Nr. 1, Februar 2014 – 36. Jahrgang **G 1193** ISSN-Nr. 1615-455X

WiK

Zeitschrift für die Sicherheit der Wirtschaft

Nicht abwehrbereit:

Große Sicherheitsrisiken durch kleine Drohnen

Seite 12

Informationsschutz:

Klassifikation hinter „Zwiebelschalen"

Seite 22

Gebäudeautomation:

Löchriger Schutz gefährdet LAN, Haus- und Sicherheitstechnik

Seite 26

ASW Zentralorganisation der Wirtschaft

ORGAN: ARBEITSGEMEINSCHAFT FÜR SICHERHEIT DER WIRTSCHAFT e.V. - ASW

Geschäftsführer Jan Wolter zu den aktuellen Perspektiven der ASW

Aus den regionalen Sicherheitsverbänden

Der aktuelle Stand:

Sichere Zutrittskontrolle per Smartphone und NFC – wie funktioniert das?

Seiten 51 ff

www.wik.info

Mittelstand braucht passende Strukturen:

Mit geringerem Aufwand zur Compliance

Gerade im Mittelstand wird die Einführung von Compliance-Strukturen als finanziell und personell kaum zu stemmende Last empfunden. Teilweise wird dies unter Verweis auf die noch oft vorhandene Kultur des Vertrauens, die Identifikation der Mitarbeiter mit dem Arbeitgeber und die Möglichkeiten zur direkten Einflussnahme auf die Prozesse sogar für überflüssig gehalten. Ein Irrtum, denn die Haftungsrisiken wie auch die Bestimmungen zu Kartellrecht, Geldwäsche und Korruption sind grundsätzlich dieselben wie für ein DAX30-Unternehmen.

Von Markus Weidenauer, München

Eigentlich scheint alles ganz einfach: Staaten und internationale Organisationen geben Gesetze und Verordnungen vor, in deren Rahmen sich Unternehmen mit allen Angestellten und externen Lieferanten bewegen müssen. Doch die dokumentierte und „Audit-sichere" Umsetzung rechtlicher Vorgaben (Compliance) setzt eine umfassende Kontrolle der Geschäftsprozesse durch die Geschäftsleitung oder einen Compliance-Manager voraus. Und hier beginnen die Probleme: Abgesehen davon, dass Mitarbeiter und Partner einer Erfassung ihrer Tätigkeiten meist wenig Wohlwollen entgegenbringen, machen Globalisierung, abnehmende Wertschöpfungstiefen und Outsourcing eine effektive Überwachung verteilter Geschäftsprozesse zur hoch komplexen Herausforderung. Zudem ist Compliance auch in der Umsetzung ein „heißes Eisen", denn die Durchsetzung der legalen Vorschriften ist selbst stark reguliert und rechtlich limitiert. Wer zum Beispiel Korruption effektiv unterbinden will, müsste eigentlich die Kommunikation der gefährdeten Fachabteilungen protokollieren: am besten präventiv, systematisch, lückenlos. Doch damit entsteht ein hohes Risiko, gegen Datenschutzauflagen, das Fernmeldegeheimnis (§206 StGB) und das Gebot informationeller Selbstbestimmung zu verstoßen.

Grenzen für ein Compliance-Monitoring

Wie schwierig es ist, Compliance rechtssicher durchzusetzen, zeigt sich bei der Internet- und E-Mail-Kommunikation. Zu beachten sind hier die Vorgaben des Bundesdatenschutzgesetzes, des Arbeits-, Straf- und Telekommunikationsrechts.

Grundsätzlich ist eine permanente Überwachung der Mitarbeiter nicht erlaubt, ein generelles Screening aller Kommunikationsdaten wird von den Gerichten prinzipiell verworfen*. Personenbezogene Daten eines Beschäftigten dürfen ausschließlich zur Aufdeckung einer Straftat erhoben, verarbeitet und genutzt werden – und nur, wenn „zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen." (§32, Abs. 1 BDSG). Eine volle Kontrolle ist also nur bei konkretem Missbrauchsverdacht zulässig, wobei sich dieser gerade nicht aus der Kontrolle herleiten darf. Das Interesse des Beschäftigten an seinen persönlichen Daten ist schutzwürdig, so dass E-Mails, Verbindungs- und Protokolldaten oder Festplatten nur in der Verhältnismäßigkeit der Mittel, also bei erheblichen Gesetzesbrüchen, analysiert werden dürfen. Andernfalls sind der (IT-)Forensik die Hände gebunden. Und selbst wenn das private Surfen, Mailen oder Chatten komplett verboten ist, bleibt die Totalüberwachung unzulässig.

Andererseits ist ein Monitoring der Kommunikation prinzipiell erlaubt, wenn es dazu dient, die unternehmerische Wertschöpfung technisch und fachlich abzusichern oder zu optimieren. Deshalb ist es für Unternehmen ratsam, die private und geschäftliche Kommunikation der Mitarbeiter zu trennen. Stichproben der dienstlichen Kommunikation sind dann ebenso erlaubt wie das Archivieren der E-Mails im Hinblick auf die Dokumentationspflichten gegenüber Finanzbehörden und Geschäftspartnern.

Das richtige Maß an Kontrolle

Geschäftsführer haben es nicht leicht: Zu laxe Kontrollen können als Verletzung der Aufsichtspflicht geahndet werden, zu strikte Kontrollen lädieren die Persönlichkeitsrechte der Mitarbeiter, können den Betriebsfrieden gefährden und die Leistungsbereitschaft mindern. Zunächst sollte bedacht werden, dass Compliance-Durchsetzung auch selbst der Compliance-Einhaltung unterliegt. Darüber hinaus sollten Kontrollmaßnahmen strikten Maßstäben unterstellt werden. Als Richtschnur gilt dabei generell: So wenig wie möglich, sie viel wie nötig. Wichtige Kriterien sind unter anderem:

* zur Videoüberwachung:
LAG Hessen, Az. 7 Sa 1586/09 v. 25.10.2010
zur Computerausspähung:
ArbG Augsburg, Az. 1 BV 36/12 v. 4.10.2012

1. Partnerschaft: Das Monitoring von Prozessen und Mitarbeitern sollte durch Vereinbarungen mit den Mitarbeitern (Betriebsrat) abgestimmt und begrenzt werden. Ansonsten sind arbeitsgerichtliche Konfrontationen und wirtschaftliche Einbußen wahrscheinlich, zum Beispiel durch ein gezieltes Unterlaufen getroffener Maßnahmen.

2. Transparenz: Da Mitarbeiter sich auch mit externen Auftraggebern oder Auftragnehmern abstimmen, sollten die getroffenen Maßnahmen im Regelfall offen kommuniziert werden, beispielsweise auch, wer Zugriff auf die Kommunikation hat.

3. Legitimation: Die aus den Vereinbarungen resultierenden Maßnahmen sollten nicht nur legal, sondern auch als legitim verstanden werden. Sie sollten also nur dann zur Anwendung kommen, wenn ein hinreichend begründeter Anfangsverdacht auf die Verletzung eines wichtigen Rechtsgutes besteht und alle anderen Mittel versagen.

4. Fairness: Die Kontrolle der Mitarbeiter sollte sich auf die Bekämpfung doloser Handlungen beschränken und nicht in die Leistungsbeurteilung einfließen.

5. Datenschutz: Der Umstand, dass im Compliance-Management personenbezogene Daten gesammelt werden, bedeutet nicht, dass zum Beispiel der Fachvorgesetzte beliebig darauf zugreifen darf. Auch hier muss auf rechtskonforme Lösungen bei Speicherung, Löschung, Anonymisierung, Verschlüsselung und Zugriffsmanagement geachtet werden.

6. Professionalität: Falls interne Ermittlungen erforderlich sind, sollte der Rat von Juristen und professionellen Ermittlern eingeholt werden. Sofern im Unternehmen vorhanden, kann sich die fallbezogene Einbindung von Fachbereichen wie Unternehmenssicherheit, Revision, Compliance, Datenschutz, Betriebsrat und HR-Management anbieten.

Die Organisation

Die Implementierung eines Compliance Management Systems schafft theoretische Sicherheit, die sich allerdings in der Praxis beweisen muss. Prävention und Gefahrenabwehr sind erst gewährleistet, wenn Täter durch Investigation identifiziert und an der Fortsetzung illegaler Machenschaften gehindert werden. Deshalb sollte das Compliance-Management neben der notwendigen juristischen Expertise auch mit den Grundregeln der Investigation vertraut sein. Daneben sind intern oder extern professionelle Ermittler gefragt, die Ziele, Pflichten und legalen Beschränkungen eines Compliance-Managers umfassend verstehen.

Rainer Sturm / pixelio.de

Auch bei Bemühungen um Compliance ist der Datenschutz einzuhalten.

Idealerweise sollte das Compliance-Management zumindest von zwei speziell geschulten Verantwortungsträgern – und eventuell einer weiteren Urlaubsvertretung – getragen werden. Mitarbeiterbefragungen und Ermittlungen erfolgen dann immer mindestens durch zwei Personen, die eine gegenseitige zeugenschaftliche Absicherung und somit gerichtsfeste Ermittlungsergebnisse sicherstellen. Sofern Mittelständlern hierfür die personellen oder finanziellen Ressourcen fehlen, wäre es ein kostengünstigeres Modell, wenn ein hauptamtlicher Compliance-Beauftragter bedarfsweise von externen Spezialisten (Beratung, Ermittlung, Schulung) unterstützt werden. Eine weitere Möglichkeit besteht für den Mittelstand in der Fokussierung auf einzelne, besonders heikle Bedrohungsszenarien. Dazu werden Programme mit strategischen und operativen Schwerpunkten aufgesetzt (Beispiel s. Kasten).

Auch Compliance unterliegt zunächst einem rein betriebswirtschaftlichen Kalkül: Unternehmen werden abzuwägen, ob es weniger kostenintensiv erscheint, Schäden zu begleichen oder Schäden zu vermeiden. Das Problem ist, dass die wirtschaftlichen Folgen von Imageschäden aufgrund von Compliance-Verstößen oder einem „Blacklisting" bei öffentlichen Ausschreibungen kaum zu beziffern, aber in der Regel erheblich sind. Deshalb wird sich kaum ein Unternehmen, auch nicht im Mittelstand, auf Dauer leisten wollen, völlig ohne Compliance-Struktur auszukommen.

Maßnahmen um Glaubwürdigkeit und das pflichtgemäße sowie rechtskonforme Handeln der Unternehmensführung sicherzustellen („Kriminalistische Management-Compliance")

Strategische Weichenstellungen:

Organisation, Abläufe und Verantwortlichkeiten: *Einführung von Präventions- und Kontrollmechanismen mit Vieraugenprinzip und klaren Funktionstrennungen*

Qualitätssicherung: *Monitoring und Optimierung aller Compliance-relevanten Prozesse*

Notfallmanagement: *Zusammenstellung von Krisenteams (Hinterlegen von Kontaktdaten) mit Anwälten, Experten für Ermittlung, IT-Forensik und Datenschutz*

Operative Maßnahmen:

Offene und verdeckte Ermittlungen: *Aufklärung krimineller Handlungen, Identifikation der Täter und Beweissicherung*

Sicherheitscheck: *Überprüfung neuer und in sensiblen Bereichen eingesetzter Mitarbeiter, auch aus Partnerunternehmen*

Observationen: *Verdachtsabklärung und gerichtsverwertbare Dokumentation, eventuell mit Technologie-Einsatz im Rahmen des rechtlich Zulässigen*

Fachschulungen *für Compliance-Beauftragte und Verhaltensschulungen für Mitarbeiter, um sie für Rechtsverletzungen zu sensibilisieren*

Über unseren Autor:

Markus Weidenauer ist Geschäftsführer der Sicherheitsberatung SecCon Group GmbH, München.
Kontakt: info@seccon-group.de

© SecuMedia Verlags-GmbH · D-55205 Ingelheim · WIK 2014/1