Sicherheit in Unternehmen

wfn 1.07.2024

Einleitung

„Mehr Sicherheit, mehr Wert“. Damit wirbt ein Unternehmen der TIC Branche, Test, Inspection and Certification. Die Formulierung, „Mit Sicherheit mehr Wert“, einprägsam, doppeldeutig, werbewirksam wurde nicht gewählt. Das Versprechen wäre schwer einlösbar. Da ging man rechtlich auf Nummer „Sicher“.

Das Thema Sicherheit war in meinem Berufsleben mein ständiger Begleiter. Sicherheit im Sinne der Beherrschbarkeit von Prozessen. Sicherheit also gegenüber einem Zustand der nicht eintreten sollte. In meinem Fall, Vermeidung von Fehlern bei der Entwicklung und Herstellung von technischen Produkten und Dienstleistungen. Um die Sache rund zu machen, kam die Energieeffizienz und der Umweltschutz dazu. Arbeitssicherheit galt als Grundvoraussetzung aber nicht immer als Selbstverständlichkeit. Informationssicherheit löste einen ungeahnten Hype aus, der bis heute anhält. Als Auditor weltweit war ich Teil dieser Expertengruppe, die sich mühte die Standards, die als ISO Anforderungen definiert sind, bekannt als ISO 9001, ISO 14001, ISO 50001, ISO 27001, IATF, auf Einhaltung zu prüfen. Nach Abhandlungen zur Zertifizierung von Managementsystem allg. (2020) und der Situation der Automobilindustrie und deren Verhältnis zum Standard IATF (verfügbar auf meiner privaten Homepage www.fuchs-nordhoff.de), jetzt meine Sicht zur Informationssicherheit.

Zwei Fragen ließen mich nicht los und beschäftigen mich auch heute noch:

Sind diese ISO Standards wirklich die Lösung der Probleme?

Sind Kosten- und Nutzenverhältnis zufriedenstellend oder gibt es Alternativen?

Ich richte die folgenden Ausführungen an Personen in Organisationen, die verantwortlich sind, für das Funktionieren von Abläufen und deren Stabilität und Robustheit. Mein Beitrag ist den Blick zu schärfen und immer fragend den scheinbar Selbstverständlichkeiten gegenüber zu treten. Das größte Risiko, das wirtschaftliche Scheitern einer Unternehmung wird hier nicht thematisiert, ist aber unterschwellig immer begleitend und nie ganz ausgeblendet.

Die nachfolgenden Ausführungen drehen sich also um das Thema Sicherheit. Nach einer groben Analyse zu diesem Begriff folgt eine Transformation auf die IT Sicherheit in Unternehmen mittlerer Größe. Hierbei wird bewusst auf technische Raffinessen verzichtet. Vielmehr geht es um übergeordnete Betrachtungen und soll eine Diskussion über Sinn und Unsinn derzeit gelebter Praxis anregen. Wie wirksam sind IT Managementsysteme, was bringt eine Zertifizierung, wie sieht die Nutzen- / Kostenbetrachtung aus? Ob etwas richtig oder falsch ist, ist schwerlich wirklich eindeutig zu ermitteln. Eine Aus- Einander-Setzung wird hiermit angestoßen. Leider ist es unumgänglich, den Begriff sicher und unsicher immer und immer wieder zu verwenden. Die deutsche Sprache lässt da nicht viel Varianten zu. Im Englischen gibt es da feine Unterscheidungen. So ist unsafe was anderes als unsure, uncertain, insecure, doubful, unstable, halting, precarious, arguable.

Im Englischen stehen die beiden Begriffe Security (englisch für „Schutz“) und Safety (englisch für „Gefahrlosigkeit“) für zwei voneinander getrennte Aspekte. Im Deutschen bildet oft zweimal das Wort „Sicherheit“ die Basis des Begriffs. Dies führt regelmäßig zu Verständigungsschwierigkeiten, da beide Seiten den Begriff unterschiedlich interpretieren können (wiki)
Der Begriff Security wird daher im Zusammenhang mit technischen Sicherungsmaßnahmen (Sicherungstechnik) genutzt, z. B. IT-Security (wiki).

Absolute Sicherheit gibt es nicht. Das ist eine Binsenweisheit. Technik ist nicht immer perfekt und Menschen sind es auch nicht. Etwas gilt als sicher, wenn es eintritt wie erwartet, bzw. vorausgesagt wurde. Wir können bis zu einem gewissen Grad Sicherheit erzeugen. Nehmen wir ein Beispiel: Um ein Fahrzeug gegen Diebstahl zu sichern gibt es entsprechende Einrichtungen

wie Zentralverriegelung, Wegfahrsperre, Alarmanlage, Trackingsysteme. Ein potentieller Täter mit wenig technischen Kenntnissen und keinerlei Erfahrung aber praktisch unendlicher Zeit für sein Vorhaben, soll nicht erfolgreich sein. Ein Anderer mit Wissen und technischer Ausrüstung aber mit sehr begrenztem temporärem Zugriff soll ebenfalls scheitern. Sind Zeit und Know how umfangreich verfügbar, dann kann u. U. ein Diebstahl nicht verhindert werden oder ist zusätzlich durch Maßnahmen mit hohen Kosten zu sichern.

Neben dem Aspekt, wie volatil die Situation ist, ist die potentielle Schadenshöhe wichtig und rechtfertigt kostenintensive Absicherungsmaßnahmen. Man kann die Situation auch vermeiden oder durch eine Versicherung abdecken. Zu unserem Beispiel oben kommt hinzu, wie wahrscheinlich ist es den, dass ein Fahrzeug gestohlen wird. Ist der Fahrzeugwert hoch, kann das Diebesgut schnell beseitigt werden, Grenznähe, gibt es Abnehmer?

Begrifflichkeiten

Sicherheit (wiki)

Frei von Gefahr. Gefahr latent oder Gefährdung (räumlich und zeitliches Zusammentreffen mit einer Gefahr. Ursprung aus sēd „ohne“ und cūra „Fürsorge“). Für Individuen und Gemeinschaften bezeichnet Sicherheit den Zustand des Nicht-bedroht-Seins der Freiheit ihrer ungestörten Eigenentwicklung in zweierlei Hinsicht:

- im Sinne des tatsächlichen (objektiven) Nichtvorhandenseins von Gefährdung – als Sicherheit im objektiven Sinne, sowie
- im Sinne der Abwesenheit von (subjektiver) Furcht vor Gefährdung – als Sicherheit im subjektiven Sinne.

Wahrscheinlichkeit In einem Briefwechsel zwischen Blaise Pascal und Pierce de Fermat 1654 tauschen die beiden ihre Überlegungen zu folgendem Sachverhalt aus: Ein Kartenspiel wird jäh unterbrochen (z. B. wegen Spielverbots, das es seit dem 4. Jahrhundert in vielen europäischen Städten gab). Wie ist der Einsatz zu verteilen. Möglicherweise war das der Beginn der Wahrscheinlichkeitsrechnung.

Grundsätzlich beginnt jedes Spiel mit Gleichheit. Jeder soll die gleichen Chancen haben. Das gilt ebenso für den Wettkampfsport. Im Golfspiel kann die unterschiedliche Spielstärke über das Handycap kompensiert werden. Der schwächere Spieler bekommt sozusagen einen Vorsprung. Im Fußball spielen Jahrgangsstufen gegeneinander. Computerspiele folgen sinngemäß der gleichen Logik. Mit zunehmender Spielpraxis schneidet man besser ab.

No risk no fun Ist der Sieg wirklich das Ziel? Ja und Nein! Die Motivation zum Spiel und Wettkampf ist das Gewinnen wollen. Aber je nach Menschentyp kann das vernachlässigt werden oder ganz ausgeblendet werden. Eine Boule Gruppe die sich regelmäßig im Stadtpark trifft, geht nicht dort hin um Siege zu feiern.

Der Ausgang des Spiels ist also unsicher, d. h. nicht vorherbestimmt und meist ist der Ausgang offen, selbst wenn es Favoriten gibt. Erst die Eintrittswahrscheinlichkeit führt zu einer bewertbaren Situation.

Unsicherheit kann „verunsichern“ (Prägnanz in der deutschen Sprache). Unsicherheit kann, wie oben gesehen aber auch Vergnügen bereiten. Ein Abenteuer, das Sicherheit verspricht ist kein Abenteuer. Da ist immer was dabei was schief gehen kann. Manche wollen beides, Sicherheit und Abenteuer. Das ist dann die geführte Alpenüberquerung mit 4 Sterne Übernachtungen zwischen den Etappen. Das Gepäck wird natürlich von jemand anderem getragen. Die Ausrüstung, nur das

Beste. Tourenführer mit Satellitentelefon. Mehr als 4 Teilnehmer würden stören. Die Bergwacht auf Abruf. Nächstes Jahr Nepal.

Das ist, sagen wir mal, ein Erlebnis, ein Abenteuer ist das nicht.

Es ist nichts zu sagen gegen das All inclusive Hotel in Lara / Türkei. Das hat auch seine Vorzüge, wenn alles stimmig ist. Das Essen, die Ausflüge, der Strand, im Urlaub auf Nummer Sicher zu gehen ist nicht unbedingt ein Fehler. Oft ist es ein Kompromiss. Die Campingtour, gerne mit unbekanntem Ziel. Viele neue Eindrücke. Aber auch ohne Verzicht auf das Weizenbier an der Uferpromenade. Oder vielleicht doch das Rafting, Paragliding oder Tiefseetauchen. Der Spaß ist groß, der Preis unter Umständen hoch. Wir können wählen.

Ambiguous tolerance ist die Fähigkeit Uneindeutigkeit auszuhalten. Nicht immer sind die Spielregeln klar. Besonders in Unternehmen mit vielen Marktteilnehmern und Anpassungsdruck muss man auch auf Glück vertrauen. Immer auf Sicht zu fahren kann riskant sein.

Komplex und Kompliziert wird selten scharf genug unterschieden. Eine Situation ist komplex, wenn es viele Einflussfaktoren gibt. Ein Fußballspiel wird „bestimmt“ durch viele Einflussfaktoren aber die Regeln sind klar und eindeutig. Komplex aber nicht kompliziert. Wirklich kontrovers wird es auf dem Platz nicht durch die Regel, sondern was jeder jeweils gesehen haben möchte. Das Funktionieren einer Armbanduhr ist wenig komplex aber kann als kompliziert betrachtet werden. Zum Lösen einer Aufgabenstellung ist es angebracht, sich klar zu machen was überwiegt.

Lernen Oberflächliches Wissen kann man sich durch Sammeln von Fakten aneignen. Tiefsitzendes Wissen erfordert mehr. Da muss man probieren, da muss auch mal was schiefgehen. Auch Können erfordert Praxis. Klavierspielen lernt man nicht mittels Youtube, es erleichtert aber den Einstieg ungemein.

Erst wenn wir Sicherheit aufgeben erwerben wir Sicherheit. Nicht ohne Sinn und Verstand. Man sollte Flügel haben, wenn man am Abgrund steht (Friedrich Nitzsche). Unsere größten Schätze sind wahrscheinlich da vergraben, wo unsere stärksten Ängste liegen.

Gefahren

Täglicher Umgang mit Gefahren

Unbewusst stellen wir uns auf zu erwartende Situationen und auch Gefahren ein. Wir wählen die richtige Kleidung, verschließen die Tür, wenn wir das Haus verlassen, haben Geld oder Kreditkarte in der Tasche, Planen den Urlaub, Sparen für Anschaffungen. Wir gehen zur medizinischen Vorsorge, leben gesund (hoffentlich), wir haben das Rauchen aufgehört. Bei alle dem glauben wir die Zukunft beherrschbar zu machen. Tatsächlich reduzieren wir Risiken. Was durchaus Sinn ergibt. Aber Gefahren lauern häufig da, wo wir sie nicht erwarten. Vorsicht ist besser als Nachsicht, keine Frage.

Und dann gibt es da noch die Überraschungen. Die guten, wie die Überraschungsparty, die schlechten, wie der plötzliche Verlust eines Menschen.

Sind Sie sicher, dass Sie sicher sind?

Mit dieser Fragestellung, im Handwerk und in der Industrie, wird der Arbeitsschutz auf den Punkt gebracht. Eine Sensibilität für die Situation soll geweckt werden. Vereinfacht dargestellt ist der Arbeitsschutz das Zusammenwirken von: Schutzausrüstung, Schutzeinrichtungen, geschultem Personal, festgelegten Verfahren und eine Arbeitsschutzorganisation. Das zentrale Instrument ist eine Risikobetrachtung, die Gefahrenanalyse oder Gefährdungsanalyse. (Genaugenommen ist es die Gefährdungsbeurteilung im Arbeitsschutz und die Risikobeurteilung in der Maschinensicherheit

zur Markteinführung). Diese muss für alle relevanten Tätigkeiten vorliegen. Also alles geplant, alles geregelt. Wenn sich alle dran halten dürfte nichts passieren.

Die Sicherheitsprofis gehen einen Schritt weiter. Eine „Kultur“ soll etabliert werden. Null Toleranz bei Verstößen. Wachsamkeit gegenüber möglichen Gefahren. Melden von Beinaheunfällen. Es besteht die Gefahr, dass das Lernen durch Fehler unterdrückt wird. Insbesondere ist das der Fall, wenn bei Prämienentscheidungen für Vorgesetzte Unfallzahlen herangezogen werden. Dann ist mitunter ein Unfall gar kein Unfall. Der Kern der Sache ist aber, eine Kultur lässt sich nicht schaffen. Eine Kultur entsteht, ist also Ergebnis nicht Vorgabe. Der Versuch eine Kultur zu installieren läuft meist ins Leere, ist bestenfalls wirkungslos, oft unglaubhaft und widersprüchlich.

Das wichtigste wird ausgeblendet. Die Mündigkeit des Mitarbeiters, das Vertrauen und on top die Selbstverantwortung. Ohne diese Selbstverantwortung geht es nicht. Das ruft Skepsis hervor, aber nochmals, für die Arbeitsqualität, für die Fehlerfreiheit, für die Sicherheit am Arbeitsplatz ist derjenige verantwortlich, der die Arbeit ausführt. Hier wird natürlich unterstellt, dass die Grundvoraussetzungen, wie oben beschrieben, erfüllt sind.

Aber da wollen noch viele andere mitmischen. Arbeitssicherheitsfachkraft, (Fachkraft für Arbeitssicherheit) Arbeitssicherheitsbeauftragter (Sicherheitsbeauftragter), Betriebsrat, Vorgesetzte, Berater und Zertifizierungsgesellschaften. Gesetzgeber unterstützen dabei. Begründet wird das mit Fürsorgepflicht.

Diese Unterstützer sind überall da, wo Unsicherheit vermutet wird. Um Missverständnisse zu vermeiden, ohne Experten geht es nicht. Wie wir später sehen werden, sind die Experten die wichtigste und wirksamste „Waffe“ gegen Unsicherheit in weiten Teilen des Unternehmens. Informationssicherheit ohne Experten ist wirkungslos.

Ist Unsicherheit gut oder schlecht?

Unsicherheit ist das Salz in der Suppe. Das Leben wird dadurch erst interessant. Es ist der Ursprung von Glück und Freude. Unsicherheit ist der Grund für Hoffnung oder einfach Zuversicht. Unsicherheit lässt uns wachsen, treibt uns zu neuen Ufern. All unser Wissen und unsere Fähigkeiten entstehen durch einen Lernprozess. Lernen entsteht durch den Wunsch die Welt begreifen zu wollen. Dass wir uns sicher in dieser Welt bewegen und unsere Möglichkeiten voll ausschöpfen.

Unsicherheit kann uns auch ausbremsen. Sie kann uns krank machen. Unsicherheit kann uns zu Fehlern verleiten. Sie kann uns an der Teilnahme am Leben blockieren. Kann uns Angst machen.

Erst wenn wir beide Seiten kennen und uns diese bewusst sind, dann können wir wählen. Die Wahl ist nicht ganz frei. Siegmund Freud sagte einmal: Wenn es um den freien Willen geht sind wir nicht Herr im eigenen Hause.

Aber die Selbstverantwortung bleibt uns erhalten, womit wir doch wieder beim Wählen sind.

Wie entsteht Sicherheit?

Wie wird aus Unsicherheit Sicherheit? Zunächst einmal sind Unsicherheit und Sicherheit keine absoluten Großen. Es handelt sich oft um ein Gefühl, dass nicht unbedingt mit den Fakten korreliert. Jeder hat seine eigene Erfahrungswelt und hält das für wahr, was in die Schablone passt. Wie wirklich ist die Wirklichkeit, könnte man wie Watzlawik fragen.

Mit Kenngrößen möchte man die Sicherheit quantifizierbar machen. Aber auch Zahlen sprechen nicht für sich selbst und werden interpretiert.

Sicherheit ist in der Betrachtung meist rückwärtsgewandt. Wieviel Probleme hatten wir noch vor 6 Monaten, wie haben wir uns verbessert. Beliebt ist dann die Aussage: wir haben viel erreicht aber wir sind noch nicht am Ziel. Wir machen da schon viel. Es erfordert aber noch viel Anstrengung. Sind die Ereignisse (Inicidents) wenige, klein in der Auswirkung und wurden schnell entdeckt, sieht man sich gut aufgestellt. Das ist nicht falsch. Man hat die Hausaufgaben gemacht. Für die täglichen, bekannten Gefahren ist man gerüstet.

Um Risiken zu bewerten, multipliziert man den Wert für Schwere der möglichen Folgen einer Gefahr mit der Eintrittswahrscheinlichkeit. Aus diesem Risikoinventar werden die Maßnahmen und Prioritäten abgeleitet. Im Bereich technischer Risiken (FMEA) kommt noch ein Faktor „severity“ hinzu. Der ist hoch bei Gefahr für Leib und Leben oder Nichteinhaltung rechtlicher Vorgaben.

So machen es eigentlich alle Firmen. Das ist so die Grundlage. Anwendbar ist das für alle Arten von Unsicherheiten, mehrheitlich wird hier von Risiken gesprochen. Im Finanzbereich ist das natürlich nicht hinreichend. Da ist das Fundament das Einhalten gesetzlicher Vorgaben, also die Pflicht. Die Kür sind dann finanztechnische Hebel wie die, die Finanz- und Ertragslage verbessern und den Unternehmenswert steigern.

Eigentlich ist die Vergangenheit kein wirksamer Indikator für die Zukunft. Zukunft ist per se unsicher. Sicherheit ist, vereinfacht, die Beseitigung von Unsicherheiten. Instrumente dafür sind Versicherungen, Vorsorgeuntersuchungen, Tragen eines Helms beim Fahrradfahren. (Das wäre eher eine Schutzmaßnahme, um die Folgen der Unsicherheit zu minimieren: Stichwort Schutzhelm statt Sicherheitshelm). Oder das Vermeiden, eben auf Alpinskifahren verzichten, sich das Rauchen abgewöhnen.

Die Maslowsche Bedürfnis Pyramide hat auf der untersten Ebene die Grundbedürfnisse wie Nahrung, Kleidung, Unterkunft ausgewiesen. In der zweiten Stufe ist man bereits bei der Absicherung der elementaren Überlebenskomponenten. Diese Betrachtung ist zwar wissenschaftlich umstritten (Menschen sind einfach zu verschieden), aber es trifft doch schon den Kern.

Wie entsteht Unsicherheit?

Meist ist sie einfach da, ungefragt. Wir wissen nur begrenzt was auf uns zukommt. Es gibt Überraschungen, die guten und die schlechten. Man will sicher sein vor bösen Überraschungen. Das geht im Grunde genommen nicht. Da bleibt dann nur die Passivität und selbst die schützt uns nicht.

Die Transformation aus einem sicheren Umfeld zu einem unsicheren kann passieren und hat dann häufig folgende Ursachen:

- Nichteinhalten von Sicherheitsvereinbarungen
- Persönliche Interessen vor offensichtlichen Notwendigkeiten stellen
- Sparen an der falschen Stelle
- Fehlende Einbindung von Experten
- Fehlende Anpassungsfähigkeit an geänderte Strukturen
- Unterschätzung von Einflüssen, Überschätzung von Stabilität, mangelnde Wahrnehmungsfähigkeit
- Eingehen neuer oder unnötiger Risiken

Es gibt Menschen für die ist alles vorbestimmt. Es ist das Schicksal, die Gene, das Glück, das Pech, die Astrologie, Gott. Oder andere sind schuld und man kann nichts machen. Die Politik, die Biographie, die Umstände. Das ist auch eine Strategie der Bewältigung von Unsicherheit und eine sehr persönliche Entscheidung.

INFORMATIONSSICHERHEIT

Die nachfolgenden Betrachtungen beziehen sich auf Unternehmen und Organisationen jeglicher Art. Es ist aber anzumerken, dass für kritische Betriebe und Einrichtungen eine Vielzahl von rechtlichen Vorgaben verbindlich einzuhalten sind und weit über das hier dargestellte hinausgehen. Sinn und Wirksamkeit von Anforderungen aus ASPICE, TISAX, KRITIS, NIS2 etc. sei jedem selbst überlassen zu bewerten. Hier wird nicht darauf eingegangen.

Es geht um schützenswerte Informationen jeglicher Art. Das können die Daten auf dem Server oder dem Laptop sein. Es können die IT Systeme selbst, die Zugangssystem virtuell oder zu den Räumen, oder die Unternehmenskenndaten sein. Die Ansage im Meeting wie und wann gehandelt werden soll. Es kann der Zettel im Papierkorb sein.

Klarheit und Einigkeit darüber, was als schützenswert gilt ist eine Grundvoraussetzung. Das muss jeder draufhaben. Das muss aber auch bedeuten, dass man vertrauen kann, dass etwas nicht als vertraulich gilt, was nicht explizit so ausgewiesen ist. Da darf es keine Selbstverständlichkeiten geben. Hier zählt nur Klarheit. Im Strafrecht StGB (nur referenziert zur Verständlichkeit) ist nur verboten was ausdrücklich mit Strafe belegt ist. Was da nicht drinsteht ist nicht strafbar.
Klarheit erlangt man aber nur, wenn es sehr einfach gehalten ist. Eine simple Betriebsanweisung sollte da reichen. Für den Mitarbeiter, z. B. im Wareneingang wird die Vertraulichkeit der IT Zugangsdaten (intern und extern) und alle ihm zugänglichen Kunden- und Lieferantendaten (extern) hinreichend sein.

<u>Hilfreich sind folgende 2 Grundannahmen zur Informationssicherheit:</u>

- Der Mitarbeiter im Unternehmen kann grundsätzlich ohne Vorsatz nichts falsch machen
- Was ein Mitarbeiter falsch machen könnte, auch Vorsatz und Fahrlässigkeit, wird adressiert, abgesichert und die Regelungen werden auf Einhaltung geprüft

Ein Framework muss als Grundlage definiert werden. Denkbar wäre, bereits existierende Grundlagen zu nutzen (z. B. die 11 goldenen Regeln der TU Braunschweig, das Grundschutzhandbuch, die ISO 27001). Ein ISMS Informationssicherheitssystem mit Rollen- und Verantwortlichkeiten ist zu definieren. Dabei gibt es 2 Betrachtungsmöglichkeiten:

1) Das ISMS als partizipatives System unter Beteiligung aller, inkl. Führungskreis
2) Das ISMS als Expertensystem

Die meisten Unternehmen favorisieren die erste Variante und setzen auf ein System der ISO 27001. Vorteil ist ganz klar, was erwartet wird ist bekannt. In Lieferantenbeziehungen dürfen bestimmte Grundsätze als eingehalten unterstellt werden. Eine unabhängige Stelle überprüft, ob die Anforderungen der Norm einhalten werden.

Vorteile einer Zertifizierung nach ISO 27001

Vertrauen. Hier sind Mindeststandards formuliert und die Zertifizierungsgesellschaft prüft jährlich die Konformität und Einhaltung der Anforderungen. Kunden und Lieferanten wissen wo sie dran sind. Elementare Risiken sind beherrscht. Alle in der Organisation sind sensibilisiert. Das stellt schon einen hohen Wert dar und die Weiterentwicklung und Anpassung darf unterstellt werden.

Kritik an der ISO 27001

Baukasten statt System

Die ISO 27001 dient als Grundlage für ein System. Ist aber kein System sondern ein Set von Anforderungen, ein Baukasten. Folgende Analogie möge erlaubt sein. Der Mensch bildet insgesamt ein kompliziertes und komplexes System. Ein verantwortlicher Mediziner wird Symptome nicht einfach behandeln, sondern wird eine Anamnese durchführen. Also alles was wichtig sein kann hinterfragen oder durch Untersuchungen ermitteln. Allergien, bekannte Erbkrankheiten in der Familie, Vorerkrankungen, Substanzmissbrauch, Arbeitsbelastung und vieles mehr. Ergebnis ist eine Gesundheitsakte, die natürlich vertraulich ist. Darauf aufbauend kommt der Therapieansatz, Stressabbau, Gewichtsreduzierung, was eben Erfolg verspricht, und auf lange Sicht hilft. Verhaltensänderung und Medikamente im ausgewogenen Verhältnis.

Bei Informationssystemen nach einer Norm fehlt die Individualität, die Historie, die Eingebundenheit in die Gesamtorganisation. Des Weiteren ist die Vertraulichkeit (Stichwort Gesundheitsakte) anzuzweifeln.

Gerne spricht man von einem gesunden Unternehmen. Produkte sind wettbewerbsfähig, Liquidität gesichert, die Mitarbeiter machen ihren Job gerne. Lieferanten werden fair behandelt. Kundenbindungen verlässlich. Langfristig hat das Unternehmen eine “sichere“ Zukunft und ist robust genug für Krisen verschiedenster Art. Informationssicherheit ist immer auch mit der vorhandenen, allgemeinen Unsicherheit des Unternehmens verbunden.

Fokusierung auf die falschen Themen

Bedingt durch die high level structure HLS der Norm wird eine Struktur vorgegeben die nicht optimal sein kann, weil sie auch für Managementsysteme für Qualität, Arbeitssicherheit und Umweltschutz passen muss

Politik, Ziele

Wozu? Die Politik ist entweder zu allgemein, damit ohne Substanz. Oder konkret und wird bei „Schlechtwetterlagen“ nicht gelebt. Ziele dürfen, anders als Standards verfehlt werden. Zielebasierende Systeme sind damit per se unsicher. Warum sind Standards besser als Ziele? Standards sind verbindlich und damit verlässlich

Partizipativ statt Expertengetrieben

Es ergibt einfach Sinn, das Thema an Experten zu übertragen. Der operative Mitarbeiter, z. B. im Vertrieb, soll sich zu 100% auf seinen Job konzentrieren können

Offenlegung der Sicherheitsstrategie

Da fehlt das überraschende Moment. Man sollte zu einem gewissen Grad „unberechenbar“ bleiben, Vertrauen und Kontrolle im gesunden Einklang

Unklare Festlegung zur Finanzierung von Sicherheit

Wie stelle ich sicher, dass alles Erforderliche auch beschafft wird. Wie stelle ich sicher, dass das richtige beschafft wird. Wie stelle ich sicher, dass das erforderliche Know how im Unternehmen

vorhanden ist. Wie schaffe ich es, nicht über das Ziel hinauszuschießen und Effizienz und Effektivität verloren gehen

Vertrauen und Selbstverantwortung
Zunächst hat jeder Mitarbeiter Anspruch auf einen Vertrauensvorsprung, ohne Vertrauen läuft nichts. Selbstverantwortung ist von allen Mitarbeitern einzufordern. Kling nicht sehr modern, ist aber die Grundlage einer Zusammenarbeit

Anregungen zu einem wirksamen ISMS

Framework mit allen notwendigen Informationen zur Architektur, Attributen und Standards (statt Zielen) Verfahren, Menschen und Technik /IT Landschaft. Passend zum Unternehmen. Festlegung von Regelungen die notwendig sind, und nur solche

Einfach statt kompliziert, nicht alles muss digitalisiert werden, „das Große aus dem Kleinen entwickeln“, skalieren, Einfachheit und Wirksamkeit widersprechen sich nicht

Budgetplanung nicht alle Wünsche können erfüllt werden aber hier liegt der Kern der Wirkfähigkeit

Experten wie werden sie gewonnen, wie werden sie gehalten, wie kann ich ihnen vertrauen

Überraschungspotential (im gesetzlichen Rahmen), wer mit EL AL (israelische Fluggesellschaft) reist wird nie erfahren wie er zu allen Sicherheitsbelangen überprüft wird

Interne Audits / möglichst täglich mit unterschiedlichen Schwerpunkten. TOYOTA führt tägliche QS Audits durch und ist erfolgreich

Whistle blower? Vertrauen ist gut Kontrolle ist besser (Lenin)

Kommunikation und Meetings, werden praktisch in allen Organisationen als Last erlebt, das muss nicht sein, das darf nicht sein

Über den Autor

Wolfgang von Fuchs-Nordhoff, Dipl. Ing Feinwerktechnik, geb. 1956, wohnhaft in Borna bei Leipzig, verheiratet, 2 Söhne in Chemnitz und Berlin, … Läufer, Golfer, Camper
<www.fuchs-nordhoff.de>

Wichtige Stationen:

- 27 Jahre bei TÜV SÜD, Auditor für Qualität, Umwelt, Energie und Informationssicherheit, weltweite Tätigkeit mit Schwerpunkt Fahrzeughersteller und deren Lieferanten, 1st and 2nd tier (Bewertung nach IATF)
- Projektmanager der Firma Gieseke & Devrient bei der Federal Reserve Bank in Baltimore USA
- Zertifizierungsauditor nach BS 7799 und ISO 27001 Deutschland und Italien
- Mitglied bei Plattform Menschen in komplexen Arbeitswelten e. V.