Krimineller oder Sündenbock? Strafrechtliche Verantwortlichkeit des CISO durch Unterlassen

Sophia Salm

§ 1 Einleitung[*]

Im Zeitalter der Digitalisierung benutzen immer mehr Unternehmen digitale Systeme zur Steuerung physischer Infrastruktur und zur Datenspeicherung. Damit werden die Einkommensquellen und Assets der Unternehmen, sensible Daten von natürlichen und juristischen Personen sowie Infrastruktur von öffentlichem Interesse der Gefahr digitaler Übergriffe ausgesetzt. Deren Schutz unter dem Begriff «Cybersecurity» oder «Cybersicherheit» wird somit immer wichtiger. Der schweizerische Gesetzgeber reagierte unter anderem, indem er die sogenannten «Computertatbestände» wie Art. 144bis StGB, Art. 147 StGB und weitere Strafnormen wie Art. 61 DSG und Art. 69a URG ausarbeitete. Auf der Seite der Unternehmen wird als Reaktion immer häufiger die Position des Chief Information Security Officer, kurz «CISO», eingeführt.

Der CISO ist in einem Unternehmen oder einer Organisation für die Cybersicherheit verantwortlich. Diese beinhaltet den Schutz elektronischer Systeme, Informationen und physischer Infrastruktur vor digitalen Angriffen.[1] Häufige Attacken sind beispielsweise Malware, welche auf Ausspähung gerichtet ist,[2] oder DDoS Angriffe, deren Ziel die Überlastung der Kapazität einer digitalen Infrastruktur – zum Beispiel Websites – sind, um so die

---

* Der nachfolgende Beitrag wurde als Masterarbeit im Rahmen des Masterstudiums der Rechtswissenschaften an der Universität Zürich am 15.4.2024 eingereicht. Der Inhalt befindet sich auf dem Stand der Einreichung. Für die Veröffentlichung wurden die Formalien inklusive Literaturverweise zum Stichtag 21.2.2025 aktualisiert. Auch sämtliche Internetlinks wurden an diesem Tag zuletzt aufgerufen. Ich bedanke mich bei Herrn Dr. iur. Lukas Staffler, L.L.M (London) für die Betreuung der Arbeit und die Ermöglichung, an der Publikation mitzuwirken. Zur besseren Lesbarkeit wird in dieser Arbeit das generische Maskulinum verwendet. Die verwendeten Personenbezeichnungen beziehen sich gleichermassen auf alle Geschlechter.

1 Brockhaus isits AG; CISA What is Cybersecurity?; vgl. BWL Minimalstandard, S. 10.

2 Pieth Wirtschaftsstrafrecht, S. 130, 139.

Verfügbarkeit dieser zu stören.[3] Resultate solcher Cyber-Angriffe sind oft massive finanzielle Schäden in Form verlorener Assets oder der Einschränkung möglichen Gewinns, die Gefährdung von Daten sowie Rufschäden.[4] Die Strafverfolgung der Cyberkriminellen ist allerdings schwierig, da deren Identität oft unbekannt und schwierig zu eruieren ist. Die Täter sind häufig Teil grösserer Organisationen und handeln aus dem Ausland.[5] Daher ist ein Rückgriff auf andere Verantwortliche, deren Identität bekannt ist und die sich in der Schweiz befinden, kriminalpolitisch wünschenswert. Hierfür kommt der CISO in Frage.

Aufgrund der Neuheit der Position variieren die spezifischen Aufgaben des CISO in der Praxis. Grundsätzlich ist er dazu verpflichtet, eine Informationssicherheits-Strategie auszuarbeiten und diese Massnahmen gemeinsam mit der IT(-Sicherheits)-Abteilung umzusetzen und zu überwachen. Dazu gehört auch die Schulung von Mitarbeitern zu Cybersicherheitsthemen. Ausserhalb dieser «Informatik-Aufgaben» dient er als Bindeglied zwischen der Organisationsleitung und der Informationssicherheit. In diesem Zusammenhang muss er regelmässig der Leitung Bericht erstatten, diese beraten und mit internen oder externen Institutionen zusammenarbeiten. Somit muss der CISO neben technischem Wissen zur Informationssicherheit auch über geschäftliches Wissen und Durchsetzungsvermögen verfügen. Bezüglich seines Bereichs ist er berechtigt, Entscheidungen zu treffen. Weitreichende Risikoentscheidungen werden jedoch seiner Entscheidungsmacht entzogen.[6]

Vor diesem Hintergrund wird dieser Beitrag der Frage nachgehen, inwiefern der CISO im Rahmen des StGB durch unechte Unterlassung zur Verantwortung gezogen werden kann. Hierfür werden zunächst die potenziell einschlägigen Straftatbestände des besonderen Teils dargelegt. Aufgrund der thematischen Nähe werden dabei auch Tatbestände des DSG vorgestellt und erklärt, weshalb der Fokus auf das StGB, nicht das DSG gesetzt wurde. Der Hauptteil des Beitrags wird sich mit dem allgemeinen Teil des

3 BACS Halbjahresbericht 2024/I, S. 26; Pieth Wirtschaftsstrafrecht, S. 131.

4 BACS Halbjahresbericht 2024/I, S. 4; Proofpoint 2024 Report, S. 11: vgl. FINMA Aufsichtsmitteilung 05/2020, S. 2 f.: Die FINMA sieht bei Betroffenheit systemrelevanter Institute zusätzlich die Funktionsfähigkeit der Finanzmärkte über die einzelnen Unternehmen hinaus gefährdet; Kaspersky Lab What it Takes to Be a CISO, S. 12; Wipro State of Cybersecurity, S. 52.

5 NCSC Allgemeine Bedrohungsformen, S. 4 ff.; Pieth Wirtschaftsstrafrecht, S. 148 f.

6 Zum Ganzen: CISO-Alliance Berufsbild CISO, S. 5 ff.; Heidrick & Struggles 2024 Survey, S. 14; Kaspersky Lab What it Takes to Be a CISO, S. 5, 8.

Strafrechts – die Begehung durch Unterlassen – beschäftigen. Dabei werden unter anderem verschiedene Garantenstellungen diskutiert. In diesem Zusammenhang wird die Rolle des CISO mit der des Compliance Officers und des Datenschutzberaters verglichen werden.

§ 2 Verhältnis des StGB zu den Strafbestimmungen des DSG

Die potenziell anwendbaren Tatbestände sind nicht auf die nachfolgend aufgelisteten Artikel begrenzt. Diese wurden lediglich exemplarisch herausgegriffen. Um das grosse Spektrum der Aufgaben des CISO darzustellen, wurden vier Tatbestände gewählt, die je eine Kategorie repräsentieren. So werden im folgenden Abschnitt ein Daten- beziehungsweise Computerdelikt, ein Eigentumsdelikt, ein Vermögensdelikt und ein Freiheitsdelikt näher beleuchtet. Ziel hierbei ist es, einen kurzen Überblick des jeweiligen Tatbestands und mögliche Anwendungsbeispiele zu geben.

Straftatbestände wie Art. 143 StGB oder Art. 146 StGB wurden trotz ihrer Häufigkeit in der Praxis bewusst ausgeschlossen, weil sie eine Bereicherungsabsicht fordern. Auch bei der Begehung durch Unterlassen muss der Täter, hier der CISO, diese erfüllen.[7] In den wenigsten Fällen wird ein CISO jedoch mit direktem Vorsatz, geschweige denn mit der Absicht, sich selbst oder jemand anderem einen Vermögensvorteil[8] dadurch zu verschaffen, handeln.

A. Potenziell einschlägige Straftatbestände des StGB

I. Unbefugtes Eindringen in ein Datenverarbeitungssystem

Gemäss Art. 143bis StGB macht sich strafbar, wer unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt. Bezüglich der Sicherung ist die Schwelle relativ tief; die Sicherungsmassnahme muss nicht zwingend den üblichen Standard der jeweiligen Branche erreichen, so dass auch einfache Massnahmen ge-

7 Niggli/Muskens BSK StGB, Art. 11 Rn. 145.
8 Maeder/Niggli BSK StGB, Art. 146 Rn. 261; Stratenwerth/Bommer Strafrecht BT I, § 15 Rn. 62.

nügen.[9] Sicherheitslücken schliessen die besondere Sicherung nicht aus.[10] Ein CISO, der also zwar Sicherheitsmassnahmen wie Passwörter einführt, jedoch in Kauf nimmt, dass diese einfach überwindbar sind, könnte möglicherweise diesen Tatbestand durch Unterlassen erfüllen. Art. 143bis StGB schützt die Freiheit des Berechtigten, zu entscheiden, wer Zugang zu einem Datenverarbeitungssystem beziehungsweise den darin enthaltenen Daten hat.[11] Auch als «Computerfrieden» umschrieben, wird damit die Unverletzlichkeit des eigenen Computers geschützt.[12]

Bei den meisten Cyberangriffen wird dieser Tatbestand erfüllt sein. Zur Installierung von Viren dringt man in ein Datenverarbeitungssystem ein. Die Benutzung von Malware ist auf die Ausspähung der Daten in Verarbeitungssystemen gerichtet. Bei Phishing Angriffen wird sodann oft die Eingabe von Anmeldedaten durch das Opfer erschlichen, damit mithilfe dieser Anmeldedaten in das Datenverarbeitungssystem eingedrungen werden kann.[13] Auch bei einem erfolgreichen Phishing Angriff kann folglich der Tatbestand erfüllt werden. Der CISO könnte sich in den vorgenannten Beispielen durch Unterlassen strafbar machen, indem er den Angriff nicht verhindert.

II. Sachbeschädigung

Art. 144 StGB stellt die Beschädigung, Zerstörung oder das Unbrauchbarmachen einer Sache, an der ein fremdes Eigentums-, Gebrauchs- oder Nutzniessungsrecht besteht, unter Strafe. Der Eingriff in die Substanz selbst ist nicht notwendig, solange die Funktionsfähigkeit beziehungsweise Brauchbarkeit beeinträchtigt wird.[14] Geschützt wird in erster Linie die unbeeinträchtigte tatsächliche Herrschaftsmacht über eine Sache.[15]

Auf den ersten Blick scheint dieses Delikt nicht passend, um einen Cyberangriff abzudecken. Jedoch soll hier aufgezeigt werden, dass die Arbeit des CISO sich nicht auf die virtuelle Welt beschränkt, sondern sich auch

9 BGE 145 IV 185 E. 2.2.2; Weissenberger BSK StGB, Art. 143 Rn. 19, Art. 143bis Rn. 14.
10 Weissenberger BSK StGB, Art. 143bis Rn. 15.
11 Weissenberger BSK StGB, Art. 143bis Rn. 5.
12 BGer 6B_456/2007 vom 18.3.2008 E. 4.2.
13 BACS Halbjahresbericht 2024/I, S. 11 ff.
14 Stratenwerth/Bommer Strafrecht BT I, § 14 Rn. 53 f.; Weissenberger BSK StGB, Art. 144 Rn. 38.
15 Weissenberger BSK StGB, Art. 144 Rn. 2; vgl. Stratenwerth/Bommer Strafrecht BT I, § 14 Rn. 48.

auf die physische Welt auswirken kann. Ein denkbares Szenario wäre beispielsweise ein Angriff auf Systeme, welche physische Infrastruktur steuern, wodurch diese über einen längeren Zeitraum ausgeschaltet werden und deren Funktionsfähigkeit aufgehoben wird.[16] Die Frage ist auch hier, ob der CISO diesen Angriff hätte verhindern müssen, wodurch er sich durch Unterlassen strafbar gemacht hat.

III. Ungetreue Geschäftsbesorgung

Nach Art. 158 Ziff. 1 StGB macht sich des Treubruchs strafbar, wer aufgrund eines Rechtsgeschäfts mit der Vermögensverwaltung für einen anderen oder mit der Beaufsichtigung solcher betraut ist, und dabei unter Pflichtverletzung zulässt, dass der andere am Vermögen geschädigt wird. Im Gegensatz zu den anderen genannten Tatbeständen handelt es sich dabei um ein echtes Unterlassungsdelikt.[17] Die für die unechte Unterlassung benötigte Garantenstellung wird hier mit der Sondereigenschaft des Vermögensverwalters ersetzt.[18] Geschützt wird dadurch fremdes Vermögen.[19]

Hauptfrage hier ist, ob der CISO als Vermögensverwalter im Sinne des Art. 158 Ziff. 1 StGB zu qualifizieren ist. Weiter vorausgesetzt wäre dann, dass aufgrund seiner Pflichtverletzung ein Cyberangriff erfolgt, der zu einem Vermögensschaden führt. Denkbar wäre zum Beispiel eine Lösegeldzahlung aufgrund einer Ransomware Attacke oder der unterbliebene Gewinn, wenn ein Webshop durch einen DDoS Angriff ausser Betrieb gesetzt wird.[20] Da diese Arbeit den Fokus auf die Garantenstellung des unechten Unterlassungsdelikts setzt, wird dieser Tatbestand nicht weiter besprochen. Trotzdem ist er aufgrund der thematischen Nähe erwähnenswert.

16 Woodtli SRF: Beim Unternehmen Swisswindows realisierte sich diese Gefahr im Jahr 2019, als ein Cyberangriff auf computergesteuerte Maschinen einen mehrwöchigen Produktionsstillstand auslöste.
17 Stratenwerth Strafrecht AT I, § 14 Rn. 8.
18 Niggli BSK StGB, Art. 158 Rn. 10, 125; Pieth Wirtschaftsstrafrecht, S. 114.
19 Niggli BSK StGB, Art. 158 Rn. 9.
20 Woodtli SRF: Das Unternehmen Comparis beispielsweise zahlte 2021 als Reaktion auf einen Ransomware Angriff Lösegeld.

IV. Nötigung

Eine Nötigung im Sinne des Art. 181 StGB ist gegeben, wenn durch Gewalt, Androhung ernstlicher Nachteile oder durch andere Beschränkung der Handlungsfreiheit ein Tun, Unterlassen oder Dulden abgenötigt wird. Geschütztes Rechtsgut ist dabei die Freiheit der Willensbildung, -entschliessung und -betätigung.[21] Die Erpressung gemäss Art. 156 StGB würde zwar bei Verlangen einer Geldzahlung vorgehen, jedoch benötigt diese im Gegensatz zur Nötigung eine Bereicherungsabsicht, weshalb sie hier für den CISO ausgeschlossen wurde.[22] Die Nötigung ist subsidiär anwendbar.[23]

Cyberangriffe wie Ransomware und DDoS zielen oft auf ein Tun oder Dulden der Geschädigten ab. Bei Ransomware wird die Publizierung von gestohlenen Daten angedroht oder Daten werden im Computersystem der Opfer verschlüsselt. Erst bei Erfüllung der erzwungenen Handlung – oft die Zahlung von Geld – werden die Daten entschlüsselt.[24] Bei DDoS Überfällen könnte sich der Nötigungserfolg im Dulden des damit verbundenen (Reputations-)Schadens durch das Unternehmen beziehungsweise im Dulden durch die Kunden, nicht auf die Website zugreifen zu können, manifestieren. Es würde sich dabei um eine Art Sitzblockade im Internet handeln. Möglich ist auch, dass ein Handeln des angegriffenen Unternehmens verlangt wird.[25] Auch hier stellt sich die Frage, ob der CISO durch Unterlassen trotz Handlungspflicht die Nötigung ermöglichte.

B. Überblick der DSG Strafbestimmungen

Nach Art. 1 DSG sind die geschützten Rechtsgüter der Persönlichkeitsschutz und die Grundrechte von natürlichen Personen. Art. 60 ff. DSG enthält die Strafbestimmungen, welche einen Teil des Nebenstrafrechts darstellen.

---

21 BGE 106 IV 125 E. 2a; Delnon/Rüdy BSK StGB, Art. 181 Rn. 5; Stratenwerth/Bommer Strafrecht BT I, § 5 Rn. 1.

22 Vgl. § 2.

23 Delnon/Rüdy BSK StGB, Art. 181 Rn. 71; Stratenwerth/Bommer Strafrecht BT I, § 5 Rn. 19.

24 BACS Halbjahresbericht 2024/I, S. 16.

25 Mozur New York Times: 2015 wurde das Unternehmen GitHub Opfer eines mehrtägigen DDoS Angriffs. Gemäss GitHub wollten die Angreifer, vermutlich der chinesische Staat, das Unternehmen dazu nötigen, zwei Websites, für die GitHub Webhosting betrieb, zu entfernen.

Für den CISO besonders relevant sind Art. 61 und Art. 64 DSG – die Verletzung von Sorgfaltspflichten und Widerhandlungen in Geschäftsbetrieben. Art. 64 Abs. 1 DSG verweist auf Art. 6 und 7 VStrR. Diese besagen, dass bei Widerhandlungen in Ausübung geschäftlicher Verrichtungen für einen anderen die Strafbestimmungen auf die natürlichen Personen anwendbar sind, welche die Tat verübt haben. Art. 64 DSG führt damit eine strafrechtliche Geschäftsherrenhaftung ein.[26] Art. 61 DSG umfasst unter anderem das Nichteinhalten der Mindestanforderungen an die Datensicherheit (lit. c). Da der CISO für die Cybersicherheit verantwortlich ist, welche die Gewährleistung der Datensicherheit einschliesst, wird insbesondere diese Variante für seine strafrechtliche Verantwortlichkeit relevant sein.

C. Zwischenfazit

Der Anwendungsbereich des StGB ist weiter als der des DSG. Das StGB schützt auch juristische Personen als Geschädigte, nicht nur natürliche Personen wie das DSG. Die Strafbestimmungen des DSG zielen nur auf den Datenschutz spezifisch ab, während das StGB den weiteren Bereich der Cybersicherheit abdeckt. Dadurch wird eine grössere Bandbreite von Rechtsgütern wie die Herrschaftsmacht über eine Sache, das Vermögen sowie die freie Willensbildung und -betätigung des einzelnen Menschen geschützt. Im Gegensatz dazu deckt das DSG nur den Persönlichkeitsschutz. Die Stellung des DSG als Nebenstrafrecht kommt zudem durch das tiefere Strafmass im DSG zum Ausdruck.

Das StGB geht auch bezüglich der geschützten Rechtsgüter in Verbindung mit Daten weiter als das DSG. So schützt Art. 143bis StGB beispielsweise die Entscheidungsfreiheit des Computerberechtigten, nicht nur des Dateneigentümers. Damit werden nicht nur die Betroffenen, sondern auch die Datenverantwortlichen geschützt. Der Unrechtsgehalt eines Cyberangriffs kann daher nicht allein anhand der DSG-Straftatbestände abgegolten werden.

Aus diesen Gründen können die Straftatbestände des StGB die Bandbreite der mit Cybersicherheit verbundenen Gefahren besser repräsentieren als das DSG allein. Daher wird zum Zweck dieser Arbeit nur die Strafbarkeit des CISO im Rahmen des StGB untersucht.

26 Gassmann OK DSG, Art. 64 Rn. 2; Simmler OFK DSG, Art. 64 Rn. 5.

§ 3 Strafbarkeit des CISO durch Unterlassen

Die meisten potenziell einschlägigen Straftatbestände sind Handlungsdelikte.[27] In der Praxis wird jedoch die aktive Tatbegehung nur äusserst selten vorkommen. Viel wahrscheinlicher ist die Begehung durch Unterlassen, beispielsweise indem Sicherheitslücken nicht behoben werden und dadurch Angriffe von Dritten ermöglicht werden. Nachdem also oben ein Überblick der BT-Straftatbestände gegeben wurde, muss nun gemäss dem allgemeinen Teil ermittelt werden, ob der CISO durch Unterlassen für das deliktische Verhalten der Cyberangreifer strafrechtlich verantwortlich gemacht werden kann.

A. Überblick des unechten Unterlassungsdelikts

Objektiv wird ein Unterlassen vorausgesetzt. Dieses wird nach herrschender Lehre anhand der Subsidiaritätstheorie bestimmt, wonach zuerst ein aktives Tun zu prüfen ist und erst bei Fehlen dessen ein Unterlassen in Frage kommt.[28] Das Unterlassen muss anschliessend zu einem tatbestandsmässigen Erfolg führen.[29]

Nach Art. 11 Abs. 2 StGB muss der Täter eine Garantenstellung innehaben. Diese kann namentlich aufgrund Gesetzes (lit. a), Vertrages (lit. b), einer freiwillig eingegangenen Gefahrengemeinschaft (lit. c) oder durch Schaffung einer Gefahr (lit. d) entstehen. Sie verpflichtet den Garanten zu handeln, um den Eintritt des tatbestandsmässigen Erfolgs abzuwenden.[30]

Zusätzlich wird eine hypothetische Kausalität verlangt. Gefragt wird hier, ob der Erfolg ausgeblieben wäre, hätte der Täter die unterlassene Handlung vorgenommen.[31] Die Tatmacht – die Möglichkeit, die gebotene Handlung vorzunehmen und dadurch den Erfolg abzuwenden – ist auch Vorausset-

27 Vgl. § 2.A.

28 BGE 129 IV 119 E. 2.2; BGE 115 IV 199 E. 2a; Niggli/Muskens BSK StGB, Art. 11 Rn. 53;
Trechsel/Noll/Pieth Strafrecht AT I, S. 236; a.M. Donatsch/Godenzi/Tag Strafrecht I, S. 315 f.

29 Donatsch/Godenzi/Tag Strafrecht I, S. 338 f.; Trechsel/Noll/Pieth Strafrecht AT I, S. 234.

30 BGE 105 IV 172 E. 4a; Donatsch/Godenzi/Tag Strafrecht I, S. 322; Niggli/Muskens BSK StGB, Art. 11 Rn. 67.

31 BGE 117 IV 130 E. 2a; BGE 108 IV 3 E. 2; Trechsel/Noll/Pieth Strafrecht AT I, S. 250.

zung der unechten Unterlassung.[32] Weiter wird gemäss Art. 11 Abs. 3 StGB die Vorwurfsidentität vorausgesetzt. Demnach muss dem unterlassenden Täter derselbe Vorwurf gemacht werden können, wie wenn er die Tat durch aktives Tun begangen hätte.

Subjektiv wird je nach Tatbestand Vorsatz oder Fahrlässigkeit genügen. Die vorgenannten potenziell einschlägigen Straftatbestände müssen alle in Verbindung mit Art. 12 Abs. 1 StGB vorsätzlich begangen werden. Der Täter muss also die Verwirklichung des Straftatbestands durch einen Dritten erkennen beziehungsweise voraussehen, sie aber trotz seiner Garantenpflicht nicht aufheben oder verhindern, weil er sie mindestens in Kauf nimmt.[33]

B. Garantenstellung des CISO

Die grösste Problematik bezüglich der Strafbarkeit des CISO durch Unterlassen liegt in der Frage, ob er eine Garantenpflicht hat. Hierfür muss zuerst die Hierarchie des CISO bestimmt werden. Ausgehend davon werden verschiedene Arten der Garantenstellung näher beleuchtet, um zu ermitteln, ob der CISO diese erfüllt.

I. Hierarchie des CISO

Weil die Position des CISO neu ist, kann keine pauschale Beurteilung seiner Stellung gemacht werden. Jede Organisation interpretiert die Rolle anders, räumt dem CISO einen unterschiedlichen Ermessensspielraum ein und teilt die Verantwortung anders auf. Teils soll der Verwaltungsrat für Cyberrisiken verantwortlich sein, teils ausschliesslich die Informatik-Abteilung und damit der CISO. Sogar innerhalb der einzelnen Unternehmen kann Unklarheit herrschen.[34]

In wenigen Unternehmen wird der CISO als Teil des Verwaltungsrats eingebunden.[35] Die Mehrheit der CISOs sind nicht direkt dem CEO un-

32 BGE 96 IV E. II.4a; Stratenwerth Strafrecht AT I, § 14 Rn. 41; Trechsel/Noll/Pieth Strafrecht AT I, S. 249 f.

33 BGE 105 IV 172 E. 4b.

34 Zum Ganzen: Hunziker/Trachsel EXPERTfocus, S. 613: Kommentiert wird zusätzlich, dass die alleinige Verantwortung der Informatik-Abteilung widerrechtlich sei.

35 Hunziker/Trachsel EXPERTfocus, S. 614: Ein CISO aus 18 befragten Schweizer Unternehmen; Kaspersky Lab What it Takes to Be a CISO, S. 14: 26 % der CISOs von 250 weltweit befragten Unternehmen.

terstellt, sondern unterstehen dem CIO oder einer anderen Person unterhalb des CEO.[36] Damit ist der CISO mutmasslich auch nicht Teil der Geschäftsleitung. Dies könnte ein Grund sein, weshalb nur eine bescheidene Mehrheit des CISOs von 58 % global beziehungsweise 64 % in Europa sich angemessen in Geschäftsentscheidungen eingebunden fühlt.[37] Dabei ist jedoch unklar, ob der CISO eine beratende Rolle hat, wobei seine Vorschläge durch die Geschäftsleitung abgesegnet werden müssen, oder ob der CISO eigenständig Entscheidungen treffen kann. Die Daten wurden länderübergreifend gesammelt, weshalb eine direkte Übertragung dieser Zahlen auf die Position eines CISO in der Schweiz nur mit einem gewissen Vorbehalt möglich ist. Jedoch deuten die Daten auf Tendenzen, welche vor allem grössere schweizerische Unternehmen vermutlich übernehmen.

In Übereinstimmung mit der oben aufgezeigten Mehrheit wird für die nachfolgenden Ausführungen angenommen, dass der CISO nicht im Verwaltungsrat ist und einer Person unterhalb des CEO unterstellt ist. Ob diese Person den Titel des CIO oder einen anderen Titel trägt, ist für die Zwecke dieser Arbeit unerheblich. Hintergrund dieser Annahme ist auch, dass der CISO sonst wie jedes andere Verwaltungsrats- oder Geschäftsleitungsmitglied verantwortlich wäre; seine Pflichten spezifisch als CISO wären weniger entscheidend.

II. Obhutsgarantenstellung aus Vertrag

Die Garantenstellung, die zunächst in Frage kommt, ist eine aus Vertrag gemäss Art. 11 Abs. 2 lit. b StGB. Hierfür reicht jedoch nicht jede vertragliche Handlungspflicht.[38] Vielmehr muss dadurch eine gesteigerte Verantwortung begründet werden, die grundsätzlich als Hauptpflicht erscheint.[39] Es muss sich um eine qualifizierte Rechtspflicht handeln.[40]

In Lehre und Praxis wird zwischen zwei Formen der Garantenpflicht unterschieden: die Obhutsgarantenstellung und die Sicherungs- beziehungs-

36 Heidrick & Struggles 2024 Survey, S. 11 48 % der 416 weltweit befragten CISOs unterstehen dem CIO, während nur 14 % direkt dem CEO Bericht erstatten; Wipro State of Cybersecurity, S. 23, 50: 51 % der circa 110 befragten Organisationen in Europa beziehungsweise 54 % der 345 Organisationen global unterstehen dem CIO.

37 Kaspersky Lab What it Takes to Be a CISO, S. 13 f.

38 BGE 140 IV 11 E. 2.4.2; Stratenwerth Strafrecht AT I, § 14 Rn. 17.

39 Niggli/Muskens BSK StGB, Art. 11 Rn. 82 f.; Stratenwerth Strafrecht AT I, § 14 Rn. 17 f.

40 BGE 141 IV 249 E. 1.1; BGE 120 IV 98 E. 2c; BGE 113 IV 68 E. 5a.

weise Überwachungsgarantenstellung. Erstere ist gegeben, wenn ein bestimmtes Rechtsgut vor unbestimmt vielen Gefahren geschützt wird, während zweitere die Überwachung einer bestimmten Gefahrenquelle zum Schutze unbestimmt vieler Rechtsgüter erfasst.[41]

Der CISO ist verpflcihtet ein Rechtsgut – die digitalen Assets des Unternehmens, mit dem er vertraglich verbunden ist – vor Gefahren zu schützen. Diese Gefahren sind digitale Angriffe, welche von einer Vielzahl von Tätern und auf verschiedene Arten ausgeführt werden. Damit kommt nur eine Obhutsgarantenstellung in Frage.

Ein Arbeitnehmer kann Garant aufgrund seines Arbeitsvertrags sein, wenn die entsprechenden Kompetenzen delegiert werden. Massgeblich ist die tatsächliche Herrschaft und Verantwortung für die Gefahrenquelle.[42] Eine pauschale Garantenstellung rein aufgrund seiner Treuepflicht wird wegen der Voraussetzung einer qualifizierten Rechtspflicht abgelehnt.[43] Ist der CISO nicht Teil der Geschäftsleitung, so ist sein Verhältnis zum Unternehmen ein arbeitsrechtliches. Fraglich ist dann, ob ihm als Arbeitnehmer die Verantwortung über die digitalen Assets delegiert wurde beziehungsweise delegiert werden kann.

Für die Garantenstellung spricht, dass er bei der Auswahl und Implementierung der Sicherheitstechnologien mithilft und Cybersicherheitsprozesse überwacht.[44] Er hat somit eine tatsächliche Möglichkeit einzugreifen und das Unternehmen zu schützen. Allerdings ist er nicht die einzige Person, welche für die Implementierung verantwortlich ist, und dies ist nur ein Teil seiner vielen Aufgaben.

Dagegen spricht vor allem die gesetzlich geregelte Verantwortung des Verwaltungsrats. Gemäss Art. 716a Abs. 1 OR gehören zu den unübertragbaren Aufgaben des Verwaltungsrats die Oberleitung der Geschäftsleitung (Ziff. 1), die Festlegung der Organisation (Ziff. 2) und die Ausgestaltung der Finanzkontrolle sowie Finanzplanung (Ziff. 3).

Die Oberleitung umfasst unter anderem die Implementierung eines Risikomanagements.[45] Die Risiken resultierend aus Cybervorfällen vermehren sich mit der schnellen und teils rechtlich unkontrollierten Entwicklung

41 Zum Ganzen: BGE 113 IV 68 E. 5b; Stratenwerth Strafrecht AT I, § 14 Rn. 13; Trechsel/Noll/Pieth Strafrecht AT I, S. 238 f.
42 BGer 6B_405/2013 vom 19. Mai 2014 E. 1.3.2.
43 BGE 113 IV 68 E. 6a; Donatsch/Godenzi/Tag Strafrecht I, S. 329.
44 CISO-Alliance Berufsbild CISO, S. 7; Kaspersky Lab What it Takes to Be a CISO, S. 5.
45 Watter/Pellanda BSK OR, Art. 716a Rn. 6; vgl. Hunziker/Trachsel EXPERTfocus, S. 613.

neuer Technologien.[46] Dies ist auch ersichtlich aus der stetig wachsenden Cyberkriminalität und den vermehrten Meldungen von Cybervorfällen.[47] Die Privatwirtschaft nennt heutzutage Cyber-Spionage und -Krieg als fünfthöchstes beziehungsweise langfristig als vierthöchstes Risiko.[48] Cyberrisiken müssen somit ohne Zweifel im Risikomanagement berücksichtigt werden.[49] Dadurch gehören Themen wie Cybersicherheitsmassnahmen und Risikoappetit bezüglich Cyberrisiken zu den unübertragbaren Aufgaben des Verwaltungsrats.[50]

In Fällen, in denen die Verantwortlichkeit intern nicht geregelt oder unklar ist, haftet auch wiederum der Verwaltungsrat für die ungenügende Festlegung der Organisation. Schliesslich spricht auch die Verantwortlichkeit über die Finanzplanung für eine Verantwortlichkeit für Cybersicherheit. Da Cybervorfälle hohe finanzielle Schäden mit sich ziehen können und Massnahmen ein gewisses Budget benötigen, müssen diese auch bei der Ausarbeitung einer Finanzplanung mitberücksichtigt werden.[51] All dies weist darauf hin, dass die Verantwortlichkeit nicht an den CISO delegiert werden kann.

Weiter wird in einem Rundschreiben der FINMA die Ausgestaltung einer geeigneten Technologieinfrastruktur explizit als Aufgabe der Geschäftsleitung genannt.[52] In einem anderen Rundschreiben wird die Genehmigung und Überwachung von Strategien für den Umgang mit Cyber-Risiken dem Oberleitungsorgan auferlegt.[53] Zudem wird die Geschäftsleitung dazu verpflichtet, Verwundbarkeitsanalysen und Penetrationstests durchführen

46 Vgl. WEF Global Risk Report, S. 38 f., 54.

47 BFS Digitale Kriminalität; BFS Gemeldete Cyber-Vorfälle: Wobei beachtet werden muss, dass auch andere Faktoren, wie beispielsweise eine erhöhte Sensibilisierung der Bevölkerung bezüglich Cybersicherheit, das Meldeverhalten beeinflussen können; FINMA Aufsichtsmitteilung 03/2024, S. 3.

48 WEF Global Risk Report, S. 17, 46: Zusätzlich nannten 2024 71 % von befragten Chief Risk Officers Cyberrisiken als grosse Bedrohung für ihre Unternehmen.

49 So auch BWL Minimalstandard, S. 5; FINMA Aufsichtsmitteilung 03/2024, S. 6; FINMA Rundschreiben 2023/1, Rz. 23.

50 So auch CISO-Alliance Berufsbild CISO, S. 5, 7, wonach die «Responsibility» an den CISO delegiert wird, jedoch die «Accountability» bei der Organisationsleitung bleibt und der CISO keine Risikoentscheidungen trifft; Hunziker/Trachsel EXPERTfocus, S. 613.

51 Vgl. Kaspersky Lab What it Takes to Be a CISO, S. 19: CISOs arbeiten auch mit Finanzabteilungen zusammen.

52 FINMA Rundschreiben 2017/1, Rz. 50.

53 FINMA Rundschreiben 2023/1, Rz. 24.

zu lassen.[54] Zwar sind beide Rundschreiben nur für gewisse Branchen anwendbar,[55] jedoch kann die darin festgehaltene Pflichtenverteilung für Unternehmen, welche die gleiche Gesellschaftsform nutzen, als Anhaltspunkt berücksichtigt werden.

Für die strafrechtliche Verantwortlichkeit ist zwar nach wohl herrschender Lehre nicht massgeblich, ob der Vertrag zivilrechtlich gültig ist, sondern nur die faktische Übernahme.[56] Diese wird im Einzelfall geprüft werden müssen. Jedoch ist die zivilrechtliche Undelegierbarkeit ein starkes Indiz für die tatsächliche Organisation. Grundsätzlich ist somit eine Garantenstellung aus Vertrag abzulehnen.

III. Garantenstellung aus Ingerenz

Die Garantenstellung nach Art. 11 Abs. 2 lit. d StGB verpflichtet diejenige Person, die eine Gefahr schafft oder vergrössert dazu, alle zumutbaren Massnahmen zu ergreifen, um die Gefahr abzuwenden.[57] Da eine solche Situation schnell entstehen kann, wird in der Lehre für Zurückhaltung plädiert.[58] Kein Garant ist unter anderem derjenige, deren Handlung die zulässige Risikogrenze nicht überschritten hat.[59] Zudem wird die Garantenstellung durch die Eigenverantwortung des Gefährdeten eingeschränkt.[60]

Eine Garantenstellung des CISO aus Ingerenz ist denkbar, wenn der CISO eine Sicherheitslücke trotz deren Kenntnis nicht beseitigt beziehungsweise keine weitere Person zur Beseitigung auffordert. Dabei muss unterschieden werden zwischen Lücken, die der CISO selbst durch mangelhafte Cybersicherheitsmassnahmen herbeigeführt hat und Lücken, die nicht durch sein Verhalten entstanden sind.

---

54 FINMA Rundschreiben 2023/1, Rz. 69.

55 FINMA Rundschreiben 2017/1, Rz. 1; FINMA Rundschreiben 2023/1, Rz. 2.

56 Donatsch/Godenzi/Tag Strafrecht I, S. 330; Stratenwerth Strafrecht AT I, § 14 Rn. 18 f.; Trechsel/Noll/Pieth Strafrecht AT I, S. 242; a.M. Von Rotz Garantenstellung des Compliance Officers, S. 94.

57 BGE 134 IV 255 E. 4.2.2; Niggli/Muskens BSK StGB, Art. 11 Rn. 92.

58 Niggli/Muskens BSK StGB, Art. 11 Rn. 95; Stratenwerth Strafrecht AT I, § 14 Rn. 22.

59 BGE 134 IV 255 E. 4.2.2; Donatsch/Forster/Schwarzenegger Strafrecht/Roxin, S. 558, 560 f.; Stratenwerth Strafrecht AT I, § 14 Rn. 24 f.

60 Donatsch/Forster/Schwarzenegger Strafrecht/Roxin, S. 562 f.; Donatsch/Godenzi/Tag Strafrecht I, S. 333; Stratenwerth Strafrecht AT I, § 14 Rn. 25; Trechsel/Noll/Pieth Strafrecht AT I, S. 245 f.

Ist eine Sicherheitslücke auf die Handlung des CISO zurückzuführen, hat er die Gefahr geschaffen. Somit könnte potenziell eine Garantenstellung für ihn bejaht werden, wonach er verpflichtet wäre, alle geeigneten Massnahmen zu treffen, um die adäquat kausalen Folgen der Untätigkeit zu verhindern.[61]

Lehre und Rechtsprechung befürworten teils eine auf dem Vertrauensgrundsatz basierende Sichtweise, wonach darauf vertraut werden kann, dass Dritte sich rechtmässig verhalten.[62] Demnach könnte der CISO darauf vertrauen, dass Cyberkriminelle die Sicherheitslücke nicht ausnutzen werden, wodurch er keine Garantenstellung hätte. Gegen die Anwendbarkeit des Grundsatzes in diesem Fall scheint zunächst das hohe Volumen von Cyberangriffen zu sprechen. Da eine grosse Anzahl von Unternehmen betroffen ist, besteht ein hohes Risiko einer Cyberattacke. Auf der anderen Seite ist jedoch auch eine grosse Menge von Sicherheitslücken festzustellen, welche zwar existieren, aber noch nicht für Angriffe benutzt wurden.[63] Nur weil eine Lücke besteht, wird diese folglich nicht zwingend ausgenutzt werden. Der Vertrauensgrundsatz kann somit durchaus Grund für die Verneinung einer Garantenstellung sein.

Wenn eine höhere leitende Person über die Sicherheitslücke benachrichtigt wird – dies kann der CIO oder der Verwaltungsrat sein –, muss zudem die Eigenverantwortung dieser Person berücksichtigt werden. Wird von ihr nichts getan, um die Lücke zu schliessen, beispielsweise durch Beauftragung externer Hilfskräfte oder Zuteilung weiterer Ressourcen, muss bei einer Cyber-Attacke die Garantenstellung des CISO verneint werden.

Die Eigenverantwortung des Unternehmens kann die Garantenstellung des CISO auch ausschliessen, wenn er sich innerhalb der vorgegebenen Risikogrenze hält. Der Risikoappetit – der Umfang der tolerierten Cyberrisiken – soll von der Organisationsleitung im Rahmen des Risikomanagements definiert werden.[64] Hält sich der CISO mit seinen Handlungen innerhalb dieses Rahmens, wird keine Garantenstellung begründbar sein, da vorrangig das Unternehmen hierfür die Verantwortung übernehmen muss.

---

61 BGE 134 IV 255 E. 4.2.2 Trechsel/Noll/Pieth Strafrecht AT I, S. 244.

62 BGE 120 IV 300 E. 3d.bb; Donatsch/Forster/Schwarzenegger Strafrecht/Roxin, S. 558 f.; vgl. auch Donatsch/Godenzi/Tag Strafrecht I, S. 369 f.

63 Donzé/Humbel/Plüss NZZ am Sonntag, S. 11: Im Juni 2023 zählten Sicherheits-Scans 106'000 Server mit Sicherheitslücken im Schweizer Netz.

64 BWL Minimalstandard, S. 6; FINMA Rundschreiben 2023/1; Hunziker/Trachsel EXPERTfocus, S. 613.

Zu beachten ist weiter, wie die Sicherheitslücke zustande kam. Denkbar ist, dass der CISO eine Sicherheitsmassnahme implementierte, um eine Lücke zu reparieren, wodurch jedoch an einer anderen Stelle erneut eine Sicherheitslücke entstand. In diesem Fall stellt sich die Frage, ob die zulässige Risikogrenze überschritten wurde. Wenn zuvor genügende Tests gemacht wurden und diese Folge unvorhersehbar war, kann argumentiert werden, dass eine solche Konsequenz als inhärentes Risiko der IT-Infrastruktur zu dulden ist und die zulässige Risikogrenze folglich nicht übertreten wurde.

Ist die Schaffung der Sicherheitslücke nicht auf den CISO zurückzuführen, beispielsweise weil ein verwendetes Programm nach einer Aktualisierung nicht mehr sicher ist, stellt sich die Frage, ob das reine Aufrechterhalten auch eine Garantenstellung begründet. Dafür könnte die Bejahung der Garantenstellung von Skiliftunternehmen, welche Massnahmen vor Naturgefahren vorkehren müssen, sprechen.[65] Die Gefahr in Form einer Lawinengefahr an sich wurde nicht vom Unternehmen selbst geschaffen. Im Urteil wird das Schaffen der Gefahr durch das Unternehmen darin gesehen, dass es Skipisten in einem Gebiet erstellt, wo eine Naturgefahr herrscht. Dies ist jedoch nicht vergleichbar mit der Situation eines CISO. Zwar hat er sich dafür entschieden, ein digitales Mittel zu benutzen, das Cybergefahren bergen könnte, aber dies wird aufgrund der Natur einer sich schnell entwickelnden Cybersicherheitsindustrie bei jeder Option der Fall sein. Das Skiliftunternehmen hätte in Theorie die Alternative, Skipisten an einem anderen Ort ohne Lawinengefahr zu eröffnen oder weniger Pisten zu erstellen, wodurch keine Gefahr geschaffen werden würde. Der CISO, der einer Geschäftsführung unterstellt ist, kann jedoch nicht eigenhändig entscheiden, keine digitalen Dienstleistungen anzubieten.

Gegen die Begründung der Garantenstellung durch reines Aufrechterhalten einer Gefahr spricht der Gesetzeswortlaut, der nur die Schaffung dieser Gefahr nennt. Eine solche Ausdehnung des Wortlautes würde zu einer uferlosen Strafbarkeit führen, wobei das Einhalten des Bestimmtheitsgebots problematisch wäre. Auch die Rechtsprechung impliziert, dass ein reines Aufrechterhalten nicht genügt, indem eine Garantenstellung ausgeschlossen ist, wenn die Person die Gefahr weder schuf noch erhöhte.[66] Der CISO kann also kein Garant sein, wenn die Entstehung der Sicherheitslücke nicht ihm zuzurechnen ist.

65 BGE 115 IV 189 E. 3a.
66 BGE 134 IV 255 E. 4.2.2.

IV. Geschäftsherrenhaftung

Die Geschäftsherrenhaftung kann auch eine Garantenstellung begründen. Trotz fehlender ausdrücklicher gesetzlicher Verankerung ist sie in Lehre und Rechtsprechung etabliert.[67] Allerdings ist in Hinblick auf das Legalitätsprinzip eine engere Auslegung geboten.[68] Bei dieser Haftung wird der Geschäftsherr für eine unter seiner Aufsicht begangene Straftat verantwortlich gemacht, auch wenn er diese nicht aktiv förderte, sondern lediglich nicht verhinderte.[69] Geschäftsherr ist, wer in einem Verantwortlichkeitsbereich des Unternehmens tatsächliche Leitungsaufgaben ausübt.[70]

Zuerst muss geprüft werden, ob der CISO als Geschäftsherr qualifiziert werden kann. Der CISO leitet in vielen Fällen entweder die Informatik- oder die IT-Sicherheitsabteilung.[71] Jedoch ist unklar, inwieweit er tatsächliche Entscheidungsbefugnisse über die Abteilung hat. Grundsätzlich ist seine Aufgabe in erster Linie als Brücke zwischen Informatik und Organisationsleitung zu verstehen. Bei der Ausarbeitung von Informationssicherheitsmassnahmen arbeitet er mit der Abteilung zusammen, was tendenziell auf eine horizontale, nicht vertikale Hierarchie deutet. Zusätzlich untersteht der CISO selbst einer Person, welche unterhalb der obersten Geschäftsführung steht.

So wie seine Position in dieser Arbeit definiert wurde, muss die Stellung des CISO als Geschäftsherr abgelehnt werden. Jedoch kann bei einer anderen hierarchischen Organisation durchaus eine strafrechtliche Geschäftsherrenhaftung in Frage kommen. In Betracht käme dafür beispielsweise die Konstellation, in welcher der CISO in den Verwaltungsrat eingebunden ist.

V. Vergleich zum Compliance Officer

Der Begriff der «Compliance» umfasst «die Einhaltung von gesetzlichen regulatorischen und internen Vorschriften sowie die Beachtung von markt-

67 BGE 96 IV 155 E. II.4a; Donatsch/Godenzi/Tag Strafrecht I, S. 399; Stratenwerth Strafrecht AT I, § 14 Rn. 31; Trechsel/Noll/Pieth Strafrecht AT I, S. 246.
68 BGE 105 IV 172 E. 4a; vgl. auch Stratenwerth Strafrecht AT I, § 14 Rn. 31.
69 BGE 96 IV 155 E. 4a; Stratenwerth Strafrecht AT I, § 14 Rn. 31; Trechsel/Noll/Pieth Strafrecht AT I, S. 249.
70 BGE 113 IV 68 E. 7; BGE 105 IV 172 E. 4a; Stratenwerth Strafrecht AT I, § 14 Rn. 31.
71 Kaspersky Lab What it Takes to Be a CISO, S. 7; vgl. Heidrick & Struggles 2024 Survey, S. 13.

üblichen Standards und Standesregeln».[72] Dazu gehört unter anderem die Verhinderung von strafrechtlichen Taten, begangen durch Organe und Mitarbeiter des Unternehmens.[73]

Die Garantenstellung des Compliance Officers wurde vor Bundesgericht bezüglich der Geldwäscherei nach Art. 305bis StGB bejaht.[74] Die unterlassene Handlung war dabei das Versäumen, verdächtige Vermögenswerte bezüglich ihrer Herkunft zu prüfen sowie diese bei der Geschäftsleitung zu melden.[75] Argumentiert wurde mit den Sorgfaltspflichten nach Art. 3–8 GwG, der Meldepflicht bei Verdacht auf Geldwäscherei gemäss Art. 9 GwG, den Pflichten im EBK-RS 98/1 und den internen Richtlinien der betroffenen Bank.[76] Das Bundesgericht stützte sich dabei auf eine Mindermeinung in der Lehre, weshalb dieser Entscheid stark kritisiert wird.[77]

Die Entscheidungskompetenz des Compliance Officers ist nicht einheitlich geregelt, sondern variiert nach Unternehmen. In einem Urteil, in dem die Verletzung der Meldepflicht in Art. 9 GwG bejaht wurde, gab der Compliance Officer an, dass er nicht angewiesen werden konnte, eine Meldung zu unterlassen.[78] Er war diesbezüglich weisungsfrei und entscheidungsbefugt.[79] Im oben angesprochenen Bundesgerichtsentscheid wurde erwähnt, dass ein Verdachtsfall der Geschäftsleitung zur Entscheidung über die Meldung oder Sperrung der verdächtigen Konten vorgelegt hätte werden müssen.[80] Dies impliziert, dass der Compliance Officer in diesem Fall bezüglich der Meldung nicht alleine entscheidungsbefugt war. Eine so grosse Entscheidungsmacht wie im ersten Fall ist beim CISO zu verneinen, da dieser nicht zu weitreichenden Entscheidungen befugt ist. Stattdessen nähert sich die Position des CISO der des Compliance Officers im zweiten Fall an, in dem solche Entscheidungen der Geschäftsleitung vorgelegt werden müssen.

72 FINMA Rundschreiben 2017/1, Rz. 7.
73 Nagel SJZ 117/2021, S. 104; Pieth Wirtschaftsstrafrecht, S. 77; Von Rotz Garantenstellung des Compliance Officers, S. 12.
74 BGE 136 IV 188 E. 6.2.2.
75 BGE 136 IV 188 E. 6.3.4.
76 BGE 136 IV 188 E. 6.2.1.1 ff.
77 Übersicht der verschiedenen Kritikpunkte in BGE 136 IV 188 E. 6.2.1; Von Rotz Garantenstellung des Compliance Officers, S. 172 f.
78 BStGer SK.2019.55 vom 28.7.2020 E. 2.3.21, 2.4.2.2.
79 BStGer SK.2019.55 vom 28.7.2020 E. 2.4.2.2.
80 BGE 136 IV 188 E. 6.3.2.

In den oben angesprochenen Urteilen wurde mit der gesetzlichen Meldepflicht nach Art. 9 GwG argumentiert. Fraglich ist, ob eine ähnliche Pflicht für den CISO bestehen könnte.

Gemäss Art. 29 Abs. 2 FINMAG müssen die Beaufsichtigten der FINMA unverzüglich Vorkommnisse melden, die für die Aufsicht von wesentlicher Bedeutung sind. Die FINMA konkretisierte, dass damit auch eine Meldepflicht von erfolgreichen Cyberattacken besteht, soweit sie wesentlich sind.[81] Zu ermitteln ist zunächst, wer verantwortlich für die Meldung ist.

Die Bestimmung im FINMAG nennt nur «Die Beaufsichtigten», aber nicht, wer innerhalb eines Unternehmens diese Meldung erstatten muss. In der Botschaft wird für juristische Personen erwähnt, die Organe seien Adressaten der Meldepflicht.[82] Die Botschaft führt auch aus, dass dieser Artikel dem damals geltenden Art. 47 Abs. 3 aVAG entspreche.[83] Demnach musste die Geschäftsleitung des Unternehmens die Aufsichtsbehörde informieren. Daraus ergibt sich, dass der CISO nicht Adressat der Meldepflicht ist. Eine gleichartige gesetzliche Meldepflicht wie die nach Art. 9 GwG ist für den CISO nicht ersichtlich.

Ein Unterschied zwischen dem CISO und Compliance Officer liegt im Umfang der Gefahren. Bei Cyberkriminellen handelt es sich um eine grosse Menge von bösartigen Angreifern, die unermüdlich und kontinuierlich versuchen, einen Angriff durchzuführen. Aufgrund der schnellen Entwicklung im IT-Bereich muss sich der CISO auf eine grosse Variation von Angriffen und neuen Technologien vorbereiten. Der Compliance Officer dagegen wird selten auf «Angreifer» stossen, welche im gleichen Mass konstant auf die Verletzung des Unternehmens zielen. Vielmehr handelt es sich mehrheitlich um fahrlässig oder eventualvorsätzlich handelnde Täter, welche nicht die gleichen Mittel und die Zielstrebigkeit wie Cyberangreifer haben. Einem Compliance Officer kann es daher eher zugemutet werden, einen strafrechtlich relevanten Vorfall zu verhindern.

Ein weiterer Vergleichspunkt ist die Interessenslage der beiden Positionen. Der Compliance Officer wird teilweise gegen die Interessen der Geschäftsleitung handeln müssen. Hält sich ein Unternehmen beispielsweise aus Vermögensinteressen nicht an gesetzliche Vorgaben, muss der Compliance Officer trotz Druck der Geschäftsleitung Meldung bei den

81 FINMA Aufsichtsmitteilung 05/2020, S. 2.
82 Botschaft 2006, S. 2880.
83 Botschaft 2006, S. 2880.

Behörden erstatten.[84] Der Compliance Officer hat damit auch eine Aufdeckungs- und Überwachungsfunktion bezüglich Handlungen der Geschäftsleitung.[85] Eine solche Aufdeckungsfunktion ist beim CISO zu verneinen. Jedes Unternehmen hat grundsätzlich ein Interesse daran, Cyberangriffe zu verhindern, um Schäden abzuwenden. Auch wenn die Geschäftsleitung vereinzelt nicht die konkreten Vorschläge des CISO gutheisst, wird sie trotzdem ihr Gesamtinteresse mit dem des CISO teilen. Dies ermöglicht, dass die Unternehmensleitung selbst die Verantwortlichkeit trägt.

Der CISO und der Compliance Officer können je nach Fall eine ähnliche Entscheidungsmacht haben. Zudem können für beide interne Richtlinien bestehen, welche den Officern eine Sorgfaltspflicht vorschreiben. Jedoch sind beim CISO keine gesetzlichen Sorgfalts- oder Meldepflichten erkennbar und es handelt sich um nicht vergleichbare Gefahren. Zusätzlich muss auch berücksichtigt werden, dass die Garantenstellung des Compliance Officers nur bezüglich der Geldwäscherei durch das Bundesgericht bestätigt wurde.[86] Aus diesen Gründen kann die für den Compliance Officer bejahte Garantenstellung nicht analog auf den CISO übertragen werden.

VI. Vergleich zum Datenschutzberater

Der Datenschutzberater kann gemäss Art. 10 Abs. 1 DSG fakultativ durch das Unternehmen eingesetzt werden. Er dient nach Art. 10 Abs. 2 DSG als Anlaufstelle für betroffene natürliche Personen und für Behörden. Seine Aufgaben umfassen insbesondere die Schulung und Beratung des Unternehmens bezüglich Datenschutzes (lit. a) und die Mitwirkung bei der Anwendung der Datenschutzvorschriften (lit. b). Eine Meldepflicht wurde nicht normiert, weshalb er eine rein unterstützende Funktion hat.[87]

Der Datenschutzberater trägt grundsätzlich nicht die alleinige Entscheidungsgewalt und somit auch nicht die Verantwortung für die datenschutzkonforme Datenbearbeitung. Letztere liegt gemäss Botschaft und Lehre weiterhin allein beim verantwortlichen Unternehmen.[88] Während der CI-

84 Vgl. Nagel SJZ 117/2021, S. 104 f.
85 Vgl. Von Rotz Garantenstellung des Compliance Officers, S. 31 f.
86 Vgl. Von Rotz Garantenstellung des Compliance Officers, S. 176: Die allgemeine Garantenstellung bleibt ungeklärt.
87 Balthasar OK DSG, Art. 10 Rn. 26 f.; Sury OFK DSG, Art. 10 Rn. 1.
88 Zum Ganzen: Botschaft 2017, S. 7033; Balthasar OK DSG, Art. 10 Rn. 29; a.M. Sury OFK DSG, Art. 10 Rn. 32 f.

SO etwas mehr Entscheidungsmacht hat als der Datenschutzberater, trägt das Unternehmen auch gegenüber dem CISO die Verantwortung für grössere Entscheidungen.[89] Nur innerhalb des Bereichs der Cybersicherheit ist er entscheidungsbefugt. In diesem Sinne sind die beiden Rollen daher vergleichbar.

Der Datenschutzberater muss gemäss Art. 10 Abs. 3 DSG lit. a fachlich unabhängig und weisungsungebunden sein. Dies wird in lit. b unterstrichen mit dem Verbot, andere Tätigkeiten auszuüben, welche unvereinbar mit der Aufgabe als Datenschutzberater sind. Grund dahinter ist die Vermeidung eines Interessenkonflikts. Die Lehre bejaht unter anderem einen Interessenkonflikt, wenn der Berater zugleich Leiter der IT-Abteilung ist.[90] Die Botschaft nennt als erlaubte Nebentätigkeit explizit den Informationssicherheitsbeauftragten.[91] Der CISO ist als Arbeitnehmer weisungsgebunden. Er schuldet seinem Arbeitgeber eine Treuepflicht nach Art. 321a Abs. 1 OR und muss seine Weisungen gemäss Art. 321d Abs. 2 OR befolgen. Dies wirkt sich auf die Beurteilung der Garantenstellung aus. Je nach Einzelfall wird diese Abhängigkeit zwar mehr oder weniger zum Vorschein kommen. Im Allgemeinen handelt es sich hierbei aber um einen grossen Unterschied zum Datenschutzberater.

Der Datenschutzberater dient gemäss Gesetzeswortlaut und in Anbetracht des Zwecks des DSG primär zum Schutz des Betroffenen. Auch die vorausgesetzte Unabhängigkeit deutet daraufhin, dass er – auch wenn er vom Unternehmen angestellt wird – nicht die Interessen des Unternehmens zu vertreten hat, sondern die derjenigen Personen, deren Daten bearbeitet werden. Der CISO vertritt im Gegensatz dazu primär die Interessen des Unternehmens. In seiner Funktion soll er schwere Folgen von Cyberangriffen verhindern. Primär stimmt das Interesse der Betroffenen, ihre Personendaten zu schützen, mit dem des Unternehmens, einen Reputationsschaden zu verhindern, überein. Daher bestätigt mutmasslich die Botschaft auch eine Vereinbarkeit der beiden Positionen. Jedoch dient der CISO auch beispielsweise zum Schutz vor finanziellen Schäden, was vorrangig ein Unternehmensinteresse darstellt. So verfolgt der CISO nicht vollständig deckungsgleiche Ziele wie der Datenschutzberater.

89 Siehe § 1.

90 Balthasar OK DSG, Art. 10 DSG Rn. 34; vgl. auch CISO-Alliance Berufsbild CISO, S. 5.

91 Botschaft 2018, S. 7033 f.

Eine Analogie zwischen dem Datenschutzberater und dem CISO ist aufgrund der unterschiedlichen Abhängigkeitsgraden und Interessensetzungen nicht möglich. Sie haben jedoch eine ähnliche Position hinsichtlich der Entscheidungsmacht und sind beide mit den Herausforderungen der Datensicherheit und damit dem IT-Bereich konfrontiert. Im Gegensatz zum Compliance Officer haben sie auch keine gesetzlichen Meldepflichten. Der Vergleich zum Datenschutzberater ist somit geeigneter als der zum Compliance Officer.

C. Weitere Voraussetzungen der unechten Unterlassung

Selbst wenn eine Garantenstellung zu bejahen wäre, müssten, wie oben im Kapitel § 3 A. aufgezeigt, weitere Voraussetzungen für die Strafbarkeit erfüllt sein. Nachfolgend werden die Tatmacht und der subjektive Tatbestand – zwei Voraussetzungen, deren Bejahung im Falle des CISO problematisch sein könnte – näher analysiert.

I. Tatmacht

Die Tatmacht setzt voraus, dass die gebotene Handlung, um den tatbestandsmässigen Erfolg abzuwenden, dem Täter möglich sein musste.[92] Das Vorhandensein der Tatmacht wird stark vom Einzelfall abhängen. Trotzdem können gewisse Pauschalisierungen gemacht werden.

In vielen Fällen wird die Tatmacht aufgrund fehlender Ressourcen wegfallen. Hat der CISO keine finanziellen oder personellen Mittel, um eine Sicherheitslücke zu schliessen oder diese gar zu bemerken, wird es ihm nicht möglich sein, einen Cyberangriff zu verhindern. Da das Gebiet der Cybersecurity neu ist, werden die finanziellen Ausgaben im Zusammenhang mit der Cybersicherheit nicht genügend im Budget des Unternehmens berücksichtigt.[93] Dazu kommt, dass Cybersicherheit oft als Teil der Infor-

92 Donatsch/Godenzi/Tag Strafrecht I, S. 338; Niggli/Muskens BSK StGB, Art. 11 Rn. 120; Stratenwerth Strafrecht AT I, § 14 Rn. 41.

93 Heidrick & Struggles 2024 Survey, S. 27: 41 % der CISOs verneinen, dass ihnen genügend Ressourcen zur Verfügung gestellt werden; Hunziker/Trachsel EXPERTfocus, S. 615; vgl. Proofpoint 2024 Report, S. 14: Die Mehrheit der ca. 1600 befragten CISOs berichten abnehmende Budgets für die Cybersicherheit aufgrund negativer Wirtschaftsentwicklungen.

matik gesehen wird und damit lediglich einen kleinen Teil des Gesamtbudgets für die Informatik erhält.[94] Selbst der Schweizer Bund räumt nur ein bescheidenes Budget für die eigene Cybersicherheit ein.[95] Aber auch wenn genügend finanzielle Mittel zur Verfügung gestellt werden, fehlt oft fachkundiges Personal, welches eingestellt werden kann, um den CISO zu unterstützen.[96]

Des Weiteren stellen Cyberbedrohungen ein neueres Phänomen dar, wobei die Täter teils höchst professionell arbeiten und viele Ressourcen zur Verfügung haben.[97] Für diese Einzeltäter, Organisationen oder gar staatlich unterstützten Akteure stellt das Ausnutzen von Sicherheitslücken ihre Haupttätigkeit dar, wodurch sie sich schnell weiterentwickeln und effektiv handeln können. Im Gegensatz dazu haben CISOs eine Vielzahl von Aufgaben, welche sie erfüllen, und sie müssen antizipierend handeln. Die Effizienz der Cyberkriminellen zeigt sich auch an der grossen Menge von erfolgten Cyberangriffen.[98] Aufgrund der hohen Anzahl ist es unmöglich, jede einzelne Sicherheitslücke zu schliessen.[99] Sogar staatliche Institutionen werden davon betroffen und können Opfer solcher Angriffe sein.[100] Wenn selbst Staaten überfordert sind, werden sicherlich CISOs von privaten Unternehmen nicht in der Lage sein, sämtliche Angriffe zu verhindern.[101]

Schliesslich ist auch zu beachten, dass der CISO nicht Kontrolle über alle Faktoren hat, welche zu erfolgreichen Cyberangriffen führen können. Häu-

94 FINMA Aufsichtsmitteilung 03/2024, S. 5; Wipro State of Cybersecurity, S. 23: 13 % der europäischen Organisationen ordnen über 12 % des Informatikbudgets der Cybersicherheit zu.

95 Donzé/Humbel/Plüss NZZ am Sonntag, S. 11.

96 Kaspersky Lab What it Takes to Be a CISO, S. 15 f.; vgl. auch Heidrick & Struggles 2024 Survey, S. 23; Wipro State of Cybersecurity, S. 17.

97 NCSC Allgemeine Bedrohungsformen, S. 3 ff.

98 BACS Halbjahresbericht 2024/I, S. 6; BFS Digitale Kriminalität.

99 Vgl. Donzé/Humbel/Plüss NZZ am Sonntag, S. 11.

100 BACS Halbjahresbericht 2024/I, S. 34 ff.: Im Kontext der Europawahlen beispielsweise fanden 2024 erfolgreiche Cyberangriffe auf Websites niederländischer und deutscher Parteien statt. 2022 und 2023 verschafften sich Cybertäter Zugriff auf das niederländische Verteidigungsministerium und 2024 wurden E-Mail-Konten französischer diplomatischer Einrichtungen kompromittiert. Auch Schweizer Parlamentarier waren 2021 betroffen; vgl. WEF Global Risk Report, S. 30, 90: Die Schweiz nannte Cyberunsicherheit – gemeint werden Risiken wie beispielsweise Cyber-Spionage – als fünfthöchste Bedrohung.

101 Vgl. auch Kaspersky Lab What it Takes to Be a CISO, S. 11: 86 % der befragten CISOs halten Verletzungen der Cybersicherheit für unvermeidlich; Proofpoint 2024 Report, S. 4 f.: 70 % der CISOs fühlen sich in den nächsten 12 Monaten dem Risiko eines Cyberangriffs ausgesetzt.

fige Attacken sind solche, wo Arbeitnehmer des Unternehmens getäuscht werden und dadurch Zugang zum System erlangt wird.[102] Eine grosse Aufgabe des CISO beinhaltet dementsprechend die Schulung der Arbeitnehmer. Aber auch wenn diese durchgeführt wird, ist schlussendlich jeder einzelne Arbeitnehmer dafür verantwortlich, das erlernte Wissen auch umzusetzen. Wird trotz ausreichender Bemühungen des CISO beispielsweise ein E-Mail Link angewählt, hat der CISO keine Tatmacht darüber.

Die Tatmacht wird folglich in den meisten Fällen verneint werden müssen, wodurch die Strafbarkeit des CISO auch aufgrund dieser Voraussetzung ausgeschlossen wird.

II. Subjektiver Tatbestand

Selbst wenn der objektive Tatbestand bejaht wäre, müsste der subjektive Tatbestand erfüllt sein. Die meisten einschlägigen Tatbestände sind nicht unter der Fahrlässigkeit strafbar, weshalb der CISO mindestens mit Eventualvorsatz handeln müsste.[103]

Zur Abgrenzung von der Fahrlässigkeit dient in erster Linie die Willenskomponente. Dabei nimmt ein eventualvorsätzlich handelnder Täter den Erfolg in Kauf, während ein fahrlässig handelnder Täter darauf vertraut, der Erfolg werde nicht eintreten.[104] Gemäss Rechtsprechung muss für die Abgrenzung zwischen Eventualvorsatz und Fahrlässigkeit zusätzlich die Grösse des dem Täter bekannten Risikos der Tatbestandsverwirklichung und die Schwere der Sorgfaltspflichtverletzung berücksichtigt werden.[105]

Das Risiko eines Cybervorfalls ist sehr hoch.[106] Besteht eine Sicherheitslücke, ist wahrscheinlich, dass Cyberkriminelle versuchen werden, diese auszunutzen. Dies ist dem CISO vermutlich bewusst. Eine schwere Sorgfaltspflichtverletzung ist denkbar, wenn ein CISO trotz Kenntnis keine interne Meldung über ein Cyberrisiko, welches er selbst nicht beseitigen kann, erstattet. Tut er dies zwar, aber die Geschäftsleitung bleibt untätig, könnte eine schwere Pflichtverletzung begründet werden, wenn er nicht

102 Proofpoint 2024 Report, S. 9 f.: 42 % der CISOs nennen unvorsichtige Arbeitnehmer, 36 % auch vorsätzlich handelnde Arbeitnehmer als Grund für Datenverlust; vgl. FINMA Aufsichtsmitteilung 03/2024, S. 6 f.

103 Siehe § 3 A.

104 Statt vieler: BGE 96 IV 99.

105 BGE 125 IV 242 E. 3c; BGE 119 IV E. 5a.

106 Vgl. §3 B.II; §3 C.I.

erneut nachfragt.[107] Das Bundesgericht würde in diesen Fällen vermutlich den Eventualvorsatz bejahen.

Eine solche Überdehnung des Vorsatzes erscheint problematisch. Durch die Annahme, die Inkaufnahme sei bei hohem Risiko gegeben, wird die Willenskomponente obsolet. Der CISO wird meistens nicht in Kauf nehmen, dass ein Cyberangriff geschieht. Stattdessen ist es naheliegender, dass er mit dem Gedanken, er habe mehr Zeit, die Sicherheitslücke nicht zeitnah meldet oder handelt. Denn vom reinen Entdecken einer Sicherheitslücke kann nicht auf einen unmittelbaren Cyberangriff geschlossen werden, insbesondere, wenn diese Lücke zuvor bereits länger bestand. Der CISO wird somit mutmasslich darauf vertrauen, dass ein zwischenzeitlicher Angriff ausbleiben wird. Daher wird hier die Meinung vertreten, der subjektive Tatbestand müsste in den überwiegenden Fällen verneint werden.

§ 4 Hinterfragung des Strafbedürfnisses

Das Strafrecht soll eine ultima ratio darstellen. Im Falle einer Sorgfaltspflichtverletzung durch den CISO, welche zu einem Schaden für das Unternehmen führt, kann der CISO bei Bedarf aufgrund seines Vertrags zivilrechtlich zur Haftung gezogen werden. Geschieht dies nicht, muss davon ausgegangen werden, dass das Bedürfnis des Unternehmens fehlt, keine Sorgfaltspflichtverletzung eingetreten ist oder dass der CISO kein Verschulden trägt. Daher ist fraglich, ob eine strafrechtliche Regelung nötig ist.

Besonders bei einer weiten und daher unbestimmten Strafbestimmung wie Art. 11 StGB muss Zurückhaltung geboten werden. Natürlich besteht ein Strafbedürfnis der Öffentlichkeit, die ein Interesse an Datensicherheit hat, der geschädigten Unternehmen und gewissermassen des Staates, da auch dieser Ziel von Cyberangriffen ist. Nur weil der primäre Täter – der Cyberkriminelle selbst – schwierig zu greifen ist, kann jedoch nicht stattdessen eine andere Person als Sündenbock dienen. Es ist Natur eines Rechtsstaats, dass nicht immer jemand strafrechtlich zur Verantwortung gezogen werden kann. Dies im Interesse, dass niemand fälschlicherweise bestraft wird.

Die Argumente, den CISO strafrechtlich verantwortlich zu machen, sind sodann zu stark auf das Resultat – also die Strafbarkeit – ausgerichtet.

107 Vgl. CISO-Alliance Berufsbild CISO, S. 6: Der CISO muss Durchsetzungsvermögen haben.

Die Auslegung des Strafrechts aus der Perspektive, man wolle lediglich ein befriedigendes Ergebnis, ist zu verneinen, da dies eine Überdehnung des in Art. 1 StGB statuierten Legalitätsprinzips bedeutet. Damit wäre nicht mehr voraussehbar, welches Verhalten strafrechtliche Folgen mit sich ziehen kann.

Zuletzt muss der Zweck der strafrechtlichen Bestimmungen betont werden. Anhand des Strafrechts sollen rechtswidrige Cyberangriffe verhindert oder zumindest deren Folgen minimieret werden. Da Cyberattacken aber so häufig sind, müssen CISOs unterstützt werden, anstatt sie durch ein hohes Risiko strafrechtlicher Verurteilungen abzuschrecken. Eine strafrechtliche Verantwortlichkeit des CISO wäre also für die Verhinderung von Cyberangriffen kontraproduktiv und würde sich somit gegen die Zielsetzung des Strafrechts richten.

§ 5 Fazit

Ziel dieses Beitrags war es, die Strafbarkeit des CISO im Rahmen des StGB durch unechte Unterlassung zu analysieren. Aus dem besonderen Teil des StGB wurden vier Tatbestände identifiziert, welche bei einem Cybervorfall relevant sein könnten: Das unbefugte Eindringen in ein Datenverarbeitungssystem, die Sachbeschädigung, die ungetreue Geschäftsbesorgung und die Nötigung.

Die Analyse der Garantenstellung ergab, dass der CISO grundsätzlich keine vertragliche Garantenstellung innehaben kann, da die Verantwortlichkeit für die Cybersicherheit zum Risikomanagement gehört. Dieses ist gemäss Art. 716a Abs. 1 OR eine unübertragbare Aufgabe des Verwaltungsrats. Für die Garantenstellung aus Ingerenz wurde differenziert, ob die Sicherheitslücke auf das Verhalten des CISO zurückzuführen ist. Ist dies zu bejahen, kann man eine Garantenstellung unter anderem aufgrund des Vertrauensgrundsatzes und der Eigenverantwortung des Unternehmens ausschliessen. Das reine Aufrechterhalten einer Lücke, die der CISO nicht zu verantworten hat, begründet auch keine Garantenstellung, da nur die Schaffung oder Erhöhung einer Gefahr strafbar wäre. Weiter wurde die Geschäftsherrenhaftung wegen der fehlenden Geschäftsherreneigenschaft abgelehnt. In den Vergleichen zum Compliance Officer und Datenschutzberater ergab sich schliesslich, dass eine direkte Analogie grundsätzlich nicht möglich ist.

Für die Strafbarkeit ist zusätzlich die Tatmacht nötig. Diese wird regelmässig verneint werden müssen aufgrund des grossen Umfangs der Cyberbedrohungen und aufgrund mangelnder Ressourcen. Somit wird die Strafbarkeit des CISO spätestens hier abgelehnt. Der auch vorausgesetzte Eventualvorsatz würde gemäss Bundesgericht vermutlich bejaht werden, ist nach der hier vertretenen Ansicht aber zu verneinen.

Zuletzt wurde besprochen, ob eine Strafbarkeit des CISO erwünscht wäre. Zwar besteht ein Strafbedürfnis, weil die primären Täter von Cyberangriffen schwer zu fassen sind. Jedoch muss unter anderem beachtet werden, dass eine Strafbarkeit nur zu einem ungewollten Mangel an CISOs führen könnte. Würde eine Strafbarkeit des CISO folglich entgegen der präsentierten Meinung bejaht werden, würde er lediglich als Sündenbock für die Taten von Cyberkriminellen dienen.

Literaturverzeichnis

Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar DSG. Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023.

Brockhaus Annika, IT-Sicherheit, Informationssicherheit und Cyber-Sicherheit: Wo liegen die Unterschiede?, isits AG International School of IT Security 2019, https://www.is-its.org/it-security-blog/it-sicherheit-informationssicherheit-cyber-sicherheit-unterschiede.

Bundesamt für Cybersicherheit (BACS), Halbjahresbericht 2024/I (Januar – Juni). Cybersischerheit: Lage in der Schweiz und International, 2024, https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2024-1.html.

Bundesamt für Statistik (BFS), Digitale Kriminalität, BFS-Nummer gr-d-16.04 – 12b-ind, 2024, https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/strategieindikatoren/sicherheit-vertrauen/digitale-kriminalitaet.html.

Bundesamt für Statistik (BFS), Gemeldete Cyber-Vorfälle, BFS-Nummer gr-d-16.04 – 12a-ind, 2024, https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/strategieindikatoren/sicherheit-vertrauen/cyber-vorfaelle.html.

Bundesamt für wirtschaftliche Landesversorgung (BWL), Minimalstandard zur Verbesserung der IKT-Resilienz, 2023, https://www.bwl.admin.ch/bwl/de/home/bereiche/ikt/ikt_minimalstandard.html.

Cybersecurity & Infrastructure Security Agency (CISA), What is Cybersecurity?, 2021, https://www.cisa.gov/news-events/news/what-cybersecurity.

CISO-Alliance, Berufsbild CISO, Ausgabe 03/2024, https://www.ciso-alliance.de/fileadmin/downloads/Berufsbilder/1_-_Berufsbild_CISO_v1.0.pdf.

Donatsch Andreas/Godenzi Gunhild/Tag Brigitte, Strafrecht I. Verbrechenslehre, 10. Aufl., Zürich/Genf 2022.

Donzé René/Humbel Georg/Plüss Mirko, Hackerangriffe: Ungeschützt im Auge des Hurrikans, NZZ am Sonntag vom 18.6.2023, Nr. 25, S.11.

Eidgenössische Bankenkommission, Rundschreiben betreffend Richtlinien zur Bekämpfung und Verhinderung der Geldwäscherei vom 26. März 1998. EBK-RS 98/1 Geldwäscherei, https://www.finma.ch/FinmaArchiv/ebk/d/publik/mitteil/1998/m3-98-2.pdf.

Eidgenössische Finanzmarktaufsicht (FINMA), Aufsichtsmitteilung 03/2024. Erkenntnisse aus der Cyber-Risiko-Aufsichtstätigkeit, Präzisierung zur FINMA-Aufsichtsmitteilung 05/2020 und zu szenariobezogenen Cyber-Übungen, 2024, https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20160707-finma-aufsichtsmitteilung-03–2024.pdf?sc_lang=de&hash=666EEE255C04FB42F01BFD0BC6C80191.

Eidgenössische Finanzmarktaufsicht (FINMA), Rundschreiben 2023/1. Operationelle Risiken und Resilienz – Banken. Management der operationellen Risiken und Sicherstellung der operationellen Resilienz, 2022, https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023–01–20221207.pdf.

Eidgenössische Finanzmarktaufsicht (FINMA), Aufsichtsmitteilung 05/2020. Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG, 2020, https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20200507-finma-aufsichtsmitteilung-05–2020.pdf.

Eidgenössische Finanzmarktaufsicht (FINMA), Rundschreiben 2017/1. Corporate Governance – Banken. Corporate Governance, Risikomanagement und interne Kontrollen bei Banken, 2016, https://www.finma.ch/de/~/media/finma/dokumente/rundschreiben-archiv/2017/rs-17-01/finma-rs-2017-01-20210506_de.pdf?sc_lang=de&hash=7F530363D0237EC203704EFC8E32C624.

Heidrick & Struggles, 2024 Global Chief Information Security Officer Organization and Compensation Survey, 2024, https://www.heidrick.com/-/media/heidrickcom/publications-and-reports/2024-global-ciso-organization-and-compensation-survey.pdf.

Hunziker Stefan/Trachsel Viviane, Cyber Risk Governance in Schweizer Unternehmen. Kernbotschaften einer Studie aus der Sicht von Risk Manager und CISO, EXPERTfocus Dezember 2022, S. 612–616, https://doi.org/10.5281/zenodo.8386970.

Kaspersky Lab, What it Takes to Be a CISO: Success and Leadership in Corporate IT Security, 2018, https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2020/05/15131106/What-It-Takes-to-Be-a-CISO_-Success-and-Leadership-in-Corporate-IT-Security-2018.pdf.

Mozur Paul, China Appears to Attack GitHub by Diverting Web Traffic, The New York Times vom 30.3.2015, https://www.nytimes.com/2015/03/31/technology/china-appears-to-attack-github-by-diverting-web-traffic.html?smid=url-share.

Nagel Thomas, Interessenkonflikte des Compliance Officers. Mit besonderer Betrachtung der Meldepflicht nach Art. 9 GwG, SJZ 117/2021, S. 102–109.

Nationales Zentrum für Cybersicherheit (NCSC), Allgemeine Bedrohungsformen, Täter und Werkzeuge, 2021, https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/fachberichte/allgemeine-bedrohungsformen.html.

Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar. Strafrecht II. Art. 137–392 StGB, Jugendstrafgesetz, 4. Aufl., Basel 2019.

Pieth Mark, Wirtschaftsstrafrecht, Basel 2016.

Proofpoint, Report 2024 Voice of the CISO. Global Insights into CISO Challenges, Expectations and Priorities, 2024, https://nationalcioreview.com/wp-content/uploads/2024/06/pfpt-us-wp-voice-of-the-CISO-report.pdf.

Roxin Claus, Ingerenz und objektive Zurechnung, in Donatsch Andreas/Forster Marc/Schwarzenegger Christian (Hrsg.), Strafrecht, Strafprozessrecht und Menschenrechte. Festschrift für Stefan Trechsel, Zürich et. al, S. 551–567.

Steiner Thomas/Morand Anne-Sophie/Hürlimann Daniel (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz, 2023, https://doi.org/10.17176/20230825-095533-0, https://doi.org/10.17176/20230812-163522-0.

Stratenwerth Günter, Schweizerisches Strafrecht. Allgemeiner Teil I: Die Straftat, 5. Aufl., Bern 2024.

Stratenwerth Günther/Bommer Felix, Schweizerisches Strafrecht. Besonderer Teil I: Straftaten gegen Individualinteressen, 8. Aufl., Bern 2022.

Trechsel Stefan/Noll Peter/Pieth Mark, Schweizerisches Strafrecht Allgemeiner Teil I. Allgemeine Voraussetzungen der Strafbarkeit, 7. Aufl., Zürich et al. 2017.

Von Rotz Madeleine, Die Garantenstellung und die Garantenpflicht des Compliance Officers einer Bank unter Berücksichtigung der strafrechtlichen Bestimmungen des Finanzmarktrechts, Zürich 2019.

Watter Rolf/Vogt Hans-Ueli (Hrsg.), Basler Kommentar. Obligationenrecht II. Art. 530–964 OR inkl. Schlussbestimmungen, 6. Aufl., Basel 2024.

Wipro, State of Cybersecurity Report. Cyber Resilience in an Age of Continuous Disruption, 2023, https://www.wipro.com/cybersecurity/state-of-cybersecurity-report-2023/.

Woodtli Nadine, Cyberattacken nehmen zu. So brutal erpressen Hacker Schweizer Firmen, SRF vom 13.10.2021, https://www.srf.ch/news/schweiz/cyberattacken-nehmen-zu-so-brutal-erpressen-hacker-schweizer-firmen.

World Economic Forum (WEF), The Global Risks Report 2025. 20th Edition. Insight Report, 2025, https://www.weforum.org/publications/global-risks-report-2025/.

Materialienverzeichnis

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941 ff., https://www.fedlex.admin.ch/eli/fga/2017/2057/de.

Botschaft zum Bundesgesetz über die Eidgenössische Finanzmarktaufsicht vom 1. Februar 2006, BBl 2006 2829 ff., https://www.fedlex.admin.ch/eli/fga/2006/303/de.