IFAM INFO NR 1
März 2022
INSTITUT FÜR AUFSICHTSRAT-MITBESTIMMUNG

INTERNES KONTROLLSYSTEM UND ORGANISATIONSVERSCHULDEN IN CYBERCRIME-ZEITEN

HANNES SCHNELLER

Mag. Hannes Schneller, Abteilung Sozialpolitik der AK Wien

Ein österreichisches Hightech-Industrieunternehmen war einem in Europa bis dato unbekannten Cybercrime-Typus mit dramatischen finanziellen Folgen zum Opfer gefallen: 54 Mio. Euro Betrugssumme, davon jedenfalls 42 Mio. verloren. Der Rest konnte auf ausländischen Konten noch rechtzeitig eingefroren werden.

„Fake President Fraud“ (fraud: Betrug) nennt sich diese Betrugsmasche, eine spezielle Variante des *„Social Engineering“*. Sie besteht im Kern aus der dauerhaften *Manipulation* von Mitarbeiter:innen mithilfe von Internet und Intranet, um Passwörter, PINs oder TANs nach monatelangem „in Sicherheit wiegen“ zu erlangen. Dass diese „Masche“ zu den Tatzeitpunkten, also bei Vornahme der massiven Manipulationen einer Finanzbuchhalterin, zumindest im deutschsprachigen Raum noch nicht bekannt war, rettete dem CEO schadenersatzrechtlich „den Hals“. Er hatte die internen Abläufe, Kontrollmechanismen und die (IT-)Sicherheitsarchitektur des Unternehmens laut OGH sehr wohl *nach größen-, komplexitäts- und branchenüblichen* sowie damals im Jahr 2014/15 „gerade noch aktuellen“ *Sicherheitsstandards* organisiert.

Der Oberste Gerichtshof verneinte daher ein Organisationsverschulden des CEO. Die auf die betrügerischen Tricks und Manipulationen „hereingefallene“ Finanzbuchhaltungs-Angestellte und andere Mitarbeiter:innen – etwa aus dem IT-Bereich des Konzerns – sind allerdings noch in laufende Schadenersatzprozesse verstrickt. Es ist zu hoffen, dass sich die den CEO betreffende haftungsbefreiende Entscheidung auch auf diese Verfahren positiv auswirkt.

OGH-Leitsätze zu IKS, Innenrevision und Controlling

Im Folgenden werden nicht die komplexen sozialpsychologischen Mechanismen des Betrugs dargestellt, sondern einige Leitsätze des OGH zu sorgfaltsgemäßer Organisation von IKS (Interne Kontrollsysteme) und IT-Sicherheit. Aufsichtsratsmitglieder sollten sich regelmäßig – zumindest jährlich, bei realen Bedrohungs- oder Verdachtsfällen aber häufiger – von der Geschäftsleitung berichten und nachweisen lassen, dass die von ihnen überwachte Gesellschaft *cyber-angriffsfest* ist.

Bis zu dieser OGH Entscheidung aus 2021 war in der Judikatur unklar, ob das gesetzlich vorgeschriebene interne Kontrollsystem (vgl. § 22 GmbHG, § 82 AktG) nur der Insolvenz-Prophylaxe dient oder ob es auch kriminellen Schädigungsabsichten vorbeugen soll. Der OGH entschied nun, dass ein sehr allgemeiner Normzweck bestehe, nämlich die generelle Sicherung des Gesellschaftsvermögens durch adäquate Maßnahmen, Methoden und „Check"-Prozesse im Rechnungswesen, Riskmanagement und Controlling.

Zweck der Kontrollsysteme
Das Ziel eines internen Kontrollsystems ist es, das Vermögen der Gesellschaft (und allenfalls ihrer Töchter) zu sichern, die Genauigkeit und Zuverlässigkeit der Abrechnungen zu gewährleisten und die Einhaltung der Geschäftspolitik zu unterstützen.

Regelmäßig basiert es auf Überwachungsmaßnahmen organisatorischer und EDV-technischer Art, wie Unterschriftenregelungen, EDV-Zugriffsbeschränkungen oder Arbeitsanweisungen. Kontrollmaßnahmen, die manuell oder automatisationsunterstützt etabliert sind, etwa Plausibilitätsprüfungen in der Buchhaltungssoftware, sind ein wichtiger Bestandteil. Hinzu kommen Richtlinien und Regelwerke zur Definition von Standardprozessen sowie deren Dokumentation und eine interne Revision, die in diesem Zusammenhang die Aufgabe hat, bei wiederkehrenden Prüfungen die Effizienz eines IKS zu kontrollieren.

Im betroffenen Unternehmen unterlag die Zahlungsfreigabe genau definierten, automatisierten Prozessen mit mehrfachen unabhängig voneinander erforderlichen Autorisierungen unter Einhaltung des Mehraugenprinzips. Auch der letzte Schritt der Kette, die Erteilung des Überweisungsauftrags an die Bank, war dahingehend geregelt, dass zwei verschiedene Bankkarten zu verwenden waren, die von zwei verschiedenen Angestellten der Finanzbuchhaltungsabteilung zu verwahren und zu verwenden gewesen wären. Das IKS war punkto Zahlungsfreigaben daher *ex ante* betrachtet gesetzeskonform in Hinblick auf die Größe, Komplexität und Branche des Unternehmens. [*ex post*, im Nachhinein ist Mensch immer klüger…], so der OGH.

Wie misstrauisch müssen Geschäftsführung oder Aufsichtsorgan sein?
Der OGH geht in seinem Erkenntnis davon aus, dass nicht davon ausgegangen werden kann, dass jene höchst professionell organisierte, mit offenkundig erheblichem Rechercheaufwand ausgeklügelte und auf mehreren kommunikativen Ebenen ausgeführte Angriffsmethode, die zum Schadensfall geführt hat, vor Ende 2015 im deutschsprachigen Raum bereits bekannt war. Die Methode bestand insbesondere aus einem monatelangen „Umgarnen" und „Einlullen" einer Finanzbuchhaltungsangestellten. Sie geht über die herkömmlichen, durch ihre zahlreichen Fehler und plumpen Formulierungen leicht als Betrugsversuch erkennbaren E-Mails erheblich hinaus.

Die Strategie dieser speziellen Form ist nicht auf eine Täuschung entscheidungsbefugter Personen ausgelegt, sondern auf die Umgehung oder unautorisierte Nutzung von vorhandenen Prozessen durch geschickte Manipulation und Täuschung eines weisungsabhängigen Mitarbeiters der Abteilung Finanzen oder der Buchhaltung.

Cyber-Fraud Mechanismen erkennen
Die Ausnutzung menschlicher Eigenschaften ist ein zentrales Element der technologisch und psychologisch versierten bis hochprofessionellen Angreifer. Dem Mitarbeiter wird durch Vertrauensbezeugungen und Lob geschmeichelt, eine Vertrauensbasis hergestellt, die durch telefonische Kontakte und vorgebliche Beteiligung seriöser Autoritäten (hier: angebliche Finanzmarktaufsicht) verstärkt wird. Vorhandene Zweifel werden zerstreut, falsche Urkunden eingesetzt. Alles mit dem Ziel, dass der Mitarbeiter die bestehenden Sicherungssysteme bewusst, vermeintlich im Auftrag des Vorstands und im Interesse des Unternehmens ausnahmsweise zu umgehen bereit ist (vgl Fritzsche, Eigenschaften von Fake President Fraud – Grundlagen zur Risikobeurteilung, Maßnahmenableitung und Reaktion im Einzelfall, Compliance-Berater 11/2017).

Grundlage der Haftung nach § 25 GmbHG ist aber immer eine individuelle, schuldhafte Pflichtverletzung. Für das Fehlverhalten von Angestellten haften Geschäftsführer nicht schon dann, wenn es möglich war und ein Schaden eingetreten ist, sondern nur, wenn sie ihre Organisations- und Überwachungspflichten schuldhaft verletzt haben und dieses Versäumnis schadenskausal war. Von dem 2015 bestehenden Wissensstand ausgehend konnte der CEO nachweisen (Beweislastumkehr: seine Sorgfaltspflicht-Erfüllung muss der Beklagte beweisen!), dass er die Sorgfalt eines ordentlichen Kaufmanns nicht verletzt hat, insbesondere nicht durch Unterlassung von objektiv gebotenen Überwachungs- und Kontrollmaßnahmen oder Warnpflichten.

Im Volltext ist die Entscheidung des OGH vom 3.8.2021 (GZ: 8 ObA 109/20t) im RIS (www.ris.bka.gv.at) nachzulesen.

AKTUELLE INFORMATIONEN ZUM COVID-19-GESG: AUSWIRKUNGEN AUF VERSAMMLUNGEN UND FRISTEN

ELISABETH LUGGER

Foto: Lisa Lux

Elisabeth Lugger, LL.B., BA, Abteilung Sozialpolitik der AK Wien

Die COVID-19-Regelungen zu Versammlungen von Gesellschafter:innen oder Organmitgliedern sowie zur Erstellung und Offenlegung von Jahresabschlüssen, inklusive sonstiger Unterlagen der Rechnungslegung, etwa des nichtfinanziellen Berichts oder Corporate Governance-Berichts, beim Firmenbuch sind weiterhin bis 30. Juni 2022 in Kraft.

Versammlungen von Gesellschafter:innen oder Organmitgliedern

Die Versammlungen bestimmter Gesellschaften, wie Aufsichtsratssitzungen in Kapitalgesellschaften, können für die Dauer der Maßnahmen zur Verhinderung der Virusverbreitung mittels Videokonferenzen abgehalten und Beschlüsse auf andere Weise – etwa mit Umlaufbeschluss – gefasst werden. In den Gesellschaftsverträgen festgelegte Fristen und Termine bleiben nach wie vor bis spätestens 30. Juni 2022 unbeachtlich. Versammlungen der Gesellschafter:innen können weiterhin innerhalb der ersten zwölf Monate des Geschäftsjahres längstens jedoch bis 30. Juni 2022 stattfinden.

Bei Gesellschaften mit einem Bilanzstichtag

- bis inklusive 30. Juni 2021 bleibt somit die gesamte verlängerte zwölf-monatige Frist für die Abhaltung der ordentlichen Haupt- und Generalversammlungen aufrecht.
- ab dem 1. November 2021 gilt wieder die reguläre Frist von 8 Monaten.

Fristen zur Erstellung und Offenlegung des Jahresabschlusses

Für Jahresabschlüsse mit einem Bilanzstichtag vor dem 1. Oktober 2021 gilt – wenn dies infolge der Pandemie notwendig ist – die erstreckte 9-monatige Erstellungspflicht und zwölf-monatige Offenlegungspflicht. Für Bilanzstichtag ab dem 1. Oktober 2021 und vor dem 31. Jänner 2022 ergibt sich hingegen eine Einschleifregelung: Obwohl die verlängerten Fristen grundsätzlich gelten, enden die Erstellungsfrist jedenfalls am 30. Juni und die Offenlegungsfrist jedenfalls am 30. September 2022. Für Bilanzstichtage ab 31. Jänner 2022 ergibt sich nun wieder die reguläre 5-monatige Erstellungsfrist und die 9-monatige Offenlegungsfrist.

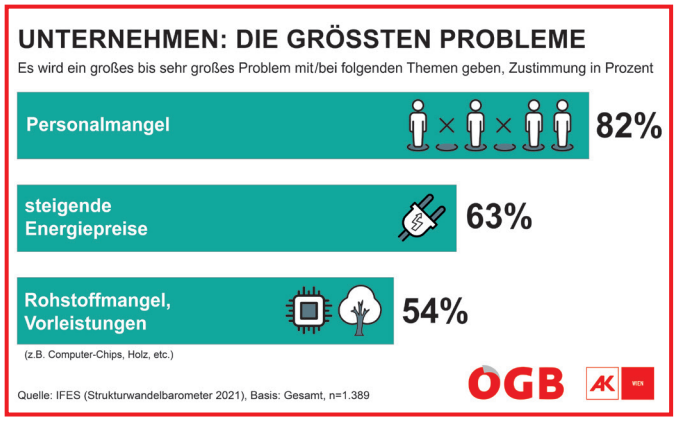
Jahresabschlüsse mit einem Bilanzstichtag am

- 30. September 2021 sind von der Geschäftsleitung innerhalb von 9 Monaten, bis spätestens 30. Juni 2022, zu erstellen und innerhalb von zwölf Monaten, bis spätestens 30. September 2022, offenzulegen.
- 31. Dezember 2021 sind innerhalb von 6 Monaten, bis spätestens 30. Juni 2022, zu erstellen und innerhalb von 9 Monaten, bis spätestens 30. September 2022, offenzulegen.

STRUKTURWANDELBAROMETER: AUF DIE BESCHÄFTIGTEN WURDE WÄHREND DER COVID-KRISE VERGESSEN

Zwei Jahre Corona haben Spuren hinterlassen

In der vom Meinungsforschungsinstitut IFES im Auftrag von AK und ÖGB alljährlich durchgeführten „Strukturwandelbarometer-Umfrage“, an der sich mehr als 1.300 Betriebsrät:innen beteiligt haben, zeigen sich diese Spuren deutlich. Denn bislang wurde in der Pandemie das Augenmerk hauptsächlich auf die Aufrechterhaltung des Betriebes gelegt. Die Beschäftigten haben alle dafür erforderlichen Maßnahmen mitgetragen, auf ihre Bedürfnisse wurde aber vergessen. Das äußert sich etwa dadurch, dass 68 % der Betriebsräte angegeben haben, dass der Arbeitsdruck extrem weitersteigt, bei 48 % verschlechtert sich das Arbeitsklima. Als größte Probleme in den nächsten Monaten sehen Betriebsräte:



www.ak.at/strukturwandelbarometer

IFAM-WAHLMODULE BIS SOMMER 2022

IFAM bietet ein breites Angebot an Wahlmodulen in den nächsten Monaten. Sie werden in Präsenz im Bildungszentrum der AK Wien stattfinden – mit Ausnahme von zwei Online Kursen.

Wir freuen uns über Anmeldungen auf der VÖGB-Homepage **www.voegb.at**

Fit & Proper im Bankenaufsichtsrat
25.–26.04.2022

Arbeitnehmervertreter:innen, die neu in den Aufsichtsrat eines Kreditinstituts entsandt werden, bekommen hier grundlegende, bankenaufsichtsrechtliche Informationen.

Im Mittelpunkt steht die Vermittlung von finanztechnischem Fachwissen, von Grundlagen des Bankwesengesetzes (BWG) und zugehöriger Verordnungen sowie relevanter Inhalte der FMA-Mindeststandards und FMA-Rundschreiben. Außerdem gibt es die Gelegenheit, die neu erworbene „Fitness“ anhand eines freiwilligen Fit & Proper-Selbsttests zu überprüfen.

Aufsichtsrat meets Abschlussprüfer
12.05.2022

Der Abschlussprüfer ist ein wichtiger Ansprechpartner des Aufsichtsrates. Hier werden die wichtigsten Prüfungstätigkeiten und Aufgaben vermittelt. Mit einem fundierten Wissen über die Prüfungstätigkeit kann der Aufsichtsrat gut mit dem Abschlussprüfer zusammenwirken. So können neben einer richtigen Finanzberichterstattung auch Verbesserungen in den Prozessen und Abläufen im Unternehmen erreicht werden.

IFRS und Aufsichtsratsarbeit im Konzern – online 16.–17.05.2022

Dieses Seminar beschäftigt sich mit speziellen Fragestellungen der Mitbestimmung auf Konzernebene und europäischer Ebene. Konzernfinanzierungsmodelle wie Cash Pooling werden ebenso erläutert wie interne Leistungsverrechnung und Gewinnabführungsverträge. Ein weiterer Seminarschwerpunkt ist die Analyse und Interpretation von IFRS und UGB Konzernabschlüssen.

Die Aufsichtsratssitzung
17.05.–19.05.2022

Theorie trifft Praxis. Die realitätsnahe Simulation einer Aufsichtsratssitzung mit erfahrenen Vorständen und Aufsichtsrät:innen aus der Wirtschaft steht im Mittelpunkt. Das bereits Erlernte wird mithilfe eines konkreten Fallbeispiels wiederholt, vertieft und zur Anwendung gebracht. Die Teilnehmer:innen erhalten inhaltliche, strategische und kommunikative Werkzeuge für die Vorbereitung und die Aufsichtsratssitzung. Ein hoher Lerneffekt wird durch Videoaufnahmen und qualifiziertes Feedback ermöglicht.

Risikomanagement und Controlling – online
19.05.2022

In diesem Online-Seminar werden ein wirksames Risikomanagementsystem und zielgerichtetes Controlling dargestellt, welche angesichts dynamischer Umwelten und zunehmender Komplexität an Bedeutung gewinnen. Arbeitnehmervertreter:innen im Aufsichtsrat sind mitverantwortlich, dass Warnsignale rechtzeitig erkannt und Maßnahmen ergriffen werden. Die wichtigsten Analyse-, Planungs- und Überwachungsinstrumente werden vorgestellt und die konkrete Arbeit eines Controllers/einer Controllerin wird vorgestellt.

Österreichische Post AG
MZ 02Z034644 M
AK Wien, Prinz Eugen Straße 20–22, 1040 Wien
VORTEILSTARIF

Herausgeber, Verleger, Medieninhaber:
Bundeskammer für Arbeiter und Angestellte
1040 Wien, Prinz-Eugen-Straße 20-22
Gestaltung: Barbara Ebeling
Alle Fotos: AK Wien, Abteilung Betriebswirtschaft
Verlags- und Herstellungsort: Wien
Offenlegung nach § 25 Mediengesetz:
siehe http://wien.arbeiterkammer.at/impressum.html