ISSN 2192-211X

Reguvis Fachmedien GmbH, Postfach 10 05 34, 50445 Köln, Jahrespreis: 317,00 € (inkl. MwSt. und Versand)

BOARD

Zeitschrift für Aufsichtsräte in Deutschland

HERAUSGEBER

Arbeitskreis deutscher Aufsichtsrat e.V. (AdAR)

Prof. Dr. Dr. h.c. Barbara Dauner-Lieb
Prof. Dr. Stefan Siepelt
Marc Tüngler
GESAMTLEITUNG

Dr. Christine Bortenlänger
Dr. Christian Bosse
Dr. Claus Buhleier
Peter Dietlmaier
Prof. Harald Eichsteller
Prof. Dr. Barbara Grunewald
Dr. Simone Hartmann
Prof. Dr. Peter Henning
Prof. Dr. Susanne Kalss
Dr. Jürgen Kunz
Prof. Dr. Ulrich Noack
Prof. Dr. Ulrich Seibert
Dr. Mirko Sickinger
Prof. Dr. Stefan Simon
Prof. Dr. Michèle Sutter-Rüdisser
Prof. Dr. Jochen Vetter
Prof. Dr. Christian Zwirner

IN KOOPERATION MIT
Deutsche Schutzvereinigung für Wertpapierbesitz e.V. (DSW)

Deutsches Aktieninstitut
Kapital. Markt. Kompetenz.

Dr. Thomas Gennert
Vorstandsvergütung und ESG – kein Vergütungssystem mehr ohne?

Prof. Dr. iur. Alexander Reuter
Aufsichtsorgane und ESG-Regeln

Christoph Schlossarek, Dr. Ricardo Gomez, Dr. Anke Nestler, Oliver Müller
Investigations aus Sicht des Aufsichtsrates

Peter Dietlmaier, Michael Schoenenberger
Ehrlichkeit und Authentizität anstatt Inszenierung

Klaus Brisch, Marco Müller-ter Jung
KI-basierte Unternehmensentscheidungen und Rechtsrahmen

4
2023

BOARD · August 2023 · S. 129–172

Reguvis

www.reguvis.de

EDITORIAL 129

AUFSÄTZE

Dr. Thomas Gennert
Vorstandsvergütung und ESG – kein Vergütungssystem mehr ohne? 131

Prof. Dr. iur. Alexander Reuter
Aufsichtsorgane und ESG-Regeln 135

Christoph Schlossarek, Dr. Ricardo Gomez, Dr. Anke Nestler, Oliver Müller
Investigations aus Sicht des Aufsichtsrates 141

Peter Dietlmaier, Michael Schoenenberger
Ehrlichkeit und Authentizität anstatt Inszenierung 145

Heike Adam
Inflation is here to stay – Ihr Einfluss auf die Arbeit von Aufsichtsräten und Beiräten 147

Klaus Brisch, Marco Müller-ter Jung
KI-basierte Unternehmensentscheidungen und Rechtsrahmen 150

Ansgar Dirkmann
Sechs Must-haves für eine sichere und effiziente Aufsichtsrats- und Gremienkommunikation 154

Matthias Goldbeck
Hope is not a plan – was Cyber-Angriffe und Corona gemeinsam haben 156

ÖFFENTLICHE UNTERNEHMEN

Lars Scheider
Compliance-Management im Rahmen der Nachhaltigkeitsberichterstattung im Public Sektor 159

DAS AUFSICHTSRATSBÜRO

Prof. Dr. Peter Henning, Gabriele Bornemann
Das Sitzungsprotokoll 162

AUS DEM DEUTSCHEN AKTIENINSTITUT

Dr. Christine Bortenlänger, Dr. Nima Ghassemi-Tabar
Das Lieferkettensorgfaltspflichtengesetz aus der Sicht des Aufsichtsrats 165

KOLUMNE

Jens Hecht, Marc Tüngler
Viele Unternehmen trauen sich auch in wirtschaftlich herausfordernden Zeiten quantitative Prognosen zu 167

RECHTSPRECHUNG

Genehmigtes Kapital: Benennung der Zwecke des Bezugsrechtsausschlusses 169

DATEN – FAKTEN – MANDATE

4. Berliner Beteiligungskongress 170

Impressum

BOARD –
Zeitschrift für Aufsichtsräte in Deutschland

ISSN: 2192-211X

Verlag: Reguvis Fachmedien GmbH
Geschäftsführung: Dr. Sascha Theißen

Reguvis
www.reguvis.de

Gesamtleitung
Prof. Dr. Dr. h.c. Barbara Dauner-Lieb
Prof. Dr. Stefan Siepelt
Marc Tüngler

Redaktion Reguvis Fachmedien GmbH
Ass. jur. Marieke Stöcker-Pritz, L.L.M.
Tel.: 0221 / 9 76 68-109
E-Mail: marieke.stoecker-pritz@reguvis.de
Leon Jülicher
Tel.: 0221 / 9 76 68-315
E-Mail: leon.juelicher@reguvis.de

Externe Redaktion
Jörg Schick
E-Mail: schick@adar.info

Manuskripte
Manuskripte sind in elektronischer Form unmittelbar an die Schriftleitung oder an die Redaktion im Verlag zu senden. Für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Verlag und Schriftleitung behalten sich das Recht zur redaktionellen Bearbeitung der angenommenen Manuskripte vor. Der Autor/Die Autorin versichert, alleinige/r Inhaber/in der urheberrechtlichen Nutzungsrechte an dem Beitrag inklusive aller Abbildungen zu sein und keine Rechte Dritter zu verletzen.
Mit der Annahme des Manuskriptes zur Veröffentlichung überträgt der Autor/die Autorin dem Verlag das ausschließliche Verlagsrecht für die Zeit bis zum Ablauf des Urheberrechts. Das Nutzungsrecht umfasst alle Verwertungs-, Verbreitungs- und Vervielfältigungsformen Print und Online insgesamt oder in Teilen sowie das Recht zu Übersetzungen, zur Einspeicherung, Verarbeitung und Verbreitung in eigenen und fremden Datenbanken, zur Speicherung und Vervielfältigung im Wege elektronischer Verfahren sowie zur Lizenzvergabe.

Urheber- und Verlagsrechte
Alle in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Jegliche Verwertung, Verbreitung oder Zugänglichmachung (Print/Online) außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das Zitieren von Rezensionen ist in vollem Umfang erlaubt.
Cover-Copyright © www.istockphoto.com

Haftungsausschluss
Die in dieser Zeitschrift veröffentlichten Beiträge wurden nach bestem Wissen und Gewissen geprüft. Eine Gewähr für die Richtigkeit und Vollständigkeit kann jedoch nicht übernommen werden. Eine Haftung für etwaige mittelbare oder unmittelbare Folgeschäden oder Ansprüche Dritter ist ebenfalls ausgeschlossen. Namentlich gekennzeichnete Beiträge geben nicht notwendig die Meinung der Redaktion wieder.

Erscheinungsweise
zweimonatlich, jeweils Mitte des geraden Monats

Bezugspreise/Bestellungen/Kündigungen
Einzelheft 50,70 € inkl. MwSt. und Versandkosten (Inland 2,50 € pro Ausgabe/Ausland 4,50 € pro Ausgabe). Der Jahresabopreis inkl. Online-Archiv beträgt 317,– € inkl. MwSt. und Versandkosten (Inland 2,50 € pro Ausgabe/Ausland 4,50 € pro Ausgabe). Bestellungen über jede Buchhandlung oder beim Verlag. Der Bezugszeitraum beträgt jeweils 12 Monate. Kündigungen müssen schriftlich erfolgen und spätestens am 15. des Vormonats, in dem das Abonnement endet, beim Verlag eingegangen sein.

Abo-Service und Anzeigen
Tel.: 0221 / 9 76 68-8500
E-Mail: wirtschaft@reguvis.de

Anzeigenpreise
Es gilt die aktuelle Anzeigenpreisliste.

Satz
TGK Wienpahl, Köln

Druck
Appel & Klinger GmbH, Schneckenlohe

Hope is not a plan – was Cyber-Angriffe und Corona gemeinsam haben ...

Matthias Goldbeck, Partner CCounselors, Düsseldorf[1]

Belegt ist, dass seit Corona die Zahl der Cyberangriffe deutlich gestiegen ist. Kausalität oder Korrelation? Zumindest hat die Zunahme von Remotework einige Einfallstore geschaffen, die es so früher nicht gab. Auch bei Cyberangriffen, egal ob DDOS oder Ransomware, stellt sich heute weniger die Frage, ob man es „bekommt", sondern vielmehr wann. Und auch hier gilt: Vorbereitung (Impfung) schützt nicht vor Angriff (Infektion), aber vielfach vor schwerem Verlauf. Dabei steht die IT-Sicherheit im Vordergrund, ebenso wie das Beachten einfacher Verhaltensregeln im Umgang mit Mails, Anhängen usw. Wesentlicher Bestandteil der Cyberimpfung für Unternehmen ist heute aber mehr denn je die Kommunikation.

I. 12 Regeln für gute Krisenkommunikation des Aufsichtsrats[1]

Das Primat guter Krisenkommunikation gilt zunächst für den Vorstand und die gesamte Organisation, aber gerade auch für den Aufsichtsrat, der sich laufend – mindestens im Prüfungsausschuss – im Rahmen der Befassung mit den Risikokontroll- sowie Risikomanagement-Systemen auch die Frage stellen muss, wie gut man in Sachen Cyberangriffe aufgestellt ist.

Dazu gehört auch, dass der Aufsichtsrat die Gewissheit hat, dass nicht erst im Fall der Fälle umtriebig reagiert wird, sondern der Vorstand gut vorbereitet in die Ausnahmesituation eines Angriffes geht.

Sowohl das Doing im Vorstand als auch die Kontrolle durch den Aufsichtsrat sollten sich an folgenden 12 Grundprinzipien orientieren:

1. Planen Sie für den Ausnahmefall

Stellen Sie interdisziplinäre Krisenteams zusammen. IT, Legal, Datenschutz, Sales, Finance, Produktion, Logistik – im Fall eines Falles sind alle Bereiche betroffen. Nutzen Sie Ihren Krisenplan und passen Sie ihn bei Bedarf an. Legen Sie schon frühzeitig fest, wer Sie im Falle eines Falles unterstützen kann. Das gilt auch und gerade für die Kommunikation. Sie brauchen Expertise und Erfahrung, Sie brauchen aber auch einfach Manpower. Simulieren Sie wahrscheinliche Szenarien und bereiten Sie Sprachregelungen vor. Klar, jede Krise ist anders. Aber in Stresssituationen nicht auf dem weißen Blatt Papier beginnen zu müssen, spart Zeit und Nerven.

2. Üben, üben, üben

Am besten mit Experten, die über Angriffe nicht nur gelesen, sondern sie auch erlebt haben. Dabei sollten interne wie externe Experten zusammen agieren und voneinander lernen. Jedes Unternehmen hat eigene Systeme, Schwachstellen, Lösungen, die es zu erlernen und zu kennen gilt.

INHALT

I. 12 Regeln für gute Krisenkommunikation in der Krise
1. Planen Sie für den Ausnahmefall
2. Üben, üben, üben
3. Kommunikation ist Kerndisziplin
4. Es gelten die Prinzipien der Krisenkommunikation
5. Monitoring für schnelles Handeln und Social Media „beherrschen"
6. Alternative Kommunikationsstrukturen etablieren
7. Interne Kommunikation ist Key
8. Aktiv und transparent nach außen kommunizieren
9. Eine Attacke darf nicht überraschen
10. Thema gehört regelmäßig auf die Tagesordnung
11. Zugriffsrechte als potenzielle Gefahrenstelle
12. Sichern von Kapazität und Kompetenz
II. Fazit

Keywords
Cyberangriff; Krisenkommunikation; Krisenmanagement

1 Matthias Goldbeck verfügt über langjährige Kommunikationserfahrung bei Finanzdienstleistern und Professional Services Firms. Er leitete die Interne Kommunikation der Commerzbank und war Kommunikationschef der Allianz Deutschland. Seit 2019 berät er als Partner bei CCounselors Unternehmen in Fragen des Reputations- und Kommunikationsmanagements.

3. Kommunikation ist Kerndisziplin

Es hilft niemandem, wenn die Kommunikationsexperten aus falsch verstandener Rücksichtnahme erst dann über das Problem informiert werden, wenn es sich nicht mehr vermeiden lässt. Kommunikation gehört an den Tisch, an dem entschieden wird, von Anfang an. Als elementarer Bestandteil der Krisenorganisation erhält sie die notwendigen Informationen im War-Room aus erster Hand.

4. Es gelten die Prinzipien der Krisenkommunikation

Ein Cyberangriff ist eine unternehmerische Ausnahmesituation. Mit zunehmender Häufung verlieren sie zwar das Skandalisierungspotenzial. Man wird heute nicht mehr dafür kritisiert, angegriffen zu werden. Sondern dafür, Daten nicht gewissenhaft geschützt zu haben oder mit der Krise unprofessionell umgegangen zu sein. Aber genau das wird durch mangelhafte Kommunikation sichtbar. Dabei gilt: nur gesicherte Erkenntnisse kommunizieren. Nichts ausschließen, was noch nicht ausgeschlossen werden kann. Und Empathie zeigen für die Betroffenen – seien es Mitarbeitende, die Sonderschichten einlegen müssen oder Kundinnen und Kunden, deren Daten vielleicht öffentlich werden.

5. Monitoring für schnelles Handeln und Social Media „beherrschen“

Sie müssen wissen, was über Ihr Unternehmen berichtet und gesprochen wird. Damit Sie schnell und angemessen reagieren können. Das gilt für Posts auf Sozialen Medien ebenso wie für Berichterstattung in klassischen Medien. Wer es schafft, vor die Welle zu kommen, behält die Deutungshoheit.

6. Alternative Kommunikationsstrukturen etablieren

Bereiten Sie sich darauf vor, dass Ihre gewohnten Kommunikationskanäle nicht einsetzbar sind. Keine beruflichen E-Mails, kein TEAMS, kein Intranet, kein Unternehmens-WLAN. Aber wie kommunizieren die Teams dann miteinander, wie erreichen die Informationen die Mitarbeitenden? Sind private E-Mail-Adressen hinterlegt? Können Sie Messenger-Dienste nutzen? Sind Kommunikationsketten – ob telefonisch, per Mail, per Messenger oder wie auch immer – festgelegt? Liegt Ihre Krisenplanung physisch vor oder auf einem Stand-alone-Rechner? Können Sie auf ein Call-Center zugreifen, um Kundenanfragen noch zu bearbeiten? Diese Fragen gehören in Ihre Szenario-Planung.

7. Interne Kommunikation ist Key

Sorgen Sie dafür, dass Ihre Mitarbeitenden sprechfähig sind. Dass sie wissen, was sie Ihren Kundinnen und Kunden sagen können. Dass sie wissen, woran gearbeitet wird und wann mit Ergebnissen zu rechnen ist. Hier hat sich auch Sichtbarkeit der Unternehmensleitung bewährt. In einer solchen Ausnahmesituation gehören die Chefinnen und Chefs auf die Brücke. Tone from the top ist wichtig. Schaffen Sie dafür Formate und Anlässe. Man kann in solchen Situationen gar nicht zu viel kommunizieren. Machen Sie aber auch klar, wie wichtig Konsistenz für den Erfolg ist. Denn eine Kakophonie von Botschaften aus der Organisation wäre verheerend für die Außendarstellung.

8. Aktiv und transparent nach außen kommunizieren

Gehen Sie davon aus – was rauskommen kann, kommt raus. Wer den Stier kommunikativ bei den Hörnern packt, behält die Deutungshoheit. Sortieren Sie dafür die Fakten. Informieren Sie Ihre Kunden auf der Website. Sprechen Sie vielleicht mit einem Journalisten Ihres Vertrauens und erläutern die Vorgänge. Zeigen Sie, an was gearbeitet wird, welche Workarounds genutzt werden. Geben Sie keine vorschnelle Entwarnung. Better safe than sorry. Wenn Sie können, sagen Sie, wann mit neuen Erkenntnissen zu rechnen ist. Beantworten Sie weitere Kunden-, Mitarbeiter sowie Medienanfragen in diesem Sinn – faktisch, unaufgeregt, lösungsorientiert.

9. Eine Attacke darf nicht überraschen

Es ist immer wieder erstaunlich, wie sehr Unternehmen von einer Cyberattacke immer noch überrascht werden. Dabei wird die Liste derer, die betroffen sind, täglich länger. Bei aller Vorbereitung in der Umsetzung und damit dem Doing in dem Fall, dass man Opfer einer Attacke wird: Man sollte sich auch vorab darüber im Klaren sein, wie man auf mögliche Forderungen der Angreifer reagiert – wenn diese dann konkret formuliert werden. Es geht eben darum, bestmöglich auf alles vorbereitet zu sein.

Allein durch die Schaffung des Bewusstseins, dass jeder und eben auch das jeweilige Unternehmen jederzeit mit einer Attacke konfrontiert sein kann, wird sich bereits in den betroffenen Abteilungen und in den Köpfen der Mitarbeiterinnen und Mitarbeiter eine Veränderung einstellen, die das Unternehmen resilienter aufstellt und das Schutzniveau unmittelbar merklich erhöht.

10. Krisenvorbereitung gehört regelmäßig auf die Tagesordnung

Heute gehört das Thema Cyberattacken und Cyberkriminalität definitiv in jedes Risikokontroll- und Risikomanagementsystem integriert. Und es gehört ausdrücklich und regelmäßig auf die Tagesordnung – nicht nur untergeordnet als ein Spiegelstrich von vielen Aspekten. Hier ist der Aufsichtsrat und sind insbesondere die Prüfungsausschüsse ausdrücklich aufgefordert, das Thema auf die Agenda zu bringen und eingehend zu erörtern.

Eine wesentliche Rolle spielen dabei auch Penetrationstests und die Prüfung mithilfe externer Dienstleister,

um zu erkennen, wo Schwachstellen im System bestehen. Bereits aus Haftungsgründen sollten – oder besser müssen – solche Tests durchgeführt werden und die Erkenntnisse daraus zur Verbesserung dieses Themas führen. Mitarbeitende müssen vorab geschult und sensibilisiert werden – um mögliche Einfallstore gar nicht erst entstehen zu lassen.

11. Zugriffsrechte als potenzielle Gefahrenstelle

Dazu gehört auch die Frage, ob die in der Vergangenheit erteilten Zugriffsrechte der Mitarbeiterinnen und Mitarbeiter sowie externer Partner neu strukturiert und damit angepasst werden müssen. Je weniger Zugriff möglich ist, umso besser ist ein System geschützt. Gerade beim letztgenannten Aspekt ist in vielen Unternehmen über die Jahre hinweg ein Geflecht entstanden, was regelmäßig überprüft und laufend zurückgeschnitten gehört. Weniger ist auch in diesem Fall mehr.

12. Sichern von Kapazität und Kompetenz

Nicht zu unterschätzen ist die bereits oben in der Checkliste angeführte Frage nach der Verfügbarkeit von externen Kapazitäten, wenn einen eine Attacke ereilt. Je nachdem, wie sensibel das Geschäftsmodell und die Abläufe in den Unternehmen auf (erfolgreiche) Angriffe reagieren könnten, gilt es, Kompetenzen zu sichern – und das eben in ruhigen Zeiten, selbst wenn dies mit teils merklichen Kosten verbunden ist.

II. Fazit

Jede Krise, auch jeder Cyberangriff ist anders. Auf der Range zwischen ausgefallenen Kommunikationskanälen über den Ausfall von Kassen- oder Warenwirtschaftssystemen bis hin zum Produktionsstillstand ist alles möglich. Wie schwer der Fall auch ist – die Grundprinzipien der Kommunikation und des Miteinander sind dieselben. Wer zuvor einen Plan entwickelt hat, kann direkt reagieren und vor allem agieren. Ein unschätzbarer Wert in der Krise.

Effizient und passgenau in Ihrem Unternehmen weiterbilden!

Reguvis

Inhouse – individuelle Trainings und Organisationsberatung

Was Ihnen die Reguvis AKADEMIE bietet:

- Inhouse-Schulungen
- Individuelle Weiterbildungskonzepte
- Organisationsberatung
- Audits

IHRE INHOUSE VORTEILE

- ✓ Individuelle Angebote für Ihre Inhouse-Trainings, in Präsenz oder Online
- ✓ Maßgeschneiderte Schulungen für Ihr Unternehmen
- ✓ Durchführung aller offenen Trainings als Inhouse-Schulung
- ✓ Sie bestimmen Inhalte, Termin, Zeit und Veranstaltungsort

Jetzt individuelles **Angebot anfragen!**

shop.reguvis.de/inhouse-schulung

shop.reguvis.de/akademie | veranstaltungen@reguvis.de | Tel: 02 21 – 976 68-8080