/ Aufsichtsräte benötigen mehr digitalen Sachverstand

gemeinsame Studie von Noerr und TU München

19.10.2022

Digital Business | Compliance & Interne Untersuchungen

Digitale Kenntnisse und Erfahrungen spielen bei der Auswahl und Bestellung von Aufsichtsratsmitgliedern aktuell keine besondere Rolle. Für weniger als ein Drittel der Unternehmen hat die digitale Kompetenz des Aufsichtsrats eine hohe oder sehr hohe Relevanz. Das ist das Ergebnis einer gemeinsamen Studie der Kanzlei Noerr und des TUM Center for Digital Public Services von Professor Dr. Dirk Heckmann an der Technischen Universität München (TUM). Für die Studie wurden 300 Führungskräfte der ersten und zweiten Ebene aus Unternehmen ab 250 Mitarbeitenden interviewt.

Dr. Sophia Habbe , Partnerin in Frankfurt und Co-Leiterin der Praxisgruppe Compliance & interne Untersuchungen, sagte: „Durch die fortschreitende Digitalisierung von Unternehmensprozessen und Geschäftsmodellen ist digitale Kompetenz für den Aufsichtsrat essenziell. Denn nur dann kann er bei der Überwachung der Geschäftsleitung seine Rolle als zentrale Kontrollinstanz ausfüllen und beurteilen, ob die Geschäftsleitung die Risiken digitaler Technologien richtig eingeschätzt hat."

Prof. Dr. Peter Bräutigam , Partner in München und laut juristischer Verzeichnisse (Juve, Chambers) einer der führenden Experten für IT-Recht in Deutschland, ergänzte: „Auch im Hinblick auf die Beurteilung von digitalen Compliance-Risiken ist entsprechender Sachverstand des Aufsichtsrats gefragt. So haben nach unserer Studie in den letzten drei Jahren 27 Prozent der Unternehmen Datenschutzvorfälle gemeldet. Eine besondere Herausforderung ist der vermehrte Einsatz von Cloud-Lösungen in Unternehmen – der Aufsichtsrat hat deshalb auch den Umgang der Geschäftsleitung mit den damit verbundenen Risiken im Auge zu behalten."

Dem Aufsichtsrat kommen vielfältige Digital-Aufgaben zu: Er muss die Geschäftsleitung im Hinblick auf digitale Geschäftsprozesse, den Einsatz neuer Technologien und eine sichere und datenschutzkonforme IT-Infrastruktur kontrollieren. Zugleich muss er sich davon überzeugen, dass die Geschäftsleitung geeignete Compliance-Strukturen im Unternehmen einrichtet.

Nach der Studie sind viele Aufsichtsräte auf diese Aufgaben nur unzureichend vorbereitet. Nur 28 Prozent der Unternehmen schätzen digitale Kompetenzen und Fähigkeiten bei der Bestellung von Aufsichtsratsposten als wichtiges Kriterium ein. Selbst bei Unternehmen, in denen es in den vergangenen drei Jahren bereits Compliance-Vorfälle gab, liegt der Wert nur bei 33 Prozent. Ein bemerkenswerter Befund, denn zugleich gaben bei der Befragung 42 Prozent der Unternehmen an, dass der Aufsichtsrat konkrete Maßnahmen ergreift, um den digitalen Sachverstand der Geschäftsleitung sicherzustellen. Andererseits beschäftigt sich auch nur gut die Hälfte (53 Prozent) der Aufsichtsräte regelmäßig mit Themen rund um die Digitalisierung – in Unternehmen mit weniger als 1.000 Beschäftigten sind es noch weniger.

Nach Compliance-Vorfällen sind Aufsichtsräte häufiger direkt in das Thema Digitalisierung involviert. In 61 Prozent der Fälle kommen Digitalthemen dann auf die Tagesordnung. Meist (39 Prozent) befasst sich der Aufsichtsrat selbst mit dem Thema, ein Viertel greift auf Experten zurück und 13 Prozent haben dafür einen Ausschuss eingerichtet. Demgegenüber sind in Unternehmen ohne Compliance-Vorfälle lediglich 22 Prozent der Aufsichtsräte regelmäßig mit der Digitalisierung befasst.

Steht die Digitalisierung regelmäßig auf der Agenda des Aufsichtsrats, genießt die IT-Sicherheit mit 61 Prozent eine ähnlich hohe Wichtigkeit wie Digitalisierungsthemen zu Geschäftsprozessen (68 Prozent).

Die hohe Aufmerksamkeit des Aufsichtsrats zu Fragen der IT-Sicherheit ist zu begrüßen, liegen hier doch wesentliche Compliance-Risiken. So hat die Studie ergeben, dass 47 Prozent der teilnehmenden Unternehmen in den vergangenen drei Jahren von digitalen Compliance-Vorfällen betroffen waren. Neben allgemeinen Datenschutzverstößen (29 Prozent) berichteten 27 Prozent der Befragten von Compliance-Vorfällen im Bereich der IT-Sicherheit.

Dabei hat die Untersuchung auch ergeben, dass flächendeckend ein Basisschutz zur IT-Sicherheit und zum Datenschutz besteht, jedoch weniger Unternehmen spezifischere Maßnahmen zum Stand der Technik im Einsatz haben. Bei der Nutzung von Cloud-Diensten sehen nur wenige Unternehmen hohe Risiken (16 Prozent). Zwar können Cloud-Lösungen meist die IT-Sicherheit erhöhen; bei der Datenauslagerung auf Server außerhalb der EU gelten jedoch erhöhte Anforderungen nach der DS-GVO. Entsprechend hat der Serverstandort für 71 Prozent der Befragten eine hohe Relevanz.

Weiteres Ergebnis der Studie: Zwei von drei befragten Unternehmen (67 Prozent) verfügen über eine eigene Abteilung oder Funktion für Datenschutz, in vier von zehn Fällen (38 Prozent) ist diese getrennt von der Compliance-Abteilung. Zwei Drittel der Unternehmen verfügen zudem über eine Stelle für IT-Sicherheit bzw. einen Informationssicherheitsbeauftragten – meist in der IT-Abteilung (51 Prozent).

Contact Person

Prof. Dr. Peter Bräutigam
Mitglied der Practice Group Digital Business
Mitglied der Practice Group Versicherung & Rückversicherung
Rechtsanwalt, Fachanwalt für Informationstechnologierecht

T +49 89 28628378

Dr. Julia Sophia Habbe
Co-Leiterin Compliance & Interne Untersuchungen
Mitglied der Practice Group Corporate
Rechtsanwältin

T +49 69 971477252

Matthias Schulte
PR-Manager

T +49 69 971477418