carmasec

security. done. right.

Whitepaper 11/2019

Was ist neu am Geschäftsgeheimnisgesetz (GeschGehG) - aus Sicht der Cybersicherheit?

Gesetz setzt bei Unternehmen Anpassungen voraus

Know-how ist die Währung der wissensbasierten Wirtschaft und schafft Wettbewerbsvorteile für Unternehmen. Im geschäftlichen Kontext kommt Geheimnissen eine besondere Bedeutung zu. Dort sind sie ein Wettbewerbsfaktor – und meist bares Geld wert! Mitunter ist die Existenz ganzer Unternehmen von der Bewahrung essenzieller Geheimnisse abhängig. Nicht zuletzt aus diesem Grund will die Europäische Union Geschäftsgeheimnisse besser schützen. Dazu trägt das Geschäftsgeheimnisgesetz bei, das im April dieses Jahres in Kraft getreten ist.

Juristische Anforderungen wie die Überarbeitung von Verträgen, aber auch die Anpassung von Unternehmensstrukturen, Prozessen und Technologien sind durch das neue Gesetz erforderlich.

GeschGehG verlangt angemessene Geheimhaltungsmaßnahmen

Bislang reichte es für den rechtlichen Schutz von Geheimnissen in Deutschland aus, wenn Unternehmen bestimmte Informationen geheim halten wollten und diesen Geheimhaltungswillen nach außen in geeigneter Form dokumentierten. Dafür genügte es in der Vergangenheit oft, wenn die Geschäftsführung Informationen und Dokumente als „geheim“ einstufte. Zudem war es nicht nötig, Mitarbeiter hierüber in Kenntnis zu setzen. Mit dem neuen Geschäftsgeheimnisgesetz ändert sich diese Ausgangssituation grundlegend.

Das neue Gesetz verlangt, dass sogenannte angemessene Geheimhaltungsmaßnahmen ergriffen werden, damit schützenswertes Know-how auch tatsächlich den gesetzlich vorgesehenen Schutz genießt. Mit der Einführung dieses Kriteriums müssen Unternehmen Geschäftsgeheimnisse nun proaktiv schützen. Nur dann greift der gesetzlich vorgesehene Schutz und gibt dem Geheimnisinhaber die Möglichkeit rechtliche Schritte, wie Unterlassungserklärungen oder Schadensersatzansprüche geltend zu machen. Je wichtiger eine Information für das Unternehmen ist, umso

strenger sind auch die Anforderungen an die getroffenen technischen und organisatorischen Maßnahmen zur Geheimhaltung.

Das geforderte zumutbare Maß an Schutzbemühungen hängt zwar von der personellen und finanziellen Leistungsfähigkeit des jeweiligen Unternehmens ab. Im Zweifel sollte aber ein hoher Mindeststandard für alle Geschäftsgeheimnisse etabliert werden, der für besonders wertvolle Geschäftsgeheimnisse noch einmal intensiviert wird. Die Tatsache, dass keine Übergangsfrist besteht, setzt besonders Unternehmen unter Handlungsdruck, die noch keine oder nur unzureichende Geheimhaltungsmaßnahmen getroffen haben.

Für Unternehmer, die einen Schutz ihres geschäftlichen Know-hows weiterhin in Anspruch nehmen wollen, besteht nun Handlungsbedarf, um bestmöglich von der neuen Rechtslage profitieren zu können. Diese birgt sowohl Chancen als auch Risiken: besonders die Cybersicherheit eines Unternehmens steht vor Herausforderungen, die kurzfristig zu bewältigen sind. Anforderungen, die das Geschäftsgeheimnisgesetz an die Geschäftsführung eines Unternehmens stellt, sind nicht nur juristischer Natur. Sie haben großen Einfluss auf die Prozesse, Strukturen und Technologien in einem Unternehmen.

Konsequenzen für die Cybersicherheit in Unternehmen

Um ihre Geschäftsgeheimnisse entsprechend zu schützen, müssen Unternehmen verschiedene Maßnahmen ergreifen. Welche Arten von Geheimhaltungsmaßnahmen erfolgen müssen, hängt von der Art des Geschäftsgeheimnisses im Einzelnen und der konkreten Nutzung ab. Das können u.a. der eindeutig geregelte Zugang zu Dokumenten sowie ihre sichere Aufbewahrung, aber auch intern neu geregelte Passwortzugänge und Vertragsanpassungen sein.

WHISTLEBLOWER

Eine richtige Übersetzung für Whistleblower existiert im Deutschen offenbar nicht. Darunter wird allerdings eine Person verstanden, die Unternehmensgeheimnisse oder Missstände verrät. In Deutschland genossen „Whistleblower" bislang keinen klar geregelten Schutz vor Strafverfolgung.

Das hat sich mit dem neuen Gesetz geändert. Geschäftsgeheimnisse dürfen künftig straffrei veröffentlicht werden, wenn damit rechtswidrige Handlungen oder Fehlverhalten aufgedeckt werden. Das gilt selbst für legales, aber unethisches Verhalten. Whistleblower dürfen solche Informationen allerdings nur enthüllen, wenn an ihnen ein öffentliches Interesse besteht.

Eindeutig geregelter Zugang zu geheimen Dokumenten

Folgendes ist zu betrachten: Wer muss bestimmte Dokumente für seine Arbeit nutzen? Nur genau diese Kollegen sollten auch Zugriff auf die entsprechenden Daten haben. Verlässt ein Mitarbeiter das Unternehmen, muss es in der Lage sein, den Zugriff des ehemaligen Mitarbeiters auf diese Informationen und Dokumente schnellstmöglich zu unterbinden.

Voraussetzung hierfür ist, die Geheimhaltungsbedürftigkeit einer Information vorher genau festzulegen:

1. Schlüsselinformation: Das Unternehmen kann in seiner Existenz gefährdet werden, wenn die Information nicht geheim bleibt.

2. Strategisch wichtige Information: Dies können zum Beispiel Informationen zu Kunden oder Einkaufspreisen sein.

3. Wettbewerbsrelevante Information: Das Bekanntwerden der Informationen ist hier vielleicht ärgerlich, hat aber keine weitreichenden Konsequenzen für das Unternehmen.

Je nach Einstufung der Geheimhaltungsbedüftigkeit einer Information, können die Zugriffe hierauf für bestimmte Beschäftigtengruppen reglementiert werden.

Sichere Aufbewahrung

Den Zugriff auf elektronische Dokumente können Unternehmer durch verschiedene Verschlüsselungstechnologien schützen. Geheime oder sensible Informationen sollten ebenfalls von den Mitarbeitern nur verschlüsselt verschickt werden. Obwohl die meisten Unternehmen aufgrund öffentlichkeitswirksamer Ereignisse rund um Datenskandale hinreichend sensibilisiert sind, bleibt der Abfluss von Geschäftsgeheimnissen aufgrund fehlender Verschlüsselung oftmals unentdeckt bzw. wird erst erkannt, wenn es zu spät ist.

Regeln zu Passwörtern

Damit Mitarbeiter sich an einem System authentisieren können, bedarf es sicherer Passwörter. Hier können Unternehmen Richtlinien erstellen, welche Mindestanforderungen Passwörter haben müssen.

Idealerweise ist es dann für Mitarbeiter technisch nicht mehr möglich, Passwörter zu erstellen, die diese Vorgaben nicht erfüllen. Empfehlenswert ist zudem der Einsatz von Applikationen für Identitäts- und Zugriffsverwaltungen, damit die regelmäßige Aktualisierung von Passwörtern und die Einhaltung von Regeln automatisiert überwacht wird. Außerdem bietet sich eine Multi-Faktor-Authentifizierung an, bei der Zugangsberechtigungen durch verschiedene unabhängige Merkmale überprüft werden.

> „Technische Schutzvorkehrungen sind dabei ebenso bedeutsam, wie Compliance-Management, Regelungen der Zugangsberechtigung, klar definierte Zuständigkeiten und ein Notfallplan für den Umgang mit einem *Leak*."
>
> *- Carsten Marmulla, Geschäftsführer*

Richtlinien und Weisungen

Nicht nur bei weniger relevanten Geschäftsgeheimnissen sind Richtlinien und Weisungen angemessene Geheimhaltungsmaßnahmen, die verständlich dokumentiert und für alle Beschäftigten zugreifbar sind. Dazu gehört auch die regelmäßige Schulung der Beschäftigten, insbesondere für jene Gruppen, zu deren Tätigkeitsbereich der Umgang mit sensiblen Informationen und Dokumenten gehört. Nicht zuletzt sollten Führungskräfte im Unternehmen die Mitarbeiter in Gesprächen oder Meetings zum Thema Geschäftsgeheimnisse sensibilisieren.

Fazit

Das in Kraft getretene Gesetz bringt zielführende Schritte zum einfacheren und effektiveren Schutz von Geschäftsgeheimnissen zugunsten der Geheimnisinhaber.

Aufgrund des neuen Erfordernisses angemessener Geheimhaltungsmaßnahmen ist für Unternehmensinhaber von besonderer Wichtigkeit eine Bestandsaufnahme durchzuführen. Es sollte festgestellt und dokumentiert werden, welche Arten und Kategorien von schützenswertem Know-how existieren. Im Groben kann dies ausgehend der Fragen erfolgen: Wo im Unternehmen gibt es welche Kategorien von Geschäftsgeheimnissen? Welche Bedeutung haben diese Informationen für das Unternehmen und wer hat darauf Zugriff?

So kann Know-how nach seiner Wichtigkeit kategorisiert und mit entsprechenden abgestuften Schutzkonzepten verbunden werden. Technische Schutzvorkehrungen sind dabei ebenso bedeutsam, wie effektives Compliance-Management, allgemeinverbindliche Regelungen der Zugangsberechtigung, klar definierte Zuständigkeiten und ein Notfallplan für den Umgang mit einem „Leak" existenzieller Geheimnisse.

Wichtig ist hierbei, dass von Anfang an die Cybersicherheit in der Umsetzung des Geschäftsgeheimnisgesetzes berücksichtigt wird, da durch diese Brille alle wesentlichen Anforderungen des neuen Gesetzes im Fokus stehen und auch Antworten bieten.

carmasec
security. done. right.

IHRE ANSPRECHPARTNER

Carsten Marmulla
Geschäftsführer

Jan Sudmeyer
Geschäftsführer

www.carmasec.com
xing.carmasec.com
contact@carmasec.com
twitter.carmasec.com
+49 (0) 201 426 385 900
linkedin.carmasec.com

Behalten Sie Ihre Cybersicherheit im Blick

Melden Sie sich für unseren Newsletter an:
www.carmasec.com/newsletter