Informationssicherheit ist Chefsache

Praktisch jedes unternehmerische Ziel, von der Kostensenkung bis hin zur Geschäftsprozessoptimierung, hängt von der Effizienz, der Effektivität sowie von der Sicherheit und Zuverlässigkeit des Informatik-Einsatzes ab. Zur Informationssicherheit gehört der ganzheitliche Schutz von Informationen.

Wolfgang Sidler

Informationssicherheit ist daher eine strategische und nicht ausschliesslich eine technische Frage. Informationssicherheit kann nur wirkungsvoll und nachhaltig umgesetzt werden, wenn sie ein fester Bestandteil der Unternehmenspolitik ist und das IT-Sicherheitsmanagement organisatorisch im Unternehmen eingebunden wird.
Erkennung und Festlegung der kritischen Informationen für ein Unternehmen und die anschliessende Auswahl der geeigneten Massnahmen zur Informationssicherheit sind Führungsaufgaben, die sich nur eingeschränkt delegieren lassen. Damit die Informationssicherheit erfolgreich umgesetzt werden kann, ist die volle Unterstützung des Managements nötig. Die Verantwortung für die Informationssicherheit liegt beim Management, welches die notwendigen Massnahmen initiieren und deren Umsetzung kontrollieren muss.

Dabei gelten die folgenden Management-Grundregeln:

- Die Verantwortung für die Informationssicherheit liegt beim Management und kann nicht delegiert werden. Es entscheidet über den Umgang mit den Risiken, stellt die notwendigen Mittel zur Verfügung und trägt das verbleibende Restrisiko.
- Informationssicherheit muss in alle Prozesse und Projekte integriert werden, bei denen Informationen verarbeitet und genutzt werden.
- Der Informationssicherheits-Prozess muss vom Management überwacht werden.
- Für den IT-Betrieb und die Informationssicherheit müssen ausreichende Ressourcen bereitgestellt werden.
- Es müssen die organisatorischen Rahmenbedingungen für die Informationssicherheit geschaffen werden.
- Die Umsetzung muss wirtschaftlich sein. Informationssicherheit darf nicht mehr kosten als die damit erreichte Risikominderung.
- Die Informationssicherheit muss in sinnvoller Relation zum Schutzbedarf stehen (Angemessenheit).
- Die Schutzmassnahmen müssen realisierbar sein und dürfen die Sicherheitslage nicht verschärfen (Praktikabilität). Sie müssen nachweisbar Bedrohungen abwehren bzw. Risiken mindern (Wirksamkeit).
- Informationssicherheit darf nicht behindern und muss von allen als Notwendigkeit verstanden werden (Akzeptanz).
- Die IT-Sicherheitspolitik(-Strategie) muss regelmässig überprüft werden.

Sicherheitspolitik

Als erstes muss die Sicherheitspolitik festgelegt werden. Sie stellt grob die allgemeine Richtung der Informationssicherheit dar. Sie gilt als Leitbild wie die Verfassung in einem Staat. Damit bestimmt die Unternehmensleitung, welchen Stellenwert sie in Sachen Sicherheit vertritt. Der Sicherheitsverantwortliche des Unternehmens und das Sicherheitskonzept unterstützen dabei die Geschäftsleitung in der Umsetzung der Strategie.

Einbindung der Mitarbeitenden

Informationssicherheit betrifft ohne Ausnahme alle Mitarbeitende in einem Unternehmen. Jeder Einzelne kann durch verantwortungs- und qualitätsbewusstes Handeln und Verhalten Schäden vermeiden und zum Erfolg beitragen. Sensibilisierung für Informationssicherheit und entsprechende Schulungen der Mitarbeitenden sowie aller Führungskräfte sind daher eine Grundvoraussetzung für eine erfolgreiche Informationssicherheit. Um Sicherheitsmassnahmen wie vorgesehen umsetzen zu können, müssen bei den Mitarbeitenden die erforderlichen Grundlagen vorhanden sein. Dazu gehört neben den Kenntnissen, wie Sicherheitsmechanismen bedient werden müssen, auch das Wissen über Sinn und Zweck von Sicherheitsmassnahmen. Auch das Arbeitsklima, gemeinsame Wertvorstellungen und das Engagement der Mitarbeitenden beeinflussen entscheidend die Informationssicherheit und steuern einen wichtigen Beitrag zu einer erfolgreichen und wirksamen Sicherheitskultur bei.
Werden Mitarbeitende neu eingestellt oder erhalten neue Aufgaben, ist eine gründliche Einarbeitung und Ausbildung notwendig. Hier empfehlen wir die neuen Mitarbeitenden beim Eintrittstag kurz über die Sicherheitspolitik mit den entsprechenden Weisungen vorzustellen. Wenn Mitarbeitende das Unternehmen verlassen oder sich ihre Zuständigkeiten verändern, muss dieser Prozess durch geeignete Sicherheitsmassnahmen begleitet werden (z.B. Entzug von Berechtigungen, Rückgabe von Schlüsseln und Ausweisen). Wichtig ist, dass die für die Informationssicherheit verantwortlichen Personen vorgestellt werden, damit die Mitarbeitenden bei Sicherheitsvorfällen schnell die entsprechenden Experten informieren können. Vergessen Sie nicht externe und temporäre Mitarbeiter entsprechend zu sensibilisieren und verlangen Sie von ihnen, dass sie eine Vertraulichkeitsvereinbarung beim Eintritt unterschreiben. Folgende Weisungen sind für ein Unternehmen zwingend notwendig:

- Umgang mit E-Mail
- Umgang mit Internet
- Umgang mit IT-Sachmittel
- Umgang mit Passwörtern

Beispiel einer Sicherheitspolitik für ein KMU

Einleitung

Zum Schutz der Informationen sowohl der Firma als auch der Kunden sowie zur Gewährleistung der Verfügbarkeit aller Daten und deren Verarbeitungssysteme, hat die Geschäftsleitung folgende Sicherheitspolitik erlassen. Die vorliegende Sicherheitspolitik wurde am TT.MM.JJJJ durch die Geschäftsleitung der [Firma] genehmigt.

Ziel und Zweck

Die [Firma] will dem gesamten Bereich der Informationssicherheit konsequent, umfassend und im rechtlich und wirtschaftlich vertretbaren Rahmen begegnen.
Die Sicherheitspolitik dient als Grundlage für alle Massnahmen und Aktivitäten zur Erreichung einer optimalen Sicherheit der [Firma].
Das Ziel der Aktivitäten im Bereich der Informationssicherheit ist es, schädigenden Ereignissen vorzubeugen und deren Auswirkungen auf ein angemessenes Minimum zu reduzieren.

Geltungsbereich

Die Sicherheitspolitik gilt für alle internen und externen Mitarbeiter der [Firma]. Bei der Zusammenarbeit mit Dritten (Lieferanten, Partner etc.) werden diese vertraglich auf die Einhaltung der hier und in nachfolgenden Dokumenten festgelegten Grundsätzen und Massnahmen zur Sicherheit verpflichtet.

Gesetzliche, vertragliche und interne Anforderungen
Gesetzlich sowie vertraglich eingegangene Verpflichtungen werden von der [Firma] und ihren Mitarbeitern strikte befolgt. Aufgrund der Tätigkeiten der [Firma] dürfen keine Gesetze verletzt und nicht gegen Rechte und Ansprüche von Mitarbeitern und Dritten verstossen werden. Bei der Verrichtung ihrer Tätigkeit haben die Mitarbeiter zudem entsprechend den internen Sicherheitsmassnahmen zu handeln.

Sicherheitsziele
Die [Firma] strebt im Rahmen ihrer Tätigkeiten und ihres Verantwortungsbereiches folgende Sicherheitsziele an:
- Schutz von Leben und Gesundheit ihrer Mitarbeiter, Kunden und Partner
- Erhaltung der in Technik, Verfahren und Wissen investierten Werte
- Sicherung von Wert und Qualität der Informationen, Dienstleistung und Produkte
- Einhaltung aller relevanten gesetzlichen Bestimmungen
- Reduzierung der im Schadenfall entstehenden Folgen auf ein angemessenes Mass

Für alle Sicherheitsaktivitäten innerhalb der [Firma] gilt der Grundsatz:
«Prävention vor Schadensausgleich – Eigenverantwortung vor Kontrolle und Überwachung»

Es ist das Ziel der [Firma], dauernd ein angemessenes Mass an Sicherheit zu erreichen, wobei absolute Sicherheit nicht erreichbar ist. Schädigende Ereignisse sind in ihrer Häufigkeit und Auswirkung auf das angemessene Mass zu minimieren.
Es ist Aufgabe der [Firma], die angestrebte Verhältnismässigkeit zu definieren. Die Überprüfung und gegebenenfalls die Neubestimmung der Angemessenheit muss ein andauernder Prozess innerhalb der [Firma] werden.

Sicherheitsorganisation
Oberstes verantwortliches Organ für die Sicherheit ist der Verwaltungsrat, der diese Verantwortung umfassend an die Geschäftsleitung delegiert. Der Verwaltungsrat genehmigt die vorliegende Sicherheitspolitik. Eine Kultur des sicheren Umgangs mit Informationen, Anwendungen und Informatiksystemen wird im Sinne dieser Politik gefördert. Die Kultur wird durch den Grundsatz geprägt, dass Prävention und Eigenverantwortung Vorrang gegenüber Kontrolle und Überwachung haben. Da Sicherheit nur durch technische Massnahmen alleine nicht realisiert werden kann, werden alle Mitarbeitenden regelmässig und stufengerecht informiert.
Für alle eingesetzten Informatikobjekte (Daten, Applikationen, Systeme) werden verantwortliche Personen bestimmt. Dies sind in der Regel die Funktionen «Inhaber der Daten», «Systemverantwortliche» und «Anwendungs-Verantwortliche». Sie sind für die Umsetzung der Sicherheitsmassnahmen verantwortlich, wenden die Konzepte der IT-Sicherheit an und arbeiten aktiv an deren Optimierung mit.

Umgang mit Risiken
Mögliche Risiken sollen generell durch die Anwendung von standardisierten Sicherheitsregeln und Massnahmen vermieden, vermindert oder überwälzt werden. Einige Risiken können mit wirtschaftlich vertretbarem Aufwand nicht oder nicht vollständig beseitigt werden. Diese werden identifiziert und bewertet (Risikoanalyse), durch entsprechende Massnahmen vermindert oder von der [Firma] bewusst eingegangen (aktive Risikoübernahme) bzw. wo möglich, auf Versicherungen abgewälzt.

Risikowahrnehmung
Um die Sicherheitsziele erreichen zu können, müssen die Risiken primär erkannt werden, um sie anschliessend zu beseitigen oder durch Prävention zu mindern.
- Prävention kommt vor Schadensausgleich.
- Erkannte Risiken werden dokumentiert, bewertet und durch angemessene, möglichst standardisierte Massnahmen abgewendet oder auf ein tolerierbares Restrisiko beschränkt.
- Risiken sind regelmässig neu zu beurteilen, die notwendigen Massnahmen sind unverzüglich zu planen, bestehende Risiken zu überprüfen.
- Stellt ein Mitarbeiter ein Risiko fest, so hat er den Geschäftsführer zu informieren, welcher seinerseits je nach Schwere und Bedeutung der Bedrohung die Behebung des Risikos selbstständig vornimmt bzw. entsprechende Massnahmen einleitet.

Aktive Risikoübernahme
Die [Firma] ist bereit, ausgewogene, kalkulierbare Risiken einzugehen, wobei diese Risiken durch die eigenen Stärken abgesichert sein und im Einklang mit den übrigen Unternehmensstrategien stehen müssen.
- Über den anzustrebenden Schutzgrad und die allfällige Zulässigkeit eines Risikos entscheiden die dafür kompetenten Stellen, in letzter Instanz die Geschäftsleitung. Ein Restrisiko besteht dann, wenn ein Risiko nicht vollständig beseitigt werden soll oder kann.
- Mitarbeiter und Vorgesetzte haben den Geschäftsführer über erkannte Risiken zu informieren.

- Bewusst einzugehende, innerhalb der [Firma] bekannt gewordene Restrisiken werden durch einen formellen Entscheid der dafür kompetenten Stellen aktiv übernommen, wobei diese Entscheide gegenüber den Mitarbeitern angemessen zu kommunizieren sind.

Ereignismanagement
Für Krisen und Notfälle, die wesentliche Auswirkungen auf die Aktivitäten der [Firma] haben, wird ein Ereignismanagement aufgebaut, das zum Ziel hat, Sofortmassnahmen schnell und effektiv einleiten zu können. Das Ereignismanagement obliegt dem Ereignisstab, welcher in Notsituationen einberufen wird und dem die Aufgabe zukommt, eine den Umständen entsprechend geordnete Geschäftstätigkeit zu garantieren, bis der Notfall behoben ist.

Grundsätze für die einzelnen Sicherheitsbereiche
Die [Firma] definiert konkrete Schutzziele und Sicherheitsmassnahmen:

Personenschutz und Arbeitssicherheit
Die [Firma] ergreift oder veranlasst die Realisierung von Massnahmen zur Abwehr von Unfallereignissen, Überfällen oder gesundheitsgefährdenden Bedrohungen innerhalb der von ihr genutzten Lokalitäten und deren haftungsrelevanten räumlichen Umgebung.

Gebäudeschutz
Massnahmen im Bereich Gebäudeschutz, -überwachung und -versicherung sind individuell zu definieren.

Zutrittsschutz zu Gebäuden und Räumen
Durch Regelung und Kontrolle der Zutrittsberechtigung zum Gebäude, den [Firma] Räumen bzw. Zonen (Büros, Informatikraum etc.) wird das Risiko des unberechtigten Betretens beträchtlich vermindert.

Informationssicherheit
Die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen sind jederzeit durch entsprechende Massnahmen sicherzustellen. Als Teilbereiche der Informationssicherheit sind der Informationsschutz (Geschäftsgeheimnisschutz), der Datenschutz (Persönlichkeitsschutz) und die Informatiksicherheit zu nennen.

Informationsschutz
Besonders schützenswerte Informationen (elektronische wie nicht elektronische) sind aufgrund ihres Schutzbedarfes zu klassifizieren und mit Hilfe spezieller Massnahmen zu schützen. Informationen werden aufgrund interner Anforderungen, aber auch aufgrund gesetzlicher oder vertraglicher Bestimmungen klassifiziert und unterliegen dadurch einer besonderen Behandlung. Generell sind alle Informationen zu schützen und deren Entstehung, Bearbeitung, Speicherung, Aufbewahrung und Vernichtung als Prozess zu definieren.
In einer Verpflichtungserklärung bzw. als Zusatz zum Arbeitsvertrag müssen die Mitarbeiter ihre Verschwiegenheit hinsichtlich aller Informationen kundtun. Dies gilt ebenfalls für alle Dritten, welche im Auftrag der [Firma] Informationen bearbeiten oder Aufträge ausführen. Für die Ausarbeitung ist die Geschäftsleitung zuständig und für die Unterzeichnung der jeweilige interne Auftraggeber verantwortlich.

Datenschutz
Jede Bearbeitung von Personendaten innerhalb der [Firma] erfolgt gemäss dem Bundesdatenschutzgesetz vom 19. Juni 1992 bzw. 3.10.2000. Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Wer personenbezogene Daten für sich selbst oder im Auftrag für andere elektronisch bearbeitet, muss aufgrund des Datenschutzgesetzes der Schweiz (DSG) durch geeignete Massnahmen den Missbrauch dieser Daten verhindern. Die [Firma] ist verpflichtet, Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten zu schützen. Mitarbeiter und Vorgesetzte haben die Bestimmungen des Datenschutzgesetzes einzuhalten. Darüber hinaus ist jeder Vorgesetzte verantwortlich für den Datenschutz in seinem Verantwortungsbereich, insbesondere für die Einführung und Überwachung der für den Datenschutz notwendigen Massnahmen.
Alle [Firma] internen Datensammlungen mit Personendaten sind dem verantwortlichen Mitarbeiter für die Informatik bekannt zu geben. Davon ausgenommen sind Datensammlungen, die nur Name und Anschrift von Personen enthalten. Die Weitergabe von Personendaten an Dritte unterliegt zwingend der Bewilligung durch die Geschäftsleitung. Diese veranlasst auch die gesetzlich vorgeschriebene Registrierung allfälliger Datensammlungen beim Eidg. Datenschutzbeauftragten.

Informatiksicherheit
Das einwandfreie Funktionieren der eingesetzten Informatik-Systeme ist für das unternehmerische Überleben der [Firma] fundamental. Ziel der Informatik-Sicherheitsbestrebungen ist es, die Verfügbarkeit, die Vertraulichkeit und die Integrität sämtlicher Informatik-Systeme und der darauf gespeicherten Informationen (Daten und Programme) jederzeit angemessen zu gewährleisten. Die Informatik-Umgebung ist so zu schützen, dass die von der Informatik zu erbringenden Dienstleistungen im Rahmen der Anforderungen dauernd gewährleistet werden können.
Fehlverhalten von Informatik-Systemen bei der Bearbeitung von Informationen sowie vorsätzliche oder fahrlässige Angriffe auf Informatik-Umgebungen, unter Einschluss der gespeicherten und übertragenen Informationen (Daten und Programme), sind zu verhindern oder zumindest rechtzeitig zu erkennen, um die Sicherheit der Informatik-Systeme, der Informationen und die Aufrechterhaltung des Geschäftsbetriebes zu gewähren.

Versicherungsschutz
Risiken welche die [Firma] aufgrund ihrer finanziellen Auswirkungen nicht tragen kann oder will, werden durch den Abschluss entsprechender Versicherungsverträge auf einen Versicherer überwälzt.
Ein allfälliger Versicherungsschutz darf jedoch sinnvolle Schadensverhütungsmassnahmen nicht ersetzen. Die [Firma] versichert ihre Mitarbeiter gegen finanzielle Folgen von Krankheit, Invalidität, Betriebs- und Nichtbetriebsunfällen. Sämtliche Sach- (Inventar, Informatik-Systeme etc.) und Haftpflichtversicherungen (Betrieb, Miete, Organ etc.) werden durch die Geschäftsleitung formuliert, untersucht oder abgeschlossen, vorbehältlich der Kompetenzen des Verwaltungsrates.
Fachbereiche und Organisationseinheiten müssen den (zusätzlichen) Bedarf an Versicherungsschutz ihrer Bereiche selbst erkennen und dies dem Geschäftsführer melden. Bei durch Versicherungen gedeckten Schäden ist unverzüglich der Geschäftsführer zu unterrichten.

Umweltschutz
Die [Firma] verpflichtet sich zum schonenden Umgang mit den natürlichen Ressourcen. Bei allen Tätigkeiten wird dafür Sorge getragen, dass möglichst keine umweltgefährdenden Einwirkungen entstehen und dass Material und Energie sparsam verwendet werden.

Einhaltung
Alle vertraglichen Verpflichtungen und gesetzlichen Bestimmungen werden von der [Firma] und ihren Mitarbeitern umfassend eingehalten. Die Geschäftsleitungsmitglieder und der Verantwortliche für die Informatik beobachten die gesetzgeberische Entwicklung und machen früh auf allfälligen Handlungsbedarf aufmerksam.

Sicherheitsregeln und -massnahmen
Besonders schützenswerte Objekte, sog. Schutzobjekte wie Informationen, werden aufgrund ihres individuellen Schutzbedarfs klassifiziert. Für den Schutz dieser Objekte werden spezielle, standardisierte Sicherheitsregeln und Massnahmen angewendet. Kann die Sicherheit trotz dieser Regeln und Massnahmen nicht angemessen garantiert werden, oder stellt sich deren Umsetzung als nicht wirtschaftlich dar, so sind individuelle, auf die jeweiligen Schutzobjekte beschränkte, Risikoanalysen mit dem Ziel durchzuführen, individuelle Sicherheitsmassnahmen zu erkennen, die dem erhöhten Schutzbedarf auch gerecht werden.

Controlling/Auditing
Gemäss den festgelegten Schutzzielen ist in sinnvollen Perioden die Einhaltung der organisatorischen wie technischen Regelungen von einer unabhängigen Funktion zu prüfen. Damit soll gewährleistet werden, dass die gesetzlichen und sicherheitsbezogenen Bestimmungen eingehalten, die Vertraulichkeit der Informationen sichergestellt, und dort wo dies angemessen erscheint, die vollständige Nachvollziehbarkeit erreicht wird. Die Prüfungen sind schriftlich festzuhalten und mit den betroffenen Personen zu besprechen.

Weisungen
Die folgenden Weisungen für die Mitarbeiter der [Firma] sind ergänzender Bestandteil der Sicherheitspolitik:
Weisung: Umgang mit Passwörter
Weisung: Umgang mit Internet
Weisung: Umgang mit E-Mail
Weisung: Umgang mit IT-Sachmittel

Gültigkeit
Die hier aufgeführten Festlegungen wurden an der Verwaltungsrats-Sitzung Nr. XXX vom TT.MM.JJJJ genehmigt.

[Ort] den, _____

Für den Verwaltungsrat:

_____
(Vorname, Name)