

## **Inhaltsverzeichnis**

<b>INHALTSVERZEICHNIS</b> .....	<b>1</b>
<b>I. INFORMATIONSSICHERHEIT EINE FÜHRUNGSAUFGABE?</b> .....	<b>2</b>
<b>1. Sechs Schlüsselgrößen des Unternehmens nach Malik</b> .....	<b>3</b>
<b>2. Ziele von Informationssicherheit sind Unternehmensziele</b> .....	<b>3</b>
2.1 Business-Prozesse sichern und Geschäft ermöglichen .....	4
2.2 Informationen, Know-how und Wettbewerbsvorteile sichern .....	4
2.3 Risiko Management betreiben .....	4
2.4 Informationssicherheitskultur leben .....	5
<b>II. ZIELERREICHUNG IN DER INFORMATIONSSICHERHEIT</b> .....	<b>6</b>
<b>1. Informationssicherheit betrifft das oberste Management (Stufen-Modell)</b> .....	<b>6</b>
<b>2. Unternehmensführung definiert die Security Governance</b> .....	<b>7</b>
2.1 Definition des Computer Ethik & der Professionalität (Code of Behavior).....	7
2.2 Definition der Führungs- und Organisationsstruktur .....	8
2.3 Klassifizierung von Vertraulichkeit, Integrität und Verfügbarkeit .....	8
2.4 Definition des Risk- und Informationsmanagement .....	8
<b>3. Softfaktoren, die der Informationssicherheit zum Erfolg verhelfen</b> .....	<b>9</b>
3.1 Führung durch Vorbild .....	9
3.2 Mitarbeiterführung .....	9
3.3 Mitarbeitersensibilisierung (Security Awareness) .....	9
<b>III. NUTZEN DER INFORMATIONSSICHERHEIT FÜR DAS UNTERNEHMEN</b> .....	<b>10</b>
<b>IV. ANHANG: ZITATE</b> .....	<b>11</b>

## Informationssicherheit ist eine Führungsaufgabe

von Martin Viselka, Chief Executive Officer, bw digitronik ag

### I. Informationssicherheit eine Führungsaufgabe?

Die These von meinem Referat lautet: „Informationssicherheit *ist* eine Führungsaufgabe“. Gem. unserer Anmeldestatistik sind heute über 50% der anwesenden Personen, Entscheidungsträger auf verschiedenen Stufen im IT-Bereich. Nun möchte ich Sie gerne um ein Handzeichen bitten auf meine gestellte These: „Informationssicherheit ist eine Führungsaufgabe. (Top Management)“ Wer von den Anwesenden stimmt dieser These zu? / Wer von den Anwesenden ist nicht einverstanden?

#### **(Das sagt die Statistik: PP-Folie)**

Verschiedene Untersuchungen und auch unsere langjährige Erfahrung im Bereich Informationssicherheit zeigen, dass diese Erkenntnis, dass Informationssicherheit eine Führungsaufgabe ist, nicht wirklich in allen Unternehmen Fuss gefasst hat.

Wir haben keine definitiven Erklärungen zu diesem Fakt gefunden. Doch haben wir einige Vermutungen, weshalb das Image der Informationssicherheit im oberen Management nicht vollständig positiv ist. Denn scheinbar ist es noch nicht bis zu allen Führungskräften vorgedrungen, dass die Informationssicherheit einen wichtigen Beitrag zum Unternehmenserfolg leistet.

Folgende drei Image-Probleme scheint die Informationssicherheit zu haben:

- A) Informationssicherheit kostet Geld (Kosten)
- B) Informationssicherheit ist umständlich (Usability)
- C) Informationssicherheit bringt wenig (Nutzen)

Wir von bw digitronik haben uns zum Ziel gesetzt, das Image der Informationssicherheit deutlich zu verbessern, indem wir den Führungskräften, vor allem solchen, die nicht direkt mit der IT zu tun haben, den Nutzen für das Unternehmen aufzeigen möchten.

Gerne unterstützen wir Ihre Anliegen auch vor Ihrem Management und sensibilisieren Ihre Führungskräfte für dieses wichtige Thema. Denn wir wissen, dass der berühmte Prophet im eigenen Land zwar alles Mögliche sagen darf, aber eben nicht wirklich verstanden wird. Und falls er zu viele negative Nachrichten überbringt, kann es ihm ergehen wie dem römischen Überbringer schlechter Nachrichten: Sein Kopf rollt. Und das wollen wir selbstverständlich verhindern.

Denn folgende drei Gründe sehen wir, weshalb dieses Image so ist:

- A) Führungskräfte haben wenig Wissen über IT & Informationssicherheit
- B) Führungskräfte sind wenig sensibilisiert zur Informationssicherheit
- C) Führungskräfte haben die Bedeutung von Informationssicherheit nicht erkannt

Doch nun kehren wir die Betrachtungsweise um und schauen uns die Informationssicherheit aus der Perspektive des Gesamtunternehmens und der Unternehmensziele an. Es gibt verschiedene Erklärungsmodelle für die Unternehmensführung und deren Zielsetzungen. Fredmund Malik ein international anerkannter Management-Experte, der sich in den Fussstapfen von Peter Drucker bewegt, hat in seinem Buch „Die neue Corporate Governance“ sechs Schlüsselgrößen definiert, die für jedes Unternehmen wichtig sind. Dabei spielt es keine Rolle, ob es sich um einen KMU-Betrieb handelt oder um einen Weltkonzern.

## 1. Sechs Schlüsselgrössen des Unternehmens nach Malik<sup>1</sup>

Betrachten wir die sechs Schlüsselgrössen eines Unternehmens:

- 1) Marktstellung
- 2) Innovationsleistung
- 3) Produktivität
- 4) Attraktivität für gute Leute
- 5) Liquidität und Cash-Flow
- 6) Profitabilität

Wenn mir nun eine Führungskraft plausibel erklären kann, wie diese sechs Schlüsselgrössen erreicht und gemessen werden können, ohne die Unterstützung von IT, erst dann werde ich aufhören davon zu erzählen, dass Informationssicherheit eine Führungsaufgabe ist.

Es hat sich bereits seit Jahren herumgesprochen, dass die gesamte Informations- und Kommunikationstechnologie Fortschritte gebracht hat in den Bereichen Produktivität und Profitabilität. Ausser Christoph Blocher und einigen anderen können die meisten Führungskräfte in der Schweiz eine E-Mail versenden und empfangen. Auf das Internet als Informationsquelle möchte wahrscheinlich auch kein Unternehmen mehr verzichten. Was wären Management-Meetings ohne Laptops und die unendlich vielen farbigen, schlecht gestalteten PowerPoint-Präsentationen? Ob Beschaffung, Lagerverwaltung, Produktion, Handel oder Verwaltung der Kundendaten: Ohne IT sind diese Prozesse nicht mehr effizient zu gestalten.

Fazit ist: Die IT und damit auch die Informationssicherheit haben einen direkten Einfluss auf die sechs Schlüsselgrössen und damit auf den Erfolg eines Unternehmens. Darum werden wir nun diese genannten Erfolgsfaktoren auf die vier Hauptziele der Informationssicherheit übertragen.

## 2. Ziele von Informationssicherheit sind Unternehmensziele

Die Ziele von Informationssicherheit kann man verschiedenen definieren. Auf alle Fälle müssen sie in der Praxis direkt von den Unternehmenszielen abgeleitet sein. Ansonsten geht die Kongruenz und allenfalls die Effizienz verloren. Zuerst eine kurze Übersicht, wie wir von bw digitronik die Ziele der Informationssicherheit im Allgemeinen definieren:

Vier allgemeine Ziele der Informationssicherheit

- A) Business-Prozesse sichern & Geschäfte ermöglichen
- B) Informationen, Know-how & Wettbewerbsvorteile sichern
- C) Risiko Management betreiben
- D) Informationssicherheitskultur leben

Doch gehen wir der Reihe nach und schauen uns an, wie sich Schlüsselgrössen des Unternehmens in der Informationssicherheit widerspiegeln können. Auch hier sei betont, dass es sich um eine allgemeine Darstellung handelt, welche doch auf die meisten Unternehmen zutrifft.

---

<sup>1</sup> Malik Fredmund, Die neue Corporate Governance, 3. erw. Aufl., Kap. 5., S. 149-176

## 2.1 Business-Prozesse sichern und Geschäft ermöglichen

Was verstehen wir unter Business-Prozesse sichern und das Geschäft ermöglichen? In den meisten Unternehmen ist ein Teil der Prozesse unterstützt durch die IT. Prozesse werden mittels IT optimiert, was zur höheren **Produktivität** führen kann. Schon sind wir bei einer ersten Schlüsselgrösse angelangt. Doch kann die Produktivität nur gewährleistet sein, wenn die IT einwandfrei funktioniert, die Risiken klar im Auge behalten werden und die IT gegen Angriffe von innen und aussen geschützt ist.

Was eng mit der Produktivität zusammenhängt ist die Schlüsselgrösse **Profitabilität**. Es geht um die Frage: Wie kann ein Unternehmen mit möglichst kleinem Aufwand eine möglichst gute Leistung für den Kunden erbringen? Die Profitabilität kann stark gesteigert werden, wenn die Informationssicherheit die Ablenkungen und Störungen auf ein Minimum reduzieren kann. Hohe Sicherheit im Bereich der verschiedenen Prozesse hat einen direkten Einfluss auf den Unternehmenserfolg.

## 2.2 Informationen, Know-how und Wettbewerbsvorteile sichern

Was verstehen wir unter Informationen, Know-how und Wettbewerbsvorteile sichern? Eine wichtige Schlüsselgrösse für ein Unternehmen ist die **Marktstellung**. Ob Nischenplayer oder Marktführer, es gilt, die gewonnene Stellung zu halten, auszubauen und in jedem Fall rasch auf den sich verändernden Markt zu reagieren. Die Marktstellung hat viel mit erarbeiteten Wettbewerbsvorteilen, wie besseren Konditionen, rascheren Entwicklungszyklen und vielem anderen zu tun.

Eng damit zusammen hängt die Schlüsselgrösse der **Innovationsleistung**. Ob Know-how in der Entwicklung eines Produkts oder bestehende Patente oder andere vertrauliche Innovationsleistungen: Sie alle können in bares Geld verwertet werden. Aber nicht nur von ihrem Unternehmen, sondern auch von den Mitbewerbern. Wenn man sich die Szene der Internetkriminellen anschaut, dann kann man feststellen, dass immer mehr gezielte Attacken auf einzelne Unternehmen gefahren werden. Egal ob über das Netzwerk oder über Social Engineering. Die Internetkriminalität hat mehr Umsatz erwirtschaftet als die gesamte Drogenmafia.

Von daher hat die Informationssicherheit die wichtige Aufgabe, vertrauliche Informationen, in welcher Form auch immer, vor dem Zugriff von unberechtigten Personen zu schützen. Dies gilt für externe und interne Zugriffe auf kritische Daten.

## 2.3 Risiko Management betreiben

Was verstehen wir unter Risiko Management betreiben? Risiko Management schätzt die Wahrscheinlichkeit von Zerstörung, Verlust oder Schaden ein. Es geht um den unerlaubten Zugriff auf sichere und vertrauliche Informationen und die Gefährdung der Integrität, der Verfügbarkeit und Vertraulichkeit von Unternehmensinformationen. Hier treffen wir auf zwei Schlüsselgrössen der Unternehmenssteuerung: Die **Liquidität** und den **Cash-Flow**. Diese Kennzahlen werden vor allem in grösseren Unternehmen mittels komplexer IT-Unterstützung ermittelt und liefern wichtige Entscheidungsgrundlagen.

Gerade nach den Abstürzen von Enron und Worldcom wurde der Ruf nach internen Kontrollen und IT-Kontroll-Prozessen laut. Daraus entstand das dicke Regelwerk Sarbanes-Oxley Act (SOX), welches an US-Börsen kotierte Unternehmen in die Verantwortung zieht, die Integrität der Daten und die Nachvollziehbarkeit der einzelnen Prozesse

genau zu strukturieren und zu dokumentieren. So können vertrauliche Daten nicht einfach manipuliert oder sabotiert werden. Durch ein gutes Risiko Management kann einerseits die Vertraulichkeit und Verfügbarkeit der Daten sichergestellt und die Integrität der Informationen besser garantiert werden.

## 2.4 Informationssicherheitskultur leben

Und als letztes Ziel der Informationssicherheit definieren wir: Informationssicherheitskultur leben. Was meinen wir damit? Die gesamte Sicherheit eines Unternehmens kann nur dann massgeblich gesteigert werden, wenn Informationssicherheit eine Kultur wird, die vom Management bis zum einfachen Angestellten von allen gelebt wird. Die Informationssicherheit muss hochgehalten werden, damit alle Mitarbeitenden sensibilisiert sind und bleiben. Es kann nicht sein, dass diese nur bei der Einstellung ein Reglement unterschreiben und danach nie wieder etwas davon hören. Nur wenn Mitarbeitende gutes und anhaltendes Training erhalten, kann sich die Informationssicherheitskultur verbessern. Und wir sind überzeugt, dass so eine Kultur auch auf die Gesamtkultur des Unternehmens einen positiven Einfluss ausüben kann. Und das bringt uns zur letzten Schlüsselgrösse von Unternehmen: **Attraktivität für gute Leute**.

Gute Arbeitskräfte schätzen eine gute Unternehmenskultur, zu der auch die Informationssicherheitskultur zählt. Denn wenn sich das Management nicht einmal für die Informationssicherheit interessiert, die einen direkten Einfluss hat auf den Unternehmenserfolg, weshalb sollte sie sich für andere Elemente einer Unternehmenskultur kümmern, die weniger relevant sind?

Folgendes Fazit können wir bis jetzt ziehen:

- Informationssicherheit hat direkten Einfluss auf die sechs Schlüsselgrössen.
- Informationssicherheit ist ein wichtiger Faktor für den Unternehmenserfolg.
- Informationssicherheit sollte darum genügend Management Attention erhalten.
- Informationssicherheitskultur funktioniert nicht ohne das Management
- Informationssicherheit funktioniert deshalb nur top-down.
- Informationssicherheit ist eine Führungsaufgabe!

## II. Zielerreichung in der Informationssicherheit

### 1. Informationssicherheit betrifft das oberste Management (Stufen-Modell)

Nachdem wir nun festgehalten haben, dass Informationssicherheit eine Führungsaufgabe ist, beschäftigen wir uns in einem zweiten Gedankengang damit, wie die Informationssicherheit ihre Ziele erreichen kann.

Ziele können nur erreicht werden, wenn eine Person oder ein Gremium dafür verantwortlich ist. In letzter Instanz jedoch ist die Unternehmensleitung für die Informationssicherheit zuständig, verantwortlich und haftbar. Im Best Practice Dokument „IT Governance für Geschäftsführer und Vorstände“ wird folgende Praxis vorgeschlagen:

„Um IT Governance leichter umzusetzen, sollen die verschiedenen Führungsebenen im Unternehmen folgende Aufgaben übernehmen: Die Mitglieder des Vorstandes sollen eine aktive Rolle in der Entwicklung der IT Strategie und in IT Steuerungsgremien haben. Das Top-Management soll organisatorische Strukturen bereitstellen, die die Implementierung der IT Strategie unterstützen. Der IT Leiter soll geschäftsorientiert denken und eine Brücke zwischen IT und den Fachbereichen schlagen. Das Management der Fachbereiche soll in die IT Steuerungsprozesse oder Komitees mit einbezogen werden.“<sup>2</sup>

Um dies etwas vereinfacht darzustellen, schlage ich ein Vierstufen-Modell vor:

#### ***Das Vierstufen-Modell der Verantwortung***<sup>3</sup>

##### **1. Verwaltungsrat**

- Verantwortung für Corporate Governance (Ziele, Leitlinien, Strategie)
- IT Governance (Ziele, Leitlinien für die IT-Infrastruktur & Prozesse)
- IT Security Governance (Ziele, Leitlinien, Klassifizierungen)

##### **2. Management-Team**

- Organisatorische Strukturen bereitstellen
- Implementierung der IT Strategie & Informationssicherheit unterstützen
- Überwachung und Messung der Ziele

##### **3. Informationssicherheitsbeauftragter (evtl. Stabstelle)**

- Risiko Management
- Umsetzung der Informationssicherheit
- Überwachung, Monitoring, Reporting

##### **4. Mitarbeitende/Benutzer**

- Einhaltung der Richtlinien
- Verantwortlich für eigenes Verhalten

Anhand dieses Modells sehen wir, dass Informationssicherheit auch das oberste Management betrifft und nicht nur eine Aufgabe des Sicherheitsverantwortlichen oder des IT Leiters ist. Nur wenn alle Stufen involviert sind, können die Ziele der Informationssicherheit auch wirklich erreicht werden.

<sup>2</sup> IT Governance Institute, IT Governance für Geschäftsführer und Vorstände, Zweite Ausg., S. 20

<sup>3</sup> Das Vierstufen-Modell ist eine Vereinfachung des Sechsstufen-Modells von E. Kritzinger. Kritzinger E., An Information Security Retrieval and Awareness Model for Industry, Diss. UNISA 2006

## 2. Unternehmensführung definiert die Security Governance

Nachdem wir nun festgehalten haben, dass die oberen Führungsstufen für die Informationssicherheit verantwortlich sind, müssen wir uns nun mit den Inhalten der Ziele beschäftigen. Was alles muss oder soll die Unternehmensführung definieren?

Die Unternehmensführung muss also in erster Linie die Security Governance definieren. „Governance bedeutet die Festlegung von Methoden und Verantwortung im Unternehmen. ... Sie muss gewährleisten, dass Ziele erreicht werden, Risiken angemessen gemanagt und Unternehmensressourcen in verantwortungsvoller Weise eingesetzt werden.“<sup>4</sup>

Wir von bw digitronik haben vier Punkte herausgeschält, wo die Unternehmensführung den Fokus darauf setzen sollte, wenn es um die Definition der Security Governance geht. Alle diese Punkte müssen von den Unternehmenszielen abgeleitet werden:

- A) Definition der Computer Ethik und der Professionalität (Code of Behavior)
- B) Definition der Führungs- und Organisationsstruktur
- D) Klassifizierung von Vertraulichkeit, Integrität und Verfügbarkeit
- C) Definition des Risk- und Informationsmanagements (Reporting & Monitoring)

### 2.1 Definition des Computer Ethik & der Professionalität (Code of Behavior)

In einem ersten Schritt soll grundsätzlich mal der Umgang mit der IT definiert werden und was unter professionellem Umgang mit diesen Hilfsmitteln zu verstehen ist. So könnte man von der Definition einer Computer Ethik oder einem „Code of Behavior“ sprechen.

In grösseren Unternehmen wird schon länger über Unternehmensethik gesprochen. Bei der Computer Ethik handelt es sich um die neueste Ergänzung in diesem Themenkomplex. Bei Computer Ethik geht es in erster Linie um die Interaktion von Mensch und Computer. Das schnelle Wachstum und der technologische Fortschritt in heutigen Unternehmensnetzwerken ziehen neue ethische Konflikte nach sich. Je nach persönlichem Hintergrund, Religion, Sprache oder Kultur werden diese Konflikte anders gelöst.

Das Resultat dieser Verschiedenartigkeit und Vielfalt ist, dass für eine Person etwas akzeptabel ist und für eine andere absolut nicht. Eine Person surft während den Geschäftszeiten Stunden im Internet, eine andere hat ein schlechtes Gewissen, wenn sie einmal in der Woche ein privates E-Mail verschickt. Darum ist es auch hier wichtig, dass jede Organisation definiert, was für sie Computer Ethik bedeutet.

Mit dem Verhaltenskodex der Computer Ethik wird auch die Professionalität definiert. „Professionalität meint die Verantwortung des Mitarbeitenden gegenüber seinem Arbeitsplatz und dem Unternehmen.“<sup>5</sup> Informationssicherheit erfordert eine höhere Stufe an Professionalität und Sensibilität. Der Sinn für Verantwortung im Bezug auf Sicherheit von Informationen muss weiter geschärft werden. Darum ist es von entscheidender Bedeutung, dass die Unternehmensführung eine Computer Ethik definiert, welche auch Basis der Informationssicherheit ist.

<sup>4</sup> IT Governance Institute, IT Governance für Geschäftsführer und Vorstände, Zweite Ausg., S. 7

<sup>5</sup> Little 1999 zitiert in:  
Kritzinger E., An Information Security Retrieval and Awareness Model for Industry, Diss. UNISA 2006

## 2.2 Definition der Führungs- und Organisationsstruktur

In einem zweiten Schritt sollte das Management die Führungs- und Organisationsstruktur für die IT und die Informationssicherheit definieren. Es ist wichtig, dass die Struktur im Bereich Informationssicherheit die Ziele unterstützt und dem Unternehmen angepasst ist. In einem kleineren Unternehmen, kann auch der Geschäftsführer für die Sicherheit verantwortlich sein. In einem mittleren Betrieb macht es Sinn, diese Rolle dem IT-Leiter zu übergeben. Und in grösseren Unternehmen hat sich in der Praxis ein Sicherheitsbeauftragter bewährt. Hierzu kann ich noch Kersten/Klett zitieren, die empfehlen: „Grundsätzlich gilt, dass die Funktion „IT-Sicherheitsbeauftragter“ nicht vereinbar ist mit der operativen Leitung beispielsweise des Rechenzentrums oder der Verwaltung, weil hierbei in der Praxis sehr schnell Interessenkonflikte – meist zum Nachteil der IT-Sicherheit – auftreten werden. Deshalb ist diese Aufgabe von anderen operativen Tätigkeiten zu trennen.“<sup>6</sup>

## 2.3 Klassifizierung von Vertraulichkeit, Integrität und Verfügbarkeit

Nachdem der Verhaltenskodex und die verschiedenen Strukturen definiert wurden, geht es im nächsten Schritt um verschiedene Klassifizierungen. Die Unternehmensführung muss die Informationen klassifizieren, indem sie beschreibt was Vertraulichkeit, Integrität und Verfügbarkeit heisst.

Jede Organisation hat andere Anforderungen bzgl. der Kontrollziele und der Höhe der Vertraulichkeit, Integrität und Verfügbarkeit. Das Management definiert die Ziele und die Methode der Umsetzung und des Reportings.

Die ISO-Norm 17799:2005 definiert die Begriffe wie folgt:

**Vertraulichkeit:** Sicherstellen, dass Informationen nur entsprechend autorisierten Personen zugänglich sind.

**Integrität:** Schutz der Genauigkeit und Vollständigkeit der Informationen und der Verarbeitungsmethoden.

**Verfügbarkeit:** Sicherstellen, dass autorisierte Personen wenn immer erforderlich Zugang zu Informationen und damit verbundenen Objekten haben.

Wenn die verschiedenen wichtigen Werte für ein Unternehmen aufgelistet und ihre Schutzziele definiert sind, kann erst ein Risiko Management aufgebaut werden.

## 2.4 Definition des Risk- und Informationsmanagement

Das Best Practice Dokument „IT Governance für Geschäftsführer und Vorstände“ definiert Risiko Management wie folgt: „Absicherung von IT Assets und Informationen sowie deren Wiederherstellung nach Katastrophen.“<sup>7</sup>

„Verantwortlich für das Unternehmensrisiko ist der Vorstand. Durch folgende Massnahmen werden Risiken eingeschränkt: 1) Feststellen, dass die signifikanten Risiken für das Unternehmen transparent sind. 2) Bewusstsein schaffen, dass die oberste Zuständigkeit für das Risikomanagement beim Vorstand bleibt. 3) Bewusstsein schaffen, dass durch den Einsatz eines internen Kontrollsystems als Risikomanagementwerkzeug auch die Kosten/Nutzen-Aspekte besser gemanagt und überprüft werden. 4) Berücksichtigen, dass ein transparentes und aktives Risikomanagement Wettbewerbsvor-

<sup>6</sup> Kersten/Klett 2005, Der IT Security Manager, S. 26

<sup>7</sup> IT Governance Institute, IT Governance für Geschäftsführer und Vorstände, Zweite Ausg., S. 36

teile schaffen kann. 5) Darauf bestehen, dass Risikomanagement in die Unternehmensaktivität integriert wird.“<sup>8</sup>

Das Management muss das Risiko Management so aufsetzen, dass es einfach überwacht werden kann und somit alle wichtigen Informationen schnell zur Verfügung stehen. In der Informationssicherheit kann es daher Sinn machen die ganzen Prozesse z. B. nach ISO-Normen zu strukturieren und zur Überwachung in ein ISMS-Tool einzubinden. So sind die wichtigen Informationen für das Risiko Management schnell verfügbar und die Entscheidungsträger sind in der Lage, rasch zu reagieren.

### 3. Softfaktoren, die der Informationssicherheit zum Erfolg verhelfen

Nun kommen wir noch zu einigen Softfaktoren, die der Informationssicherheit zum Erfolg verhelfen:

#### 3.1 Führung durch Vorbild

Ein erster Softfaktor ist: Führung durch Vorbild. Ohne das vorbildliche Verhalten des Managements kann keine Informationssicherheit erfolgreich gelebt werden. Wenn Mitarbeitende bei ihren Führungskräften ein mangelndes Interesse für das Thema Informationssicherheit sehen, werden sie dies als „unwichtig“ interpretieren. So kann keine Informationssicherheitskultur gelebt werden, welche die Sicherheit einer ganzen Organisation erhöht. Hier können wir von bw digitronik einen wichtigen Beitrag als externe Security-Berater für ein Unternehmen erbringen. Gerne unterstützen wir Sicherheitsverantwortliche in der Sensibilisierung des Managements im Bezug auf Informationssicherheit. Diese Awareness bringt ihrem Thema eine höhere Management Attention ein und als Verantwortlicher können sie ihre Aufgabe optimaler ausfüllen.

#### 3.2 Mitarbeiterführung

Führung mit Vorbild hat auch ihren Niederschlag in der direkten Mitarbeiterführung. Wir haben bereits im Bereich der Computer Ethik darüber gesprochen, dass verschiedene Menschen Regeln verschieden interpretieren. So liegt es an der Führungskraft in der Linie oder in einem Projektteam, die Regeln der Informationssicherheit oder der Computer Ethik jedem seiner Mitarbeitenden klar zu machen, damit dieser sie individuell versteht. Denn jeder Persönlichkeitstyp interpretiert klare Verhaltensregeln anders. So kann eine Weisung über „Vertraulichkeit von Informationen“ von Typ A (G-Typ) interpretiert werden, dass er keiner lebenden Seele je etwas davon erzählen wird. Typ B (I-Typ) interpretiert das Wort „Vertraulichkeit von Informationen“ so, dass er es niemandem erzählen oder weitersagen kann, ausser seinen zehn besten Freunden. Auch in diesem Zusammenhang ist das Führen mit Vorbild wichtig, weil es klare Bench Marks setzt, wie man in einzelnen Fällen vorzugehen hat.

#### 3.3 Mitarbeitersensibilisierung (Security Awareness)

Nur wenn das Management und alle Führungskräfte sensibilisiert sind für das Thema Informationssicherheit, macht es Sinn, auch alle anderen Mitarbeitenden zu schulen im Bereich Security Awareness.

<sup>8</sup> IT Governance Institute, IT Governance für Geschäftsführer und Vorstände, Zweite Ausg., S. 36-37

Wichtig ist auch, dass nicht alle Mitarbeitenden in der gleichen Art und Weise geschult und sensibilisiert werden. Führungskräfte brauchen ein grösseres Verständnis für die Zusammenhänge und die Konsequenzen für die Organisation. Personen aus Fachabteilungen brauchen ein vertieftes Wissen über die technologischen Themen. Mitarbeiter im Support oder Helpdesk müssen sensibilisiert werden für Social Engineering.

Und alle anderen Mitarbeiter müssen entsprechend ihrem Aufgabengebiet und ihrer Verantwortung geschult werden. So gibt es Mitarbeiter in der Entwicklung, die haben mit geschäftskritischen und vertraulichen Daten zu tun. Diese müssen umfassender ausgebildet werden. Andere, welche nur das E-Mail-System und das Internet benützen können, müssen im richtigen Umgang geschult sein. Es gibt kein Standard-Konzept für Security Awareness. Es muss von der Sicherheitsrichtlinie abgeleitet werden, damit es nicht nur bei einer Schulung bleibt, sondern zur gelebten Kultur wird. Nur so kann Informationssicherheitskultur einen wichtigen Betrag zur umfassenden Sicherheit eines Unternehmens leisten.

### **III. Nutzen der Informationssicherheit für das Unternehmen**

Als kurze Zusammenfassung möchte ich die wichtigsten Punkte nochmals nennen. Wir haben gesehen, dass Informationssicherheit tatsächlich eine Führungsaufgabe ist und das Management eines Unternehmens verschiedene Ziele, Leitlinien und einen Verhaltenskodex definieren muss, damit Informationssicherheit überhaupt sinnvoll umgesetzt werden kann. Wir haben festgestellt, dass eine blosser Verordnung top-down noch keine Informationssicherheitskultur hervorbringt. Das Management muss sich aktiv darum bemühen und als Vorbild vorangehen.

Der Nutzen von Informationssicherheit für Unternehmen ist gross. Denn dadurch können IT Ziele erreicht und Risiken auf eine Art und Weise gemanagt werden, dass durch den IT Einsatz Unternehmenswert generiert wird. So wird das Unternehmen aufrechterhalten und das Wachstum sichergestellt.

Aus allen diesen Massnahmen und Definition resultiert mit der Zeit eine Informationssicherheitskultur, welche Unternehmen zu einer höheren Stufe der Sicherheit führt. In der heutigen, sich ständig ändernden Umwelt, müssen Organisationen darum bemüht sein, eine gesunde Informationssicherheitskultur zu leben. Eine Informationssicherheitskultur fokussiert darauf, die Organisation zu ermutigen, eine saubere Planung und ein Management von allen Aspekten der Informationssicherheit aufrechtzuerhalten, speziell seit Unternehmen so abhängig sind von ihren Daten, Informationen, Netzwerken und Systemen, wie dies heute der Fall ist. Informationssicherheit muss ein Teil der täglichen Kultur der Mitarbeitenden werden.

Besten DANK für Ihre Aufmerksamkeit.

Anzahl Wörter: 3'015 (Ziel: max. 3'000 Wörter)