RA Arno Lohmanns
RA Sebastian Helmschrott, LL.M EuR

rbi Rechtsanwaltsgesellschaft

Verteilung der Verantwortlichkeit für die IT Security

Begriff und Ziele der Unternehmenssicherheit

1. Schutz des Unternehmens/der Mitarbeiter/der Geschäftspartner vor Unfällen und den Einflüssen höherer Gewalt; Sicherstellung der Kontinuität der Geschäftsabläufe des Unternehmens;
2. Schutz des Unternehmens/der Mitarbeiter vor Haftungsrisiken resultierend aus dem Vertrieb der eigenen Produkte und Services;
3. Schutz von Betriebsgeheimnissen, Know How und IP des Unternehmens;
4. Schutz von (personenbezogenen) Daten und Informationen des Unternehmens/der Mitarbeiter/der Geschäftspartner;
5. Schutz des Unternehmens/der Mitarbeiter/der Geschäftspartner vor internen und externen kriminellen Angriffen (Cyber-Crime, Bestechung, Verrat von Betriebsgeheimnissen);
6. Sicherstellung der Innovationskraft, der Wettbewerbsfähigkeit des Unternehmens.

Rechtliche Vorgaben für den Vorstand in Hinblick auf die Unternehmenssicherheit

1. gegenüber den Mitarbeitern:
- arbeitsrechtliche Fürsorgepflicht,
- Gesetze betreffend Arbeitssicherheit, Urlaub- und Arbeitszeiten

2. gegenüber dem Unternehmen:
- Art. 91 II AktG: Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft und gefährdende Entwicklungen früh erkannt werden;
- gesetzliches Datenschutz- und Telekommunikationsrecht;
- gesetzliches Zivilrecht mit dem Grundsatz der vollen und unbegrenzten Verantwortung und Haftung des Unternehmens für sein Handeln im Geschäftsverkehr;
- Vorschriften des Straf- und Ordnungswidrigkeitenrechts (Verrat von Betriebsgeheimnissen, Verletzung des Telekommunikationsgeheimnisses, Verletzung des Datenschutzrechts)

3. gegenüber den Geschäftspartnern:
- vertragliche Treuepflichten und vertragliche Haftungsregelungen;
- vertragliche Verschwiegenheitsvereinbarungen zum Schutz vertraulicher Informationen
- Produkt- und deliktische Haftung

Die Rolle der IT bei der Unternehmenssicherheit

- Dezentralisierung der Rechenzentrumsstruktur, Einführung von Back-Up Systemen zum Schutz vor höherer Gewalt und zur Sicherstellung der Kontinuität der Geschäftsabläufe,
- IT-gestützte Planung und Organisation der Unternehmensressourcen, der Bestell-, Produktions-, Qualitätsmanagement- , logistischen Prozesse zur Vermeidung von Haftungsrisiken und zur Erhöhung der Innovationskraft,
- Sicherheit der IT-Systeme vor internen Missbrauch und externe
- Kriminalität und vor Datenabfluss
- Einführung von IT-Systemen zur Stärkung der Innovationskraft, der Wettbewerbsfähigkeit des Unternehmens

Die Verantwortung des Vorstandes für die Unternehmenssicherheit

Die Verantwortung für die Unternehmenssicherheit liegt beim **Vorstand:**

- Der Vorstand hat ein **Überwachungssystem** im Unternehmen einzuführen, bleibt aber selbst immer die letzte Überwachungsinstanz **(**Art. 91 II AktG).

- Der Vorstand hat diejenigen Maßnahmen zur Unternehmenssicherheit zu ergreifen, die auf Grundlage der sog. **Business Judgement Rule** notwendig sind. Danach hat der Vorstand seine unternehmerische Entscheidung über die zu treffenden Sicherheitsmaßnahmen **sorgfältig**, auf der Grundlage **ausreichender und objektiver Information** und **zum Wohle der Gesellschaft** zu treffen (Art. 93 I AktG).

Überwachungssystem bestehend aus folgenden Elementen:

1. Personelle Maßnahmen: Einführung einer Compliance- oder Risk-Management Organisation

1. Rechtliche Maßnahmen: Einführung von Richtlinien, die das Verhalten von Mitarbeitern zum Schutz der Unternehmenssicherheit konkretisieren, entweder genereller oder sehr spezifischer Natur, z.B.

- Compliance-Richtlinie
- Richtlinie zum Umgang mit der Unternehmens-IT/mobile Devices
- Vertretungsrichtlinien
- Produkthaftungsrichtlinien
- Datenschutzrichtlinien
- Reisekosten- und Spesenrichtlinien
- Richtlinie für den Umgang mit vertraulichen Informationen:
- Standortrichtlinie
- Eskalations- und Reporting-Richtlinien

Anzahl, Inhalt und Regelungstiefe der Richtlinien hängen vom jeweiligen Geschäftsfeld eines Unternehmens und den betreffenden Risiken ab.

Qualitative Anforderungen an Maßnahmen

Die Überwachung aller Aspekte der Unternehmenssicherheit durch den Vorstand muss vollständig und lückenlos sein, d.h. der Vorstand hat sicherzustellen, dass

- die Compliance Organisation funktioniert, d.h.er hat zu sorgen für
  - eine lückenlose Verteilung und Delegierung von Aufgaben,
  - die Einführung von speziellen Befugnissen der Compliance-Orga. wie z.B. zur Durchführung interner Ermittlungen und Audits,
  - die Einführung von Reporting-, Melde- und Eskalationsprozessen,
  - die Sicherstellung der Objektivität und Effektivität der Organisation,
  - eine saubere Abgrenzung zu den Zuständigkeiten anderer Abteilungen (Legal Department, Human Resources, Datenschutzbeauftragten),
- die internen Unternehmens-Richtlinien in der notwendigen Anzahl und Regelungstiefe vorhanden sind;
- die notwendigen Trainings und Einweisungen der Mitarbeiter in diese Richtlinien erfolgt; und
- ein Prozess der ständigen Überwachung stattfindet.

Delegierung der Vorstandsverantwortung

Grenzen der Delegierung

- Der Vorstand kann Aufgaben zur Sicherstellung der Unternehmenssicherheit delegieren, trägt aber immer die Verantwortung als ultimative Überwachungsinstanz. Dieser Verantwortung kann sich der Vorstand nicht entziehen und auch nicht vollständig an Mitarbeiter, wie z.B. Mitarbeiter der Compliance-Organisation, delegieren.

- Diese Vorstandsverantwortung trifft auch jedes einzelne Mitglied des Vorstandes, soweit nicht innerhalb des Vorstandes eine wirksame Ressortzuteilung stattgefunden hat und das Sicherheitsthema nur dieses Ressort betrifft.

Voraussetzung für die Delegierung von Aufgaben

Soweit der Vorstand Aufgaben delegiert, ist folgendes sicherzustellen:

Delegation von Aufgaben muss klar geregelt und zugeordnet werden:

Beispiel: Wer ist zuständig für die Meldung von, Überwachung der und die Compliance mit aktuellen Gesetzesänderungen im Datenschutzrecht? Legal Department, CIO und/oder Datenschutzbeauftragter?

Die Erfüllung delegierter Aufgaben muss durch funktionierende abgestufte Reporting-/Controlling-/Melde- und Eskalationsprozesse überwacht werden.

Beispiel:

- Meldung durch HR, dass ein für die Unternehmenssicherheit relevanter Mitarbeiter seine Aufgaben nicht erfüllt;
- Meldung durch Compliance oder die IT, dass Angriffe auf die IT-Systeme zunehmen und ein erhöhter Schutz notwendig wird.

Nur soweit diese Voraussetzungen erfüllt sind, haftet der Vorstand dem Unternehmen nicht für ein singuläres individuelles Fehlverhalten, eine singuläre Fehlentscheidung eines Mitarbeiters.

Verantwortung des CIO für die IT-Sicherheit

Aufgaben des CIO als Angestellter

•

Die Aufgaben des CIO ergeben sich **vorrangig** aus der Aufgaben- und Funktionsbeschreibung im **Arbeitsvertrag**.

Soweit die vertragliche Aufgabenbeschreibung im Arbeitsvertrag nicht hinreichend genau/konkrer ist, werden die Aufgaben des CIO durch

- **internationale Definitionen, Standards** (z.B. Cobit, ISO 2000, ITIL etc.), und/oder
- **durch ein international praktiziertes Leitbild des CIO** mitbestimmt.

In der internationalen Praxis ist das Bild des CIO seit mehr als 15 Jahren wie folgt im Wandel: weg von der Funktion eines IT-Fachmanns, dessen IT-Organisation das Unternehmen unterstützt hin zu einem betriebswirtschaftlich geprägten Manager, der auch Verantwortung für das Unternehmen übernimmt in Bezug auf Strategie, Innovation und Change Management im Unternehmen unter dem speziellen Blickwinkel der IT.

Konsequenz:

Der CIO hat eine umfassende Verantwortung für die Sicherheit eines Unternehmens, soweit der Einsatz von IT in irgendeiner Form für die Sicherheit eine Rolle spielt, es sei denn, der Arbeitsvertrag schränkt dies ein.

Die Verantwortung für IT-Sicherheit trifft daher CIO und Vorstand gleichermaßen; es gibt keine abgestuften Zuständigkeitsbereiche. Zur Haftungsverteilung zwischen CIO und Vorstand siehe Slide 5 unten.

CIO als leitender Angestellter nach deutschem Recht

Soweit der CIO im Konzern nach deutschem Recht die Funktion eines sog. leitenden Angestellten hat,

- haftet er dem Unternehmen bei schuldhafter Verletzung seines Arbeitsvertrages unbegrenzt;
- hat er die vertragsgemäße Erfüllung seines Vertrages im Zweifelsfall nachzuweisen;
- hat er ihm laut Arbeitsvertrag zu treffenden unternehmerischen Entscheidungen zur IT-Sicherheit – ebenso wie der Vorstand - nach Maßgabe der Business Judgement Rule zu treffen, d.h.
- sorgfältig,
- auf der Grundlage ausreichender und objektiver Information und
- zum Wohl der Gesellschaft (Art. 93 I AktG)

Nach deutschem Recht ist ein CIO als leitender Angestellter zu qualifizieren

Verteilung der Haftung zwischen CIO und Vorstand/Compliance für Fehler bei der IT-Sicherheit

Realisieren sich im Unternehmen Risiken für die IT- oder Datensicherheit wird man zwischen folgenden Szenarien für die Haftungsverteilung zu unterscheiden haben:

Fallgruppe 1: Risiko realisiert sich primär wegen Mängeln des Überwachungssystems:

Beispiele:

- Gesetzliche Änderung im Datenschutzrecht wird nicht oder nicht rechtzeitig umgesetzt, weil diese Aufgabe nicht klar delegiert wurde;
- richtlinienkonformes Verhalten der Mitarbeiter wird nicht überwacht oder sanktioniert, weil diese Überwachungsaufgabe nicht delegiert wurde;
- Es fehlen erforderliche interne Richtlinien wie z.B. zur Nutzung des Firmen e-mail-accounts für private Zwecke;

In diesen Fällen liegt die Verantwortung in der Regel überwiegend bei der Compliance-Organisation und damit beim Vorstand und nicht beim CIO.

Fallgruppen

Fallgruppe 2: CIO verletzt seine arbeitsvertragliche Aufgaben

Beispiel:

CIO soll selbständig über die Durchführung eines kleineren IT-Projekts entscheiden, unterschätzt aber die Risiken, weil er seine Entscheidung auf einer nicht ausreichenden oder nicht objektiven Informationsgrundlage getroffen hat.

Anm: Bestehen interne Melde- Reporting oder Eskalationsrichtlinien und der CIO hat diese nachweislich eingehalten, scheidet eine Haftung des CIO aus seinem Arbeitsvertrag in der Regel aus.

Fallgruppen

Fallgruppe 3: CIO verletzt seine arbeitsvertragliche Aufgabe und es liegt gleichzeitig ein Mangel im Überwachungssystem vor.

Beispiele:

- CIO hat die Aufgabe für die Einführung eines Lizenzmanagements;
  - eine übermäßige Nutzung von Lizenzen durch Mitarbeiter bleibt über Jahre unentdeckt sowohl wegen Mängeln im Lizenzmanagement-System als auch wegen mangelnder Überwachung des richtlinienkonformen Verhaltens der Mitarbeiter;
  - CIO entscheidet sich trotz der damit verbundenen Datenschutzrisiken für die Einführung einer Cloud-Lösung; zu dieser Entscheidung kommt es nur, weil die konzerninternen Prozesse keine Einbindung der Datenschutzbeauftragten und der Compliance-Organisation vorsehen.

In diesen Fällen kann es zu einer Aufteilung der Verantwortung kommen, wobei ein überwiegendes Verschulden der einen Seite zur vollständigen Entlastung der anderen Seite führt (§ 254 BGB).

Verhaltensregeln für IT-Verantwortliche (inkl. angestellten CIO)

Soweit IT-Mitarbeiter arbeitsvertraglich für die IT-Sicherheit verantwortlich sind, sollten sich diese an die folgenden Verhaltensregeln halten. Dies gilt insbesondere für leitende Angestellte.

- **Klärung des Umfangs der eignen arbeitsvertragliche Aufgaben**

- **Einhaltung der Melde-, Reporting- und Eskalationsprozesse**

Regel: Was zu melden ist, liegt nicht mehr in der Verantwortung des Angestellten; ein umfassendes und detaillierten Melde- und Reportingwesen entlastet den Angestellten

- **Soweit unternehmerische Entscheidungen an den Angestellten (bei leitenden Angestellten) delegiert werden, ist die Business Judgement Rule einzuhalten**

- Sorgfältige Entscheidung
- auf Grundlage ausreichender und objektiver Informationen
- zum Wohl des Unternehmens

Beispiel: Will der CIO eine Machbarkeitsstudie für ein IT-Projekt von seinen Mitarbeitern erstellen lassen, hat er die Objektivität der Begutachtung gegebenenfalls auch durch externen Sachverstand (Zweitbegutachtung) sicherzustellen.

- **Sorgfältige Dokumentation von Maßnahmen nach 2. und 3**

Insbesondere leitende Angestellte trifft die Beweislast für die vertragsgemäße Erfüllung ihrer Pflichten aus dem Arbeitsvertrag; dies sollten sie unbedingt dokumentieren.

Beispiel: Vorschläge und Budgetanträge an den Vorstand für erforderlich gehaltene IT-Sicherheitsmaßnahmen;