schwere und Raffinesse von Ransomware-Angriffen während der Coronapandemie zugenommen. Die NMLRA enthält wertvolle Informationen zu aktuellen Trends bei Ransomware-Angriffen, zu denen u. a. das RaaS-Modell und Double-Extortion-Methoden gehören. Außerdem zeigt die NMLRA zahlreiche Geldwäsche-Typologien auf, z. B. die Nutzung ausländischer Kryptowertedienstleister, die bei Lösegeld-Einzahlungen nach einem Ransomware-Angriff nur schwachen oder gar keinen AML-/CFT-Kontrollen für unterliegen. Die Feststellungen der NMLRA flossen in die Nationale Strategie zur Bekämpfung von Terrorismusfinanzierung und anderer illegaler Finanzmittelbeschaffung von 2022 ein, die Empfehlungen für den Umgang mit den Risiken illegaler Finanzmittelbeschaffung enthält, sowie in den Aktionsplan zur Bekämpfung der Risiken illegaler Finanzmittelbeschaffung im Zusammenhang mit Kryptowerten.

Quelle: USA

Nationale Zusammenarbeit und Koordinierung

88. Nach FATF-Empfehlung 2 sollten die Länder dafür sorgen, dass es zwischen den politischen Entscheidungsträgern, der FIU, den Strafverfolgungsbehörden und anderen zuständigen Behörden innerstaatliche Mechanismen zur Zusammenarbeit und Koordinierung sowie zum Informationsaustausch gibt. Ransomware betrifft ein breites Spektrum von Bereichen, weshalb neben den

klassischen AML-/CFT-Behörden auch andere Akteure wie z. B. Cybersicherheits- und Datenschutzbehörden in Ermittlungen eingebunden sein können. Effektive innerstaatliche Koordinierungsmechanismen sind von entscheidender Bedeutung, um relevante Informationen und verschiedene Experten, auch aus dem Privatsektor, zusammenzubringen und so einen ganzheitlichen Ansatz zur Eindämmung der von Ransomware und der damit verbundenen Geldwäsche ausgehenden Risiken zu gewährleisten. Dadurch wird auch ein Informationsaustausch zwischen den die Vortatermittlungen durchführenden Strafverfolgungsbehörden und den parallel laufenden Finanzermittlungen ermöglicht, der von entscheidender Bedeutung ist.

89. Eine bewährte Praxis ist die Einrichtung von Strafverfolgungsteams oder multidisziplinären Stellen, die sich speziell mit Cyberkriminalität (oder sogar konkret mit Ransomware) befassen. Diese Stellen können die Ermittlungen zu Ransomware und der damit verbundenen Geldwäsche koordinieren, die ein breites Spektrum an Fachwissen voraussetzen (z. B. seitens Experten der FIU oder Strafverfolgungsbehörden, Staatsanwaltschaften, IT-Ingenieuren, Verhandlungsführern usw.). Dieser Ansatz schließt in der Regel Strafverfolgungsbeamte mit Fachkenntnissen im Bereich der Rückverfolgung virtueller Vermögenswerte ein und kann – insbesondere bei begrenzten Ressourcen oder Kapazitäten – eine nützliche Methode sein, um technisches Fachwissen zentral zu bündeln.

Kasten 22. Koordinierungsmechanismen zur Bündelung nachrichtendienstlicher und ermittlungstechnischer Expertise

Zur Bewältigung der zunehmenden Herausforderungen der Cyberkriminalität hat die US-Regierung 2008 die National Cyber Investigative Joint Task Force (NCIJTF) gegründet. Sie besteht aus über 30 Partnerbehörden aus den Bereichen Strafverfolgung und Nachrichtendienste sowie dem Verteidigungsministerium, deren Vertreter gemeinsam an einem Standort arbeiten, um den Auftrag der Taskforce aus gesamtstaatlicher Perspektive zu erfüllen.

Als behördenübergreifendes Cyber-Zentrum ist die NCIJTF einzigartig und in erster Linie für Koordinierung, Integration und Informationsaustausch zuständig, um Ermittlungen zu Cyber-Bedrohungen zu unterstützen, nachrichtendienstliche Analysen für die Entscheidungsträger bereitzustellen bzw. zu unterstützen und sonstige laufende Bemühungen im Kampf gegen die landesweite Cyber-Bedrohung zu verstärken.

Ende 2014 richtete die NCIJTF das Virtual Currency Team (VCT) ein, das sich auf die Rückverfolgung von Kryptowährungstransaktionen im Zusammenhang mit Cyberkriminalität konzentriert. Dieses Team übernimmt für alle NCIJTF-Mitglieder die Rückverfolgung von Kryptowerten. Im Rahmen ihrer eigenen Ermittlungsbemühungen haben NCIJTF-Mitglieder wie das FBI und der U.S. Secret Service (USSS) eigene Teams zur Nachverfolgung von Kryptowerten eingerichtet, da deren Einsatz bei verschiedenen Arten von Verbrechen zunimmt.

Anfang 2022 richtete das FBI die Virtual Assets Unit (VAU) als Schaltzentrale für die Krypto-Programme des FBI ein, von der Erkenntnisse, Technologien und operative Unterstützung in andere Abteilungen einfließen sollen. In der VAU sind Krypto-Experten und abteilungsübergreifende Ressourcen in einer Taskforce gebündelt, um Erkenntnisse und Operationen innerhalb des FBI nahtlos zusammenzuführen.

Quelle: USA

Zusammenarbeit mit und Handreichungen für den Privatsektor

90. Wie in Abschnitt 5.2 erörtert, kann der Dialog mit dem Privatsektor dazu beitragen, einige der in diesem Bericht aufgezeigten Herausforderungen zu bewältigen. So haben die Verpflichteten möglicherweise Schwierigkeiten, verdächtige Transaktionen im Zusammenhang mit Ransomware zu erkennen und zu identifizieren. Einige Länder konnten die Häufigkeit und Qualität von Verdachtsmeldungen im Zusammenhang mit Ransomware erfolgreich steigern, indem sie die Verpflichteten einbezogen und ihnen Handreichungen (einschließlich Warnindikatoren, siehe FATF-Publikation „Bekämpfung der Finanzmittelbeschaffung durch Ransomware: mögliche Risikoindikatoren“ (2023)) und Leitfäden zur Aufdeckung verdächtiger Transaktionen zur Verfügung gestellt haben.

Kasten 23. Australiens Leitfäden zur Finanzkriminalität

Die australische Fintel Alliance[1] veröffentlicht eine Reihe von Handreichungen, u. a. Leitfäden zur Finanzkriminalität, die Unternehmen dabei helfen sollen, verdächtige Finanztransaktionen zu verstehen, zu erkennen und zu melden, damit kriminelle Aktivitäten aufgedeckt und verhindert werden können.

Die Leitfäden zur Finanzkriminalität enthalten ausführliche Informationen zu den finanziellen Aspekten verschiedener Kriminalitätsformen. Dazu gehören Fallbeispiele und Indikatoren, die dem Finanzsektor bei der Identifizierung und Aufdeckung verdächtiger Transaktionen helfen sollen.

Um den Kampf gegen Ransomware zu unterstützen, veröffentlichte die australische FIU (AUSTRAC) im April 2022 Leitfäden zur Finanzkriminalität, die sich schwerpunktmäßig mit dem kriminellen Missbrauch digitaler Währungen und der Aufdeckung und Unterbindung von Ransomware-Aktivitäten befassen. Diese beiden Leitfäden enthalten praktische Informationen und wichtige Risikoindikatoren, um leichter zu erkennen, ob jemand möglicherweise Opfer bzw. Begünstigter einer Ransomware-Zahlung ist, und dann entsprechend reagieren zu können. Beide Leitfäden sind auf der AUSTRAC-Website verfügbar, siehe

- Detecting and stopping ransomware payments | AUSTRAC
- Preventing the criminal abuse of digital currencies | AUSTRAC

Quelle: Australien

1. Die Fintel Alliance ist eine australische öffentlich-private Partnerschaft, in der Experten verschiedener Unternehmen und Behörden zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und anderen schweren Verbrechen zusammenarbeiten. Zur Fintel Alliance gehören große Banken, Finanztransferdienstleister und Glücksspielanbieter sowie australische und ausländische Strafverfolgungs- und Sicherheitsbehörden.

91. Form und Umfang der Zusammenarbeit mit dem Privatsektor bei der Bekämpfung von Ransomware unterscheiden sich von Land zu Land. Öffentlich-private Partnerschaften (ÖPP) sind ein nützliches und allgemein anerkanntes Modell, wobei sie sich in vielen Ländern nach wie vor auf die klassischen Akteure konzentrieren (insbesondere Banken und andere Finanzinstitute), auch wenn zunehmend Vertreter des Nichtfinanzsektors beteiligt sind. Die konkrete Zusammensetzung hängt von den jeweiligen Zielen der ÖPP ab, kann aber auch nicht herkömmliche Akteure umfassen. Mit Blick auf die wirksame Verhinderung und Aufdeckung von Ransomware sollten ÖPPs genutzt werden, um Strafverfolgungsbehörden, das lokale CERT, die FIU und Kryptowertedienstleister sowie Cybersicherheitsfirmen, Telekommunikationsanbieter und Blockchain-Analyse-Firmen (z. B. als Untergruppe oder operativer Arm einer bestehenden ÖPP) zusammenzubringen.

92. Zu den gemeinsamen Zielen solcher ÖPPs gehören die Sensibilisierung für Ransomware und damit verbundene Geldwäscheaktivitäten, der Informationsaustausch über aktuelle Trends sowie die Analyse neuer und bestehender Bedrohungen. Diese Mechanismen können auch engere Beziehungen zum Privatsektor sowie die Abgabe von Verdachtsmeldungen fördern.

93. Einige Länder nutzen ÖPPs auch, um diverse Strafverfolgungsziele zu erreichen. ÖPPs bieten eine nützliche Plattform für den Austausch taktischer Hinweise zur Erkenntnisgewinnung, ermöglichen einen sektorübergreifenden Informationsaustausch zur besseren Aufdeckung von Finanzagenten- und Geldwäschenetzwerken und können Ermittlungen voranbringen.

94. Da Kryptowertedienstleister über für eine erfolgreiche Strafverfolgung äußerst wichtige Informationen verfügen (z. B. zu Wallet-Eigentümern und Auszahlungen in Fiatgeld), kann der Aufbau kooperativer Beziehungen zu diesem Sektor den Behörden auch einen schnellen Zugriff auf Informationen für die Rückverfolgung von Kryptowerten und deren wirksame Sicherstellung und Einziehung ermöglichen.

Kasten 24. Projekt GATEWAY und Operation Cyclone von Interpol

Das 2016 ins Leben gerufene **Projekt GATEWAY** bietet einen Rahmen für den Datenaustausch mit privaten Unternehmen im Zusammenhang mit Cyberkriminalität. Das Projekt fördert Partnerschaften zwischen Strafverfolgungsbehörden und der Privatwirtschaft, um Bedrohungsdaten aus verschiedenen Quellen zu generieren und den Polizeibehörden die Verhinderung von Angriffen zu ermöglichen. Die an dem Projekt beteiligten Unternehmen sind wichtige Akteure im Kampf gegen Cyberkriminalität und umfassen Cybersicherheitsfirmen, Bedrohungsanalysefirmen, Kryptowertedienstleister sowie Banken.

Dieser Rahmen ermöglicht den wechselseitigen Austausch von Informationen zu Cyberkriminalität zwischen Interpol und dem Privatsektor sowie eine privatwirtschaftliche Unterstützung von Interpol bei der Analyse von Cyberstraftaten. Die privatwirtschaftlichen Partner werden aufgrund ihres technischen Fachwissens herangezogen, um – falls nicht bekannt – die Art des Ransomware-Befalls festzustellen und bei der Analyse von Hinweisen auf mögliche Täter zu helfen.

Die **Operation Cyclone**[1] folgte auf weltweite Polizeiermittlungen zu Angriffen einer Ransomware-Bande namens C10p auf koreanische Unternehmen und US-Bildungseinrichtungen. Die im Juni 2021 durchgeführte globale Operation führte zur Festnahme von sechs Mitgliedern der berühmt-berüchtigten Ransomware-Bande und wurde von Interpol mit koreanischen, ukrainischen und US-amerikanischen Strafverfolgungsbehörden koordiniert. Die Verdächtigen sollen für die Ransomware-Bande die Überweisung und Auszahlung von über 500 Mio. USD veranlasst haben. Interpol führte diese Operation mithilfe von Informationen durch, die von seinen privaten Partnern im Rahmen des Interpol-Projekts Gateway bereitgestellt wurden.

Quelle: Interpol

1. Weitere Informationen hierzu siehe: www.interpol.int/en/News-and-Events/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrime-ring

Vorgeschlagene Maßnahmen

- Die Länder sollten sicherstellen, dass die von Ransomware-Angriffen ausgehenden Geldwäscherisiken in ihren nationalen Risikoanalysen ermittelt und analysiert werden. Aufgrund der dezentralen Struktur von Kryptowerten und Ransomware-Banden gilt dies auch für Länder mit Kryptowertesektoren, für die Ransomware-Angriffe derzeit keine nationale Bedrohung darstellen. Die im Rahmen der Risikoanalyse gewonnenen Erkenntnisse können wiederum in nationale Cyberstrategien einfließen, da sie einen ganzheitlichen, nationalen Überblick über die Ransomware-Risiken ermöglichen.
- Die Länder sollten zwischen den zuständigen Behörden Koordinierungsmechanismen entwickeln, und zwar von den Strafverfolgungs-, AML-/CFT- und Cyberkriminalitätsbehörden bis hin zu nicht traditionellen Partnern wie Cybersicherheits- oder Datenschutzbehörden. Dies fördert den Austausch von Informationen und Erkenntnissen und schafft eine nützliche Plattform für den wechselseitigen Austausch von Fachwissen.
- Die Länder sollten Mechanismen zur Förderung der öffentlich-privaten Zusammenarbeit einrichten. In diese Kooperationsmechanismen sollten ggf. auch Kryptowertedienstleister und andere nicht traditionelle Partner eingebunden werden.

Internationale Zusammenarbeit

95. Ransomware-Angriffe und die damit verbundenen Geldflüsse sind oftmals grenzüberschreitend und multinational. In der Regel sind Ransomware-Kriminelle in einem anderen Land ansässig als die zahlreichen Länder, in denen die Gelder (insbesondere Kryptowerte) gewaschen und schließlich „ausgezahlt" werden. Angesichts der Komplexität und Herausforderungen von Geldwäschemodellen im Zusammenhang mit Ransomware bedarf es einer kontinuierlichen grenzüberschreitenden Zusammenarbeit zwischen den Strafverfolgungsbehörden, die über die entsprechenden Informationen, Instrumente und Fachkenntnisse verfügen. Der Ausbau und die Nutzung bestehender Mechanismen der internationalen Zusammenarbeit sind für erfolgreiche Finanzermittlungen und die Abschöpfung von Vermögenswerten, insbesondere im Zusammenhang mit Ransomware, unerlässlich.

Kasten 25. Gemeinsame internationale Ermittlungen bei Angriff mit Lockergoga

Im Januar 2019 wurde ein großes französisches Unternehmen Opfer eines Ransomware-Angriffs. Die Schadsoftware Lockergoga wurde als der Ransomware-Stamm identifiziert, der zur Verschlüsselung mehrerer Dateien und interner Server des Unternehmens verwendet wurde. Wenngleich nach Verhandlungen ein Lösegeld von 410 Bitcoin gefordert wurde, zahlte das Unternehmen das Lösegeld nicht. Es wurde

jedoch festgestellt, dass der Lockergoga-Stamm auch bei zahlreichen anderen Angriffen eingesetzt wurde.

Im Rahmen von Eurojust/Europol wurde mit mehreren europäischen Ländern eine gemeinsame Ermittlungsgruppe eingerichtet. Dies führte zu einem effizienten Informationsaustausch, einschließlich justizieller Zusammenarbeit über Europäische Ermittlungsanordnungen (EEA) und Rechtshilfeabkommen, wodurch die Ermittlungen beschleunigt werden konnten. Darüber hinaus leisteten Europol/Eurojust sowohl technische Unterstützung mittels umfangreicher Hardwarekapazitäten als auch finanzielle Unterstützung. In der Folge wurden eine kriminelle Befehls- und Kontrollinfrastruktur identifiziert, der Nachrichtenstrom der Hacker entschlüsselt und die Bande schließlich in einem östlichen Land ausfindig gemacht. So konnten in dem betreffenden Land mehrere Festnahmen erfolgen.

Die Ermittlungen laufen noch. Mithilfe der Blockchain-Analyse konnten die Ermittler die verschiedenen verwendeten Peel-Chain-Methoden aufdecken. Dies führte zur Festnahme eines der größten Geldwäscher in der Schweiz. Außerdem wurden in verschiedenen Ländern mehrere weitere Finanzagenten festgenommen. Die Ermittlungen ergaben ferner, dass die gezahlten Lösegelder nicht allein dem Hacker zugutekamen. So mussten beispielsweise illegale Zahlungen an verschiedene kriminelle Partner geleistet und für die Infrastruktur (Software-Ingenieure und -Entwickler, schusssichere Hosts für sichere Server, schusssichere VPN-Dienste zur Verschleierung der Kommunikation oder Verbindung zu den Befehls- und Kontrollservern, Geldwäschedienste zur Organisation von Peel-Chain-Bewegungen usw.) sowie für die Suche nach Finanzagenten und Auszahlungsmöglichkeiten verwendet werden.

Quelle: Frankreich

96. Die in internationalen Ersuchen angeforderten Informationen beziehen sich in der Regel sowohl auf forensische Beweise, die für Vortatermittlungen benötigt werden, als auch auf für Geldwäscheermittlungen erforderliche Finanzdaten. Dazu gehören ausländische IP-Adressen, verwendete Namen bzw. Decknamen, Teilnehmerinformationen sowie Angaben zum wirtschaftlich Berechtigten, Transaktionsdaten und Informationen zur Gegenpartei bei von ausländischen Kryptowertedienstleistern gehosteten Wallets.

Besondere Herausforderungen bei der Nutzung von Kryptowerten

97. Die Nutzung von Kryptowerten bei Geldwäsche im Zusammenhang mit Ransomware kann neue Schwierigkeiten für die grenzüberschreitende Zusammenarbeit mit sich bringen. Unterschiede bei der materiellrechtlichen Behandlung oder Regulierung von Kryptowerten in den verschiedenen Rechtssystemen – sowie begrenzte oder fehlende staatliche Eingriffe in oder Aufsicht über den Sektor in einigen Ländern – können die Fähigkeit oder Bereitschaft der Behörden zur internationalen Zusammenarbeit erschweren.

98. So kann es für Länder, in denen Kryptowertedienstleister nicht registriert oder beaufsichtigt werden, schwierig sein, Unternehmen zu ermitteln, von denen sie Informationen anfordern können. Selbst wenn ein entsprechendes

Unternehmen ausfindig gemacht wird, müssen die Behörden dann möglicherweise Zwangsmaßnahmen ergreifen, um ein internationales Amtshilfeersuchen erfüllen zu können. Dies kann die über informelle Kooperationswege einholbaren Informationen einschränken.

99. Diese Problematik wird noch dadurch verschärft, dass viele Länder, in denen die Ransomware-Kriminellen und ihre Finanzagenten sitzen bzw. die zum Waschen und Auszahlen ihrer illegalen Gewinne genutzten Kryptowertedienstleister ansässig oder tätig sind, diese Aktivitäten tolerieren und ausländische Rechtshilfeersuchen möglicherweise gar nicht beantworten. Zudem fehlen Kryptowertedienstleistern aus Ländern ohne AML-/CFT-Pflichten möglicherweise einfach die entsprechenden Aufzeichnungen, die sie den Strafverfolgungsbehörden vorlegen könnten. Dadurch werden laufende Finanzermittlungen und Anstrengungen zur Vermögensabschöpfung letztendlich behindert. Diese Probleme unterstreichen erneut, wie wichtig es ist, die weltweite Umsetzung der FATF-Empfehlung 15 (einschließlich Travel-Rule) zu beschleunigen.

Kasten 26. Ermittlungshindernisse aufgrund nicht kooperativer ausländischer Kryptowertedienstleister

Firma X war Opfer eines Ransomware-Angriffs, bei dem es sich vermutlich um den Caley-Stamm handelte. Nach Verhandlungen zahlte das Opfer 0,25 Bitcoin an den Ransomware-Kriminellen und erhielt per E-Mail den Entschlüsselungsschlüssel, um wieder den Normalbetrieb aufnehmen zu können.

Die Behörden erfuhren von dem Vorfall erst später durch eine Anzeige, die das Opfer mehrere Tage nach Zahlung des Lösegelds bei der Polizei erstattet hatte, sodass die Spur der Zahlung bereits kalt war. Anhand einer Blockchain-Analyse konnte die Lösegeldzahlung zu einem ausländischen Kryptowertedienstleister rückverfolgt und die Überweisung von 0,0081 Bitcoin an die von dem ausländischen Kryptowertedienstleister verwaltete Wallet festgestellt werden, der auch auf mehrere Informationsersuchen nicht reagierte. Erschwert wurden die Ermittlungen noch durch die Tatsache, dass zur Verschleierung der Transaktionen ein Mixer zwischengeschaltet worden war. Aufgrund dieser Umstände konnte der Täter nicht ermittelt werden und keine Vermögensabschöpfung oder Festnahme erfolgen.

Quelle: Singapur

100. Auch die weit verstreuten Strukturen einiger Kryptowertedienstleister (mit Aktivitäten in zahlreichen Ländern)kann für die Strafverfolgungsbehörden ein erhebliches Ermittlungshindernis darstellen, da dadurch die Identifizierung des richtigen Unternehmens bzw. Landes, welches um Informationen ersucht werden kann, erschwert wird. Ein Land nannte z. B. Schwierigkeiten bei der Identifizierung des richtigen Landes für ein Informationsersuchen anhand einer IBAN, die vermutlich zu einem Bankkonto gehört, das von einem Kryptowertedienstleister bei einem ausländischen Finanzinstitut verwaltet wird. Ein anderes Land stellte fest, dass einige Kryptowertedienstleister keine physische Präsenz zu haben scheinen, was die Identifizierung eines für die Zusammenarbeit geeigneten Landes ebenfalls erschweren kann.

Die Notwendigkeit schneller Zusammenarbeit

101. Da Ransomware-Kriminelle über die ganze Welt verstreut sein und Kryptowerte nahezu in Echtzeit überwiesen werden können, müssen die Strafverfolgungsbehörden schnell handeln, um die grenzüberschreitende Verschiebung von mit Ransomware verbundenen Gewinnen zu verfolgen und zu verhindern. Dazu bedarf es in der Regel förmlicher Mechanismen der internationalen Zusammenarbeit (wie der Rechtshilfe), um im Rahmen eines Strafverfahrens Beweise zu erheben und Sicherstellungen vorzunehmen. Diese förmlichen Kooperationsmechanismen tragen jedoch nicht unbedingt zu schnellem Handeln bei und können daher die Ermittlungen erheblich verlangsamen, verzögern oder gar verhindern. Diese Schwierigkeiten werden durch die Komplexität von Ermittlungen bei Ransomware aufgrund der Vielzahl der beteiligten Länder und Unternehmen noch verschärft, da hier die internationale Zusammenarbeit noch mehr Zeit und Ressourcen in Anspruch nimmt als bei anderen kriminellen Aktivitäten.

102. Um diese Schwierigkeiten zu überwinden, können informelle Kooperationskanäle nützlich sein und zu einer zügigeren Bearbeitung von Rechtshilfeersuchen beitragen. Mit Blick auf eine schnellere Zusammenarbeit wiesen einige Länder auf die Bedeutung bestehender Kontakte und etablierter informeller Kanäle für den Kontakt und Austausch mit ausländischen Partnern hin. Diese fördern einen zügigen und somit für ein Strafverfahren nützlichen Informationsaustausch, während gleichzeitig die zum Schutz der Informationen erforderlichen Verfahren eingehalten werden. Zwischen den FIUs ist solch ein informeller Informationsaustausch über das Egmont Secure Web möglich, während die Polizeibehörden über Interpols I-24/7 sowie andere informelle Netzwerke wie das Camden Asset Recovery Inter-Agency Network (CARIN) und die regionalen Asset Recovery Inter-Agency Networks (ARINs) zusammenarbeiten können. Die Behörden sollten für die vorhandenen internationalen und regionalen Kooperationskanäle entsprechende Verfahren und Kontaktstellen vorsehen, um eine schnelle Rückverfolgung und effektive Abschöpfung der Gelder zu unterstützen.

103. In einigen Ländern hat sich auch die Zusammenarbeit über etablierte bilaterale Kontakte bewährt. Der Einsatz spezieller Verbindungsbeamter für Cyberkriminalität, die ins Ausland entsandt werden, kann den Austausch von Informationen und Erkenntnissen zwischen dem Gast- und Heimatland des Verbindungsbeamten erheblich erleichtern und es den Behörden ermöglichen, bei Ermittlungen im Zusammenhang mit Ransomware Beweise aus dem Ausland zu beschaffen bzw. bereitzustellen. Zur Förderung der bilateralen Zusammenarbeit sollten die Behörden die entsprechende Verfahren und Kontaktstellen nach Möglichkeit bekannt geben, um insbesondere zu einer schnellen Rückverfolgung und Vermögensabschöpfung beizutragen.

Kasten 27. Projekt CODA

Ein kanadischer Cyber-Krimineller, der mit Ransomware-Kampagnen und Cyberangriffen auf Behörden und medizinische Einrichtungen in Alaska in Verbindung stand, wurde im November 2021 verhaftet und wegen mehrerer Straftaten im Zusammenhang mit Cyberkriminalität angeklagt. Bevor das FBI seine internationalen Partner kontaktierte,

führte es Ermittlungen zu verschiedenen damit verbundenen Cyberangriffen durch. Nachdem die Person identifiziert und lokalisiert worden war, setzte sich das FBI mit seinem bilateralen Kontakt bei der Ontario Provincial Police (OPP) in Verbindung.

In beiden Ländern wurden zeitgleich Ermittlungen eingeleitet, wobei die OPP und das FBI von dem kanadischen nationalen Cybercrime Coordination Centre (NC3), Europol und den niederländischen Strafverfolgungsbehörden Unterstützung erhielten. Das NC3 stellte im Rahmen der internationalen Ermittlungen über einen Zeitraum von 23 Monaten operative Unterstützung, Daten- und Verhaltensanalysen, nachrichtendienstliche Kurz- und Lageberichte sowie Rückverfolgungs- und Auswertungsdienste für die Kryptotransaktionen bereit. Dank dieser Bemühungen konnte die Identität der gesuchten Person bestätigt und diese anschließend verhaftet werden. Der Einsatz modernster technischer Analysemethoden und spezieller Tools wie die Rückverfolgung von Kryptowerten ist bei dieser Art von Ermittlungen im Bereich der Cyberkriminalität entscheidend.

Quelle: Kanada und USA

Die Bedeutung multilateraler Koordinierung

104. Fallbeispiele für erfolgreiche Strafverfolgungsmaßnahmen beinhalten in der Regel das Zusammenspiel der zuständigen Behörden aus mehreren Ländern. Dies spiegelt die internationale und dezentrale Dimension von Ransomware-Angriffen und der damit verbundenen Geldwäsche wider. Eine zentrale Voraussetzung für den Erfolg ist die internationale Zusammenarbeit aller betroffenen Länder, damit Cyberkartelle und ihre Affiliates gleichzeitig aufgespürt und zerschlagen werden können. Dadurch wird auch das Risiko minimiert, dass diese kriminellen Vereinigungen ihre digitalen Aktivitäten einfach in einen anderen „sicheren Hafen“ verlagern.

105. Hierfür können die Strafverfolgungsbehörden verschiedene internationale Koordinierungsmechanismen wie Europol/Eurojust oder Interpol nutzen. Diese Organisationen verfügen über Datenbanken und leisten zur Koordinierung der Akteure aus verschiedenen Ländern mit Logistik und Fachwissen Unterstützung. Diese multilateralen Mechanismen können hilfreich sein, insbesondere wenn es darum geht, mit Blick auf Finanzermittlungen und Vermögensabschöpfung schnell wichtige Informationen auszutauschen.

Kasten 28. Operation GoldDust[1]

Die rumänischen Behörden haben im November 2021 zwei Personen festgenommen, die im Verdacht standen, mit der Ransomware Sodinokibi/REvil Cyberangriffe verübt zu haben. Sie sollen für 5000 Angriffe verantwortlich sein, bei denen insgesamt eine halbe Million Euro Lösegeldzahlungen kassiert wurden. Seit Februar 2021 haben die Strafverfolgungsbehörden außerdem drei weitere Affiliates von Sodinokibi/REvil sowie zwei Verdächtige im Zusammenhang mit GandCrab festgenommen. Das sind einige Ergebnisse der Operation

GoldDust, an der 17 Länder[2], Europol, Eurojust und Interpol beteiligt waren. Sämtliche Festnahmen wurden durch die gemeinsamen internationalen Strafverfolgungsmaßnahmen ermöglicht. Dazu gehörten Identifizierungs- und Abhörmaßnahmen sowie die teilweise Beschlagnahme der von der Sodinokibi/REvil-Ransomwarebande, die als Nachfolger von GandCrab gilt, genutzten Infrastruktur.

Ausgangspunkt der Operation waren Hinweise aus früheren Ermittlungen gegen GandCrab, die unter rumänischer Federführung mit Unterstützung von Europol sowie Strafverfolgungsbehörden verschiedener Länder, einschließlich Großbritannien und USA, durchgeführt worden waren.

Europol erleichterte den Informationsaustausch, unterstützte die Koordinierung der Operation, leistete operative Unterstützung und steuerte Krypto-, Malware- und forensische Analysen bei. Außerdem entsandte Europol an jeden Standort Experten und richtete zur Koordinierung der Aktivitäten vor Ort eine virtuelle Kommandozentrale ein. Durch die internationale Zusammenarbeit konnte Europol Maßnahmen zur weiteren Schadensbegrenzung mit anderen EU-Staaten effektiv abstimmen. So konnte verhindert werden, dass weitere Unternehmen Opfer der Sodinokibi/REvil-Ransomware wurden.

Unterstützt wurde die Operation durch die bei Europol angesiedelte Joint Cybercrime Action Taskforce (J-CAT). Hierbei handelt es sich um ein ständiges operatives Team von Cyber-Verbindungsbeamten aus verschiedenen Ländern, die von einem gemeinsamen Büro aus an hochkarätigen Ermittlungen im Bereich Cyberkriminalität arbeiten.

Quelle: Europol

Fußnoten

1. Näheres hierzu siehe www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged
2. Teilnehmende Länder: Australien, Belgien, Deutschland, Frankreich, Großbritannien, Kanada, Luxemburg, Niederlande, Norwegen, Philippinen, Polen, Rumänien, Schweden, Schweiz, Südkorea, Kuwait und USA.

Vorgeschlagene Maßnahmen

Die Länder sollten bilaterale, regionale und multilaterale Mechanismen einrichten und sich aktiv daran beteiligen, z. B. durch Verbindungsbüros oder die Einrichtung rund um die Uhr besetzter Kontaktstellen, um eine zügige internationale Zusammenarbeit und einen schnellen Informationsaustausch zu ermöglichen.

Fazit

106. Trotz des jüngsten Anstiegs von Geldflüssen im Zusammenhang mit Ransomware weltweit mangelt es weiterhin an entsprechenden Geldwäscheermittlungen. Die vorliegende Studie zeigt, dass es sich bei Ransomware um ein multidisziplinäres und internationales Problem handelt. Um dieser Bedrohung wirksam zu begegnen, bedarf es daher eines koordinierten Vorgehens. Hierzu sollten die Länder Partnerschaften nutzen, und zwar auf drei Ebenen: öffentlich-öffentlich, öffentlich-privat sowie mit ausländischen Partnerländern und multilateralen Organisationen.

107. Die vorliegende Studie hat außerdem gezeigt, wie wichtig eine schnellere Umsetzung der FATF-Standards ist, um einen effektiven Rahmen für den Umgang mit Gewinnen aus Ransomware-Angriffen zu schaffen, insbesondere mit Blick auf die beteiligten Kryptowerte und Kryptowertedienstleister. Die FATF wird sich weiterhin für die Umsetzung der FATF-Standards in diesem Sektor einsetzen.

108. Nicht zuletzt stellen die Verwendung von Kryptowerten zur Geldwäsche von Ransomware-Gewinnen sowie die ständig neuen Methoden der Ransomware-Banden weitere Herausforderungen dar. Die zuständigen Behörden sollten dafür sorgen, dass ihre Rechtsvorschriften auf dem neuesten Stand sind und sie über die erforderlichen Fähigkeiten und Kapazitäten verfügen, um in einem dynamischen digitalen kriminellen Umfeld schnell handeln zu können.