Regina Stoiber

IT-Sicherheit und Datenschutz: Compliance der Zukunft – welche Risiken drohen und welche Chancen entstehen?

Vor fast vier Jahren ist die DSGVO in Kraft getreten und hat viele Unternehmen aufgeschreckt und tätig werden lassen. Sollte inzwischen also nicht auch das letzte Unternehmen ´up to date´ sein in Sachen Datenschutz?

Einhergehend damit auch das Thema der IT-Sicherheit. Sind nicht alle Unternehmen mit Virenscanner, Firewall und Co. ausgestattet? Reicht das denn immer noch nicht?

In der Realität muss man klar sagen: Nein. Das reicht nicht! Es muss uns in den Unternehmen klar sein, dass wir den Themen IT-Sicherheit und Datenschutz permanent Aufmerksamkeit schenken müssen und diese nicht als einmaligen Aufwand verbuchen können.

Worauf sollten also Unternehmen in den nächsten Jahren ihren Schwerpunkt setzen, wenn es um die Sicherheit der Informationen geht? Dabei ist es erst einmal egal, ob wir von personenbezogenen Daten im Sinne des Datenschutzes oder anderen geschäftsrelevanten Informationen sprechen. Schützenswert sind alle diese Informationen.

Im Dezember des letzten Jahres hat uns eine Meldung um eine Schwachstelle gezeigt, welche Auswirkungen eine Lücke in einem kleinen Programm haben kann, wie verwundbar Unternehmen dadurch sein können. Dass weiterhin Schwachstellen auftreten werden, können wir nicht verhindern. Im Umkehrschluss heißt das aber, dass sich die Organisation darauf vorbereiten muss, mit solchen Vorfällen umzugehen.

Agieren statt reagieren muss die Devise sein. Natürlich ist regelmäßiges Patchen und das zeitnahe Einspielen von Sicherheitsupdates eine notwendige Voraussetzung. Damit allein wird es aber in Zukunft nicht getan sein.

Wo liegen die Herausforderungen?

Neutral gesehen ist Informationssicherheit erst einmal ein Kostenfaktor im Unternehmen. Geld verdient wird damit nicht. Inwieweit sich eine gesteuerte und funktionierende Informationssicherheit auf den Umsatz auswirkt und damit Chancen bietet, lässt sich meistens nur schwer oder schwammig nachvollziehen. Nichtsdestotrotz kann aber umgekehrt leichter analysiert werden, welche Risiken fehlende Informationssicherheit nach sich zieht.

Ohne an dieser Stelle schon konkret auf die Risiken einzugehen, gibt es doch allgemeine Herausforderungen, die Compliance einzuhalten.

Regelmäßige Neuerungen

Neue oder angepasste Gesetze, Urteile und Bußgelder sind kaum mehr im Überblick zu behalten. Trotzdem ist es für Unternehmen wichtig, einen Blick darauf zu haben, um eventuelle Auswirkungen auf die eigene Organisation zu erkennen und auch um darauf reagieren zu können.

Adäquate Umsetzung

Darauf reagieren zu können ist das eine. Das Ganze sollte aber auch an die Anforderungen angepasst sein. Wer bewertet, was ein Urteil für Ihr Unternehmen bedeutet? Wer entscheidet, ob und welche Maßnahme umgesetzt wird oder ob alles so belassen wird wie bisher?

Risikobasierter Ansatz

Das führt uns zum risikobasierten Ansatz. Ein allgemeines richtig oder falsch gibt es selten. Richtig ist, was für Ihr Unternehmen richtig ist. Das heißt, Sie müssen bewerten, welcher potenzielle Schaden für Ihr Unternehmen eintreten würde, wenn Sie auf ein neues Gesetz nicht oder nicht umfänglich reagieren oder Sie nach einem aktuellen Urteil bezüglich Unternehmensseiten in den sozialen Medien Ihre Seite weiter betreiben wie bisher. Sie bewerten den möglichen Schaden und betrachten eine potenzielle Eintrittswahrscheinlichkeit. Fallen Sie in den Fokus einer behördlichen Prüfung? Könnte sich ein Kunde beschweren? Wenn ja, wie wahrscheinlich ist das? Aus dieser Kombination von möglichem Schaden und der Eintrittswahrscheinlichkeit ergibt sich ein Risiko. Jetzt entscheiden Sie, ob und wenn ja, in welchem Umfang Sie auf diese neue Anforderung reagieren.

Risikobasierter Ansatz im Datenschutz

Grundsätzlich ist die Betrachtung des Risikos immer ein richtiger Ansatz, um Ihre individuellen Aktionen zu ermitteln. Im Datenschutz dürfen Sie allerdings nicht vergessen, den Betroffenen in den Mittelpunkt zu stellen. Wenn Sie die Risiken betrachten, müssen sich diese auf die betroffene Person (z. B. Kunden, Mitarbeiter etc.) beziehen und nicht auf ein mögliches Risiko Ihres Unternehmens.

Handlungsfähig bleiben

Egal, ob Urteil, Bußgeld oder gesetzliche Anforderung. Sie müssen eine Lösung finden, mit der Sie handlungsfähig bleiben. Die gesetzlichen Änderungen im Datenschutz haben schnell den Ruf nach zu viel Bürokratismus laut werden lassen und wurden als „Verhinderer" dargestellt.

Den Bürokratismus bürden wir uns an vielen Stellen selbst auf oder lassen ihn uns aufbürden. Die Abwägung, wie die Anforderungen der Gesetze und Normen umgesetzt werden können und welche pragmatischen und praxisorientierten Lösungen möglich sind, ist wohl eine der größten Herausforderungen.

Risiken bei fehlender Informationssicherheit

Wenn wir uns die Risiken in Bezug auf Informationssicherheit ansehen, müssen wir mindestens die drei Grundwerte Verfügbarkeit, Vertraulichkeit und Integrität betrachten. Welche Szenarien möchten Sie in Ihrem Unternehmen vermeiden?

- Durch fehlende Bewertung der Verfügbarkeitsanforderung von IT-Diensten und/oder Daten kann im Falle eines Ausfalls der Service nicht rechtzeitig zur Verfügung gestellt werden. Dies führt zu Ausfällen

bis hin zum Kunden, da dieser seine Produkte nicht rechtzeitig erhält oder Dienste nicht entsprechend der Vereinbarung nutzen kann.

- Durch fehlende Sensibilisierung der Mitarbeiter werden persönliche Informationen von Kunden einem falschen Empfängerkreis zugänglich. Dies kann zu Identitätsdiebstahl oder wirtschaftlichen Folgen beim Betroffenen führen. Im schlimmsten Fall kann sogar ein Reputationsschaden für Ihr Unternehmen daraus folgen.
- Beistellungen Ihres Kunden A, die sich noch in der Entwicklungsphase befinden, sind bei Ihnen im Haus, im Rahmen Ihrer Tätigkeit für den Kunden. Ein Wettbewerber (Kunde B) Ihres Kunden kommt zu Ihnen und erlangt unrechtmäßig Einsicht auf diese Beistellungen. Damit kann der Wettbewerbsvorteil mit dieser Entwicklung von Kunde A sehr schnell an den Kunden B übergehen. Ihr Unternehmen hat die vertraglichen Anforderungen an die Geheimhaltung nicht erfüllt und muss ggf. sogar eine Vertragsstrafe zahlen. Zudem wird Kunde A wohl nicht länger bei Ihnen Kunde sein.
- Ihr Onlinemarketing-Team plant Werbeanzeigen in sozialen Medien, die die Interessenten auf verschiedene Landingpages leiten, und nach Eingabe der Daten diese Personen entsprechend bewerben. Die gesetzlichen Anforderungen des Datenschutzes wurden allerdings nicht umfänglich umgesetzt. Sie werden bei der zuständigen Aufsichtsbehörde von einer Person gemeldet und erhalten im schlimmsten Falle ein Bußgeld.

Vier sehr pauschale Risiken aus Ihrer Sicht? Könnte das eine oder andere vielleicht doch auch bei Ihnen zutreffen?

Informationssicherheit als strategisches Thema

Die besten Chancen ergeben sich für Ihr Unternehmen, wenn Sie die Themen Informationssicherheit inkl. Datenschutz und IT-Sicherheit als strategisches Thema auf der obersten Ebene betrachten. Informationssicherheit wird nämlich nicht in der IT-Abteilung „gemacht“, wie man es manchmal vermuten möchte. Hier muss die nächsten Jahre ein starker Wandel in der Denkweise erfolgen. Natürlich ist die IT-Abteilung dafür verantwortlich, die Schutzmaßnahmen wie Firewall, Mehr-Faktor-Authentifizierung und Co. zu betreiben. Sie muss als interner Dienstleister fungieren. Ein Dienstleister, der natürlich auch eine beratende Funktion innehat. Die Beratung endet aber, wenn es um die Entscheidung geht, welcher Schutz für Geschäftsanwendungen notwendig ist. Was heißt das konkret? Sehen wir uns das Beispiel der Berechtigungen in einer Systemanwendung an. Die IT-Abteilung als technischer Betreiber des Systems soll natürlich fordern, dass Berechtigungen vergeben werden. Die Entscheidung, welche Rechte einer Rolle zugewiesen werden, darf jedoch nicht von der IT übernommen werden. Über die Schutzanforderungen von Geschäftsdaten ist allein der Geschäftsprozess-Eigner verantwortlich. Das zieht die Konsequenz nach sich, dass von dieser Stelle die Vorgaben für das Sicherheitsniveau gemacht werden müssen. Die IT und andere unterstützende Abteilungen sollen, wie schon gesagt, mit ihrem Wissen beratend zur Seite stehen. Eine Entscheidung muss aber immer durch den operativen Eigner kommen – nicht von den unterstützenden Stellen. Aus der Historie heraus, gibt in vielen Unternehmen noch immer die IT-Abteilung den Ton in Sachen Sicherheitsniveau an. Was vor Jahren mit rudimentären Schutzmaßnahmen sicherlich auch sinnvoll war, birgt heute Risiken.

Ihre operativen Geschäftsprozesse verarbeiten verschiedene Arten von Informationen. Dies kann in digitaler Form, auf Papier oder auch im gesprochenen Wort erfolgen. Manche dieser Informationen sind öffentlich verfügbar, andere wiederum sind als hoch vertraulich für das Unternehmen einzustufen.

Welche Informationen wie wichtig für Ihr Unternehmen sind und welche Daten vielleicht in Bezug auf den Datenschutz schützenswert sind, muss der Eigner des Geschäftsprozesses wissen, z. B. welcher Schaden für das Unternehmen entstehen würde, wenn einige Informationen nicht mehr verfügbar wären oder die Vertraulichkeit verletzt werden würde.

Erst aufgrund dieser potenziellen Schadensszenarien in Kombination mit einer möglichen Eintrittswahrscheinlichkeit (= klassische Risikoanalyse) können Schutzmaßnahmen in Betracht gezogen werden. Mit diesen Informationen kann die IT-Abteilung gezielt technische Maßnahmen vorschlagen, die diese Risiken der operativen Geschäftsprozesseigner minimieren oder komplett obsolet machen.

Ebenso kann erst mit der Einstufung der Verfügbarkeitsanforderungen an den Geschäftsprozess (Business Impact Analyse) die IT-Abteilung umfänglich entscheiden, welche Schutzmaßnahmen getroffen werden müssen, um die Anforderungen umzusetzen. Nicht jedes IT-System muss hoch verfügbar sein. Welche Systeme allerdings hoch verfügbar sein müssen, muss der Geschäftsprozess fordern.

Um in Zukunft gerüstet zu sein, sollten Sie dieses Thema von allen Seiten betrachten, aber vor allem den Top-down Ansatz berücksichtigen.

Um IT-Sicherheit und Datenschutz nicht als Selbstzweck zu sehen und zu betreiben, ist der erste Schritt, den Beitrag zum operativen Business, wie gerade beschrieben, zu betrachten.

Damit eröffnen Sie sich Chancen in mehrerlei Hinsicht:

- Die Schutzmaßnahmen sind auf die tatsächlichen Bedürfnisse der Sicherheit der Informationen ausgerichtet.
- Damit vermeiden Sie finanzielle Investitionen, die an mancher Stelle zu viel sind (der Speiseplan der Kantine muss nicht wirklich mit einer 2-Faktor-Authentifizierung abgesichert werden).
- Sicherheit ist manchmal auch unbequem und erschwert an der einen oder anderen Stelle auch das Arbeiten. Um hier das Arbeitsumfeld und die Tätigkeit so einfach wie möglich zu gestalten, aber so sicher wie nötig, ist es wichtig, die genannten Betrachtungen vorher durchzuführen.
- Aber der wichtigste Aspekt ist es natürlich für Ihr Unternehmen, handlungsfähig zu bleiben, auch wenn es einmal zu einem Vorfall kommt. Durch die genaue Betrachtung der Geschäftsprozesse und die Analyse der Risiken sind die IT-Services so ausgelegt, dass der kontinuierliche Geschäftsbetrieb sichergestellt werden kann. Damit unterscheiden Sie sich von vielen Wettbewerbern.

Anforderungen an die Informationssicherheit

Im eigenen Interesse sollte jedes Unternehmen bestrebt sein, die Informationssicherheit im Unternehmen entsprechend den Anforderungen umzusetzen.

Informationssicherheit im eigenen Interesse

Der wohl löblichste Ansatz, die Informationssicherheit im Unternehmen aus eigenem Antrieb umzusetzen, ist der selbst gewollte bestmögliche Schutz der Informationen und eine tatsächlich gesteuerte Informationssicherheit.

Meistens geht dies aber auch mit einem erhofften Vorteil auf dem Markt einher. Die Zertifizierung eines Managementsystems für Informationssicherheit z. B. nach ISO 27001 (ISMS) oder ein zertifiziertes Datenschutzmanagement nach ISO 27701 (PIMS) optimiert sicherlich Ihre internen Prozessabläufe. Nach außen hin lässt es sich auch gut als Marketinginstrument verwenden.

Mehr wert noch als ein zertifiziertes Datenschutzmanagement wird in Zukunft wohl der zertifizierte Datenschutz im Sinne einer „Produktzertifizierung" sein. Hier scheint der Weg in Richtung zertifizierter Datenschutz nach Art. 42 DSGVO zu führen.

Immer mehr allerdings macht sich bemerkbar, dass der Druck an eine gesteuerte Informationssicherheit auch von außen an die Unternehmen herangetragen wird.

Gesetzliche Anforderungen

Vor allem im Datenschutz wissen wir um das Bestehen gesetzlicher Anforderungen. Daneben gibt es aber noch weitere gesetzliche Vorgaben, die Auswirkungen auf Unternehmen haben können. Für bestimmte Branchen sind zum Beispiel das IT-Sicherheitsgesetz oder die KRITIS Anforderungen einzuhalten. Damit bewegt sich die gesetzliche Anforderung sehr nah an den normativen Anforderungen für Informationssicherheitsmanagementsysteme.

Auch gibt es seit 2019 das Geschäftsgeheimnisgesetz, das an vielen Unternehmen vorbei gegangen ist. Mit einem funktionierenden ISMS deckt man allerdings den Großteil der in diesem Gesetz geforderten Passagen ab.

Und ganz aktuell greift nun auch die EU-Whistleblowing-Richtlinie. Hier steht wieder mehr der Datenschutz im Vordergrund. Ziel ist der Schutz der meldenden Person. Genauso beim vor Kurzem in Kraft getretenen TTDSG, das eine Brücke zwischen Datenschutzgesetzen, Telemediengesetz und Telekommunikationsgesetz schlägt.

Die genannten Punkte können nicht abschließend alle Anforderungen abdecken. Es zeigt sich allerdings klar, dass die gesetzlichen Anforderungen an die Themen Informationssicherheit und explizit Datenschutz mehr werden und auch in kürzeren Abständen angepasst werden. Um hier auf dem Laufenden zu bleiben und kurzfristig handeln zu können, sollte im Unternehmen eine gesteuerte Informationssicherheit, die auch den Datenschutz umfasst, gelebt werden.

Gerade im Datenschutz hat sich in den letzten Jahren eine hohe Taktfrequenz bei Urteilen oder Veröffentlichungen der Aufsichtsbehörden bemerkbar gemacht. Selbst wenn auch nicht jedes Urteil für Ihr Unternehmen relevant ist, muss es doch erst einmal geprüft werden. Dies zu steuern und die daraus resultierenden Maßnahmen adäquat, praxisorientiert und pragmatisch umzusetzen, ist die Kunst.

Kundenanforderungen

Kundenanforderungen nach Informationssicherheit spiegeln sich häufig darin, dass der Kunde wünscht, dass sich Ihr Unternehmen nach einem bestimmten Standard ausrichten soll. Allein die interne Ausrichtung reicht oft nicht aus. Am besten soll noch ein unabhängiger Prüfer die Einhaltung der Standards bescheinigen.

Eine Zertifizierung nach ISO 27001 deckt viele der Anforderungen ab. Branchenspezifisch geht es aber weitaus tiefer in die Informationssicherheit. Für Dienstleister in der Finanzindustrie gilt zum Beispiel der PCI DSS Standard, der auch technisch weiter in die Tiefe geht als die ISO27001.

Gerade sehr beliebt ist die VDA ISA/TISAX® Anforderung der Automobilindustrie, mit der sich Zulieferer und Dienstleister gerade beschäftigen. Basis ist auch hier wieder ein ISMS ähnlich ISO 27001, allerdings mit weiteren Anforderungen on top.

Anforderungen der Stakeholder

Man müsste ja meinen, gesetzliche Anforderungen und die Wünsche der Kunden sollten ausreichen, um von extern Druck bezüglich Compliance der Informationssicherheit aufzubauen.

In der Praxis sprechen noch mehr mit und werfen ihre Anforderungen in den Topf. Verstärkt fordern Versicherungen – besonders Cyber Security Versicherungen – einen Nachweis, dass im Unternehmen die Informationssicherheit nicht nur gelebt, sondern auch gesteuert wird. Viele Versicherungen fordern einen Nachweis für das implementierte Managementsystem der Informationssicherheit.

Konkrete Maßnahmen für Ihr Unternehmen

Um Informationssicherheit- und Datenschutz-Compliance nachweisen zu können, reichen je nach Unternehmen manchmal auch kleinere und, wie oben genannt, auch pragmatische und praxisorientierte Lösungen.

Nachfolgende Themen sollten Sie in Ihrem Unternehmen auf die Agenda nehmen, wenn noch nicht passiert, um Risiken vorzubeugen und – noch besser – um Chancen einer guten Informationssicherheit zu nutzen.

Datenschutz-Basics

Wenn Sie bisher noch nicht aktiv geworden sind in Sachen Datenschutz, sollten Sie dies wirklich dringend tun. Aber auch hier können Sie sehr praxisorientiert bleiben, was Ihrem Unternehmen auch eine gute Ausrichtung in die Zukunft ermöglicht:

1. Verfahrensverzeichnis: Listen Sie alle Prozesse, die im Unternehmen personenbezogene Daten verarbeiten. Betrachten Sie hierzu die einzelnen Abteilungen und deren Funktionen (z. B. Personal, Buchhaltung, Vertrieb, IT-Abteilung etc.).
2. Basierend auf dem Verfahrensverzeichnis erstellen Sie die Informationspflicht nach Art. 13 und Art. 14 DSGVO für Ihre Kunden, Mitarbeiter und alle anderen.
3. Prüfen Sie, ob Sie Auftragsverarbeiter sind oder ob Sie Auftragsverarbeitungsverträge Ihrer Lieferanten und Dienstleister anfordern müssen – auch das ergibt sich aus dem Verfahrensverzeichnis.
4. Gibt es Verfahren, für die Einwilligungen der Betroffenen nötig sind? Häufig ist dies bei Marketing-Verfahren notwendig.

5. Bewerten Sie Ihre IT-Sicherheit und analysieren Sie Risiken, gegen die weitere Schutzmaßnahmen notwendig sind.
6. Sensibilisieren Sie Ihre Mitarbeiter.

IT-Sicherheitsrichtlinie(n)

Regeln Sie die Informationssicherheit im Unternehmen. Nicht alles kann mit technischen Schutzmaßnahmen umgesetzt und damit erzwungen werden. Folgende Inhalte sollten durch die Richtlinie abgedeckt werden:

- Grundsätzlicher Umgang mit Informationen: Gibt es besonders schützenswerte Informationen, die einen höheren Schutzbedarf nach sich ziehen?
- Umgang mit digitalen Daten: Speicherort, lokale Ablage erlaubt (ja oder nein)?
- Sind externe Medien erlaubt? Wenn ja, welche und wozu?
- Allgemeine Weitergabe von Daten und Informationen.
- Verbot privater E-Mail-Nutzung des geschäftlichen E-Mail Accounts.
- Private Internetnutzung (ja oder nein), wenn ja unter welchen Voraussetzungen?
- Installation von Software.
- Nutzung privater Hard- und Software (BYOD).
- Private Nutzung von geschäftlicher Hard- und Software.
- Nutzung von mobilen Geräten.
- Sauberer Arbeitsplatz (Clean-Desktop Policy).
- Arbeiten im Homeoffice.
- Verhalten bei Informationssicherheitsvorfällen.
- Hinweis, dass das Nichteinhalten zu arbeitsrechtlichen oder strafrechtlichen Konsequenzen führen kann.

Im Idealfall haben Sie Ihr internes Sicherheitslevel schon definiert und nutzen es als Grundlage für die Erstellung der Richtlinie. Häufig ist dies nicht der Fall. Trotzdem sollten Sie eine Informationssicherheitsrichtlinie an Ihre Mitarbeiter ausgeben und schulen.

Wenn Sie zu einem späteren Zeitpunkt Ihr Sicherheitslevel definieren und feststellen, dass sich Anpassungen in der Richtlinie ergeben, muss diese angepasst werden.

Definition Sicherheitslevel - unternehmenskritische Werte

„Start small – think big“ sollte Ihre Devise hier sein. Um im gesamten Unternehmen über alle Unternehmenswerte eine Bewertung der Informationssicherheit vorzunehmen, brauchen Sie sicherlich Monate. Starten Sie mit einem kleinen Bereich und gehen Sie nicht gleich zu tief. Ziel soll im ersten Schritt sein, Ihre sogenannten „Kronjuwelen“ zu identifizieren. Das sind die höchst zu schützenden Unternehmenswerte im Sinne der Informationssicherheit. Man spricht von ca. fünf Prozent der Unternehmenswerte, die ein Unternehmen als Kronjuwelen identifiziert.

Haben Sie diesen Schritt geschafft, sind Sie einen großen Schritt weitergekommen auf dem Weg zu einer gesteuerten Informationssicherheit. Sie kennen Ihre wichtigsten Unternehmenswerte und können einen Fokus bei den Schutzmaßnahmen daraufsetzen.

Prüfen von Auswirkungen der gesetzlichen Änderungen

Die schon genannten Gesetze wie TTDSG, Geschäftsgeheimnisgesetz und EU-Whistleblowing-Richtlinie haben gegebenenfalls Auswirkung auf Ihr Unternehmen. Prüfen Sie oder lassen Sie prüfen, ob Maßnahmen für Ihre Organisation notwendig sind.

Ausblick

Wie schon eingangs erwähnt, erhöht sich die Schlagzahl der Änderungen und Anpassungen an den Anforderungen an die gesamte Informationssicherheit. Unternehmen müssen sich diesem Thema nicht nur einmalig, sondern dauerhaft stellen.

Konkret das Thema Datenschutz wird weiter an Bedeutung gewinnen. Wo bisher noch das Gesetz die Vorgabe an die Unternehmen gemacht hat, wird es in Zukunft dazu übergehen, dass die Betroffenen selbst mehr den Schutz ihrer Daten fordern.

Immer mehr werden personenbezogene Daten über uns und unser Verhalten als das Gold der Zukunft gehandelt. Wir als Endverbraucher bezahlen schon jetzt mit unseren Daten für kostenlosen Content. Die Awareness bei den Betroffenen hat sich diesbezüglich noch kaum gebildet. Dies wird aber immer mehr an Bedeutung gewinnen. Damit werden die Betroffenen die Unternehmen mehr fordern, als es jetzt die Gesetze tun.

Eine frühzeitige Ausrichtung der Organisation an den Schutz der Daten von Betroffenen als eines der wichtigsten Ziele kann daher ein weitaus größerer Marktvorteil werden, als dies jetzt der Fall ist.

Aber nicht nur der Endverbraucher hat Wünsche an die Unternehmen. Der Kundendruck an die allgemeine Informationssicherheit wird weiterwachsen. Was bisher nur in einzelnen Branchen gefordert wird, wird sich Schritt für Schritt weiter über alle Branchen ausbreiten. ISMS Standards im KRITIS-, Finanz- und

Automotivbereich werden erweitert auf medizinische Einrichtungen und Dienstleistungssektoren.

Falls Sie es bisher noch nicht betrachtet haben, sollten Sie dieses Thema in Ihre strategische Unternehmensplanung mit aufnehmen. Eine gut funktionierende Informationssicherheit muss gesteuert werden. Wie schon bekannte Managementsysteme aus Qualität, Umwelt und Arbeitsschutz muss sich auch die Informationssicherheit im Unternehmen etablieren und mit der Zeit wachsen und festigen.

Trotz allem lassen Sie sich nicht zum Bürokratismus verleiten und behalten den praxisorientierten Blick. Risiken abwägen und pragmatische Ansätze helfen auch, die Akzeptanz im Unternehmen zu schaffen. Informationssicherheit ist ein Mehrwert für Ihr Unternehmen, Ihre Kunden und Ihre Mitarbeiter!

Regina Stoiber ist Geschäftsführerin der Datenbeschützerin GmbH. Nach einer Ausbildung zur Energieelektronikerin kam sie über das Studium der Wirtschaftsinformatik und anfänglicher Tätigkeit in der IT-Administration zum Thema Informationssicherheit. Seit 2007 beschäftigt sich Frau Stoiber mit der Materie Informationssicherheit, IT-Sicherheit und Datenschutz. Erst als Leiterin der Abteilung Informationssicherheit und Datenschutz in einem großen internationalen Unternehmen, später mit ihrer eigenen Firma. Ihr Unternehmen, die Datenbeschützerin GmbH, unterstützt mittelständische und große Firmen dabei, sicher im Business zu bleiben. Partnerschaftliche Zusammenarbeit, Transparenz und komplexe Inhalte einfach aufzubereiten sind das Markenzeichen ihrer Firma bei der Umsetzung von Datenschutz und ISMS-Projekten (Managementsystem für Informationssicherheit).