books24x7
ein SkillSoft-Unternehmen

ExecBlueprints™

in Kooperation mit Aspatore Books

Aktionspunkte

I. **Unternehmensweite Compliance**
Ein Programm für die Technologie-Compliance muss Mitarbeiter aus dem gesamten Unternehmen mit einbeziehen.

II. **Das Endergebnis**
Unternehmen müssen heutzutage größte Sorgfalt auf den Umgang mit personenbezogenen Daten zu Kunden, Lieferanten und Mitarbeitern verwenden.

III. **Zentrale Compliance-Themen**
Konflikte zwischen Datenschutz und -offenlegung, Fragen der Datensicherheit sowie die Einhaltung internationaler Gesetze und Vorschriften sind drei hochbrisante Themen.

IV. **Die goldenen Regeln für eine grundlegende Datensicherheit**
Einführung wirksamer Schutzmechanismen gegen unbefugten Datenzugriff. Umsetzung geeigneter Authentifizierungsverfahren. Überwachung der Datenspeicherung. Einführung einer universellen Verschlüsselung. Durchführung regelmäßiger Risikoabschätzungen.

V. **Wichtige Ergebnisse**
In einem dynamischen Wirtschaftsumfeld mit ständig weiterentwickelten Technologien und Prozessen werden immer neue Gesetze erlassen, um auf neuartige Herausforderungen und Probleme zu reagieren. IT-Manager müssen sich daher mit Experten aus dem gesamten Unternehmen zusammenschließen, um gemeinsam alle Compliance-Anforderungen erfüllen zu können.

Inhalt

Drei führende Compliance-Experten der Kanzleien Baker & McKenzie, LLP, Sonnenschein Nath & Rosenthal, LLP, und Drinker, Biddle and Reath, LLP, äußern sich im Folgenden zum Thema:

Entwicklung eines nachhaltigen IT-Compliance-Programms

Ruth Hill Bro
Partner, Baker & McKenzie LLP

I. Edward Marquette
Partner, Sonnenschein Nath & Rosenthal LLP

Melissa L. Klipp
Partner, Drinker, Biddle and Reath LLP

Die Compliance-Szenerie im IT-Bereich wird zunehmend unübersichtlicher. Die Ursache hierfür ist sowohl im legislativen Umfeld als auch in der Technologie selbst zu suchen. Ersteres ist gerade im IT-Bereich enorm komplex und einem rapiden Wandel unterworfen. Unternehmen müssen heutzutage Bestimmungen auf regionaler, nationaler und internationaler Ebene entsprechen, die äußerst vielschichtig sind und sich nur allzu häufig widersprechen. Gleichzeitig werden bei Compliance-Lücken und einer Verletzung des Datenschutzes schwindelerregende Strafzahlungen fällig. Parallel dazu führen neue Technologietrends zu einer immer größeren Komplexität der IT-Umgebung und machen die Einhaltung sämtlicher Vorschriften zu einem Kampf gegen Windmühlen. IT-Manager müssen sich daher zwingend mit Fachleuten aus dem gesamten Unternehmen zusammentun, um ein umfassendes Compliance-Programm zu erarbeiten, das sowohl robust als auch anpassungsfähig genug ist, um den ständig wechselnden Rahmenbedingungen gerecht zu werden. ■

Die Verfasser

Ruth Hill Bro

Partner, Baker & McKenzie LLP

Ruth Hill Bro arbeitet als Partner in der Chicagoer Niederlassung von Baker & McKenzie LLP, ist Gründerin und Herausgeberin des weltweit erscheinenden monatlichen Newsletters ihrer Kanzlei und US-Gründungsmitglied des globalen Lenkungsausschusses von Baker & McKenzie zum Thema Datenschutz. Ruth Hill Bro berät Unternehmen zu Privacy-Strategien, globaler Compliance, Informationsmanagement und relevanten Thematiken aus den Bereichen Website-, HR- und Kunden-/Third Party-Management, internationale Geschäfte, Sicherheit und Marketing.

Als Gründerin des E-Privacy-Ausschusses der American Bar Association (ABA) hatte Frau Bro von 2000 bis 2005 den Vorsitz dieser Vereinigung inne. Sie ist gewählte Vorsitzende der für Wissenschafts- und Technologierecht zuständigen ABA-Sektion und seit 2002 Mitglied des Sektionsrats. Darüber hinaus gründete sie 2007 den ABA-Ausschuss zur Förderung von Wissenschafts-/Technologierecht und -ausbildung (CASTLE), dem sie auch vorsteht. Ruth Hill Bro sitzt in der Redaktionsleitung der vierteljährlichen Fachpublikation ihrer Kanzlei, *The SciTech Lawyer*, für die sie die „CPO Corner", eine Kolumne mit Interviews führender Privacy-Manager, verfasst. Sie ist Mitglied der Redaktionsleitung von Internet Law & Strategy und hatte 2005/06 die Funktion eines Redaktionsleiters/Vorsitzenden beim Fachmagazin *The Privacy & Data Protection Legal Reporter* inne. Frau Bro äußert sich regelmäßig in diversen Medien und veröffentlichte kürzlich ihr neuestes Buch *The E-Business Legal Arsenal: Practitioner Agreements and Checklists* (ABA 2004, Redaktion).

Ruth Hill Bro genießt höchsten Respekt in der Branche und wurde z. B. von Chambers USA zu einer der führenden Business-Anwältinnen der USA ernannt. Ihr Name findet sich auch in der „Legal 500 U.S."-Liste, dem internationalen Who's Who der Internet- & E-Commerce-Anwälte, und der Liste der besten US-Anwälte. Zu ihren weiteren Ehrentiteln gehört der Titel „Illinois Super Lawyer". „Leading Lawyers Network: The Top Lawyers", „Top 50 Leading Women Lawyers in Illinois", „Top 50 Leading Women Business Lawyers in Illinois" und „40 Illinois Attorneys Under 40 to Watch" (veröffentlicht von der Law Bulletin Publishing Company, Illinois) sind weitere Auszeichnungen, die sie im Lauf ihrer Karriere erwarb.

Ihre Beiträge wurden im *Wall Street Journal*, der *New York Times*, dem *International Herald Tribune, dem National Law Journal, Corporate Counsel* sowie im BNA „Privacy & Security Law Report" veröffentlicht und in Bloomberg Radio sowie CNBC ausgestrahlt.

Für ihre Kurzgeschichte „Privilege" erhielt sie den 1. Preis beim Annual Fiction Contest des New York Law Journal im Jahr 2006.

Nach einem B.A. an der Northwestern University machte Frau Bro ihren Juris Doctor-Abschluss an der University of Chicago, für die sie auch heute noch als Mentorin im Rahmen des University of Chicago Law School Women's Mentoring Program aktiv ist.

☛ *Ruth Hill Bro zum Thema (Seite 3)*

I. Edward Marquette

Partner, Sonnenschein Nath & Rosenthal LLP

Ed Marquette ist Partner bei Sonnenschein Nath & Rosenthal LLP, einer Kanzlei mit nahezu 800 Anwälten in neun Städten. Als Business-Anwalt mit dem Spezialgebiet Technologie und geistige Eigentumsrechte befasst er sich besonders mit den US-spezifischen und internationalen Aspekten von Lizenzierung, Hightech-Beschaffung und -Verteilung.

Ed Marquette hält Vorträge für die verschiedensten Zielgruppen. Dazu zählen Unternehmen für die Technologiebeschaffung (z. B. CAUCUS) ebenso wie Berufsverbände zertifizierter Purchasing Manager, Computernutzer, Herausgeber von Fachpublikationen, Wirtschafts- und Rechtsverbände, Bibliothekare, Produktionsfirmen und interessierte Akademiker. In seinen Artikeln und Beiträgen beschäftigt er sich mit Technologien, ihrer Beschaffung und Verteilung, dem globalen Marktplatz, der Technologieentwicklung und den Herausforderungen aus der Entstehung neuartiger Informationstechnologien, Compliance-Problemen in Zusammenhang mit der Softwarelizenzierung sowie mit dem Thema Urheberrechtsschutz, Markenschutz, Antitrust und dem Schutz von Webinhalten.

Herr Marquette war Mitglied des ABA-Ausschusses zur Informationsinfrastruktur in den USA. Ferner war er Vorsitzender des Ausschusses für neue Informationstechnologien und zweiter Vorsitzender des Ausschusses, der sich innerhalb der ABA-Sektion zu geistigen Eigentumsrechten mit dem Themengebiet Softwarelizenzierung befasst. Daneben wurde er mehrmals zum Vorsitzenden des Computer- und Technologierechtsausschusses der Kansas City Metropolitan Bar Association (KCMBA) gewählt und ist Mitglied der KCMBA-Taskforce zu Technologiefragen. Herr Marquette wird seit mehr als zehn Jahren in *The Best Lawyers in America* als Experte für geistige Eigentumsrechte geführt und berät die Herausgeber dieser Liste regelmäßig bei der Auswahl von Qualifikationen und in Frage kommenden Anwälten.

Ed Marquette berät seine Klienten innerhalb und außerhalb der USA auf den Gebieten Technologiebeschaffung, Entwicklung, Lizenzierung und Produktverteilung im Franchise- und Non-Franchise-Sektor. Er erwarb einen J.D. cum laude an der Harvard University School of Law.

☛ *Ed Marquette zum Thema (Seite 6)*

Melissa L. Klipp

Partner, Drinker, Biddle and Reath, LLP

Melissa L. Klipp vertritt als Partner für Handelsrecht und geistige Eigentumsrechte die Niederlassung der Kanzlei Drinker, Biddle and Reath, LLP, in New Jersey. In den Bereichen Technologie, geistige Eigentumsrechte und Computer bietet sie ihren Klienten Unterstützung bei Rechtsstreitigkeiten und fachkundige Beratung.

Melissa Klipp veröffentlichte u. a. Beiträge in Reuters, Associated Press, *USA Today*, Wired.com, *The Star-Ledger, New Jersey Lawyer, New Jersey Business, e-commerce Times* und *NJ Biz*. Sie ist Mitglied der Arbeitsgruppe 1 der Sedona Conference, die Best Practices für Litigation Hold- und Document Retention-Richtlinien erarbeitet. Darüber hinaus wurde sie kürzlich zur leitenden Ansprechpartnerin der Sedona-Arbeitsgruppe 6 ernannt, die sich mit dem internationalen elektronischen Datenverkehr und grenzüberschreitenden Problematiken befasst. Sie ist außerdem Mitglied der Association of Record Managers and Administrators International (ARMA) sowie der International Association of Privacy Professionals (IAPP).

Frau Klipp ist häufig als Rednerin bei Business- und Industrieseminaren eingeladen. Im Juni 2007 nahm sie an zwei Webinaren zum Thema elektronische Datenoffenlegungs- und Datenschutzrechte in der Europäischen Union teil. Anfang 2008 hielt sie einen Vortrag vor der Handelskammer von Morris County über den wirksamen Schutz von Unternehmen im digitalen Zeitalter. Im Oktober 2006 veröffentlichte Melissa Klipp einen Artikel in *Metropolitan Corporate Counsel* mit dem Titel „Electronically Stored Information and the Pending Federal Rule Changes: If No Suit Is Pending, This Doesn't Affect Me…Right?"

2006 wurde Frau Klipp von *NJ Biz* in die Liste der „New Jersey's Best 50 Women in Business" aufgenommen. Sie ist Mitglied des United Way of Morris County-Lenkungsausschusses, der sich mit Frauen in Führungspositionen beschäftigt, und gehört der NJ 300 an, einer 1998 in New Jersey gegründeten Gruppe, die das Augenmerk auf führende weibliche Wirtschaftskräfte in diesem Bundesstaat lenken will.

Melissa Klipp ist Mitglied der New Jersey State, New York State und American Bar Associations sowie der ABA-Sektion zu geistigen Eigentumsrechten und sitzt außerdem im Ausschuss der New Jersey State Bar Association zum Thema Internet- und Computerrecht. Sie ist Mitglied der American Intellectual Property Law Association, der Intellectual Property Owner's Association und gehört dem John J. Gibbons American Inn of Court an. Frau Klipp war 1991/92 als Law Clerk für Philip A. Gruccio, Richter am Superior Court von New Jersey in der Berufungsabteilung tätig.

Nach einem B.A. am Dickinson College machte sie ihren J.D. an der Dickinson School of Law (Penn State), wo sie auch Redaktionsmitglied der Zeitschrift *Dickinson Law Review* war.

☛ *Melissa Klipp zum Thema (Seite 8)*

Ruth Hill Bro

Partner, Baker & McKenzie LLP

Neue Herausforderungen

Eine der größten Herausforderungen für die IT-Compliance in Unternehmen besteht im Konflikt zwischen Datenschutz und Datenoffenlegung. Ende 2006 traten in den USA neue E-Discovery-Bestimmungen in Kraft. Um diesen kosteneffektiv entsprechen zu können, haben viele US-Unternehmen Computersysteme installiert, die nach Daten suchen und automatisch auf Offenlegungsanfragen reagieren. Die Einführung dieser Systeme ohne Rücksicht auf die jeweilige Rechtssituation kann jedoch schnell zum Problem werden, da verschiedene Gesetze den Schutz personenbezogener Daten und Datenübertragungen ganz unterschiedlich weit fassen.

Datensicherheit ist ein brandaktuelles Thema für die IT-Compliance. Durch die Vorgänge um den Datenhändler ChoicePoint, die neben anderen unangenehmen Folgen die Verhängung eines Bußgelds von US $ 15 Mio. durch die FTC nach sich zogen, geriet der Schutz personenbezogener Daten erstmals ernsthaft auf den Radar vieler Unternehmen. In jüngerer Vergangenheit musste die Geschäftswelt aus dem Fall TJX lernen, dass auch renommierte Unternehmen vor derartigen Sündenfällen keineswegs gefeit sind. Auch im besten Unternehmen können hinter den Kulissen unappetitliche Dinge geschehen.

Im Falle der US-Discountkette TJX waren gigantische Zahlen im Spiel. So wurde bekannt, dass die SEC-Files des Unternehmens Settlement-Kosten in Höhe von rund US $ 40 Mio. vorsahen und erhebliche Summen für Prozesskosten und Kreditüberwachung eingestellt worden waren. Derartige Beträge sind keine Peanuts. Aber auch kleinere Beträge wie sie beispielsweise für die Kreditüberwachung anfallen, summieren sich schnell zu drückenden Lasten, wenn es um die Verletzung der persönlichen Daten von Millionen Menschen geht. Hier gilt also eindeutig das Vorsorgeprinzip, denn nur so lässt sich Schlimmeres verhüten.

Das politische Klima

In den USA ist seit einiger Zeit ein Bundesgesetz im Gespräch, das die Meldung von Datenschutzverletzungen verbindlich vorschreiben soll. 2008 könnte es endlich Realität werden. Derzeit verfügen 39 Bundesstaaten und einige US-Territorien über derartige Gesetze, die sich an dem bahnbrechenden kalifornischen Privacy-Gesetz aus dem Jahr 2003 orientieren. Dank des kalifornischen Vorreiters und seiner Nachfolger sind Unternehmen nun gezwungen, betroffene Personen bei einer Vielzahl von Datenschutzverletzungen zu informieren, und auch die Presse reagiert zunehmend sensibel. Dieser Trend bleibt auch in anderen Ländern nicht unbemerkt. Auch dort denkt man über die Einführung von Meldevorschriften nach, sofern die bestehenden Gesetze dies nicht bereits vorsehen.

Anstelle der von Bundesstaat zu Bundesstaat variierenden Gesetze würden viele Unternehmen einem landesweit geltenden Gesetz den Vorzug geben. Die bundesstaatlichen Vorschriften unterscheiden sich nicht nur hinsichtlich der Kategorisierung personenbezogener Daten, sie definieren auch die meldepflichtigen Ereignisse völlig unterschiedlich und enthalten jeweils verschiedene Ausnahmeregelungen. In einigen Fällen muss z. B. eine bundesstaatliche Stelle benachrichtigt werden.

Vor diesem Hintergrund verwundert es nicht, dass der Ruf nach einer US-weit einheitlichen Regelung lauter wird. Bei den zahlreichen Gesetzesvorschlägen, über die derzeit beraten wird, besteht jedoch Uneinigkeit über den Geltungsumfang und über so wichtige Fragen wie z. B., welche personenbezogenen Daten durch welche Gesetze abgedeckt sind und welche Ereignisse eine Meldepflicht auslösen. In den USA haben Bundesgesetze zu Datenschutz und Datensicherheit nicht automatisch Vorrang vor Gesetzen auf

Ruth Hill Bro
Partner
Baker & McKenzie LLP

„Angesichts schwieriger wirtschaftlicher und außenpolitischer Herausforderungen und der nahen Präsidentschaftswahl weiß keiner, wie die Chancen für eine landesweit geltende gesetzliche Meldepflicht bei Datenschutzverletzungen stehen."

- *Gründerin und Vorsitzende des E-Privacy-Ausschusses der ABA 2000 bis 2005*
- *Gründerin und Herausgeberin des weltweit erscheinenden Privacy-Newsletters ihrer Kanzlei und US-Gründungsmitglied des globalen Lenkungsausschusses zum Thema Datenschutz*
- *Geführt in Chambers USA: America's Leading Business Lawyers; The Legal 500 U.S.*

E-Mail-Kontakt:
ruth.bro@execblueprints.com

Anstelle der von Bundesstaat zu Bundesstaat variierenden Gesetze würden viele Unternehmen einem landesweit geltenden Gesetz den Vorzug geben.

Ruth Hill Bro
Partner
Baker & McKenzie LLP

Die USA stehen im Ruf einer prozesswütigen Nation; entsprechend wichtig ist die Extrahierung und Erfassung prozessrelevanter Daten. Gleichzeitig finden sich in den Vereinigten Staaten Dutzender unterschiedlicher Privacy-Gesetze – eine Situation, die von der Einheitlichkeit einer Europäischen Union weit entfernt ist. Diese Kombination sorgt für Konfliktstoff, da europäische Behörden meist nicht verstehen, warum US-Unternehmen derart viele Informationen (Kontaktdaten, persönliche Daten usw.) benötigen. Die Unternehmen wiederum sitzen tendenziell zwischen allen Stühlen. Wie sollen sie den einander widersprechenden Gesetzen Genüge leisten und gleichzeitig die Gefahr einer Compliance-Verletzung vermeiden?

Ruth Hill Bro
Partner
Baker & McKenzie LLP

Bundesstaatsebene. Trotz dieser Einschränkung würden viele Unternehmen ein Bundesgesetz zu diesem Thema sehr begrüßen.

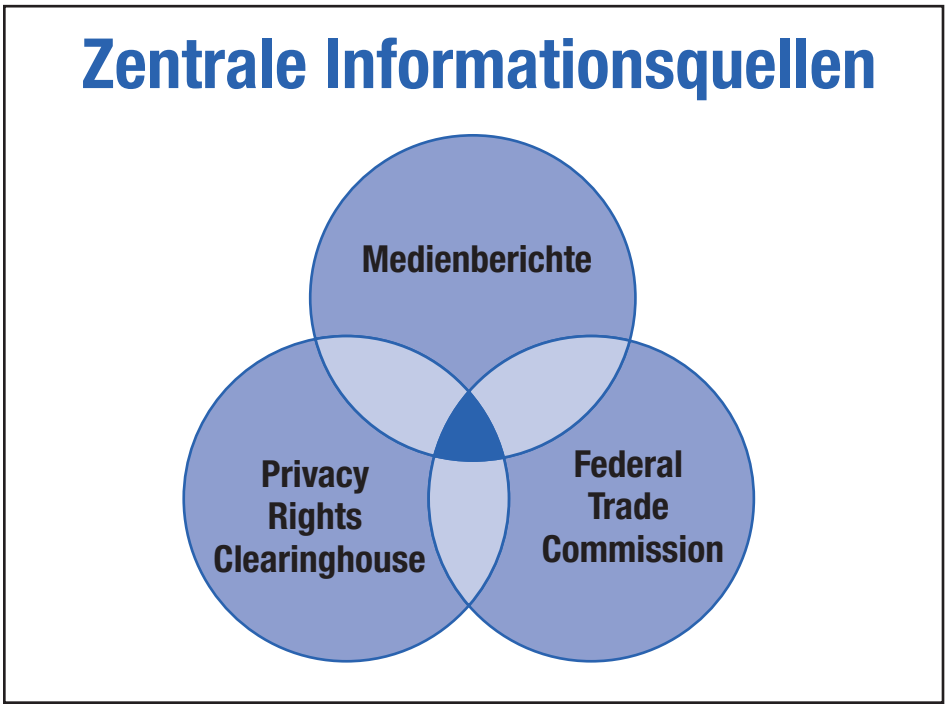
Auf dem neuesten Stand bleiben

Um über neue Entwicklungen beim Datenschutz auf dem Laufenden zu bleiben, sollten Unternehmen die relevanten Medien, seien sie online oder offline, intensiv verfolgen. So berichten die *New York Times, das Wall Street Journal, USA Today* und msnbc.com nicht nur über alle größeren Compliance-Vorkommnisse, sondern auch über neue Gesetze und Vorschriften.

Privacy Rights Clearinghouse (unter www.privacyrights.org) unterhält eine umfangreiche Website, die Datenschutzverletzungen in den USA bis zum Januar 2005 archiviert. Es ist ungemein nützlich und informativ, die in den Medien veröffentlichten Vorkommnisse regelmäßig mitzuverfolgen. Denn in den meisten Unternehmen stellt sich nicht die Frage, ob, sondern vielmehr wann personenbezogene Daten missbraucht werden.

Auf der FTC-Website findet sich ein Abschnitt zu Privacy-Initiativen mit einer umfassenden Liste aktueller Fälle, bei denen es sich häufig um Datenschutzverletzungen handelt. Sie können als Leitlinie dienen, um häufig vorkommende Fallstricke zu erkennen und zu beseitigen. Laut FTC muss jedes Unternehmen über ein effektives Datenschutzprogramm verfügen, wenn es nicht Gefahr laufen will, wegen unfairen und unlauteren Wettbewerbs belangt zu werden. Die FTC betont jedoch auch, dass hundertprozentige Sicherheit nicht erwartet werden kann; auch die Behörden wissen, dass Irren menschlich ist und Fehler deshalb nicht ausgeschlossen werden können. Sie erwarten jedoch, dass die Unternehmen die notwendigen Schritte ergreifen, um Gefahren abzuwenden, die sie kennen bzw. kennen sollten. Dabei wissen wir alle, dass auch der US-Regierung auf nationaler und internationaler Ebene durchaus Patzer bei der Datensicherheit unterlaufen.

Die von der FTC veröffentlichten Praxisfälle machen aber deutlich, welche Basisanforderungen von jedem Unternehmen zu erfüllen sind. Zwingend



notwendig sind z. B. geeignete Schritte gegen bekannte Gefahren wie beispielsweise SQL-Attacken. Die Unternehmen müssen in der Lage sein, unbefugten Zugriff auf Daten zu erkennen. Sie müssen über wirksame Authentifizierungsverfahren verfügen. Daten sollten nicht länger als von den Unternehmensrichtlinien oder dem Gesetz vorgeschrieben gespeichert werden. Dateien mit sensiblem Inhalt dürfen nicht mit Standard-IDs und -Kennwörtern geschützt werden. Die Kennungen der Personen, die auf Daten zugreifen möchten, müssen überprüft werden. Personenbezogene Daten werden immer häufiger nicht nur bei der Übertragung, sondern auch bei der Speicherung verschlüsselt. Dies gilt zumindest für sensible personenbezogene Daten. Vielleicht die wichtigste Anforderung besteht aber in der Durchführung regelmäßiger Risikoabschätzungen und der Einführung geeigneter Kontrollen, mit denen sich die so ermittelten Lücken schließen lassen.

Finanzielle und sonstige Risiken

Unternehmen ohne nachhaltiges Compliance-Programm gehen erhebliche Risiken ein. Eines der größten besteht in negativer PR. Verbraucher, die einem Unternehmen nicht vertrauen, kaufen auch nicht dessen Produkte. Auch die Börsenkurse eines Unternehmens können bei Compliance-Problemen leiden. Und schließlich werden Datenschutzverletzungen und ihre Folgen in den bei der SEC eingereichten Unterlagen offenbar.

In den USA werden Verletzungen von Datenschutz und Datensicherheit von einer Vielzahl staatlicher Stellen überprüft; Beispiele hierfür sind die FTC, die SEC und der Generalstaatsanwalt. Außerhalb der USA müssen verdächtige Unternehmen mit unangemeldeten Prüfungen durch Datenschutzbehörden und einer Unterbrechung ihres Datenstroms rechnen. Prozesse, Zahlungen, Geldbußen und andere Schäden für das Unternehmen sind die Folge. Weitere Konsequenzen sind schmerzhafte Geschäftseinbußen, Produktivitätsverluste und höhere Versicherungsprämien. Mitunter werden sogar strafrechtliche Prozesse angestrengt. Und selbst wenn ein Unternehmen mögliche Geldbußen billigend in Kauf nimmt, wird es wohl kaum Mitarbeiter finden, die bereit sind, eine eventuelle Gefängnisstrafe auf sich zu nehmen. Angesichts dieser drastischen Risiken rollen bei größeren, der Öffentlichkeit bekannt gewordenen Vorfällen immer häufiger Köpfe; infolge schwerwiegender Compliance-Verletzungen mussten bereits einige GCs, CIOs und andere Führungskräfte ihren Hut nehmen – unter den Argusaugen der Medien. ■

I. Edward Marquette

Partner, Sonnenschein Nath & Rosenthal LLP

Neue Elemente: MySpace, Blogs und Internet-Festplatten

IT-Compliance-Programme beinhalten heute eine Reihe neuer Elemente, die sich aus der Nutzung des Internet z. B. in Form von MySpace oder Blogs ergeben. Immer mehr Menschen äußern sich im Internet vor großem Publikum über ihre Sicht der Dinge; dabei fließen zwangsläufig auch Informationen aus der Arbeitswelt mit ein. Manchmal sind dies Informationen, die besser unveröffentlicht geblieben wären.

Personalabteilungen überprüfen mittlerweile routinemäßig Blogs, wenn es um die Einstellung neuer Mitarbeiter geht. Dabei finden sich mitunter Informationen und Ansichten, die den Bewerbungsunterlagen widersprechen oder sogar dazu führen, dass eine Bewerbung aussortiert wird. Wenn das Unternehmen erst nach der Einstellung feststellt, dass ein Mitarbeiter inakzeptable Informationen im Web veröffentlicht, müssen Maßnahmen ergriffen werden. Ein potenziell schwieriges Unterfangen, wenn im Vorfeld keine entsprechende Warnung ausgesprochen wurde bzw. keine eindeutige Firmenpolitik zu diesem Thema vorhanden ist.

Erst kürzlich bearbeitete unsere Kanzlei einen derartigen Streitfall, bei dem ein hochrangiger Mitarbeiter eine Mischung aus persönlichen und Unternehmensinformationen auf einer Internet-Festplatte gespeichert hatte, auf die er über seinen Firmenrechner zugriff. Die Festplatte war kennwortgeschützt, und nur der Mitarbeiter, nicht aber das Unternehmen, verfügte über dieses Kennwort. Wie kann das Unternehmen also eine missbräuchliche Nutzung seines Rechners ausschließen? Die Speicherung von privaten Daten unter Verwendung unternehmenseigener Computer sollte unserer Ansicht nach untersagt sein.

Der von unserer Kanzlei erstellte Entwurf einer Datenschutzrichtlinie räumte Unternehmen das Recht ein, firmeneigene IT-Ausrüstung in regelmäßigen Abständen zu überprüfen, ohne dass die Mitarbeiter dabei ein Recht auf Schutz ihrer Privatsphäre geltend machen konnten. Mittlerweile hat sich die Situation jedoch geändert. Mitarbeiter verfügen nun über Festplatten, für die sie privat bezahlen, die sie routinemäßig im Büro nutzen, die sich aber nicht im Besitz des Unternehmens befinden. So genannte Thumb Drives, also extrem kleine externe Speicherlösungen, werden einfach an einem USB-Anschluss des Computers eingesteckt und wie eine Festplatte genutzt.

Es gibt so viele neue, kreative und ungewöhnliche Möglichkeiten, das Internet zu nutzen, dass es quasi nichts gibt, wozu ein Webbrowser heutzutage nicht verwendet werden kann.

I. Edward Marquette
Partner
Sonnenschein Nath & Rosenthal LLP

Natürlich wäre es wünschenswert, alle neuen Entwicklungen in einer Richtlinie zu berücksichtigen. Angesichts der Geschwindigkeit, mit der neue Technologien und Anwendungen entstehen, dürfte dies aber kaum machbar sein. Es gibt so viele neue, kreative und ungewöhnliche Möglichkeiten, das Internet zu nutzen, dass sich nicht vorhersagen lässt, wozu ein Webbrowser alles dienen kann.

Einflüsse der Politik

In den kommenden 12 Monaten werden Gesetze für den IT-Bereich auf der politischen Agenda stehen. Dies wird ganz sicher auch den Umgang mit privaten Daten betreffen. Internet- und Computersicherheit sind von kaum zu überbietender Bedeutung. Ein Unternehmen, das Opfer von Hackern wird, hat nicht nur mit negativer Publicity, sondern auch mit handfesten finanziellen Folgen zu kämpfen.

Daher müssen sich die Unternehmen mit allen gängigen Methoden gegen Sicherheitslücken schützen. Gleichzeitig müssen sie jedoch auch wissen, wo sich personenbezogene Daten befinden. Dies ist nicht immer einfach. Einer unserer Klienten hat diese Marktlücke erkannt und entwickelt ein Produkt, das auch in großen, unübersichtlichen Systemen präzise feststellt, wo derartige Daten gespeichert sind.

Viele Richtlinien schreiben einen bestimmten Speicherort für personenbezogene Daten vor, nur leider halten sich die Mitarbeiter nicht daran. In der Praxis sind diese Daten im gesamten System verteilt. Der Datenschutz rückt immer mehr ins Blickfeld unserer Regierung. Und auch im Kreditkartenbereich bzw. bei der Verarbeitung von Kreditkartendaten schreiben Visa und andere Kartenunternehmen nun die Einhaltung der strengen PCI (Payment Card Industrie)-Standards vor.

I. Edward Marquette
Partner
Sonnenschein Nath & Rosenthal LLP

„Das Internet eröffnet den Menschen die Möglichkeit zu völlig neuartigem – und manchmal nicht angemessenem – Verhalten".

- *Kanzlei mit 800 Anwälten in neun Städten*
- *Seit über zehn Jahren in der Liste der* Best Lawyers in America *geführt (Fachgebiet geistige Eigentumsrechte)*
- *Ehemaliges Mitglied des ABA-Ausschusses zur Informationsinfrastruktur in den USA*
- *Ehemaliger Vorsitzender des Ausschusses für neue Informationstechnologien der ABA-Sektion mit dem Schwerpunkt geistige Eigentumsrechte*

E-Mail-Kontakt:
edward.marquette@execblueprints.com

I. Edward Marquette

Partner, Sonnenschein Nath & Rosenthal LLP

(Forts.)

Best Practices

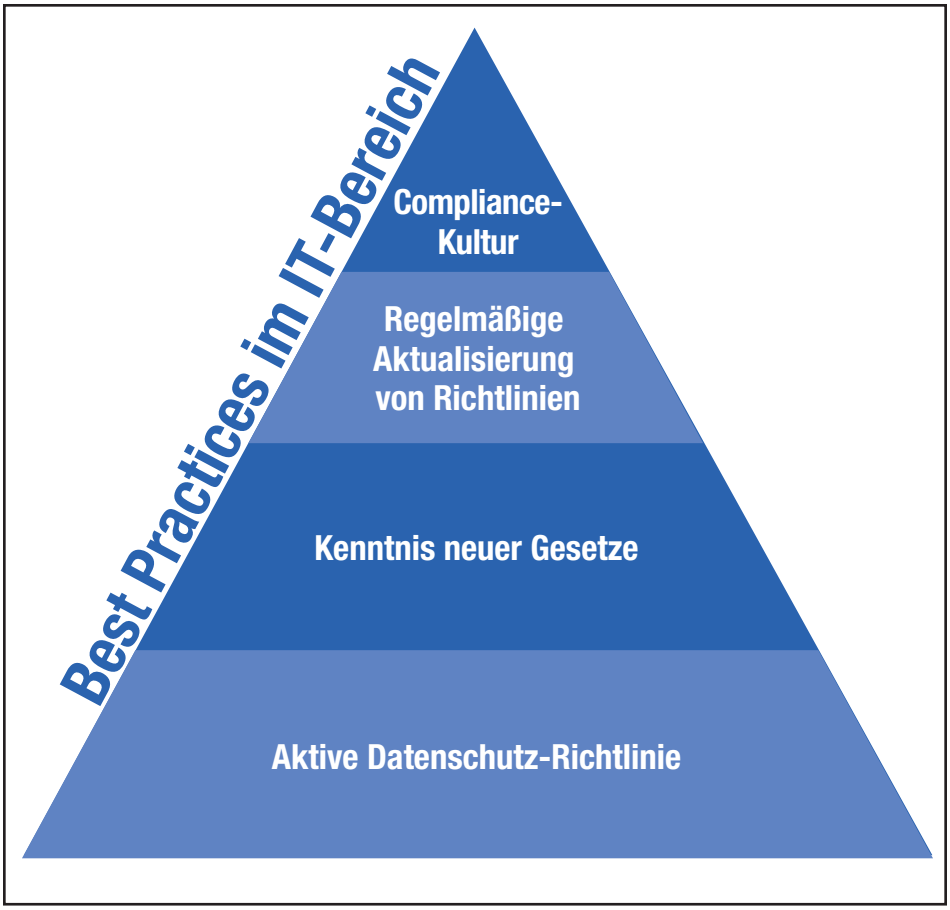
Unternehmen mit nachhaltig ausgelegten IT-Programmen kann ich nur raten, ihre Richtlinien aktiv umzusetzen. Es ist wenig sinnvoll, eine Richtlinie zu entwickeln und anschließend zu vergessen. Sie muss vielmehr ständig überprüft und weiterentwickelt werden.

In den USA wurden neue Gesetze zur Offenlegung elektronischer Informationen (E-Discovery) verabschiedet. Unternehmen stehen daher vor der dringenden Aufgabe, ihre bisherigen Richtlinien zur Dokumentenaufbewahrung zu überprüfen. Diese Richtlinien müssen an die neuen Vorschriften und Gesetze zu Datenschutz und Datensicherheit angepasst werden. Nicht nur die IT-Politik, sondern auch die Unternehmensrichtlinien zur Dokumentenaufbewahrung müssen immer wieder auf neue Gegebenheiten abgestimmt werden.

Internationale Compliance-Anforderungen

Weltweit tätige Unternehmen gehen besondere Risiken ein. Der Datenschutz ist nicht nur in den USA, sondern auch in anderen Teilen der Welt, beispielsweise in Europa, ein sensibles Thema. In der EU gelten sehr viel strengere Bestimmungen als in den Vereinigten Staaten.

Die Haltung vieler europäischer Unternehmen zum Thema Daten unterscheidet sich drastisch von unserer eigenen. International tätige US-Firmen müssen dies wissen und berücksichtigen. Viele Amerikaner sind der Meinung, dass hierzulande die strengsten Bestimmungen überhaupt gelten. Sie sind der Überzeugung, dass mit der Einhaltung unserer Gesetze automatisch auch die Vorschriften in anderen Ländern erfüllt werden. Weit gefehlt, besonders beim Thema Daten und Datenschutz.



So sind in Frankreich Daten nicht automatisch Eigentum der Person, die sie erzeugt hat. Vielmehr gehören sie der Person, auf die sie sich beziehen. Als US-Amerikaner sammle ich Daten zum Einkaufsverhalten meiner Kunden samt ihrer Sozialversicherungsnummer und ihrer Geburtsdaten und halte diese Informationen für ein wertvolles Absatzinstrument. Ein Europäer wäre hier ganz anderer Ansicht. Seiner Meinung nach gehören die Daten nicht mir, nur weil ich sie gesammelt habe. Sie gehören den Kunden, auf die sie sich beziehen.

Wenn ich Daten in Europa erfasse, kann ich dies nicht einfach von den USA aus tun. Vielmehr gelten für den Transfer personenbezogener Daten aus Europa in die USA äußerst strenge Vorschriften, die aber nur den wenigsten bewusst sind. Grundsätzlich ist festzustellen, dass die US-amerikanische Einstellung zum Datenschutz vergleichsweise lax ist. ■

Aufgrund der Vielzahl sensibler Daten nimmt das Risikopotenzial für unsere Klienten ständig zu. In Zukunft werden Unternehmen noch mehr Augenmerk darauf richten, wie, wo und in welchem Ausmaß sie personenbezogene Daten zu Kunden, Lieferanten und Mitarbeitern sicher verschlüsseln.

I. Edward Marquette
Partner, Sonnenschein Nath & Rosenthal LLP

Melissa L. Klipp

Partner, Drinker, Biddle and Reath, LLP

Neue Entwicklungen

Die technologische Weiterentwicklung bei der Speicherung elektronischer Daten resultierte in neuen Gesetzen, die die Datenarchivierung im Rahmen von IT-Compliance-Programmen regeln. Sie schreiben die Ausgabe von Litigation Hold-Benachrichtigungen vor und verpflichten Unternehmen dazu, die Abänderung oder Vernichtung elektronischer Beweismittel zu verhindern, wenn sie sich nicht der Gefahr aussetzen wollen, dafür belangt zu werden.

Im Zuge dieser Entwicklung wurden nicht nur neue Anforderungen an die Identifizierung, Archivierung und Offenlegung elektronisch gespeicherter Informationen formuliert, sondern die bestehenden Litigation-Vorschriften wurden durch zusätzliche Bestimmungen ergänzt. In der aktuellen Rechtssprechung wurden Unternehmen bereits verurteilt, da sie Daten nicht archiviert hatten, relevanter E-Mail-Verkehr nicht abrufbar war und die nötigen Schritte zur Lokalisierung relevanter Informationen nicht ergriffen worden waren. In einigen Fällen wurden sowohl die Anwälte als auch die Führungskräfte der betroffenen Unternehmen persönlich für Mängel bei Datenschutz und -archivierung haftbar gemacht.

Diese Entwicklung hat dazu geführt, dass die IT- und HR-Abteilungen so wichtig sind wie nie zuvor. Da auch Anwälte zur Erfüllung ihrer Aufgaben auf Technologien angewiesen sind, benötigen sie die Unterstützung der IT-Mitarbeiter. Folglich müssen diese Mitarbeiter wissen, welche Erwartungen seitens des Gesetzgebers an ihr Unternehmen gestellt werden. Nun denken technisch ausgerichtete Menschen meist in konkreten Sachverhalten. Wenn ihnen jemand eine Aufgabe erteilt, erledigen sie genau diese Aufgabe, nicht mehr und nicht weniger. Wenn ein Anwalt daher mit der Umsetzung der Vorschriften zum Umgang mit elektronischen Daten befasst ist, muss er berücksichtigen, dass IT-Mitarbeiter in der Regel konkrete Anweisungen benötigen. Er muss klar und unmissverständlich definieren, was die Mitarbeiter tun müssen, um ihre Tätigkeit innerhalb des geänderten Gesetzesumfelds effizient und wirksam auszuüben.

Die Verantwortung für den IT-Bereich eines Unternehmens sollte nie allein beim CIO liegen.

Melissa L. Klipp
Partner
Drinker, Biddle and Reath, LLP

Die Abstimmung von IT, Archivierung und HR – eine Aufgabe des Response Teams

Im Rahmen eines Programms zur Technologie-Compliance sollte ein Response Team geschaffen werden. Den Kern dieses Teams müssen IT-Mitarbeiter bilden; darüber hinaus sollte es Experten für das Records Management beinhalten, die wissen, wie lange Dokumente aufbewahrt werden müssen und wie relevante Informationen abgerufen werden können. Auch die Personalabteilung sollte involviert sein, da deren Mitarbeiter über Änderungen der Branche, des Marktes sowie der Nutzervorlieben am besten informiert sind. Selbstverständlich muss auch die Rechtsabteilung einbezogen sein, um die Einhaltung der geltenden Gesetze und Vorschriften sicherzustellen.

Die Verantwortung für den IT-Bereich eines Unternehmens sollte nie allein beim CIO liegen. Vielmehr sollte auch das mittlere Management einbezogen werden, denn diese Führungskräfte wissen, wo und wie die Nutzer ihre Daten ablegen und kennen die Vorlieben der einzelnen Mitarbeiter. Sie wissen am ehesten, ob ein bestimmter Mitarbeiter seine E-Mails jeden Abend löscht, Daten an ein gemeinsam genutztes Laufwerk überträgt oder auf ein externes Speichermedium herunterlädt. Dieses Wissen ist nur in der täglichen Praxis zu erwerben und findet sich daher mit größerer Wahrscheinlichkeit eher beim mittleren Management als beim CIO. Im Falle eines Litigation Hold oder einer Subpoena-Vorladung müssen umfassende Kenntnisse über die Datensätze der betroffenen Mitarbeiter vorliegen. Wenn jemand über das Archivierungsverhalten dieser Personen Bescheid weiß, spart dies sehr viel Zeit und Aufwand.

Neben IT übernimmt auch die Personalabteilung eine wichtige Aufgabe, indem sie sicherstellt, dass die Mitarbeiter angemessen und in regelmäßigen Abständen geschult werden. Die für das Records Management zuständigen Mitarbeiter sorgen dafür, dass geeignete Aufbewahrungs- und Archivierungsrichtlinien für papiergestützte und elektronische Daten vorhanden sind.

Melissa L. Klipp
Partner
Drinker, Biddle and Reath, LLP

„In einem dynamischen Wirtschaftsumfeld mit ständig weiterentwickelten Technologien und Prozessen werden immer neue Gesetze erlassen, um auf neuartige Herausforderungen und Probleme zu reagieren."

- *Geführt in der Liste der „New Jersey's Best 50 Women in Business" aus dem Jahr 2006*
- *Mitglied der NJ 300, einer in New Jersey gegründeten Gruppe zu Ehren der führenden weiblichen Wirtschaftskräfte des Bundesstaats*
- *Mitglied der ABA-Sektion zu geistigen Eigentumsrechten sowie des Ausschusses der New Jersey State Bar Association zum Thema Internet- und Computerrecht*

E-Mail-Kontakt:
melissa.klipp@execblueprints.com

Melissa L. Klipp
Partner, Drinker, Biddle and Reath, LLP

Heutzutage sehen immer mehr Unternehmen ein, dass die Bandsicherung kein angemessenes Archivierungsverfahren mehr darstellt. Umso wichtiger ist es, dass die betreffende Abteilung über das notwendige Fachwissen zu geeigneten elektronischen Systemen verfügt und weiß, wie diese implementiert werden.

Im Prozessfall können Sicherungsbänder zu einer verhängnisvollen Belastung werden. Wenn die gegnerische Seite die Offenlegung sämtlicher E-Mails eines bestimmten Zeitraums fordert und die IT-Abteilung dieser Forderung nicht entsprechen kann, wird häufig die Vorlage von Backup-Bändern verlangt, um so sicherzustellen, dass keine Beweismittel vernichtet wurden. Die Sicherungsbänder enthalten jedoch unter Umständen nicht prozessrelevante Informationen, die nicht offenbart werden sollen. Es kann äußerst kostspielig werden, jedes einzelne Band von einem Anwalt auf geschützte oder vertrauliche Informationen durchsuchen zu lassen. Wenn bei der Bandsicherung die von IT, Records Management und HR gemeinsam entwickelten Richtlinien beachtet wurden, befindet sich das Unternehmen dagegen in einer sehr viel besseren Position.

Beurteilung von IT-Programmen

Benchmarks sind immer abhängig von der Größe und Art des Unternehmens; dessen ungeachtet sollten grundlegende Benchmarks für den IT-Bereich zumindest die Faktoren Dokumentenaufbewahrung, Einhaltung von Gesetzen und Vorschriften sowie Mitarbeiterschulung zur Computer- und Internetnutzung umfassen. Bei der Beurteilung eines Compliance-Programms sollten die für das Unternehmen maßgeblichen Bestimmungen zugrunde gelegt werden. So sollten bei der Einhaltung der SOX-Bestimmungen die Aufbewahrungszeiträume z. B. so kurz gehalten werden, wie dies gesetzlich zulässig und für das Unternehmen machbar ist.

Die IT-Compliance sollte auch auf Mitarbeiterebene gemessen werden, da diese unbedingt in der ordnungsgemäßen Handhabung von E-Mails geschult werden müssen. Ergänzend hierzu war ich an der Verfassung einer Reihe von Record Retention-Richtlinien beteiligt, in denen die Art der im Unternehmen (temporär oder permanent) vorkommenden Datensätze genau beschrieben wird. Je nach Art der Datensätze wird darin festgelegt, wie die Mitarbeiter bezüglich ihrer Verwendung, Verwaltung und Vernichtung zu schulen sind.

Die enorme Spannbreite des IT-Bereichs, gepaart mit der Tatsache, dass 97 Prozent der Unternehmenskommunikation mittlerweile per Computer abgewickelt werden, verleiht der IT-Compliance eine völlig neue Bedeutung. Aus Sicht eines Anwalts sind elektronische Daten und IT-Compliance zwei zentrale Elemente in jedem Prozess. Dabei ist es äußerst schwierig, alle Faktoren dieser so spezifischen Materie zu berücksichtigen; die oben erwähnten Benchmark-Kriterien bilden jedoch einen ersten Anhaltspunkt.

Die Entwicklung der IT-Compliance in nächster Zukunft

Angemessene Record Retention-Richtlinien für elektronisch gespeicherte Informationen sind heutzutage unverzichtbar für jedes IT-Compliance-Programm. Dies gilt besonders angesichts der riesigen Mengen an Backup-Bändern, die nur darauf warten, als Beweismittel aufgerufen zu werden. In vielen Fällen sind diese Bänder für das Unternehmen völlig wertlos, da sie in erster Linie für die Disaster Recovery gedacht sind. Häufig sind sie so alt, dass die Technologie für ihre Wiedergabe nicht mehr existiert. Da sich Sicherungsbänder nicht ohne menschliches Zutun durchsuchen lassen und es nur sehr wenige Anbieter und Technologien gibt, die eine effektive Suche gestatten, kann dies schnell enorme Summen verschlingen. Richtlinien zur Datenaufbewahrung oder -vernichtung, die festlegen, wie lange ein Unternehmen Sicherungsbänder archivieren muss und wann diese vernichtet werden können, sind daher aus Unternehmenssicht

Damit ein Compliance-Programm erfolgreich ist, muss es vom C-Level-Management unterstützt werden. Ohne diese Unterstützung ist auch ein noch so durchdachtes Programm zum Scheitern verurteilt. Die Führungsebene des Unternehmens muss daher im Detail mit dem Thema IT-Compliance vertraut sein, sich rückhaltlos dafür einsetzen und wissen, welche Relevanz, Bedeutung und Konsequenz es für die Unternehmenszahlen haben kann.

Melissa L. Klipp
Partner
Drinker, Biddle and Reath, LLP

zwingend erforderlich. Wenn hieb- und stichfeste Richtlinien vorhanden sind, ist eine Haftung für Bänder auch im Streitfall ausgeschlossen. Dies gilt selbst dann, wenn der Prozessgegner ihre Offenlegung fordert, das Unternehmen dem aber nicht entsprechen kann, da die Tapes bereits vernichtet wurden.

Unternehmen, die auch außerhalb der USA tätig sind, sehen sich mit einer Fülle von Datenschutzbestimmungen konfrontiert. So entspricht in der EU der Schutz elektronischer Daten und E-Mails quasi einem Verfassungsrang in den Vereinigten Staaten. Mit Ausnahme einiger weniger Fälle können Einzelpersonen Einspruch dagegen erheben, dass ihre E-Mails von einem Server abgerufen werden, selbst wenn diese im Rahmen eines Prozesses in den USA als Beweismittel dienen. Die Europäische Union hat auf die Offenlegungsanforderungen der US-amerikanischen Gerichte reagiert und im Interesse eines wirksamen Datenschutzes Blockaden errichtet, die die Weitergabe von Daten als Beweismittel verhindern.

Wenn daher ein Unternehmen in den USA von einem Gericht zur Vorlage von Daten aufgefordert wird, die in der EU gespeichert sind, kann dies hohe Kosten nach sich ziehen. Dies gilt besonders dann, wenn der betreffende Server sowohl Daten aus der EU als auch aus den USA enthält. Kaum vorstellbar, mit welchen Schwierigkeiten Unternehmen zu kämpfen haben, die in Dutzenden von Ländern aktiv sind! Wenn diese Unternehmen nicht über ausgeklügelte Richtlinien verfügen, die ihnen den Weg durch diesen Dschungel weisen und definieren, wann und wie die Zustimmung der Mitarbeiter zur Datenoffenlegung eingeholt werden kann, müssen sie bei Rechtsstreitigkeiten mit hohen Ausgaben rechnen. Gleichzeitig müssen sie versuchen, dem Gericht klarzumachen, warum die als Beweismittel aus der EU angeforderten E-Mails nicht ohne weiteres vorgelegt werden können.

Die Zwickmühle, in der sie sich befinden, eröffnet wiederum Anbietern von Datenspeicherungstechnologien und -services einen millionenschweren Markt. Die meisten Anwälte bescheinigen den heute erhältlichen Lösungen für die Verarbeitung elektronisch gespeicherter Daten mehr oder weniger schwere Mängel. Angesichts der Tatsache, dass Daten immer schneller, effizienter und besser verarbeitet werden müssen, gibt es hier noch jede Menge Entwicklungsbedarf. Technologiefirmen, die der Wirtschaft dabei helfen, dieser Aufgabe gerecht werden, dürften einen lukrativen Markt für ihre Produkte finden. ■

Weiterführende Ideen & Aktionspunkte

I. Unternehmensweite Compliance

Ein Technologie-Compliance-Programm muss Mitarbeiter aus dem gesamten Unternehmen mit einbeziehen.

- Den Kern des Compliance-Teams müssen IT-Mitarbeiter bilden; darüber hinaus muss das Team eine Reihe von Experten aus anderen Fachbereichen beinhalten.
- Dies gewährleistet eine ganzheitliche und aktuelle Sicht auf Compliance-Sachverhalte im gesamten Unternehmen.

Die Verantwortung für den IT-Bereich eines Unternehmens sollte nie allein beim CIO liegen. Beteiligt werden müssen:

- IT-Führungskräfte des mittleren Managements
  - Sie wissen, wo und wie die Nutzer ihre Daten ablegen und kennen die Vorlieben der einzelnen Mitarbeiter.
- Die Personalabteilung
  - Die Personalabteilung stellt sicher, dass die Mitarbeiter angemessen und in regelmäßigen Abständen geschult werden.
- Das Records Management
  - Die für das Records Management zuständigen Mitarbeiter sorgen dafür, dass geeignete Aufbewahrungs- und Archivierungsrichtlinien für papiergestützte und elektronische Daten vorhanden sind.
- Die Führungsebene
  - Damit ein Compliance-Programm erfolgreich ist, muss es vom C-Level-Management unterstützt werden.
  - Die Führungsebene des Unternehmens muss mit dem Thema IT-Compliance im Detail vertraut sein, sich rückhaltlos dafür einsetzen und wissen, welche Relevanz, Bedeutung und Konsequenz es für die Unternehmenszahlen haben kann.

II. Das Endergebnis

Unternehmen müssen heutzutage größte Sorgfalt auf den Umgang mit personenbezogenen Daten zu Kunden, Lieferanten und Mitarbeitern verwenden.

- Eine Lücke in der Datensicherheit ist nicht nur ein legales Problem, sondern auch ein PR-Desaster.
- Ein Unternehmen, das Opfer von Hackern wird, hat nicht nur mit negativer Publicity, sondern auch mit handfesten finanziellen Folgen zu kämpfen.

Unternehmen mit nachhaltig ausgelegten IT-Programmen kann ich nur empfehlen, ihre Richtlinien aktiv umzusetzen.

- Es ist wenig sinnvoll, eine Richtlinie zu entwickeln und anschließend zu vergessen. Sie muss vielmehr ständig weiterentwickelt und umgesetzt werden.
- Dies erfordert zwar eine kontinuierliche Investition, der finanzielle Schaden aus einer unzureichenden Umsetzung wäre jedoch sehr viel größer.

III. Zentrale Compliance-Themen

Konflikte zwischen Datenschutz und Datenoffenlegung

Eine der größten Herausforderungen für die IT-Compliance in Unternehmen besteht im Konflikt zwischen Datenschutz und Datenoffenlegung.

Datensicherheit

- Datensicherheit ist ein brandaktuelles Thema für die IT-Compliance, da die FTC immer striktere Vorschriften zur Speicherung personenbezogener Kundendaten erlässt.
- Durch die Vorgänge um den Datenhändler ChoicePoint geriet der Schutz personenbezogener Daten erstmals ernsthaft ins Blickfeld vieler Unternehmen.

Internationale Compliance-Anforderungen

- In der EU gelten sehr viel strengere Datenschutzbestimmungen als in den USA, und auch die Rechtsumgebung sieht völlig anders aus.
- International tätige Unternehmen müssen daher mit den Gesetzen in Europa und anderswo unbedingt vertraut sein.

IV. Die goldenen Regeln für eine grundlegende Datensicherheit

Einführung wirksamer Schutzmechanismen gegen unbefugten Datenzugriff.

- Unternehmen müssen geeignete Schritte gegen bekannte Gefahren wie beispielsweise SQL-Attacken ergreifen.
- Sie müssen in der Lage sein, unbefugte Datenzugriffe zu erkennen und sich dagegen zu schützen.

Umsetzung geeigneter Authentifizierungsverfahren.

Die Kennungen der Personen, die auf Daten zugreifen möchten, müssen überprüft werden.

Überwachung der Datenspeicherung.

- Daten sollten nicht länger als von den Unternehmensrichtlinien oder dem Gesetz vorgeschrieben gespeichert werden.
- Dateien mit sensiblem Inhalt dürfen nicht mit Standard-IDs und -Kennwörtern geschützt werden.

Einführung einer universellen Verschlüsselung.

Personenbezogene Daten werden immer häufiger nicht nur bei der Übertragung, sondern auch bei der Speicherung verschlüsselt.

Durchführung regelmäßiger Risikoabschätzungen.

Unternehmen müssen regelmäßige Risikoabschätzungen vornehmen und geeignete Kontrollen durchführen, mit denen sich die ermittelten Lücken schließen lassen.

V. Wichtige Ergebnisse

In einem dynamischen Wirtschaftsumfeld mit ständig weiterentwickelten Technologien und Prozessen werden immer neue Gesetze erlassen, um auf neuartige Herausforderungen und Probleme zu reagieren.

Compliance ist eine fortlaufende Aufgabe, die ständige Selbstüberprüfungen und Aktualisierungen erfordert.

IT-Manager müssen sich daher mit Experten aus dem gesamten Unternehmen zusammenschließen, um gemeinsam alle Compliance-Anforderungen erfüllen zu können.

Technologische Lösungen müssen durch Unterstützung der Rechts- und HR-Abteilungen sowie des C-Level-Managements ergänzt werden. ■

Weiterführende Ideen & Aktionspunkte (Forts.)

10 zentrale Fragen und Diskussionspunkte

1. Welche neuen Elemente sind in den vergangenen 12 Monaten zum IT-Compliance-Programm hinzugekommen? Welche Faktoren stehen hinter den jüngsten Änderungen? Wie lassen sich diese neuen Elemente in bestehende Programme eingliedern? Wie hoch sind die Kosten für ihre Integration?

2. Wie wird sich das politische Klima in den kommenden 12 Monaten auf die IT-Gesetzgebung auswirken? Welche wichtigen Themen zeichnen sich ab? Wer ist für diese Themen zuständig? Wie kann das IT-Management auf dem neuesten Stand der Entwicklung bleiben?

3. Welche Best Practices kommen in Unternehmen mit nachhaltigen IT-Programmen zum Einsatz? Welche Verfahrensweisen für die fortlaufende Compliance-Verbesserung werden angewendet? Wie sind die Zuständigkeiten geregelt? Wie wird die Wirksamkeit der Anstrengungen überprüft und gemessen?

4. Wie sehen die Benchmarks für ein vorbildliches IT-Compliance-Programm aus? Was wird dabei gemessen? Wie sorgen diese Metriken für Nachhaltigkeit? Warum sind sie wichtig? Welche Aspekte lassen sich am schwierigsten messen? Welche Technologie kommt bei der Erfassung und Berechnung dieser Daten zum Einsatz?

5. Wie kann ein internationales Unternehmen die Einhaltung aller maßgeblichen Gesetze und Vorschriften sicherstellen? Welche Zusatzkosten entstehen durch internationale Transaktionen oder Holding-Gesellschaften? Wie lassen sich diese Kosten durch ein nachhaltiges Programm minimieren? Welches Technologie- und Humankapital sollte näher untersucht werden?

6. Welche Faktoren haben den größten Anteil am operativen Budget für das Compliance-Programm? In welche Einzelposten gliedert sich das Budget?

7. Welcher ROI wird mit dem Programm angestrebt? Wie wird er berechnet? Welche nichtfinanziellen Vorteile werden erwartet? Was kann getan werden, um die Rendite zu erhöhen? Wie kann dies geschehen?

8. Welche Best Practices lassen sich auf das Projekt anwenden? Wer ist zuständig für das Projektmanagement? Wie wird der Projektfortschritt erfasst? Wie werden Ziele festgelegt? Welches Budget ist für das Projekt vorgesehen? Welche anderweitigen Ressourcen werden benötigt?

9. Wie lässt sich eine maximale Flexiblität des IT-Compliance-Programms erzielen? Worauf muss reagiert werden können? Welche politischen und wirtschaftlichen Einflussfaktoren gibt es? Wie lässt sich mithilfe von Technologie eine größtmögliche Compliance realisieren? Welche Review-Prozesse werden benötigt, damit die IT-Abteilung auf Ereignisse und Trends reagieren kann?

10. Welche Gruppen sollten in die Entwicklung des Programms mit einbezogen werden? Welche Nachteile hat die Einbeziehung anderer Abteilungen? Welche Vorteile? Wie hoch liegen die Kosten für eine derartige Einbeziehung? Wie lässt sich ein ausgewogenes Verhältnis zwischen Kosten und Vorteilen sicherstellen?