

IT Security – eine rechtliche Betrachtungsweise

Mag. Christian Urban
Leitung Recht & Strategischer Einkauf



Corporate Governance (Quelle: Wikipedia)

Corporate Governance kann grundsätzlich als die Gesamtheit der organisatorischen und inhaltlichen Ausgestaltung der Führung und Überwachung von Unternehmen verstanden werden.

Die Diskussion zur Corporate Governance beschäftigt sich mit Regelungen, die für Mitarbeiter von Unternehmen oder die Unternehmen selbst gelten und die eine **"gute", verantwortungsvolle und zielgerichtete Führung und Überwachung von Unternehmen** bewirken sollen.

Wer diese Regeln setzt, ist dabei unterschiedlich. Es können der Gesetzgeber, die Eigentümer, die Mitarbeiter, der Aufsichts- oder Verwaltungsrat, das Management, die Gesellschaft oder andere Interessenten sein. Je nachdem, wer sie setzt, stehen sie in einem Gesetz, in Richtlinien, einem Kodex, im Unternehmensleitbild, in Absichtserklärungen oder sind beispielsweise als Usus möglicherweise gar nicht schriftlich fixiert. Corporate-Governance-Regeln können dadurch sowohl verpflichtend als auch unverbindlich ausgestaltet sein, bei letzteren ist die Einhaltung dann gern gesehen.

Einleitung

Compliance (aus Wikipedia)

In der Fachsprache wird der Begriff **Compliance** bzw. **Komplianz** verwendet, um die **Einhaltung von Gesetzen und Richtlinien**, aber auch freiwilligen Kodizes in Unternehmen zu bezeichnen. Die Sicherstellung von Compliance/Regelüberwachung in Unternehmen können organisatorische Maßnahmen stützen.

Hierzu richten einige Unternehmen eigene Compliance/Überwachungs-Abteilungen ein. Sie wachen beispielsweise darüber, dass die nationalen und internationalen Gesetze und Richtlinien gegen kriminelle Handlungen (z.B. Betrug), Finanzsanktionen, Marktmissbrauch, Interessenkonflikte, Datenschutz, Insiderhandel oder eingehalten werden. Einige dieser Compliance Abteilungen kümmern sich ausschließlich um die Überwachung und Einhaltung wesentlicher Vorschriften und Richtlinien und übernehmen in der Regel keine weiteren operativen Aufgaben.

Daneben gilt Compliance/Überwachung als ein bedeutendes Element der ordnungsgemäßen Unternehmensführung (Corporate Governance). Zunehmend von Bedeutung für die Compliance/Regelüberwachung ist auch die Informationssicherheit.

Verantwortung des Managements

§ 22 GmbHG IKS – Internes Kontrollsystem

Die Geschäftsführer haben dafür zu sorgen, dass ein Rechnungswesen und ein internes Kontrollsystem geführt werden, die den Anforderungen des Unternehmens entsprechen

§ 82 AktG

Der Vorstand hat dafür zu sorgen, dass ein Rechnungswesen und ein internes Kontrollsystem geführt werden, die den Anforderungen des Unternehmens entsprechen

Diese Verpflichtung gilt unabhängig von der Größe des Unternehmens

Deutschland: Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

Verantwortung des Managements

Begriff „internes Kontrollsystem“

- Unter internen Kontrollen sind die Abläufe und Maßnahmen zu verstehen, die die Verlässlichkeit des Rechnungswesens (va. auch des externen), die Wirksamkeit und Effizienz der Geschäftstätigkeit und die Einhaltung anzuwendender gesetzlicher Bestimmungen sicherstellen.
- Interne Kontrollen sprechen Risiken an, die die Erreichung dieser Ziele gefährden könnten. Sie werden von den für die Unternehmensführung verantwortlichen Mitarbeitern (Management usw.) entworfen und umgesetzt.
- Das Ziel der internen Kontrollen ist die Ausschaltung der Risiken
- Die Gesamtheit aller Kontrollen = internes Kontrollsystem

Verantwortung des Managements

Bekannteste Grundlagen eines Internen Kontrollsystems sind folgende Prinzipien:

- **Das Prinzip der Transparenz:** Dieses Prinzip besagt, dass für Prozesse Sollkonzepte etabliert sein müssen, die es einem Außenstehenden ermöglichen zu beurteilen, inwieweit Beteiligte konform zu diesem Sollkonzept arbeiten. Gleichzeitig wird dadurch die Erwartungshaltung der Organisationsleitung definiert.
- **Das Prinzip der Vier Augen:** Dieses Prinzip besagt, dass keine einzelne Person alleine verantwortlich für einen Prozess sein darf. Vielmehr müssen fachlich dazu ausreichend geeignete Personen den Vorgang bearbeiten, um mögliche Abweichungen und Kontrollschwächen zu erkennen und auszuschalten. Dazu gehört auch, dass Verfügungen über das Vermögen des Unternehmens nicht durch Einzelne getroffen werden dürfen.
- **Das Prinzip der Funktionstrennung:** Dieses Prinzip besagt, dass eine Trennung zwischen Auftragserfüllung (operative Verantwortung) und Auftragskontrolle (Soll-Ist-Vergleich) zu etablieren ist.
- **Das Prinzip der Mindestinformation:** Dieses Prinzip besagt, dass für Mitarbeiter nur diejenigen Informationen verfügbar sein sollen, die sie für ihre Arbeit brauchen. Dies schließt auch die entsprechenden Sicherungsmaßnahmen bei IT-Systemen mit ein.

Verantwortung des Managements

Was ist zu tun?

- Identifizierung der Risiken für den Geschäftsbetrieb
- Bewertung der Eintrittswahrscheinlichkeiten der identifizierten Risiken
- Erstellung von Regelungen zur Vermeidung der Risiken (Policies/Prozesse/Guidelines ect.)
- Evaluierung des Prozesses im Unternehmen zum Ausrollen der erstellten Regulative
- Etablierung eines Überwachungsprozesses ob die Regeln eingehalten werden (Audits)
- Etablierung eines Prozesses wie bei Verstößen vorzugehen ist
- An sich ziehen der Entscheidungskompetenz wenn die Missstände bestehen bleiben

Gefahrenpotential

Einige mögliche Gefahrenpotentiale

- Viren, Würmer, Trojaner und ähnliches Ungeziefer
- Spams, Phishing Attacken, Backscatter Mails
- unterlassene oder unzureichende Firewall, Antivirenlösung, ect.
- Denial of Service Attacken (zB als Opfer oder unfreiwilliger Mittäter eines Botnet)
- Dokumenten – Verlust, Verfälschung, unberechtigte Löschung, Datenintegrität
- Datendiebstahl – durch Konkurrenz / durch Mitarbeiter

SCHADEN

Zivilrechtliche Grundlagen

Haftung des Geschäftsführers/Vorstand

§ 25 GmbHG

(1) Die Geschäftsführer sind der Gesellschaft gegenüber verpflichtet, bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.

(2) Geschäftsführer, die ihre Obliegenheiten verletzen, haften der Gesellschaft zur ungeteilten Hand für den daraus entstandenen Schaden.

§ 84 AktG gleiche Verhaltensanordnung für den Vorstand

Zivilrechtliche Grundlagen

IT Sicherheit & IT Risk Management ist primär Chefsache

§§ 25 & 22 GmbHG; §§ 84 & 82 AktG; § 3 VerbVG

Doch es haftet nicht nur der „Chef“

Die Verantwortung trifft im Rahmen der Delegation auch die Fachverantwortlichen (wie etwa IT Leiter)

Ebenso den einzelnen Mitarbeiter, welcher sich über Bestehende Richtlinien oder gar Gesetze hinwegsetzt



Zivilrechtliche Rechtsfolgen

Schadenersatz

- Gegenüber Kunden
- Gegenüber Lieferanten
- Gegenüber dem eigenen Unternehmen
- Haftung mit Privatvermögen
- DNHG tlw. Nur bedingt anwendbar
- **FAHRLÄSSIGKEIT** reicht aus

Strafrechtliche Grundlagen

Cyber Crime Convention (Europarat 23.11.2001)

Das Übereinkommen ist die erste internationale Vereinbarung über mittels Internet oder sonstiger Computernetze begangene Straftaten.

Es betrifft vor allem Verletzungen des Urheberrechts, Betrug per Computer, Kinderpornographie und Verstöße gegen die Sicherheit von elektronischen Netzen.

Das Übereinkommen enthält auch eine Reihe von Ermächtigungen und Verfahrensvorschriften wie etwa zur Suche in Computernetzen und zum Abfangen von Nachrichten.

Hauptzweck ist laut der Präambel die Verfolgung einer gemeinsamen Strafrechtspolitik zum Schutz der Gesellschaft vor Straftaten per Computer (sog. cybercrimes), und zwar insbesondere durch entsprechende gesetzliche Regelungen und die Förderung internationaler Zusammenarbeit.

Strafrechtliche Grundlagen

Strafgesetzbuch (StGB; auszugsweise)

- § 118a – Widerrechtlicher Zugriff auf ein Computersystem (zB. Password guessing ect.)
- § 119 – Verletzung des Telekommunikationsgeheimnis
- § 119a – Missbräuchliches Abfangen von Daten (zB. Sniffing usw.)
- § 126a – Datenbeschädigung
- § 126b – Störung der Funktionstüchtigkeit eines Computersystems
(zB. DDoS (Distributed Denial of Service) Attack – Angreifer verwendet zuvor gehackte „Zombies/Botnets“ um ein System anzugreifen
- § 126c – Missbrauch von Computerprogrammen oder Zugangsdaten

Sonstige Grundlagen

Datenschutzgesetz – DSG 2000

§ 51 Datenverwendung in Gewinn- oder Schädigungsabsicht

- (1) Wer in der Absicht, sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.
- (2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Sonstige Grundlagen - Urheberrecht

Aktuelle Fälle - Microsoft Internet Explorer

Adresse <http://www.microsoft.com/austria/originalsoftware/aktuellefaelle.mspix>

Auf Kundenseite

- Ein Metallbearbeitungsbetrieb in der Nähe von Steyr/OÖ verpflichtete sich im **August 2006** nach einer gerichtlichen Hausdurchsuchung zu einer Schadenersatzzahlung von EUR 29.000,- aufgrund von Verwendung unlizenzierter Software von Autodesk und Microsoft. Darüber hinaus hat das Unternehmen die Pauschalgebühren des gerichtlichen Vergleichs zu tragen und die Pauschalkosten des Strafverfahrens zu ersetzen, sowie für jede weitere einzelne Verletzung eine Vertragsstrafe von EUR 300,- zu bezahlen. Weiters muss das Unternehmen Lizenzen nachkaufen.
- Im **September 2006** verpflichtete sich ein Spenglereibetrieb in Linz nach einer gerichtlichen Hausdurchsuchung aufgrund eines Strafverfahrens gegen den Geschäftsführer zu einer Schadenersatzzahlung von EUR 90.000,- aufgrund von Verwendung unlizenzierter Software von Adobe, Autodesk und Microsoft. Darüber hinaus hat das Unternehmen die Pauschalgebühren des gerichtlichen Vergleichs zu tragen und die Pauschalkosten des Strafverfahrens zu ersetzen, sowie für jede weitere einzelne Verletzung eine Vertragsstrafe von EUR 300,- zu bezahlen. Die gesamte Unternehmensgruppe muss im großen Umfang Lizenzen nachkaufen.
- Gegen die Geschäftsführerin eines Consulting- und Schulungsunternehmens in Wien-Innere Stadt war ein Strafverfahren anhängig. Das Unternehmen verpflichtete sich im **September 2006** nach einer gerichtlichen Hausdurchsuchung zu einer Schadenersatzzahlung von EUR 18.000,- wegen Verwendung unlizenzierter Software von Adobe und Microsoft. Weiters hat das Unternehmen die Pauschalgebühren des gerichtlichen Vergleichs zu zahlen und die Pauschalkosten des Strafverfahrens zu ersetzen, sowie für jede weitere einzelne Verletzung eine Vertragsstrafe von EUR 300,- an die Geschädigten zu bezahlen. Das Unternehmen muss auch Lizenzen nachkaufen.
- Im **Mai 2005** hat sich ein Computerhändler mit Sitz in Fussach, Vorarlberg gegenüber der Microsoft Corporation verpflichtet:
 1. es ab sofort zu unterlassen, nicht lizenzierte Kopien von Computerprogrammen der unbefugt zu vervielfältigen und/oder unbefugt hergestellte Kopien zu gebrauchen und/oder unbefugt hergestellte Kopien davon zu verbreiten.
 2. einen pauschalierten **Schadenersatzbetrag** in der Höhe von **€ 18.500** zu Händen ihrer Rechtsvertreter zu bezahlen, die Pauschalkosten des gerichtlichen Vergleichs zu tragen und die Pauschalkosten des Strafverfahrens zu ersetzen.
- Im **Juli 2004** unterzeichnete ein Unternehmen des Montagebaus mit Sitz in Unterkärnten und dessen Geschäftsführer einen Vergleich. Dieser enthielt unter anderem eine **Schadenersatzzahlung** in Höhe von **€ 125.000** aufgrund der Verwendung von unlizenzierter Software mehrerer Hersteller, weiterhin hat das Unternehmen die Pauschalkosten des gerichtlichen Vergleichs zu tragen und die Pauschalkosten des Strafverfahrens zu ersetzen.
- Im **Juli 2003** mußte ein Marketingdienstleistungsunternehmen in Wien nach erfolgtem Strafantrag und einer Hausdurchsuchung, bei der auf mehreren PCs unlicenzierte Software gefunden worden war, im Rahmen eines Vergleiches **€63.000.-Schadenersatz** zahlen.
- Mitte **Mai 2003** unterzeichnete ein Unternehmen in Tirol einen Vergleich, der ua eine **Schadenersatzzahlung** in Höhe von **€ 25.000.-** wegen unlizenzierter Verwendung von Microsoft Computerprogrammen zum Inhalt hatte.

Fertig 24 von 24 - Zwischenablage
Element wurde der Sammlung hinzugefügt.

Start | 2 M... | Micr... | 4 I... | H:\... | Micr... | Po... | 2 A... | Micr... | 14:29

Sonstige Grundlagen - Urheberrecht

Konsequenzen von Urheberrechtsverstößen § 91 UrhG:

- Vorsätzliche Verletzungen des Urheberrechts sind strafbar und werden gerichtlich verfolgt!
- Unternehmen, die Software unlizenziert einsetzen, machen sich strafbar und müssen mit zivil- oder strafrechtlicher Ahndung rechnen.
- Im Rahmen des so genannten Organisationsverschuldens haftet in den allermeisten Fällen der Geschäftsführer eines Unternehmens.
- Geldstrafen bis zu 360 Tagessätzen oder Freiheitsstrafen bis zu 6 Monaten - bei Gewerbsmäßigkeit sogar bis zu 2 Jahren - ,
- Hausdurchsuchungen, Beschlagnahmen, Vernichtung und Unbrauchbarmachung von Eingriffsgegenständen und Eingriffsmitteln sowie Urteilsveröffentlichungen;
- Zivilrechtlich bestehen darüber hinaus Ansprüche auf Unterlassung, Beseitigung, Urteilsveröffentlichung, angemessenes Entgelt oder (bei Verschulden) Schadenersatz, Gewinnherausgabe und Rechnungslegung.

Sonstige Grundlagen

Verbandsverantwortlichkeitsgesetz

- Seit 1.1.2006 in Kraft
- Neben Strafbarkeit der natürlichen Personen nun auch Strafbarkeit des Unternehmens
- strafbare Handlung zum Vorteil des Unternehmens
- Unternehmen hat keine zumutbaren Maßnahmen gesetzt um Handlungen zu unterbinden (zB. Sicherheitsvorkehrungen, Richtlinien)
- Geldstrafen bis max. 1,8 Mio Euro
- Vorrangig von den Gewinnen einzubehalten
- Vom Mitarbeiter nicht regressierbar
- **GESCHÄFTSKRITISCH !!**

Mögliche Konsequenzen

Strafrechtlich

- Geldstrafe
- Haftstrafe
- und damit Vorstrafe (kein Leumund)
- Beschlagnahme von Systemen und sonstigen Gegenständen

Strafrechtsdelikte sind fast ausschließlich Vorsatzdelikte

Zusammenfassung

- Das Gesetz sagt ihnen nicht wie ihre Systemlandschaft auszusehen hat bzw. einzurichten ist
- Dies deshalb, weil der Gesetzgeber mit der technologischen Entwicklung nicht mithalten kann
- Dennoch gibt es zahlreiche Regelungen, die von ihnen zu beachten sind
- Die Zuordnung ist aber oft nicht einfach und bedarf rechtlicher Grundkenntnisse (zB. Analogieverbot im Strafrecht)
- Rechtliche Regelungen in Hinblick auf Security finden sie u.a. im DSG 2000, StGB, ZuKG, UGB, UrhG, ect.
- Welchen Sorgfaltsmaßstab (auch in technischer Hinsicht) sie dabei anzuwenden haben, finden sie in Richtlinien und Standards wie zB. IT Grundschutz, Cobit, ISO x.x, ITIL usw.

Mag. Christian Urban
Leitung Recht & Strategischer Einkauf

Kapsch BusinessCom AG | Abteilung
Wienerbergstraße 53 | A-1120 Vienna | Austria

Tel. +43 (0) 50 811 5474
Mobil +43 (0) 664 628 5474
Fax +43 (0) 50 811 99 5474
e-mail christian.urban@kapsch.net
www.kapsch.net