Mitarbeiter-information

zur Verhinderung von Betrug und sonstigen strafbaren Handlungen

kompakt

DG VERLAG

Mitarbeiterinformation

zur Verhinderung von Betrug und sonstigen strafbaren Handlungen

Muster

DG VERLAG

Muster

Lizenzausgabe für die genossenschaftliche FinanzGruppe:

DG Nexolution eG, Leipziger Straße 35, 65191 Wiesbaden

© 4. Auflage 2022 by Bank-Verlag GmbH, Wendelinstraße 1, 50933 Köln

Das Werk einschließlich seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Hinweise, Ratschläge und Wertungen sind von den Autoren und dem Verlag sorgfältig erwogen und geprüft, dennoch kann eine Garantie nicht übernommen werden. Eine Haftung der Autoren bzw. des Verlages und seiner Beauftragten für Personen-, Sach- und Vermögensschäden ist ausgeschlossen.

Der Inhalt dieses Buches wurde auf FSC-zertifiziertes Papier gedruckt.

Druck: ICS Communications-Service GmbH, Troisdorf

Bestell-Nr.: 963 020

Inhaltsverzeichnis

Muster

Über folgenden Link erhalten Sie weiterführende und aktualisierte Informationen zum Thema „Verhinderung von Betrug und sonstigen strafbaren Handlungen“:

Muster

1 Zielsetzung

Banken und Finanzdienstleister haben von jeher die Pflicht, die Zuverlässigkeit ihrer Mitarbeiter zu überwachen und Gefährdungen des ihnen anvertrauten Kapitals durch kriminelle Handlungen vorzubeugen. Schon in der ersten Fassung des Geldwäschegesetzes vom 25. Oktober 1993 gehörte zu den internen Sicherungsmaßnahmen in § 14 Abs. 2 Ziff. 3 GWG „die Sicherstellung, dass die Beschäftigten, die befugt sind, bare und unbare Finanztransaktionen durchzuführen, zuverlässig sind".

Mit dem 4. Finanzmarktförderungsgesetz vom 26. Juni 2002 wurde dann erstmalig eine Vorschrift in das KWG eingefügt, die den Instituten auferlegte, Prävention gegen betrugsähnliche Handlungen in ihre Organisationsstrukturen einzubeziehen (damals § 25a Abs. 1, Satz 3 Nr. 6 KWG).

Schon seit der Neufassung des Gesetzes im Jahr 2008 hat die „Verhinderung von betrügerischen Handlungen" jeglichen schädigenden Angriff auf das Institut im Rahmen des angemessenen Risikomanagements möglichst zu unterbinden. Damit rücken auch **Schadhandlungen Dritter**, die nicht bei einem Finanzdienstleister angestellt sind, in den Fokus.

Mit der Neuformulierung der Anforderungen im Jahr 2017, die mit der Umsetzung der 4. EU-Geldwäscherichtlinie einherging, wurden klare Kriterien formuliert, welche Art von Transaktionen besondere Aufmerksamkeit bei der Prävention verlangen: besonders komplexe oder große Transaktionen mit möglicherweise ungewöhnlichem Ablauf oder ohne erkennbaren wirtschaftlichen oder rechtlichen Zweck. Jeder Mitarbeiter eines Kreditinstituts oder eines Finanzdienstleisters ist gehalten, diesen Konstellationen besondere Aufmerksamkeit zu widmen.

Mit der 5. EU-Geldwäscherichtlinie im Jahr 2018 und der 6. EU-Geldwäscherichtlinie im Jahr 2021 ging eine Erweiterung der bisherigen Anforderungen einher, die auch Auswirkungen auf die Betrugsprävention hat: Da

Muster

nunmehr jede strafbare Handlung taugliche Vortat der Geldwäsche im Sinne des § 261 StGB sein kann, sind die gebotenen Kontrollmechanismen auch insoweit auf alle Straftaten mit möglichen Vermögenseinbußen für das Institut auszuweiten.

Fast täglich sind in der Presse Meldungen wie diese zu lesen:

Der illegale Handel mit Konten floriert
„Der illegale Handel mit Bankverbindungen, die Ebay-Betrügern oder Betreibern von Fake-Shops offenstehen, floriert.
(…)
Der Schaden geht mittlerweile in die Millionen."

(Quelle: Süddeutsche Zeitung Online-Artikel vom 07.06.2019.)

Muster

Neben dem Risiko sanktionsfähiger Handlungen der Angestellten und Leitungspersonen von Banken und Finanzdienstleistern aufgrund eigenen Fehlverhaltens gehen für Banken und Finanzdienstleister auch finanzielle Risiken mit dem inkriminierten Verhalten von Kunden oder sonstigen Dritten einher. In der Folge sind auch Schlagzeilen wie die folgende nicht selten:

Bank muss trotz Weitergabe von Zugangsdaten an Ehepartner zahlen
„Tätigt ein Ehepartner Bankgeschäfte mit dem Login des anderen, ist es unerheblich, wer Opfer einer Betrugsmasche im Internet wird. Das Finanzinstitut muss den entstandenen Schaden jedenfalls zahlen."

(Quelle: FAZ vom 08.03.2021 betreffend das Urteil vom Landgericht Nürnberg-Erlangen – Az. 6 O 5935/19.)

Der Bankenverband warnt in seiner Broschüre „Zielscheibe Unternehmen: Cyberkriminalität":

Zielscheibe Unternehmen: Cyberkriminalität

„Hinter dem Begriff „Social Engineering" verbergen sich Telefonanrufe in böswilliger Absicht, E-Mails oder andere Manipulationen, die Mitarbeiter dazu bringen sollen, bestimmte Handlungen auszuführen oder Informationen preiszugeben. Vielen der … Betrugsarten geht eine gezielte Beschaffung von Informationen über das Unternehmen voraus (zum Beispiel über den Internetauftritt, öffentliche Register, beruflich und privat genutzte soziale Netzwerke). Die Strategien der Angreifer sind vielfältig. Allen gemein ist, dass menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt werden. Mitarbeiter werden so manipuliert, dass sie gutgläubig handeln und dabei das eigene Unternehmen unbewusst schädigen."

(Quelle: Bundesverband deutscher Banken e.V. (Hrsg.): Zielscheibe Unternehmen: Cyberkriminalität, September 2019, S. 2.)

Muster

Angriffe Dritter, die die vorhandenen Systeme des Instituts nutzen, nehmen mit der Erweiterung automatisierter und digitalisierter Dienstleistungsangebote stark zu. Auch „Phishing" und „Skimming" sind aktuelle Beispiele der Schädigung des Kunden durch Missbrauch von Finanzdienstleistungen. Weitere Beispiele für den Missbrauch von Bankdienstleistungen zu betrügerischen Zwecken gibt es unzählige. Ihnen allen ist gemeinsam, dass mit der Neuregelung des § 25h KWG die erweiterte Verpflichtung an die Banken und Finanzdienstleister herangetragen wird, dagegen systemische Vorkehrungen zu treffen, und zwar im Einzelfall wie generell.

Polizei fasst Führungsriege von betrügerischer Finanzplattform

Vor wenigen Tagen konnten deutsche Staatsanwälte und Polizeibeamte abermals die Pläne von internationalen Drahtziehern des betrügerischen „Cybertrading" durchkreuzen. Wie die Zentralstelle Cybercrime Bayern (ZCB) aus Bamberg und diverse Polizeibehörden aus Bayern mitteilten, wurden schon am 19. Oktober in Georgien und Israel 11 Haftbefehle erfolgreich vollstreckt und 15 Gewerbeobjekte durchsucht. …

Wie in anderen Ermittlungskomplexen spiegelten die Verdächtigen potentiellen Kunden vor, über digitale Plattformen mit hochriskanten Finanzinstrumenten wie Contracts for Differences (CDF), Forex und Kryptowährungen handeln zu können. …

Laut bisherigen Erkenntnissen fanden eine Investition oder Platzierung von Optionen sowie spätere Gewinnausschüttung nie statt.

(Quelle: FAZ vom 28. Oktober 2021, S. 25.)

Muster

Der **Schutz des Instituts und seines Vermögens** sowie der Kunden und des Kundenvermögens ist damit zweigeteilt: Erstens sind gegen Handlungen, die aus dem Institut heraus, also durch Mitarbeiter zulasten des Instituts oder des Kunden erfolgen, Schutzmechanismen zu implementieren. Zweitens sind Angriffe Dritter auf das Vermögen des Instituts ebenfalls bestmöglich systemisch zu verhindern. ***Beides ist nur denkbar mit Ihrer Hilfe.*** Diese Broschüre möchte Sie deshalb informieren, welche Aufgaben Sie in diesem Zusammenhang übernehmen sollen und wo Ihre Aufmerksamkeit als Mitarbeiter besonders gefordert ist.

963 020