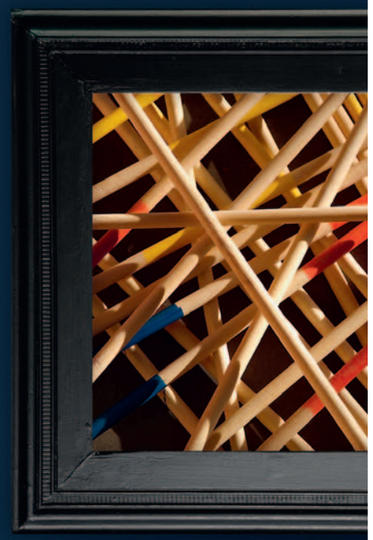
Leitfaden IT-Sicherheits-management 2012

Inhalt

BUSE HEBERER FROMM
RECHTSANWÄLTE · STEUERBERATER PARTG

INTARGIA

IT-Sicherheitsrisiken sind eine ständig wachsende Herausforderung für jedes Unternehmen und jede öffentliche Einrichtung.



MANAGEMENT DER INFORMATIONSSICHERHEIT

BEDROHUNGSMANAGEMENT

ZUGANGSMANAGEMENT

IT-COMPLIANCE

1 Einleitung

Für ein erfolgreiches IT-Sicherheitsmanagement ist die Erkennung und Bewertung bestehender Sicherheitsrisiken Grundvoraussetzung. 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 der IT-Sicherheit schnell in die Nähe einer existenziellen Bedrohung geraten. In den vergangenen Jahren erhöhte sich die Zahl spektakulärer Hackerattacken auf zentrale IT-Systeme von Unternehmen jeder Größe signifikant.

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 – IT-Sicherheit ist daher mittlerweile auf der Agenda der meisten Unternehmensleitungen zu einem der wichtigsten Themen geworden und als geschäftskritischer Faktor akzeptiert.

Um möglichen Risiken wirksam begegnen zu können, benötigen Unternehmen und öffentliche Einrichtungen ein geplantes, strukturiertes und methodisches IT-Sicherheitsmanagement sowie die notwendige Sensibilität für Warnsignale und potentielle Sicherheitslücken.

Die Grundlagen, Anforderungen und ein strukturierter Ansatz für effektives IT-Sicherheitsmanagement werden im Folgenden aus technischer, organisatorischer und rechtlicher Perspektive beleuchtet. Der Schlüssel zum Erfolg der Umsetzung der einzelnen Bausteine eines (stets unbedingt angeratenen) IT-Sicherheitsmanagements ist idealerweise ein individuelles Vorgehensmodell mit Augenmaß.

Die IT-Sicherheitsexperten der INTARGIA Managementberatung und BUSE HEBERER FROMM Rechtsanwälte Steuerberater Partnerschaftsgesellschaft möchten Ihnen mit diesem Leitfaden einen praktischen Ratgeber zur Beantwortung Ihrer wichtigsten unternehmerischen Fragen im Bereich IT-Sicherheitsmanagement an die Hand geben. Vor diesem Hintergrund freuen wir uns, Ihnen unseren gemeinsamen Leitfaden präsentieren zu dürfen.

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

Stephan Menzemer
Rechtsanwalt
Wirtschaftsmediator
Partner
BUSE HEBERER FROMM
Rechtsanwälte Steuerberater
Partnerschaftsgesellschaft

Steffen Weber, M.Sc.
Partner
ISO 27001 Lead Auditor
INTARGIA Managementberatung GmbH

Tim Christopher Caesar
Rechtsanwalt
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. Die treibenden Kräfte 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 noch weiter 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 IT-Sicherheit unter den CIOs der Unternehmen mit großem Abstand und zum wiederholten Male ein Top-Thema hinsichtlich der 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. Die Anbindung der lokalen Netze an öffentliche Weitverkehrsnetze wie das Internet vergrößert diese Bedrohung noch, da Angreifer nun von jedem Punkt 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 einigen 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 neuen, 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 Millionen Euro: Ca. 250.000 Emissionsberechtigungen (zu je 12 Euro) 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 umfangreichen Ermittlungen der Strafverfolgungsbehörden, die der Reputation nicht zuträglich sind, drohen den Verantwortlichen der aufgrund mangelnder (IT-)Sicherheitsvorkehrungen geschädigten Unternehmen auf zivilrechtlicher Ebene stets Schadenersatzansprüche.

In einem weiteren prominenten Fall gab das berufliche soziale Netzwerk LinkedIn Anfang 2012 bekannt, Opfer von Hackerattacken aus Russland geworden zu sein. Diese koordinierten Angriffe sorgten dafür, dass die Hacker tausende von Nutzerkonten samt Passwörtern erbeuten konnten.

Google musste sich 2010 Hackerattacken aus China stellen: Hacker legten wiederholt über Monate hinweg Google-Webseiten lahm. Zu den Kosten der Fehlerbehebung und der daraus folgenden Erhöhung von IT-Sicherheitsmaßnahmen macht das Unternehmen allerdings keine Angaben.

Dass IT-Sicherheitsthemen auch in der Politik ernst genommen werden sollten, zeigen zwei Vorfälle bei SPD (2012) und CDU (2011): Beiden Parteien wurden Zugangsdaten und Passwörter ihrer Online-Nutzer gestohlen.

Hilflos gegenüber Hacking-Attacken schien der mittelständische Computerhändler K&M Elektronik – von seinen Servern wurden im Juni und August 2011 in Summe ca. 840.000 Kundendatensätze mit unverschlüsselten Passwörtern entwendet. Studien wie z. B. „Netz- und Informationssicherheit in Unternehmen" des Netzwerks Elektronischer Geschäftsverkehr (NEG), die ihren Focus vor allem auf kleine und mittelständische Unternehmen in Deutschland richten, zeigen, dass durchschnittlich jedes zehnte der befragten Unternehmen Opfer eines Angriffs wurde. Dies macht deutlich, dass Netz- und IT-Sicherheit auf allen Ebenen eine gewichtige Rolle spielt und spielen muss.

BEDROHUNGSMANAGEMENT
IT-Sicherheitsmanagement 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 systemischen 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 für eine 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 **zu ergreifenden Maßnahmen** richten sich nach der Art und dem Umfang der Bedrohung eines IT-Systems, nämlich gegen:

- 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 die Teildisziplinen, die in Summe sämtliche wichtigen Aspekte der Gewährleistung von IT-Sicherheit abdecken (s. Tabelle rechts oben).

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, Tablets und Laptops sowie drahtlose Kommunikationsverfahren, wie GSM, UMTS, LTE, Bluetooth und WLAN ein. Darüber hinaus erzeugt auch der neue Trend „Bring your own device (BYOD)" neue IT-Sicherheitsprobleme. Für die mobile Nutzung von Informationstechnik insgesamt 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.

Teildisziplinen der IT-Sicherheit

Teildisziplin	Abgedeckte Themen
Identitätsmanagement	• Digitale Identitäten und Rollenmodelle • Methoden d. Identitäts- und Authentisierungsprüfung • Verzeichnisdienste • Single-Sign-on • Public-Key-Infrastrukturen • Identitätsträger (Chipkarten etc.)
Zugangsmanagement	• System-Zugriffsschutz • Netzwerk-Zugriffsschutz (Firewalls etc.) • Chiffrierung • Data Ownership
Entwicklung/ Integration	• „Trusted Computing Base" • Sichere Softwareentwicklung • Integration, Testen und Wartung
Bedrohungsmanagement	• 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 Informationssicherheit	• Zusammenzug der Event-Information • Auditierung von Sicherheits-Events • Compliance-Überprüfung (zyklisch) • Überwachung, Alarmierung, Eskalation • Integration, Korrelation und Bewertung von Sicherheits-Events • Incident Response und Koordination
Rahmenbedingungen	• 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"

„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 27000 ff. und BSI 100-1 bis 100-4 in Verbindung mit den IT-Grundschutz-Katalogen des BSI.

5 Ein Ansatz für effektive IT-Sicherheit „mit Augenmaß"

Effektives IT-Sicherheitsmanagement gewährleistet Vertraulichkeit, Integrität und Verfügbarkeit von Prozessen, IT-Systemen und Informationen. Im Folgenden möchten wir Ihnen gerne unsere Beratungsmodule vorstellen, die unabhängig voneinander oder im Idealfall integrativ für eine effektive Verbesserung Ihres IT-Sicherheitsniveaus sorgen:

Beratungsmodul 1: IT-Sicherheits-Quick-Check

Zur Analyse und Bewertung Ihres existierenden IT-Sicherheitsniveaus dient der **INTARGIA IT-Sicherheits-Quick-Check.** Alle relevanten IT-Sicherheitsthemen werden einbezogen, so dass aus den daraus gewonnenen Erkenntnissen direkt sinnvolle technische und organisatorische Maßnahmen abgeleitet werden können. Konkret besteht der IT-Sicherheits-Quick-Check aus folgenden Schritten:

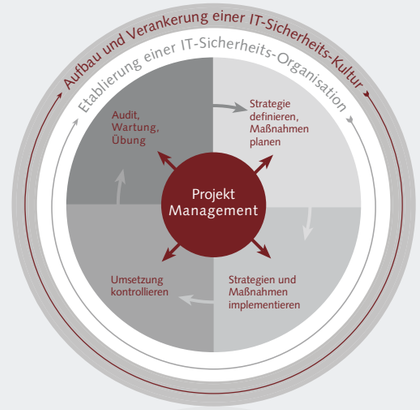
- Durchführung einer IT-Strukturanalyse: Vorhandene Dokumente über die IT-Infrastruktur und Applikationen werden ausgewertet und in Gesprächen mit den Verantwortlichen ergänzt, so dass ein ausreichender Überblick über die relevanten Untersuchungsobjekte vorliegt.
- Erstellung eines Prüfplans: Auf Basis der IT-Strukturanalyse wird ein individueller Prüfplan definiert, gegen den in der Prüfungsphase geprüft wird.
- Prüfungsphase: In Vor-Ort-Gesprächen wird ein Abgleich des Ist-Zustandes der Sicherheitsmaßnahmen mit den Soll-Vorgaben des Prüfplans durchgeführt. Ausgewählte Angaben werden durch Stichprobenprüfungen veri- oder falsifiziert.

  Der Prüfplan umfasst folgende IT-Sicherheitsschichten:
  – Schicht 1: Übergeordnete Aspekte
  – Schicht 2: Infrastruktur
  – Schicht 3: IT-Systeme
  – Schicht 4: Netze
  – Schicht 5: IT-Anwendungen

  Themen der einzelnen Schichten sind beispielsweise:
  – IT-Sicherheitsleitlinie
  – Organisation und Management der Informationssicherheit
  – Personelle Sicherheit
  – Physische und umgebungsbezogene Sicherheit
  – Betriebs- und Kommunikationsmanagement
  – Zugangskontrolle
  – Beschaffung, Entwicklung und Wartung von Informationssystemen
  – Umgang mit Informationssicherheitsvorfällen
  – Business Continuity Management
  – Einhaltung von rechtlichen Vorgaben (IT-Compliance)
- Die gewonnenen Erkenntnisse und Handlungsempfehlungen werden in enger Abstimmung mit dem Kunden im Auditbericht dokumentiert und im Rahmen der Ergebnispräsentation vorgestellt und diskutiert.

Beratungsmodul 2: Einführung eines IT-Sicherheits-management-Systems (ISMS)

Nachhaltigkeit und Effektivität können sich nach unserer Überzeugung nur durch einen geplanten, systematischen und zyklischen Prozess einstellen. Deshalb haben wir das TÜV-zertifizierte INTARGIA-ISMS auch am generischen Management-Kreislauf „Planen, Durchführen, Kontrollieren, Handeln" orientiert.



> **Phase 1: IT-Sicherheits-Quick-Check / regelmäßige IT-Sicherheitsaudits**
Phase 1 entspricht im ersten Zyklus dem bereits beschriebenen IT-Sicherheits-Quick-Check, in späteren Zyklen regelmäßigen Wiederholungsaudits. Zusätzlich zur IT-Strukturanalyse (die eine IT-/System-orientierte Sicht hat) wird gemeinsam mit den Prozessverantwortlichen die Kritikalität hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit der einzelnen Geschäftsprozesse definiert. Anschließend werden die Erkenntnisse aus Struktur- und Risikoanalyse zusammen geführt, die Kritikalitätsanforderungen der Prozesse gegen die IT-Elemente abgeglichen. Somit wird eine geschäftsprozessorientierte Priorisierung der zu betrachtenden Elemente der IT-Infrastruktur erreicht.

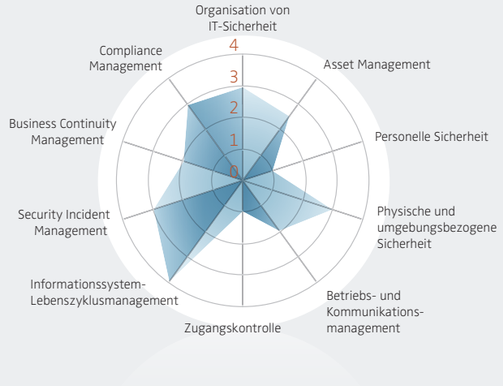
> **Phase 2: Strategie definieren und Maßnahmen planen**
Abgeleitet von Phase 1 wird die IT-Sicherheitsstrategie entwickelt und geeignete technische und organisatorische Maßnahmen zur Umsetzung abgeleitet und priorisiert. Gespeist werden diese Maßnahmenempfehlungen durch die relevanten gesetzlichen Vorgaben, „Best Practices" und die langjährige Erfahrung der INTARGIA IT-Sicherheitsexperten von INTARGIA. Abschließend wird gemeinsam ein Zeitplan erarbeitet und die Frequenz für zukünftige Audit-Zyklen festgelegt.

Weiter auf der nächsten Seite >

> **Phase 3: Strategien und Maßnahmen implementieren**
Die ausgewählten technischen und organisatorischen Maßnahmen werden anschließend gemäß der festgelegten Priorisierung umgesetzt. Während des gesamten Projektes steht INTARGIA mit seinen IT-Sicherheitsexperten und Kooperationspartnern 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: Umsetzung kontrollieren, Re-Audit/Wartung und Übung**
Die Effektivität der umgesetzten Maßnahmen wird in Kooperation mit dem Kunden regelmäßig in sogenannten Wiederholungsaudits kontrolliert. Zur Bewertung wird ein Reifegradmodell genutzt, das einerseits einen übersichtlichen Überblick 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-Sicherheitsmaßnahmen ableiten. Regelmäßiges Reporting an die Verantwortlichen im Unternehmen gehört ebenso zur Umsetzungskontrolle wie die professionelle Dokumentation von Status und Fortschritt des ISMS.

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 zeigt sehr deutlich, dass ohne eine vorhandene Sensibilität der Mitarbeiter und weiterer Stakeholder im Unternehmen kein zufriedenstellendes IT-Sicherheitsniveau geben kann. Deshalb liegt ein Hauptfokus darauf, die Handelnden im Unternehmen für die Notwendigkeit von IT-Sicherheit zu sensibilisieren, z. B. durch Schulungen oder regelmäßige Sicherheitshinweise im Intranet oder per Newsletter. Zusätzlich ist eine funktionierende IT-Sicherheitsorganisation zu etablieren, die für die Weiterentwicklung des ISMS zuständig ist.

Beratungsmodul 3: Übernahme der Rolle des IT-Sicherheitsbeauftragten oder Coaching des internen IT-Sicherheitsbeauftragten
Zusätzlich zu den in den Beratungsmodulen 1 und 2 genannten Beratungsleistungen übernehmen wir auch die Funktion des IT-Sicherheitsbeauftragten. Unternehmen, die einen internen IT-Sicherheitsbeauftragten beschäftigen, bieten wir ein fachliches Coaching bei der Umsetzung der Handlungsempfehlungen an.

Zertifizierte IT-Sicherheit

Zertifizierte Managementsysteme spielen immer wichtigere Rolle um Compliance-Konformität nachzuweisen. Organisationen, die einen bestimmten ISMS-Reifegrad erreichen, erhalten von INTARGIA das in Zusammenarbeit mit dem TÜV entwickelte INTARGIA-IT-Sicherheitssiegel. Damit kann gegenüber Kunden, Mitarbeitern, Behörden und Wettbewerbern signalisiert werden, dass IT-Sicherheit ein erfolgskritischer Faktor ist und ernst genommen wird.

Die Vorteile:
- Professionalität durch neutrale und praxiserprobte IT-Sicherheitsberatung
- Schaffung von Vertrauen bei Kunden, Mitarbeitern und Lieferanten
- Werbewirksames Marketinginstrument

Kundenstimme

Marcus Sassenrath, CEO, one2one IT GmbH
„2011 hat sich unser Unternehmen entschieden, das IT-Sicherheitsmanagement mit externer Expertenunterstützung weiter zu professionalisieren. INTARGIA hat uns in einem ersten Schritt, dem IT-Sicherheits-Quick-Check, auf objektive und transparente Weise Optimierungspotenziale im IT-Sicherheitsmanagement aufgezeigt und gemeinsam mit uns die Handlungsempfehlungen in konkrete und zielorientierte Maßnahmen überführt.

Anschließend stand uns INTARGIA bei der Entwicklung und Implementierung der ausgewählten Maßnahmen beratend zur Seite, so dass sich unser IT-Sicherheitsniveau sukzessive erhöht hat. Wir haben INTARGIA in den letzten Jahren als kompetenten und zuverlässigen Partner erlebt, der uns stets mit der notwendigen Professionalität und Neutralität unterstützt hat."

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 Vorstand 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 (2006/43/EG) und Basel II ergänzt.

IT-Risikoprävention gemäß § 91 Absatz 2 AktG

Durch die Verabschiedung des KonTragG im Jahr 1998 wurden u.a. wesentliche Normen des AktG und des HGB ergänzt. Die damaligen 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 KonTragG folgt jedoch, dass die Neuregelungen im AktG Ausstrahlungswirkung auf den Pflichtenrahmen der Geschäftsführer anderer Gesellschaftsformen haben.

Compliance mit ISO 27000 ff.

Die Standards der ISO 27000 ff. sind Teil der aktuell durch die ISO (International Organization for Standardization) 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.

§

Der Schlüssel zum Erfolg ist ein individuelles Vorgehensmodell mit Augenmaß.

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 solchen 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 also der Kläger die Kausalität der Handlung für den Schadenseintritt erst einmal beweisen. Ein solcher Beweis dürfte in der Praxis schwer zu führen sein, da sich der Kläger den Einwand entgegenhalten lassen muss, dass sein Schaden genauso gut auch auf anderen Ursachen, wie z. B. anderer schadhafter Software oder mangelhafte Installation, beruhen kann.

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 auch bei den ISO-Standards nicht um Normen von Gesetzesrang, sondern lediglich um unverbindliche technische Empfehlungen handelt.

Für die Unternehmensführung bedeutet dies, dass der Vorsorgeaufwand in ein Verhältnis zum Nutzen zu setzen 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.

Zu diesem Themenkreis zählt u.a. das Lizenzmanagement. Die konkrete Haftungsgefahr, die es hier zu managen gilt, liegt – kurz gesagt – in der Diskrepanz zwischen der Zahl der genutzten Kopien einer Software und den erworbenen Lizenzen. Insbesondere auch die Nutzung von Open-Source-Software bietet in der Praxis neben den bekannten Vorteilen stets erhebliches rechtliches Konfliktpotential. Allerdings lassen sich in beiden Bereichen durch Optimierung und gut beratene Absicherung des Lizenzmanagements u.a. erhebliche Kosteneinsparungen realisieren.

Outsourcing und Anforderungen an die Auftragsdatenverarbeitung nach dem BDSG

Hat sich die Unternehmensführung dazu entschlossen, 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. Das IT-Notfallkonzept des Unternehmens muss gewährleisten, dass der Outsourcing-Provider in den IT-Notfallplan vertraglich einbezogen wird.

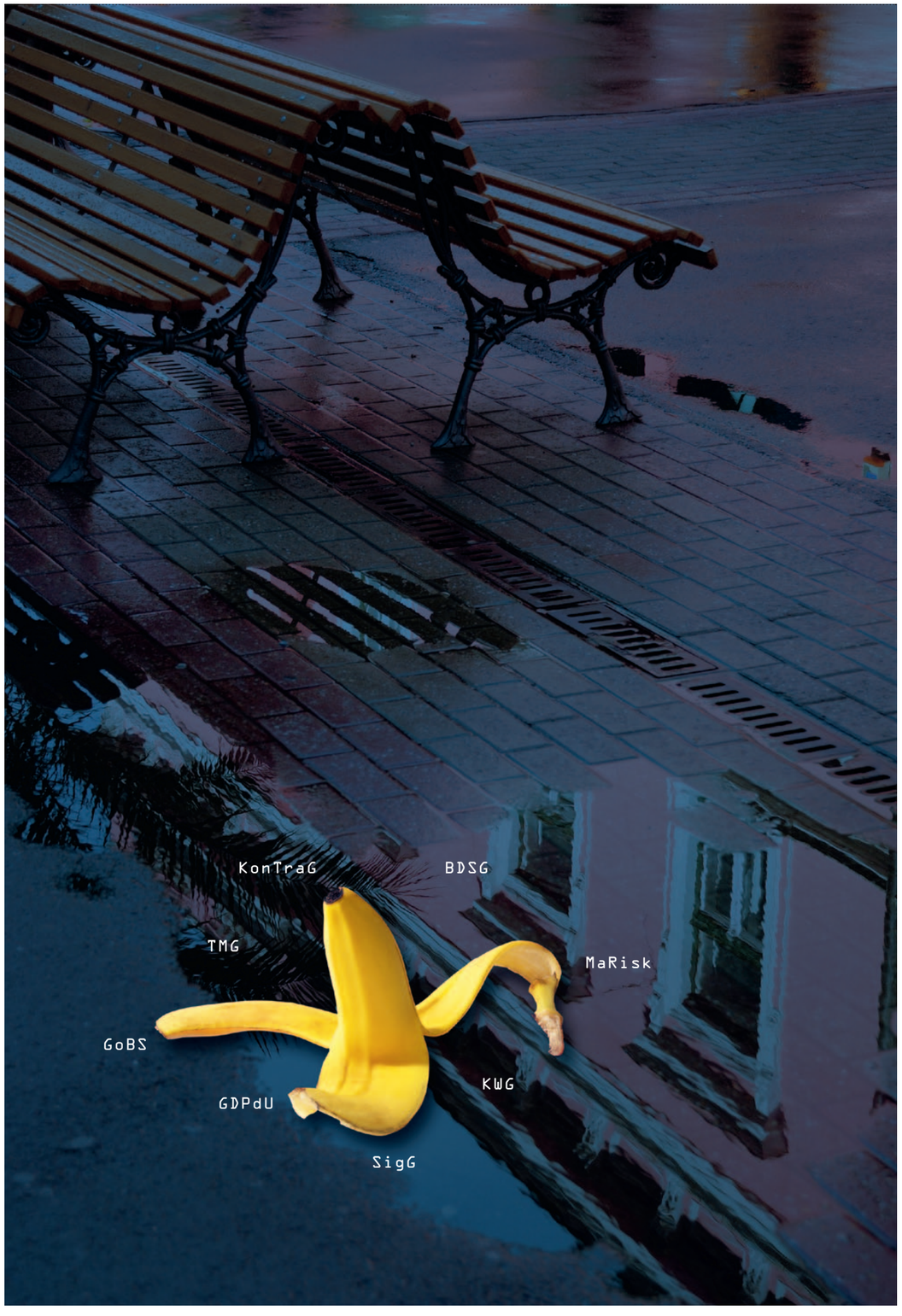
Ist die Verarbeitung personenbezogener Daten Gegenstand des Outsourcingprozesses, ergeben sich datenschutzrechtliche Konsequenzen in Abhängigkeit davon, ob es sich um eine Auftragsdatenverarbeitung gemäß § 11 BDSG (Auftragnehmer als „verlängerter Arm“ des Auftraggebers) oder eine Funktionsübertragung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

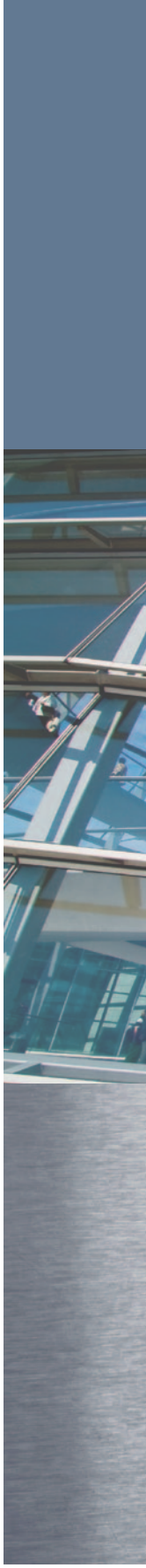
Im Rahmen der BDSG-Novellen 2009 wurden die Pflichten, die den Auftraggeber einer Auftragsdatenverarbeitung treffen, substantiell erhöht.

§ 11 Abs. 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). 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 Euro, wobei die Geldbuße den wirtschaftlichen Vorteil, der aus der Ordnungswidrigkeit erlangt worden ist, übersteigen soll. Falls die erlangte Summe höher als 50.000 Euro sein sollte, ist die zuständige Bußgeldbehörde berechtigt, diesen Betrag nach pflichtgemäßem Ermessen zu überschreiten.

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 erforderliche 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

INTARGIA Managementberatung GmbH

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

Steffen Weber, M.Sc.
Partner
ISO 27001 Lead Auditor
> steffen.weber@intargia.com
Telefon 06103 50860

BUSE HEBERER FROMM
RECHTSANWÄLTE · STEUERBERATER PARTG

BUSE HEBERER FROMM
Rechtsanwälte Steuerberater
Partnerschaftsgesellschaft

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

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

10/2012