Leitfaden IT-Sicherheits-management 2011

Inhalt

BUSE HEBERER FROMM
RECHTSANWÄLTE · STEUERBERATER PARTG

INTARGIA
IDEE.IT.ZIEL

„Die Risikofaktoren der IT-Kultur von Unternehmen sind eine ständig wachsende Herausforderung für deren Corporate Governance."

1 Einleitung

Für ein erfolgreiches IT-Sicherheitsmanagement ist die Erkennung und Bewertung bestehender Sicherheitsrisiken Voraussetzung. Dies gilt umso mehr, als IT-Systeme und -Prozesse in Unternehmen vielfältigen gesetzlichen Anforderungen genügen müssen. Gerade kleine und mittelständische Unternehmen können bei Missmanagement im Bereich IT-Sicherheit schnell in die Nähe einer existenziellen Bedrohung geraten. In den vergangenen Jahren erhöhte sich aber auch die Zahl spektakulärer Firmenzusammenbrüche und Hackerattacken auf zentrale IT-Systeme von Großunternehmen.

Die umfassende Nutzung von Netzwerkinfrastrukturen und der zunehmende Einsatz von mobilen, medienkonvergenten Endgeräten erhöhen dabei zwangsläufig das Sicherheitsbedürfnis der Unternehmen, denn mit der Komplexität und Anzahl der genutzten ITK-Systeme wachsen auch Anzahl und Schweregrad möglicher Angriffe. Es drohen Ausfälle im Geschäftsbetrieb, Imageverlust, Informationsmissbrauch sowie Schadensersatzansprüche.

Um diesen Risiken im Bereich der IT-Sicherheit wirksam begegnen zu können, benötigen Unternehmen und öffentliche Einrichtungen ein geplantes, strukturiertes und methodisches IT-Risikomanagement sowie die notwendige Sensibilität für Warnsignale und potentielle Sicherheitslücken.

Nicht zuletzt die durch das Bilanzmodernisierungsgesetz eingeführten Neuregelungen unterstreichen die Pflicht zur Errichtung eines IT-Risikomanagements gemäß § 91 Absatz 2 AktG. Die Umsetzung der neu eingeführten Anforderungen kann mit hohem Aufwand verbunden sein – insbesondere die Organisation und Abläufe in den Fachabteilungen betreffend. Die hieraus resultierenden spezifischen Pflichten der Geschäftsleitung im Hinblick auf das IT-Risikomanagement werden nachstehend aus technischer und rechtlicher Perspektive dargestellt. Der Schlüssel zum Erfolg der Umsetzung der einzelnen Bausteine des (stets notwendigen) IT-Sicherheitsmanagements ist also ein individuelles Vorgehensmodell mit Augenmaß.

Die Datenschutz- und IT-Sicherheitsexperten von INTARGIA Managementberatung und Buse Heberer Fromm Rechtsanwälte Steuerberater möchten Ihnen mit diesem Leitfaden einen praktischen Ratgeber zur Beantwortung Ihrer wichtigsten unternehmerischen Fragen im Bereich IT-Sicherheitsmanagement an die Hand geben. Herrn Rechtsanwalt Dr. Marco Rau, Telefónica o2 Germany GmbH & Co. OHG, München, danken wir für wertvolle Beiträge und die gute Zusammenarbeit.

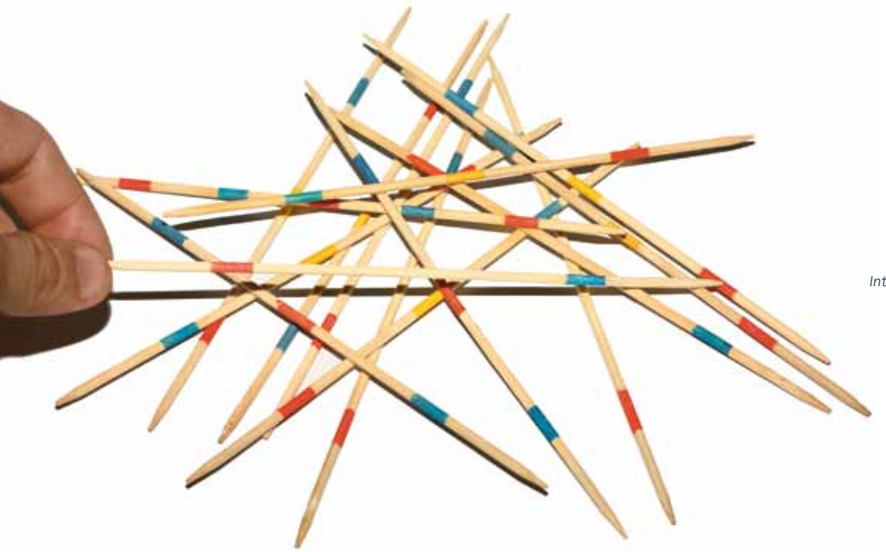
Wir freuen uns, Ihnen diesen gemeinsamen Leitfaden präsentieren zu dürfen.

Dr. rer.pol., Dipl.-Ing. Thomas Jurisch
Geschäftsführender Gesellschafter
ISO 27001 Lead Auditor
INTARGIA Managementberatung GmbH

Stephan Menzemer
Rechtsanwalt, Partner
Buse Heberer Fromm Rechtsanwälte
Steuerberater Partnerschaftsgesellschaft

Dipl. Betriebswirt (FH) Steffen Weber
Berater
ISO 27001 Lead Auditor
INTARGIA Managementberatung GmbH

Tim Christopher Caesar
Rechtsanwalt, Associate
Buse Heberer Fromm Rechtsanwälte
Steuerberater Partnerschaftsgesellschaft



MANAGEMENT DER INFORMATIONSSICHERHEIT
Sensible Prozesse hängen von einer soliden Integrität der IT-Landschaft in Organisationen ab.

2 Die Bedeutung von IT-Sicherheit für Unternehmen und öffentliche Einrichtungen

Unternehmen und öffentliche Einrichtungen im 21. Jahrhundert sind Teil der globalen Informations- und Wissensgesellschaft. Treiber für die zunehmende Bedeutung von Informationen und Wissen sind die Internationalisierung und Globalisierung von Märkten, Produkten und Ressourcen, die ansteigende Verfügbarkeit von elektronischen Informationen und die zunehmende Ubiquität vernetzter Informations- und Kommunikationstechnologie.

Aus Unternehmenssicht ist die Auseinandersetzung mit diesen Themen erfolgskritisch. Unternehmensziele wie die Fokussierung auf das Kerngeschäft, „Operational Excellence", effizientes Sourcing, Compliance oder organisatorische Umbrüche, z.B. durch Akquisition, Fusion oder Kooperation, sind nur durch eine enge Verzahnung von Unternehmens- und IT-Strategie zu erreichen.

Analog zu den Chancen, die diese Entwicklungen Unternehmen bieten, sehen Sie sich auch einem wachsenden Risiko gegenüber. Elektronisch vorliegende Informationen sind heute leicht zu vervielfältigen, zu verfälschen und zu verteilen. Darauf muss ein Unternehmen reagieren, um seine Informationen zu schützen und deren Integrität, Vertraulichkeit und Verfügbarkeit zu gewährleisten.

Aktuelle Studien zeigen: Unternehmen sehen sich in wachsendem Maße internen und externen Bedrohungen der Unternehmens-IT und somit hochsensibler Unternehmensinformationen in Verbindung mit einer zunehmenden „Professionalisierung" der Angriffe konfrontiert.

Wie ernst Unternehmen diese Bedrohungen nehmen, wird insbesondere dadurch deutlich, dass unter den IT-Verantwortlichen (z.B. CIOs) der Unternehmen Security bzw. IT-Risikomanagement mit großem Abstand und zum wiederholten Male ein Top-Thema hinsichtlich Wichtigkeit von IT-Themen in den kommenden Jahren darstellt.

Sobald IT-Systeme durch ein Netzwerk miteinander verbunden sind, besteht ohne weitere Schutzmaßnahmen die Gefahr unbefugter Zugriffe auf die Systeme von anderen Rechnern aus. Die Anbindung der lokalen Netze an öffentliche Weitverkehrsnetze wie dem Internet vergrößert diese Bedrohung noch, da Angreifer nun von überall auf der Welt versuchen können, die IT-Systeme zu kompromittieren.

Sowohl organisierte Gruppen mit kriminellem Hintergrund als auch „spezialisierte" Einzeltäter versuchen, sich durch die Penetration von Sicherheitssystemen bekannter deutscher Unternehmen wirtschaftliche Vorteile zu verschaffen oder sich in der Hacker-Szene einen Namen zu machen. Dies ist aber nur die sichtbare Spitze des Eisbergs – das „Geschäftsfeld" der Cyberkriminalität stellt tatsächlich eine reale Bedrohung für alle Unternehmen und öffentlichen Einrichtungen dar.

3 Prominente Vorfälle

Die herausragende Bedeutung der IT-Sicherheit für Unternehmen und öffentliche Einrichtungen lässt sich nicht zuletzt an vielen Aufsehen erregenden Vorfällen aus der Praxis ablesen. So erlangten z.B. Ende Januar 2010 Cyber-Kriminelle durch einen weltweit angelegten Phishing-Angriff die Passwörter und Zugangsdaten einiger Händler und Unternehmen der Deutschen Emissionshandelsstelle (DEHSt).

Sie schickten dazu eine fingierte, vermeintlich von der DEHSt stammende E-Mail an die gelisteten Unternehmen des online abgewickelten Emissionshandels mit der Aufforderung, sich (zum „Schutz vor Hackern") erneut zu registrieren. Für die angeblich erforderliche Neuregistrierung war das aktuelle DEHSt-Passwort anzugeben. Immerhin sieben der 2000 angeschriebenen Zertifikate-Nutzer reagierten (trotz vorheriger Warnungen durch die DEHSt) auf die E-Mail-Anfrage. Daraufhin wurden die von diesen Nutzern auf einer zu Betrugszwecken erstellten (Phishing-) Website eingetragenen Log-In-Daten genutzt, um Emissionsberechtigungen auf Konten in Großbritannien und Dänemark weiterzuleiten und sie anschließend zu verkaufen.

Dieser Angriff führte zu einem Schaden von über 3 Mio. Euro: ca. 250.000 Emissionsberechtigungen wurden ohne Einwilligung und Kenntnis der Berechtigten gehandelt und anschließend durch die unbekannten Täter verkauft. In 17 EU-Staaten wurden daraufhin die CO_2-Datenbanken vorübergehend geschlossen, so dass zwar der Handel getätigt werden konnte, die Transaktionen aber zunächst nicht rechtswirksam registriert wurden.

Neben den umfangreichen Ermittlungen der Strafverfolgungsbehörden, die der Reputation des Emissionshandelsplatzes mit Sicherheit nicht zuträglich waren, drohen den Betreibern des virtuellen Handelsplatzes sowie den IT-Verantwortlichen der aufgrund mangelnder (IT-) Sicherheitsvorkehrungen geschädigten Unternehmen auf zivilrechtlicher Ebene Schadenersatzansprüche.

In einem weiteren prominenten Fall gab Google Anfang 2010 bekannt, Opfer von Hackerattacken aus China zu sein. Diese koordinierten Angriffe richteten sich scheinbar gegen mehrere US-Amerikanische Firmen, unter anderem auch Adobe. Daraufhin begannen breit angelegte Ermittlungen, um die Hintergründe dieser Angriffe aufzudecken. Am 18.02.2010 wurde dazu über die New York Times bekannt, dass die Angriffe bereits im April 2009 begonnen haben könnten. In einem Artikel wurde vermutet, diese seien von der Shanghai Jiaotong University sowie von der Lanxiang Vocational School ausgegangen. Tatsächlich bleibt im Unklaren, wer die Täter hinter den Angriffen sind. So könnten die Angriffe auch von einem Drittland aus zur Verschleierung der Identität (sog. ‚false flag') über die Hochschulen durchgeführt worden sein.

Nach Auskunft von Google sind die durch die Angriffe beeinträchtigten Systeme zwischenzeitlich wieder voll funktionsfähig; zu den Kosten der Fehlerbehebung und der nun erfolgenden Erhöhung von IT-Sicherheitsmaßnahmen macht das Unternehmen allerdings keine Angaben.

Eine im Jahr 2009 durchgeführte Studie über „Netz- und Informationssicherheit in Unternehmen 2009" des Netzwerks Elektronischer Geschäftsverkehr (NEG), die ihren Fokus vor allem auf kleine und mittelständische Unternehmen in Deutschland richtete, ergab zudem, dass jedes zehnte der befragten Unternehmen bereits Opfer eines Angriffs wurde. Dies zeigt deutlich, dass Netz- und IT-Sicherheit auf allen Ebenen eine gewichtige Rolle spielt und spielen muss.

BEDROHUNGSMANAGEMENT
IT-Risikomanagement hilft beim Schutz vor unangenehmen Überraschungen in Sicherheitsarchitekturen.

4 Grundlagen der IT-Sicherheit

Um einen Überblick über das Thema IT-Sicherheitsmanagement zu ermöglichen, sollen an dieser Stelle die wichtigsten Grundlagen vorgestellt werden:

Ein IT-System stellt einen systematischen Verbund informationstechnischer Komponenten dar. IT-Sicherheit sorgt dafür, dass die Risiken für diesen Verbund – in welcher Größe oder Ausprägung auch immer – erkannt, bewertet und gemanagt werden. In der Definition des Bundesamts für Sicherheit in der Informationstechnik (BSI) bezeichnet IT-Sicherheit dementsprechend „[...] einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind."

Ziele von IT-Sicherheit

Man unterscheidet folgende Sicherheitsziele einer Organisation:

- **Vertraulichkeit:** Sicherheit vor unbefugtem Zutritt, Zugang oder Zugriff
- **Integrität:** Sicherheit vor unbefugter Modifikation von Informationen.
- **Verfügbarkeit:** Sicherheit vor Beeinträchtigung der Funktionalität von IT-Systemen oder des Zugangs zu IT-Systemen

Zusätzlich zu diesen sogenannten klassischen Zielen der IT-Sicherheit können weitere Ziele benannt werden, z.B. Zurechenbarkeit, Authentizität und Revisionsfähigkeit.

IT-Sicherheit ist gewährleistet, wenn die individuell definierten Sicherheitsziele für das jeweils betrachtete System durch angemessene Maßnahmen erreicht und laufend überwacht werden. Die Erreichung der genannten Ziele tritt jedoch nicht automatisch ein, da für jede Organisation individuelle Bedrohungen existieren.

Hierzu zählen:

- Bedrohungen durch höhere Gewalt (Erdbeben, Feuer etc.)
- Vorsätzliches Handeln (Manipulation, Hacking, Wirtschaftsspionage, Social Engineering etc.)
- Fahrlässigkeit und menschliches Fehlverhalten
- Technisches Versagen (Hardware- oder Stromausfall etc.)
- Organisatorische Mängel (z.B. Fehlendes oder mangelhaftes Berechtigungskonzept, ungeschultes Personal etc.)

Als Folge realisierter Bedrohungen können für Unternehmen monetäre Schäden entstehen sowie weitere Konsequenzen wie z.B. Image- oder Kreditwürdigkeitsverlust eintreten.

Teildisziplinen der IT-Sicherheit

Die Disziplin IT-Sicherheit umfasst alle Teildisziplinen, die in Summe alle wichtigen Aspekte der Gewährleistung von IT-Sicherheit abdeckt (s. Tabelle rechts oben).

Teildisziplinen der IT-Sicherheit

Teildisziplin	Abgedeckte Themen
Identitäts-management	• Digitale Identitäten und Rollenmodelle • Methoden d. Identitäts- und Authentisierungsprüfung • Verzeichnisdienste • Single-Sign-on • Public-Key-Infrastrukturen • Identitätsträger (Chipkarten etc.)
Zugangs-management	• System-Zugriffsschutz • Netzwerk-Zugriffsschutz (Firewalls etc.) • Chiffrierung • Data Ownership
Entwicklung / Integration	• „Trusted Computing Base" • Sichere Softwareentwicklung • Integration, Testen und Wartung
Bedrohungs-management	• Bedrohungen und Schwachstellen • Angreifer und Intentionen • Inhaltliche Kontrolle und Management (Antivirus, -SPAM, -Spyware, aktive Inhalte, URL-Filter, usw.) • Schwachstellen-/Verwundbarkeitsmanagement und „Security Policy Compliance" (System Hardening und/oder Baselining) • Intrusion Detection / Prevention (host- und/oder netzwerkbasiert)
Management der Informations-sicherheit	• Recht und Regulation • Standards und „Best Practices" • Corporate Governance • Dienstleistungen und Kunden/Märkte • Mitarbeiter (Sicherheitsbewußtsein, Know-how etc.) • Aufbau-/Ablauforganisation der Unternehmung • Hersteller/Lieferanten, Abhängigkeiten, Due Diligence • Öffentlicher Ruf/Ruf der Unternehmung usw.
Compliance	• Sicherheitsstandards und Sicherheitsinstrumente • Unternehmensinterne organisatorische Fragen • Externe Auflagen • Konsequenzen der „Non-Compliance"

Mobile IT-Sicherheit

Um den Anforderungen einer zunehmend internationalen und immer stärker virtuellen Arbeitswelt gerecht zu werden, setzen Unternehmen in immer größerem Umfang mobile Endgeräte wie z.B. Smartphones, PDAs und Laptops sowie drahtlose Kommunikationsverfahren, wie GSM, UMTS, Bluetooth und WLAN, ein. Für die mobile Nutzung von Informationstechnik ergeben sich allerdings spezifische Risiken, etwa durch den möglichen physischen Verlust mobiler Endgeräte durch Diebstahl oder Nachlässigkeit oder durch Ausspähung kritischer Daten durch Dritte (z.B. Firmenwissen oder vertrauliche interne Informationen). Daraus ergeben sich für Organisationen besonders hohe Anforderungen an die IT-Sicherheit.

„Best Practice"-Ansätze für IT-Sicherheit

Dem Schutz von Informationen, IT-Systemen und informationsverarbeitenden Geschäftsprozessen kommt eine wachsende Bedeutung zu. Zur Unterstützung der Entwicklung, Implementierung und Optimierung angemessener Sicherheit auf allen Ebenen in Unternehmen oder Behörden wurde eine Vielzahl an Hilfsmitteln geschaffen.

Sie alle haben zum Ziel, für den jeweiligen Themenbereich „Best Practice-Ansätze" zu liefern. Diese bieten einer Unternehmung die Möglichkeit, mit bewährten Methoden und einem dem Schutzbedarf angemessenem Aufwand eine gute Abdeckung für die Informationssicherheit zu erreichen.

Zu den wichtigsten Best Practice-Ansätzen in Deutschland zählen die Standards ISO 27000ff. und BSI 100-1 bis 100-4 in Verbindung mit den IT-Grundschutz-Katalogen des BSI.

5 Ein Ansatz für ganzheitliches IT-Sicherheitsmanagement „mit Augenmaß"

Nachhaltigkeit und Effektivität können sich nur durch einen geplanten, systematischen und zyklischen Prozess einstellen. Deshalb ist auch im Bereich IT-Sicherheit das Managementsystem, mit den Elementen „Planen, Durchführen, Kontrollieren, Handeln" eine sinnvolle Methode.

Das Hauptziel eines effektiven IT-Sicherheitsmanagements ist es, die Geschäftsprozesse und die darin verarbeiteten Informationen hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit zu schützen. In einem Initial-Audit wird der Status quo des IT-Sicherheitsmanagements im Unternehmen auditiert. Dabei sollte der individuelle Bedarf an IT-Sicherheitsmaßnahmen immer mit Augenmaß und in Abhängigkeit der zu schützenden Geschäftsprozesse definiert werden. Auf Basis dieser Ergebnisse wird die IT-Sicherheitsstrategie definiert. Des Weiteren werden die aus den Handlungsempfehlungen des Audits resultierenden technischen und organisatorischen Maßnahmen geplant und umgesetzt. Die Umsetzung wird kontrolliert, regelmäßig hinsichtlich Effektivität und Effizienz (re-)auditiert und durch bedarfsabhängige IT-Sicherheitsberatung ergänzt. Eingebettet in eine funktionierende IT-Sicherheits-Organisation und -Kultur wird durch professionelles Projektmanagement sichergestellt, dass die Ziele unter Berücksichtigung von Zeit, Kosten und Qualität erreicht werden können.

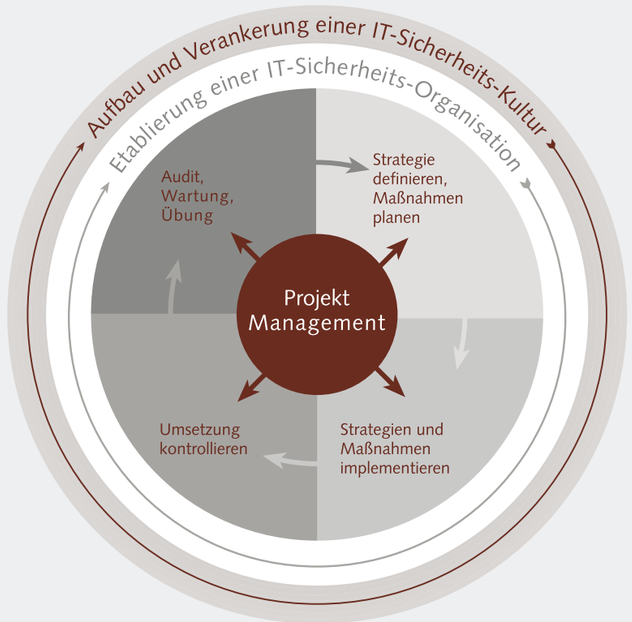
> Phase 1: Ist-Analyse

Effektives IT-Sicherheitsmanagement gewährleistet Vertraulichkeit, Integrität und Verfügbarkeit der Geschäftsprozesse des Unternehmens und die in ihnen verarbeiteten Informationen. Wie gut die bestehenden Maßnahmen diese Aufgabe erfüllen, wird im Rahmen eines Initial-Audits analysiert und bewertet. Auf Basis dieser Erkenntnisse können im Anschluss der weitere Projektverlauf systematisch geplant und die einzurichtenden technischen und organisatorischen Maßnahmen ausgewählt werden. Folgende Schritte werden beim Initialaudit durchgeführt:

IT-Risikoanalyse

Die Risikoanalyse gibt im Ergebnis Aufschluss über die IT-Infrastruktur, die die technische Grundlage für effektive und effiziente Geschäftsprozesse ist. Für alle relevanten Geschäftsprozesse wird gemeinsam mit den Prozessverantwortlichen eine Einschätzung der Kritikalität hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität vorgenommen. Anschließend werden die für die Ausführung der Geschäftsprozesse notwendigen Applikationen, IT-Systeme, Räume und Gebäude aus den Ergebnissen der Strukturanalyse ausgewählt. Die Kritikalität des betrachteten Geschäftsprozesses „vererbt" sich auf die darunterliegende IT-Infrastruktur.

Weiter auf der nächsten Seite >



Vor-Ort-Interviews
Zur Einschätzung des IT-Sicherheitsniveaus wird der Ist-Zustand der Sicherheitsmaßnahmen für definierte Elemente mit Soll-Vorgaben verglichen. Hierzu wird ein eigens entwickelter Auditkatalog genutzt, der unter Berücksichtigung der Vorgaben der wichtigsten Standards für IT-Sicherheit erstellt wurde. Dieser Katalog wird auf die Rahmenbedingungen des jeweiligen Unternehmens individuell angepasst. Angaben des Unternehmens werden durch Stichprobenuntersuchungen vor Ort verifiziert. Die Ergebnisse der Untersuchung und konkrete Handlungsempfehlungen werden anschließend im Auditbericht zusammengefasst.

> **Phase 2: Strategie definieren und Maßnahmen planen**
Die Ergebnisse des Audits werden dem Unternehmen im Rahmen einer Ergebnispräsentation vorgestellt und erläutert.

Basierend auf diesen Ergebnissen wird gemeinsam mit den Verantwortlichen eine IT-Sicherheitsstrategie entwickelt und geeignete technische und organisatorische Maßnahmen zur Umsetzung abgeleitet.

Neben technischen Maßnahmen aus dem Bereich IT- und Informationssicherheit werden auch organisatorische Maßnahmen wie die Etablierung einer IT-Sicherheitsorganisation, Festlegung der Verantwortlichkeit für IT-Sicherheit im Unternehmen, Schulungs- und Sensibilisierungsmaßnahmen für die Mitarbeiter oder die Erstellung und Veröffentlichung des IT-Sicherheitshandbuchs berücksichtigt.

Alle diese Maßnahmen werden in dieser Phase geplant. Abschließend wird nach einer Priorisierung der Maßnahmen ein Zeitplan erarbeitet und die Frequenz für zukünftige Audit-Zyklen festgelegt.

> **Phase 3: Strategien und Maßnahmen implementieren**
Die geplanten technischen und organisatorischen Maßnahmen werden gemäß der festgelegten Priorisierung vom Unternehmen umgesetzt. Während des gesamten Projektes steht INTARGIA und Buse Heberer Fromm Rechtsanwälte Steuerberater mit ihren zertifizierten IT-Sicherheitsexperten jederzeit beratend zur Verfügung. Dies gilt für Anfragen der Geschäftsleitung ebenso wie für Anfragen von Mitarbeitern und externen Stakeholder wie Kunden oder Lieferanten.

> **Phase 4: Re-Audit/Wartung und Übung**
Als wichtiger Bestandteil des IT-Sicherheitsmanagements wird der Implementierungsgrad der Maßnahmen in Folgeaudits zyklisch kontrolliert und ausgewertet. Dazu wird ein Reifegradmodell verwendet, welches einerseits eine Übersicht über den aktuellen Status der IT-Sicherheit im Unternehmen zulässt und zum anderen einen direkten Vergleich mit früheren Auditergebnissen ermöglicht. Hieraus lassen sich jederzeit Aussagen über die Weiterentwicklung von IT-Sicherheit im Unternehmen ableiten. Regelmäßiges Reporting an die Verantwortlichen im Unternehmen gehört ebenso zur Umsetzungskontrolle wie die professionelle Dokumentation von Status und Fortschritt des Informationssicherheits-Managementsystems.

Grafische Darstellung des IT-Sicherheitsreifegrads nach untersuchten Bereichen.

> **Begleitende Aktivität: Etablierung einer IT-Sicherheitsorganisation und -Kultur:**
„Der Mensch ist das größte Sicherheitsrisiko im Unternehmen." – Diese weitläufig akzeptierte Aussage zur Kritikalität von Gefahrenquellen zeigt sehr deutlich, dass ohne eine ausreichende Sensibilisierung (z.B. durch gezielte Schulungen) aller Mitarbeiter im Unternehmen, kein den Anforderungen entsprechendes Maß an IT-Sicherheit erreicht werden kann.

ENTWICKLUNG / INTEGRATION / MA-RISKS
Gerade in laufenden Projektprozessen sollten die rechtlichen Richtlinien den Rahmen für das eigene Vorgehen gestalten.

6 Ausblick: IT-Sicherheitsmanagement als Faktor für IT-Compliance

Das IT-Sicherheitsmanagement ist für Unternehmen ein wesentlicher Faktor der IT-Compliance. Die Begriffe IT-Sicherheitsmanagement und Compliance sind mit einer juristischen Bewertung von IT-Prozessen verbunden, die die Haftung der Organe der Gesellschaft (z.B. des Vorstandes oder der Geschäftsführer) in den Mittelpunkt stellt.

Vor diesem Hintergrund sind die im Folgenden dargestellten informationstechnischen Sicherheitsstandards zwingend zu gewährleisten und mit den entsprechenden Sicherheitsinstrumenten zu handhaben. Soweit diese Mindeststandards nicht eingehalten werden, stellt sich stets die Frage nach rechtlichen Konsequenzen.

Folgende Gesetze, Verordnungen und Richtlinien für das IT-Risikomanagement der Geschäftsführung sind von besonderem Interesse und werden nachstehend anhand ausgewählter, praxisrelevanter Konstellationen untersucht: das Bundesdatenschutzgesetz (BDSG), das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), die Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS), die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) sowie das Signaturgesetz (SigG).

Ergänzt werden diese durch verschiedene branchenspezifische gesetzliche Anforderungen wie das Telemediengesetz (TMG), die Mindestanforderungen an das Risikomanagement (MaRisk) oder das Gesetz über das Kreditwesen (KWG). Auf internationaler Ebene werden diese gesetzlichen Anforderungen an das IT-Risikomanagement in erster Linie durch die US-Gesetzgebung (SOX) sowie die 8. EU-Richtlinie und Basel II ergänzt.

IT-Risikoprävention gemäß § 91 Absatz 2 AktG

Durch die Verabschiedung des KonTraG im Jahr 1998 wurden u.a. wesentliche Normen des AktG und des HGB ergänzt. Die Neuregelungen führten zu einer substantiellen Erhöhung der Qualität der Abschlussprüfung durch erhöhte Anforderungen an die Prüfungsinhalte und den Prüfbericht selbst. Im Zusammenhang mit dem IT-Risikomanagement des Unternehmens ist § 91 Abs. 2 AktG von herausragender Bedeutung. Der Vorstand des Unternehmens hat danach „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden". Verstöße gegen diese Verpflichtungen haben schwerwiegende Haftungsfolgen, da im Fall der Verletzung dieser Pflichten eine persönliche Haftung

des Vorstandes auf Schadenersatz gegenüber der Gesellschaft droht (§ 93 Abs. 2 AktG). Das Unterlassen eines ordnungsgemäßen Risikomanagements kann zudem die außerordentliche Kündigung eines Vorstandes rechtfertigen. Zwar wurde in das GmbH-Gesetz keine Regelung analog zu § 91 Abs. 2 AktG aufgenommen, aus den Gesetzesmaterialien zum KonTraG folgt jedoch, dass die Neuregelungen im AktG Ausstrahlungswirkung auf den Pflichtenrahmen der Geschäftsführer anderer Gesellschaftsformen haben.

§

Der Schlüssel zum Erfolg ist ein individuelles Vorgehensmodell mit Augenmaß.

Compliance mit ISO 27XXX

Die Standards der ISO 27000 ff. sind Teil der aktuell durch die ISO (International Organization for Standartization) gemeinsam mit der IEC (International Electronical Commission) erarbeiteten Gruppe von IT-Sicherheitsstandards (sog. 27000 ff. Serie). Die ISO 27000 ff. geben verschiedene Guidelines für das IT-Riskomanagement vor, deren Einhaltung z.B. durch eine Zertifizierung des Unternehmens im Anschluss an ein erfolgreiches Auditing im Auftrag der Unternehmensführung nachgewiesen werden kann.

Aus rechtlicher Perspektive ist die Nichtbeachtung nationaler oder internationaler technischer Standards, wie beispielsweise der ISO 27000 ff.-Familie als Indiz für eine haftungsrechtlich relevante Pflichtverletzung des Unternehmens gegenüber Dritten (sog. „Haftung im Außenverhältnis“) zu werten. Sollte die Geschäftsführung die aus den ISO-Standards folgende, strukturierte Anleitung missachten, so droht zudem die Gefahr einer persönlichen Haftung des Vorstandes gegenüber der Gesellschaft (sog. „Haftung im Innenverhältnis“).

So hat der Bundesgerichtshof zur Nichtbeachtung von technischen DIN-Normen durch ein Unternehmen entschieden, dass bei einer Nichtbeachtung dieser technischen Standards eine (widerlegliche) Vermutung besteht, dass der eingetretene Schaden kausal auf der Handlung des schädigenden Unternehmens beruht. Hätte dieses die relevanten DIN-Normen eingehalten, müsste der Kläger die Kausalität der Handlung für den Schadenseintritt erst einmal beweisen.

Zwar existiert eine analoge Rechtsprechung zu den IT-sicherheitsrelevanten ISO 27000 ff.-Normen in Deutschland bisher nicht, es ist aber davon auszugehen, dass bei Nichtbeachtung der ISO 27000 ff. -Vorschriften die Gerichte von einer Pflichtverletzung bzw. einem Vertretenmüssen für die Pflichtverletzung ausgehen, obwohl es sich bei den ISO-Standards nicht um Normen von Gesetzesrang, sondern lediglich um unverbindliche technische Empfehlungen handelt.

Für die Unternehmensführung bedeutet dies, dass der Vorsorgeaufwand im Verhältnis zum Nutzen zu setzen ist und stets zu analysieren ist, ob sich präventive Maßnahmen im Hinblick auf die potentiell eintretenden Schadensfolgen als sinnvoll darstellen.

Compliance und Kostenreduktion

Die Selbstverpflichtung eines Unternehmens im Rahmen der Compliance mit dem Ziel der Vermeidung sowohl eines negativen Images als auch von Haftungsfällen bzw. Schadensersatzklagen stellt einen weiteren wichtigen Baustein des IT-Risikomanagements dar.

Outsourcing und neue Anforderungen für die Auftragsdatenverarbeitung nach den BDSG-Novellen 2009

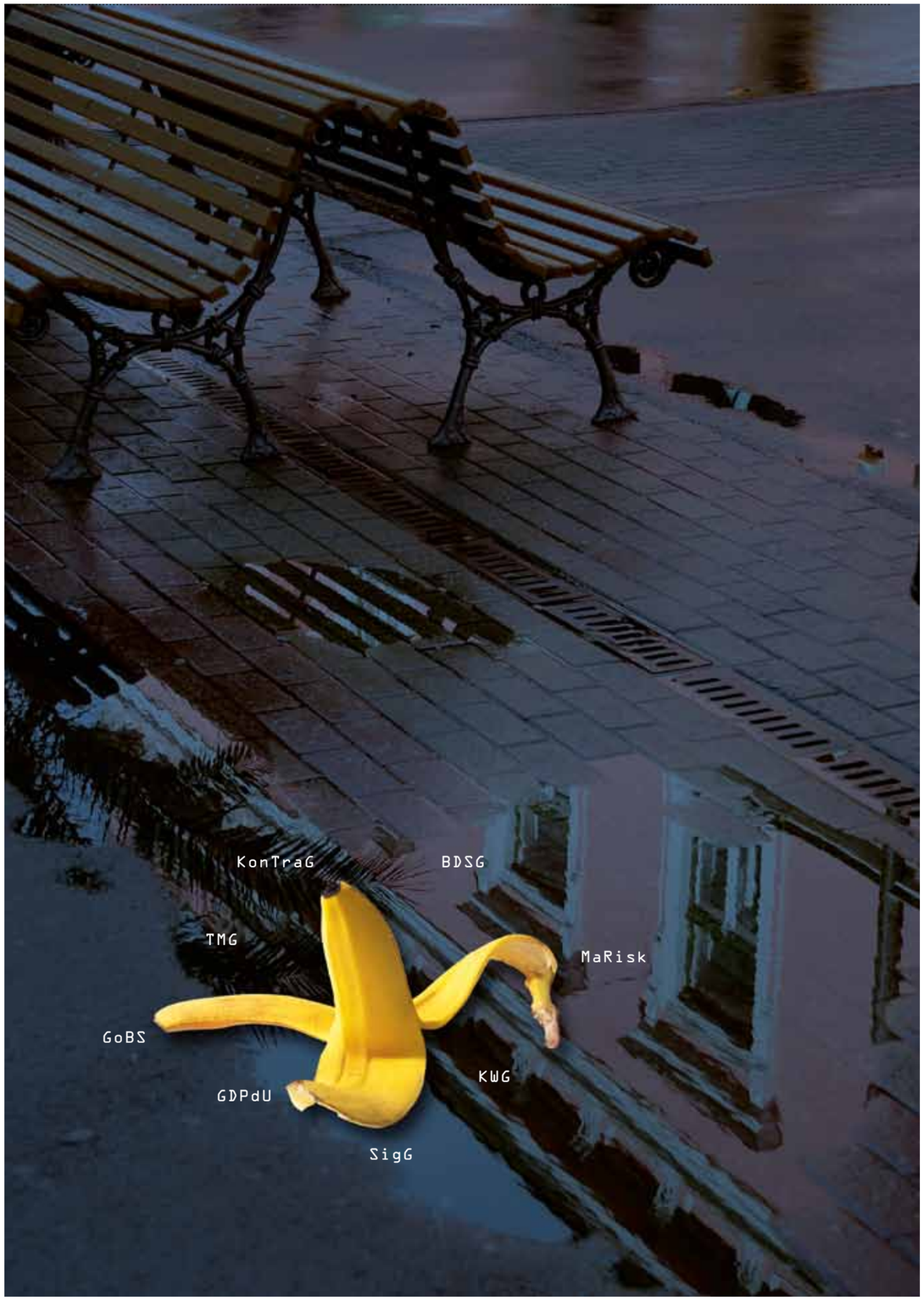
Hat sich die Unternehmensführung dazu entschieden, ein Outsourcing für bestimmte Bereiche des Unternehmens umzusetzen, stellt sich die Frage der Verantwortlichkeit des Unternehmens für die Handlungen des Outsourcing Providers (z.B. im Rahmen eines BPOs). Diesbezüglich gilt als Grundsatz, dass die Unternehmensführung durch ein Outsourcing nicht die Verantwortung für das IT-Risikomanagement des Unternehmens auf den Provider überträgt. Insbesondere sind im Hinblick auf das IT-Risikomanagement die Verfügbarkeit der IT durch Verhandlung hinreichender Service Level Agreements (SLAs) abzusichern. Für das IT-Notfallkonzept des Unternehmens ist zu gewährleisten, dass der Outsourcing Provider in den IT-Notfallplan vertraglich einbezogen wird.

Ist die Verarbeitung personenbezogener Daten Gegenstand des Outsourcingprozesses, ergeben sich datenschutzrechtliche Konsequenzen in Abhängigkeit davon, ob es sich um eine Auftragsdatenverarbeitung gemäß § 11 BDSG oder eine Funktionsübertragung handelt. Liegt eine Auftragsverarbeitung vor, bleibt das outsourcende Unternehmen sog. verantwortliche Stelle im Sinne des Datenschutzrechts.

Im Rahmen der BDSG-Novellen 2009 wurden die Pflichten, die den Auftraggeber einer Auftragsdatenverarbeitung treffen, substantiell erhöht. § 11 Absatz 2 BDSG definiert nunmehr einen Katalog von 10 Punkten, die bei einer Auftragserteilung schriftlich zu regeln sind (u.a. Art und Umfang der Datenverarbeitung, Regelungen zu einer etwaigen Unterauftragsvergabe, etc.). Der Auftraggeber muss sich zudem während der gesamten Dauer der Auftragsdatenverarbeitung davon überzeugen, dass der Auftragnehmer die technisch-organisatorischen Maßnahmen zur Abwicklung der Datenverarbeitung erfüllt. Sollte der Auftraggeber gegen eine der vorgenannten Pflichten verstoßen, so droht ein Bußgeld in Höhe von bis zu 50.000 €.

Fazit

Die Einführung und kontinuierliche Verbesserung des IT-Sicherheitsmanagements im Unternehmen erfordert die volle Aufmerksamkeit der Unternehmensführung und sollte durch ein engmaschiges Reporting abgesichert werden. Dies mag auf den ersten Blick eine erhebliche Allokation von Unternehmensressourcen bedeuten, zahlt sich jedoch durch eine erhebliche Reduzierung der Haftungsrisiken für die Geschäftsführung sowie die Sicherstellung der Authentizität, Sicherheit und Verfügbarkeit der IT-Systeme des Unternehmens nicht zuletzt ökonomisch messbar aus.



Kontakt und Informationen

INTARGIA Managementberatung GmbH

Dr. rer. pol., Dipl.-Ing. Thomas Jurisch
Geschäftsführender Gesellschafter
ISO 27001 Lead Auditor
> thomas.jurisch@intargia.com
Telefon 06103 50860

Dipl. Betriebswirt (FH) Steffen Weber
Berater, ISO 27001 Lead Auditor
> steffen.weber@intargia.com
Telefon 06103 50860

Buse Heberer Fromm
Rechtsanwälte Steuerberater Partnerschaftsgesellschaft

Stephan Menzemer
Rechtsanwalt
Partner
> menzemer@buse.de
Telefon 069 971097 913

Tim Christopher Caesar
Rechtsanwalt
Associate
> caesar@buse.de
Telefon 069 971097 911

10/2010