Es ist also an der Zeit, sich dem Thema IT-Sicherheit nachhaltig zu widmen. Und da dieser Bereich ein Kaninchenbau ist, in dem man sich sehr leicht verlieren kann, ist eine allgemeine Kategorisierung sinnvoll:

- Was versuchen wir zu schützen?
- Was kann man eigentlich angreifen?
- Von wem geht Gefahr aus?
- Welche Risiken können entstehen?

Um sich dem Thema Cyberkriminalität als potenziell betroffene Person oder Organisation zu nähern, benötigt es eine strukturierte Denkweise, anhand derer die Komplexität der inzwischen im Internet anzutreffenden Gefahren enumeriert, bewertet und dementsprechend Maßnahmen formuliert und priorisiert werden können. Im Folgenden wird auf Schutzziele eingegangen, auf Akteure, die diese Schutzziele verletzen wollen, sowie materielle und immaterielle Dinge, deren Schutzziele verletzt werden können. Aus der Kombination dieser Komponenten ergibt sich ein individuelles Gefahrenmodell. Die hier angeführten Denkweisen sind nicht nur in der Analyse der IT-Sicherheit hilfreich, sondern dienen allgemein dazu, Risiken bestmöglich zu navigieren.

2. Schutzziele

In der IT und Informationssicherheit gibt es den Begriff der „CIA-Triade". CIA steht für

- **Confidentiality**, die Vertraulichkeit
- **Integrity**, die Integrität
- **Availability**, die Verfügbarkeit

Grob lassen sich alle Gefahren in der IT auf einen oder mehrere dieser drei Bereiche zurückführen.

2.1. Vertraulichkeit

Informationen haben einen Adressatenkreis. Eine verschlüsselte persönliche Nachricht in einer Messaging-App geht nur die beiden Personen innerhalb der Konversation etwas an. Gelingt es nun einer dritten Person (auf welchem Weg auch immer), die Nachricht ebenfalls zu lesen, so ist das Schutzziel der Vertraulichkeit verletzt. Dies gilt aber auch für Applikationen und IT-Systeme: Kann in einer Software auf Daten zugegriffen werden, auf die eigentlich kein Zugriff bestehen sollte, ist ebenfalls das Schutzziel Vertraulichkeit verletzt. Zum Beispiel sind dem US-Unternehmen Equifax im Jahr 2017 143 Millionen Nutzerdaten, darunter die US-Sozialversicherungsnummer, abhandengekommen.[3]

3 BleepingComputer, Highly Sensitive Details of 143 Million Users Stolen in Equifax Hack https://www.bleepingcomputer.com/news/security/highly-sensitive-details-of-143-million-users-stolen-in-equifax-hack/ (24.9.2024).

2.2. Verfügungsbefugnis

Die alleinige Verfügungsbefugnis über das System oder über einen Teil des Systems muss für eine Strafbarkeit nach §§ 118a, 126b StGB ausgeschlossen sein. Das bedeutet, dass der Täter nur dann tatbestandsmäßig handelt, wenn er sich zu einem Computersystem Zugang verschafft oder die Funktionsfähigkeit eines Computersystems beeinträchtigt, über das er nicht oder nicht alleine verfügen darf. Die Verfügungsbefugnis ist daher grundsätzlich mit einer eigentümerähnlichen Position zu vergleichen.[18] Nach § 126a StGB ist verfügungsberechtigt, wer über die automationsunterstützt gespeicherten Daten unter Ausschluss anderer verfügen darf. Wem der Datenträger gehört, auf dem sich die Daten befinden, ist hier aber unerheblich.[19]

2.3. Kritische Infrastruktur

Die Legaldefinition der kritischen Infrastruktur wurde mit dem StRÄG 2015 im Zuge der Umsetzung der EU-Richtlinie über Angriffe auf Informationssysteme eingeführt. Der Begriff wird im Wesentlichen iZm Qualifikationen der einzelnen Cybercrime-Delikte und bei den klassischen Straftatbeständen bei der schweren Sachbeschädigung nach § 126 StGB und dem schweren Diebstahl nach § 128 StGB gebraucht.[20] Ist durch die Tatbegehung die kritische Infrastruktur betroffen bzw beeinträchtigt, sind höhere Freiheitsstrafen angedroht.

Die kritische Infrastruktur umfasst gem § 74 Abs 1 Z 11 StGB Einrichtungen, Anlagen, Systeme oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit, die Landesverteidigung oder den Schutz der Zivilbevölkerung gegen Kriegsgefahren, die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, das öffentliche Abfallentsorgungs- und Kanalwesen oder den öffentlichen Verkehr haben. Es handelt sich bei der abschließenden Aufzählung daher um für das Gemeinwohl besonders bedeutsame Sektoren.[21] Öffentlich bedeutet der Allgemeinheit zugänglich bzw für diese bestimmt, unabhängig davon, ob der Betreiber der Staat oder ein Privater ist.[22]

2.4. Kriminelle Vereinigung

Höhere Strafen drohen auch, wenn gewisse Taten im Rahmen einer kriminellen Vereinigung begangen werden. Eine kriminelle Vereinigung ist gem § 278 Abs 2 StGB ein auf längere Zeit angelegter Zusammenschluss von mehr als zwei Per-

18 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht, 2. Kapitel Rz 2.12 f.
19 *Rebisant* in *Höpfel/Ratz*, WK-StGB² § 126a Rz 27.
20 *Jerabek/Reindl-Krauskopf/Ropper/Schroll* in *Höpfel/Ratz*, WK-StGB² § 74 Rz 60/39.
21 *Jerabek/Reindl-Krauskopf/Ropper/Schroll* in *Höpfel/Ratz*, WK-StGB² § 74 Rz 60/20 ff.
22 *Fabrizy/Michel-Kwapinski/Oshidari,* StGB¹⁴ § 74 Rz 31; für weitere Ausführungen zur kritischen Infrastruktur siehe auch *Benedik/Demal*, Kapitel VI.

stärken. Sie geben sich ua als Beamte von Finanzbehörden, Polizisten oder sogar Regierungsmitglieder aus. Mittels vermeintlicher Behördenschreiben werden ua Überweisungen aufgrund angeblicher Steuernachzahlungen, Straftaten sowie zur Verifizierung gefordert oder um Übermittlung persönlicher Daten ersucht.[18] Eine erhöhte Wachsamkeit und Skepsis gegenüber ungewöhnlichen Behördenkontakten ist daher notwendig.

2.4. Fake Invoice und Overpayment Fraud

Bei Fake Invoice Fraud versenden die Täter gefälschte Rechnungen an Unternehmen, um rechtswidrig Zahlungen zu erwirken. Die Rechnungen erscheinen oft legitim und enthalten maßgeschneiderte Informationen über angeblich erbrachte Dienstleistungen oder gelieferte Waren, die jedoch nie bestellt oder geliefert wurden. Teilweise werden hier sogar die Kontaktdaten und Logos tatsächlicher Kunden oder Lieferanten des Unternehmens missbraucht und „lediglich" vorgetäuscht, dass es zu einer Änderung der Zahlungsverbindungen kam. Teilweise werden auch QR Codes auf Rechnungen manipuliert. Dabei werden binnen weniger Sekunden fälschlich Zahlungen durchgeführt, bei denen abweichende Zahlungsdaten unbemerkt bleiben. Bei Overpayment Fraud geben Betrüger an, irrtümlich einen zu hohen Betrag gezahlt bzw eine Überweisung an den falschen Empfänger durchgeführt zu haben und ersuchen um Rücküberweisung. Die Überweisung ist teils sogar im Bankensystem des Gegenübers abgebildet, wird jedoch anschließend von den Tätern wieder selbständig revidiert, insb über Paypal.

Praxistipp

Unternehmen sollten strikte interne Kontrollprozesse zu Eingangsrechnungen und -zahlungen, die insb die Überprüfung von Rechnungsdetails iZm bestehenden Verträgen über die zuständige Abteilung, die Kontaktaufnahme mit bekannten Lieferanten bei Änderungen von Zahlungsdaten und die Schulung von Mitarbeitern, um verdächtige Rechnungen und Zahlungen zu erkennen, implementieren. Die Einführung eines Systems zur doppelten Autorisierung von Rechnungen und Zahlungen kann ebenfalls dazu beitragen, das Risiko von Fake Invoice oder Overpayment Fraud sowie insb die Haftung der Geschäftsleitung[19] zu minimieren.

2.5. Fake Shops

Bei dieser Form der Cyberkriminalität setzen die Täter entweder gefälschte Online-Shops auf oder bilden bestehende Online-Shops nach, um Personen zu Zahlungen zu bewegen. Opfer zahlen für Produkte oder Dienstleistungen, die nie geliefert

18 FMA-Info, Reden wir über Geld: Betrugsmasche Authority Scam vom 25.2.2022, 14/2022; Europol, Beware: scams involving fake correspondence from Europol, https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/beware-scams-involving-fake-correspondence-europol#:~:text=If%20you%20receive%20a%20communication,or%20file%20from%20the%20internet (12.10.2024).

19 Siehe zur Haftung der Geschäftsleitung im Detail Kap XVI.

5.2.3.3. Beeinträchtigung wesentlicher Bestandteile der kritischen Infrastruktur

Weitere alternative Voraussetzung ist die Beeinträchtigung der „kritischen Infrastruktur". Hierbei handelt es sich um die Qualifikation des Abs 4 Z 2 der §§ 126a und 126b StGB.

Die kritische Infrastruktur wird in § 74 Abs 1 Z 11 StGB legaldefiniert. Demnach handelt es sich bei kritischer Infrastruktur um Einrichtungen, Anlagen, Systeme oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit, die Landesverteidigung oder den Schutz der Zivilbevölkerung gegen Kriegsgefahren, die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, das öffentliche Abfallentsorgungs- und Kanalwesen oder den öffentlichen Verkehr haben. Hierbei handelt es sich um eine taxative Aufzählung der für das Gemeinwohl besonders bedeutsamen Aufgaben.[49]

„*Einrichtungen, Anlagen, Systeme oder Teile davon*" sind nicht nur im technischen Sinne zu verstehen, sondern weit auszulegen. Auch Organisationen wie das Rote Kreuz werden als Einrichtungen verstanden sowie die ihnen zur Verfügung stehenden (beweglichen und unbeweglichen) Mittel.[50]

Einschränkende Voraussetzung ist aber, dass diese Einrichtungen, Anlagen, Systeme oder ihre Teile eine wesentliche Bedeutung für die oben beschriebenen Aufgabenbereiche haben.[51] Die Beurteilung, ob sie eine wesentliche Bedeutung haben, erfolgt im Wege einer Einzelfallprüfung.[52] Hier sind Parameter wie die Größe des betroffenen Ortes oder die Anzahl der betroffenen Personen ausschlaggebend.[53]

Auch hier reicht alleine die Gefährdung nicht aus, sondern muss entsprechend dem Gesetzeswortlaut tatsächlich eine Beeinträchtigung eintreten.

Weitere Voraussetzung ist, dass sich die Beeinträchtigung auf **wesentliche Bestandteile** der kritischen Infrastruktur[54] (§ 126a Abs 4 Z 2 StGB) bzw auf Com-

49 *Bergauer*, Das materielle Computerstrafrecht 608 f; *Jerabek/Ropper* in *Höpfel/Ratz*, WK² StGB § 74 Rz 60/41 (Stand 1.5.2024, rdb.at).

50 *Jerabek/Ropper/Reindl-Krauskopf/Schroll/Oberressl* in *Höpfel/Ratz*, WK² StGB § 74 Rz 60/40 (Stand 15.5.2023, rdb.at).

51 *Tipold* in *Leukauf/Steininger*, StGB⁴ Update 2020 § 74 Rz 36; *Bergauer*, Das materielle Computerstrafrecht 608 f; näher zu den einzelnen Aufgabenbereichen siehe *Jerabek/Ropper* in *Höpfel/Ratz*, WK² StGB § 74 Rz 60/43 ff (Stand 1.5.2024, rdb.at).

52 *Jerabek/Ropper* in *Höpfel/Ratz*, WK² StGB § 74 Rz 60/41 (Stand 1.5.2024, rdb.at); nach Ansicht von *Bergauer* sind solche Bestandteile immer schon dann wesentlich, wenn sie für den bestimmungsgemäßen Betrieb unentbehrlich sind, siehe *Bergauer* in *Kert/Kodek*, Das große Handbuch Wirtschaftsstrafrecht², Rz 11.50.

53 *Jerabek/Ropper* in *Höpfel/Ratz*, WK² StGB § 74 Rz 60/41 (Stand 1.5.2024, rdb.at).

54 Vgl hierzu auch *Tipold* in *Leukauf/Steininger*, StGB⁴ Update 2020 § 74 Rz 36.

Dieser Aspekt macht Bitcoin für die Geldwäsche attraktiv. Über Bitcoin kann verfügen, wer über eine ihm zugewiesene Adresse („Wallet") mittels kryptographischen Codes zugreifen kann. Weitere Zugriffshindernisse gibt es nicht, vor allem nicht irgendwelche Identifikationspflichten und KYC-Überprüfungen. Ebenso wenig kann eine dezentrale Bitcoin-Wallet etwa durch behördlichen Akt gleichsam von der Ferne „eingefroren" werden.[35] Zugriff auf Bitcoins auf einer dezentralen Wallet erscheint zwar möglich, indem der private Schlüssel oder die Wiederherstellungsphrase sichergestellt wird. Selbst dann kann aber nicht ausgeschlossen werden, dass der Besitzer über die Bitcoins dennoch verfügt, etwa, wenn er die Wiederherstellungsphrase auswendig weiß oder sie sich noch woanders notiert hat und die Behörde die Bitcoins nicht schnell genug auf eine eigene Wallet transferiert. Wird der private Schlüssel oder die Wiederherstellungsphrase nicht aufgefunden, ist ein Zugriff auf die Bitcoins ohne die Kooperation des Besitzers der Wallet nicht möglich.[36]

4.2.2. Eignung von Bitcoin zur Geldwäsche

Aus diesem Grund wurde Bitcoin auch für Kriminelle attraktiv, zB Erpresser, die fremde IT-Systeme lahmlegten und nur gegen Lösegeld in Bitcoin wieder freigaben.[37] Sie gaben dem Opfer die öffentliche Adresse ihrer Bitcoin-Wallet bekannt. Über einmal dorthin überwiesene Bitcoins kann nur der Inhaber der Wallet (dh derjenige, der den kryptographischen Zugangscode kennt) verfügen. Von dort war es für Kriminelle ein Leichtes, die erbeuteten Bitcoins in beliebig kleinen Teilen an beliebig viele weitere Adressen zu überweisen und damit deren Herkunft zu verschleiern. Ebenso entgegen kommt Kriminellen der Umstand, dass das Bitcoin-Netzwerk de facto keine Landesgrenzen kennt. Um über eine bestimmte Bitcoin-Wallet und die darauf registrierten Bitcoin zu verfügen, benötigt man bloß den erwähnten Zugangscode und eine Internetverbindung, egal wo auf der Welt man sich befindet. Damit ist es möglich, Bitcoin aus illegaler Quelle in einem beliebigen Staat der Welt an einen Krypto-Dienstleister zu senden, der nur geringe Geldwäschesorgfaltsanforderungen hat, und dort in Cash einzutauschen bzw normales Buchgeld einzuwechseln.

35 Anders ist die Lage, wenn ein Kunde seine Bitcoins durch einen Custodian oder sonstigen Kryptodienstleister verwalten lässt. In diesen Fällen kann ein exekutives Verfügungsverbot erlassen werden, das auch dem Custodian oder Kryptodienstleister als Drittschuldner zugestellt wird, und so auf das Guthaben des Kunden zugegriffen werden (§ 328 EO).

36 UU kann auf eine Exekution zur Erwirkung unvertretbarer Handlungen gem § 354 EO zurückgegriffen werden. Dies wird aber nicht mehr in Betracht kommen, wenn der Verpflichtete glaubhaft macht, selbst keinen Zugriff mehr auf die Bitcoins zu haben, weil er etwa den privaten Schlüssel bzw die Wiederherstellungsphrase vergessen oder verloren hat. So haben zB irische Strafverfolgungsbehörden im Jahr 2019 von einem verurteilten Drogendealer Bitcoins im Wert von EUR 380 Mio beschlagnahmt. Sie haben darauf aber keinen Zugriff, weil der Täter die privaten Schlüssel zu seinen Wallets verloren haben soll; vgl https://dig.watch/updates/irish-authorities-unable-to-access-380m-in-bitcoin-seized-from-drug-dealer (besucht am 11.10.2024).

37 Vgl zum Beispiel die WannaCry-Ransomware-Attacke aus 2017 (https://en.wikipedia.org/wiki/WannaCry_ransomware_attack, besucht am 23.7.2024).

oder Berufslebens. Tathandlung ist die Drohung mit dem Zugänglichmachen, Bekanntgeben oder Veröffentlichen von Tatsachen oder Bildaufnahmen betreffend den höchstpersönlichen Lebensbereich. Bekanntgeben ist die unmittelbare Mitteilung, während beim Zugänglichmachen nur die Möglichkeit des Zugriffs auf den Inhalt geboten wird. Veröffentlichen ist die Zugänglichmachung für einen unbestimmten Personenkreis. Der Begriff der Tatsachen umfasst auch unrichtige Tatsachen.[24]

Beispiele

A und B hatten eine Beziehung, welche zwischenzeitlich in die Brüche gegangen ist. B droht, damals im Einvernehmen aufgenommene Sexvideos im Internet zu veröffentlichen. Dies erfüllt den Straftatbestand der gefährlichen Drohung.

C und D sind zwei Jugendliche, welche in ihrem Alltagssprachgebrauch öfters Schimpfwörter verwenden und auch in den sozialen Medien entsprechend mit „Drohungen" kommunizieren. Wenn C dem D schreibt *„Ich werde mit meinem Baseballschläger zu Dir kommen, Du Arsch!"* wird dies wohl nicht als gefährliche Drohung zu qualifizieren sein.

Der Straftatbestand der gefährlichen Drohung verlangt betreffend das Ziel des Täters (also das Opfer in Furcht und Unruhe zu versetzen) **Absichtlichkeit** iSd § 5 Abs 2 StGB.

Der Straftatbestand behandelt die gefährliche Drohung gegen Einzelpersonen. Die Bedrohung von Personenmehrheiten sowie der Öffentlichkeit schlechthin wird durch den Straftatbestand des Landzwangs gem § 275 StGB unter Strafe gestellt.

2.3. Beharrliche Verfolgung (§ 107a StGB)

Wer eine Person widerrechtlich beharrlich verfolgt, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.[25] **Beharrlich verfolgt** eine Person, wer in einer Weise, die geeignet ist, sie in ihrer Lebensführung unzumutbar zu beeinträchtigen, eine längere Zeit hindurch fortgesetzt[26]

- ihre räumliche Nähe aufsucht,
- **im Wege einer Telekommunikation** oder unter Verwendung eines sonstigen Kommunikationsmittels oder **über Dritte Kontakt zu ihr** herstellt,
- unter Verwendung ihrer personenbezogenen Daten Waren oder Dienstleistungen für sie bestellt,
- unter Verwendung ihrer personenbezogenen Daten Dritte veranlasst, mit ihr Kontakt aufzunehmen oder
- Tatsachen oder Bildaufnahmen des höchstpersönlichen Lebensbereiches dieser Person ohne deren Zustimmung veröffentlicht.

24 ErläutRV 689 BlgNR 25. GP 15; *Fabrizy,* StGB[12] § 74 Rz 20.
25 § 197a Abs 1 StGB.
26 § 107a Abs 2 StGB.

3.2. Strafbarkeit wegen der Verwendung der Daten

3.2.1. Strafbarkeit nach dem StGB

Für eine Strafbarkeit wegen der Verwendung der fremden Daten kommt grundsätzlich jenes Delikt in Betracht, das der Täter – wenn auch unter einer fremden Identität – verwirklicht. Je nachdem, wofür der Täter die Daten seines Opfers missbraucht, kann er sich zB wegen Betrugs, Datenfälschung, Suchtmittelhandel, Geldwäscherei oder nach einem Äußerungsdelikt strafbar machen.[41]

Verwendet der Täter fremde Identitätsdaten, um durch die Täuschung an Vermögenswerte zu kommen, fällt dieses Verhalten unter die klassischen Betrugsdelikte (§§ 146 ff StGB). Beispiele hierfür sind der Bestell- und Verkaufsbetrug[42] oder der CEO Fraud. Erstellt der Täter für eine Online-Bestellung im fremden Namen einen falschen Datensatz, kann dieses Verhalten zudem den Tatbestand der Datenfälschung (§ 225a StGB) erfüllen.[43] Wenn Täter im Namen ihrer Opfer Bankkonten eröffnen und diese anschließend als Empfängerkonten für Zahlungen der betrogenen Personen und zur Weiterüberweisung dieser Geldbeträge missbrauchen, kommt eine Strafbarkeit wegen Geldwäscherei (§ 165 StGB) in Betracht.[44] Missbrauchen Täter die Social-Media-Konten ihrer Opfer dazu, um beleidigende, rassistische, extremistische oder verleumderische Äußerungen zu machen, sind Delikte wie Fortdauernde Belästigung im Wege einer Telekommunikation oder eines Computersystems („Cyber-Mobbing", § 107c StGB), Üble Nachrede (§ 111 StGB), Beleidigung (§ 115 StGB), Verhetzung (§ 283 StGB) oder Verleumdung (§ 297 StGB) einschlägig.[45]

3.2.2. Strafbarkeit nach dem DSG

Darüber hinaus findet sich im Datenschutzrecht eine Strafbestimmung (§ 63 DSG), welche die Datenverarbeitung in Gewinn- und Schädigungsabsicht unter Strafe stellt. Strafbar macht sich demnach, wer personenbezogene Daten, die ihm aus-

41 Siehe dazu auch *Reindl-Krauskopf*, ÖJZ 2015/19, 115.

42 Beim Bestellbetrug bestellen die Täter mit den gestohlenen Daten Produkte und Dienstleistungen, für die das Opfer zwar bezahlen muss, die es aber nie erhält. So bestellen die Täter zB Waren auf Rechnung, wobei sie die Ware nicht an die Adresse der Betroffenen, sondern an eine Abholstation oder eine alternative Lieferadresse liefern lassen. Ebenso verwenden die Täter fremde Daten, wie zB Passkopien, um Mobilfunkverträge abzuschließen, oder Kreditkartendaten, um Abos für kostenpflichtige Streaming-Dienste, Online-Dating-Portale oder Premium-E-Mail-Accounts abzuschließen. Die Opfer erfahren oft erst dann vom Betrug, wenn sie eine Rechnung, ein Mahn- oder Inkassoschreiben erhalten oder unbekannte Abbuchungen auf ihrem Konto bemerken. Beim Verkaufsbetrug hacken Cyberkriminelle die Konten von legitimen Verkäufern und schließen Verträge mit Konsumenten ab. Die Kunden bezahlen dann für Produkte, die sie jedoch nie erhalten siehe dazu *ÖIAT*, Identitätsdiebstahl. Die Folgen für Betroffene und wie ihnen geholfen werden kann, April 2022, 12 f.

43 Siehe hierzu auch Kap III.3.4.

44 Siehe hierzu ausf Kap VII.3.

45 Zu diesen Straftatbeständen siehe auch ausf Kap VIII.

Sofern ein auf § 65 StGB gestütztes inländisches Verfahren geführt wird, ist zu klären, ob die betreffende Tat auch nach dem Recht des Tatorts mit gerichtlicher Strafe bedroht ist. Konkret sind Feststellungen dazu zu treffen, ob die Tat die objektiven und subjektiven Tatbestandsmerkmale einer der in Betracht kommenden ausländischen Strafnormen erfüllt.[20]

Darüber hinaus ist zu beachten, dass die zu beurteilende Tat – den Grundsätzen der §§ 1 und 61 StGB entsprechend – sowohl im Zeitpunkt ihrer Begehung als auch im Zeitpunkt der Beurteilung nach beiden Strafrechtsordnungen konkret strafbar sein muss.[21]

Ein Auslieferungshindernis wegen der Art der Tat besteht insbesondere bei **geringfügigen Straftaten**. Wenn eine Tat das nach den anzuwendenden Auslieferungsbestimmungen (insb § 11 ARHG, EUJZG) geforderte Mindestmaß der Strafdrohung nicht erreicht, so ist eine Auslieferung gemäß § 65 Abs 1 Z 2 StGB nicht zulässig.[22] In einem solchen Fall ist allerdings gemäß § 65 Abs 1 Z 2 StGB auch kein inländisches Strafrecht anwendbar.

Zudem ist eine Auslieferung gemäß § 65 Abs 1 Z 2 StGB bei bestimmten Eigenschaften der Tat unzulässig. Darunter fallen insbesondere **Auslieferungsverbote begründende politisc he, militärische und fiskalische strafbare Handlungen** (§§ 14 und 15 ARHG). Zu beachten sind dabei allerdings internationale und bilaterale Vereinbarungen, die auch für solche Delikte Auslieferungspflichten vorsehen können.[23] Wenn die Auslieferung aufgrund politischer, militärischer oder fiskalischer Eigenschaften der Tat nicht möglich ist, besteht gemäß § 65 Abs 1 Z 2 StGB ebenso keine inländische Gerichtsbarkeit.

4. Zuständigkeit bei ausgewählten Cybercrime-Delikten

4.1. Erfolgsdelikte im Allgemeinen (Betrug, Erpressung)

Bei Erfolgsdelikten in Form von Distanzdelikten, welche sich dadurch kennzeichnen, dass der Handlungs- und der Erfolgsort auseinanderfallen, sind sowohl der Ort der Handlung als auch der Ort des Erfolgs Tatort.[24] Dies ist insbesondere bei Cybercrime-Delikten von Relevanz, wenn ein im Ausland handelnder Täter auf betrügerische oder erpresserische Weise Personen bzw Unternehmen in Österreich zur Durchführung von Überweisungen von ihrem österreichischen Bankkonto bewegt.

20 OGH 25.3.2021, 12 Os 134/20b; OGH 8.1.2021, 11 Os 49/20w.
21 *Schwaighofer* in *Hinterhofer*, SbgK StGB § 65 Rz 12; JABl 1975/52.
22 *Schwaighofer* in *Hinterhofer*, SbgK StGB § 65 Rz 28 ff.
23 *Schwaighofer* in *Hinterhofer*, SbgK StGB § 65 Rz 34; OGH 21.8.2008, 15 Os 108/08h.
24 *Spornberger* in *Zankl,* Rechtshandluch der Digitalisierung, 320.

4.1. Notfallplan

Eingebettet im breiteren Rahmen des Business Continuity Management ist ein Notfallplan ein Dokument, welches unterschiedliche Szenarien (wie auch mögliche Cyberangriffe) und die dementsprechend zu tätigenden Maßnahmen beinhaltet. Wichtige Punkte bei der Erstellung eines solchen Planes können sein:

- Kontaktdaten aller relevanten Personen (auch Kommunikationskanäle außerhalb der Organisation, zB das private Mobiltelefon).
- Wer wird wann von einem Vorfall informiert und was ist die Rolle der entsprechenden Person?
- Von wem wird die Forensik durchgeführt? Wie werden die Ergebnisse Dritten zur Verfügung gestellt?
- In welcher Reihenfolge werden Systeme wiederhergestellt?
- Unternehmensexterne Ressourcen: Die Kontaktdaten der Incident Responder, der Cyberversicherung, Rechtsanwälten, PR-Beratern und wie diesen Parteien welche Informationen zur Verfügung gestellt werden.
- Informationen zur Cyberversicherungs-Polizze.
- Möglichst aktuelle Dokumentation des Netzwerkes und sonstiger IT-Assets.
- Handling der Übergabe in die längerfristige Wiederherstellung.
- Vorformulierte Statements an das Team, Kunden und sonstige Stakeholder.
- Rechtliche Rahmenbedingungen (zB Meldepflichten).

Externer Input kann bei der Formulierung des Notfallplans sehr wertvoll sein. Existiert eine brauchbare Version dieses Planes, so sollte dieser (inklusive aller Anhänge) ausgedruckt (!) und auffindbar abgelegt werden. Ein Notfallplan, auf den aufgrund eines verschlüsselten Fileservers nicht mehr zugegriffen werden kann, ist nicht besonders hilfreich.

4.2. Kontakte zur Incident Response

Die Wahrscheinlichkeit ist sehr hoch, dass im Fall eines schwerwiegenden IT-Security-Vorfalls die Situation nicht mehr nur mit internen Ressourcen behoben werden kann. In diesem Fall ist es lohnend, ein Verzeichnis bekannter *Incident-Response*-Unternehmen zur Hand zu haben, die Erfahrung sowohl in der Wiederherstellung als auch der forensischen Analyse besitzen. Diese Unternehmen bieten auch Service Level Agreements, bei denen sie für eine monatliche Summe garantieren, innerhalb kürzester Zeit zur Verfügung zu stehen. Je nach Gefahrenmodell sollte hier also so ein Vertrag existieren. Die Unternehmen, die Incident Response anbieten, sind meist sehr gut gebucht.

4.3. Parallelinfrastruktur für den Notfall

Ist tatsächlich potenziell die gesamte Infrastruktur von einem Cybersecurity-Vorfall betroffen, so müssen auch die internen Kommunikationsmöglichkeiten als

Anspruch auf kostenlose psychosoziale und **juristische Prozessbegleitung** gemäß § 66 Abs 2 StPO.

Als Opfer im Strafverfahren kann unter anderem Akteneinsicht begehrt werden (§ 66 Abs 1 Z 2 StPO), und Privatbeteiligte haben die Möglichkeit, Beweisanträge zu stellen (§ 67 Abs 6 Z 1 StPO). So lassen sich jedenfalls wichtige Informationen auch für die unternehmensinterne Aufarbeitung des Vorfalles erlangen und auf einen erfolgversprechenden Verlauf des Ermittlungsverfahrens auch aus opferrechtlicher Sicht hinwirken.

Praxishinweis

Aus opferrechtlicher Sicht äußerst unbefriedigend ist die Tatsache, dass sichergestellte Krypto-Assets im Zuge des Ermittlungsverfahrens nicht an das Opfer ausgefolgt werden können. Zwar sieht § 69 Abs 3 StPO die Möglichkeit vor, dass sichergestellte Gegenstände von der Staatsanwaltschaft an Opfer auszufolgen sind. Diese Bestimmung bezieht sich aber bloß auf körperliche Sachen. Da Krypto-Assets keine körperlichen Sachen sind, können diese Beträge im Ermittlungsverfahren nicht an Opfer ausbezahlt werden, um etwa Schadenersatzansprüche zu befriedigen (OGH 28.3.2023, 14 Os 137/22m). Eine solche Übertragung von Vermögenswerten bzw Auszahlung ist erst mit der Erfüllung einer die Anklage erledigenden Gerichtsentscheidung im Sinne des § 367 StPO möglich. Unbefriedigend ist dieser Umstand insofern, als eine Anklageerhebung und damit die Einleitung eines Hauptverfahrens gerade in Fällen von Cybercrime oft dann nicht möglich ist, wenn Täter sich der Strafverfolgung entziehen oder nicht ausgeforscht werden können, weil Konten mit falschen Daten eröffnet wurden.

4.3.2. Lösegeldforderung

Gerade im Zusammenhang mit Ransomware kommt es zu Lösegeldforderungen. Lösegeld und seine Zahlung im geschäftlichen Bereich tangieren eine ganze Reihe an rechtlichen Fragen und rechtsrelevanten Überlegungen, die immer auf den konkreten Einzelfall bezogen sein müssen und zu beurteilen bzw zu entscheiden sind. Die Entscheidung, ob eine Zahlung erfolgt oder nicht, wird letztlich immer auf **betriebswirtschaftlichen Überlegungen** basieren. Ungeachtet dessen sollte die Entscheidung gut überlegt und dokumentiert sein. *„Eine im Vorfeld erfolgte absolute Festlegung, dass ein Unternehmen keinesfalls Lösegeld bezahlt, ist […] genauso gefährlich, wie eine vorschnelle, uninformierte Zahlung.“*[44] Die in Punkt 4.1. in diesem Kapitel genannten Sorgfaltspflichten machen es notwendig, dass die *„Argumentation der Zulässigkeit der Zahlung einer Lösegeldforderung“*[45] in jedem Fall gut dokumentiert wird. Dies beispielsweise aus nachstehenden Gründen:

44 *Anderl/Tlapak*, Sinnhaftigkeit einer Lösegeldforderung, in *Anderl* (Hrsg), #Cybercrime; Handbuch für die Praxis (2023) 193.

45 *Anderl* (Hrsg), #Cybercrime; Handbuch für die Praxis (2023) 8.