# Worthülse oder grosser Nutzen?

Integrale Sicherheit – ein vielversprechender, moderner Ausdruck für ein umfassendes Sicherheitsmanagement. Aber wofür und mit welchem Ziel sollte eine Organisation ihre Sicherheitsanstrengungen integral verstehen und lenken? Was heisst das? Welches ist konkret der Nutzen für das Unternehmen?

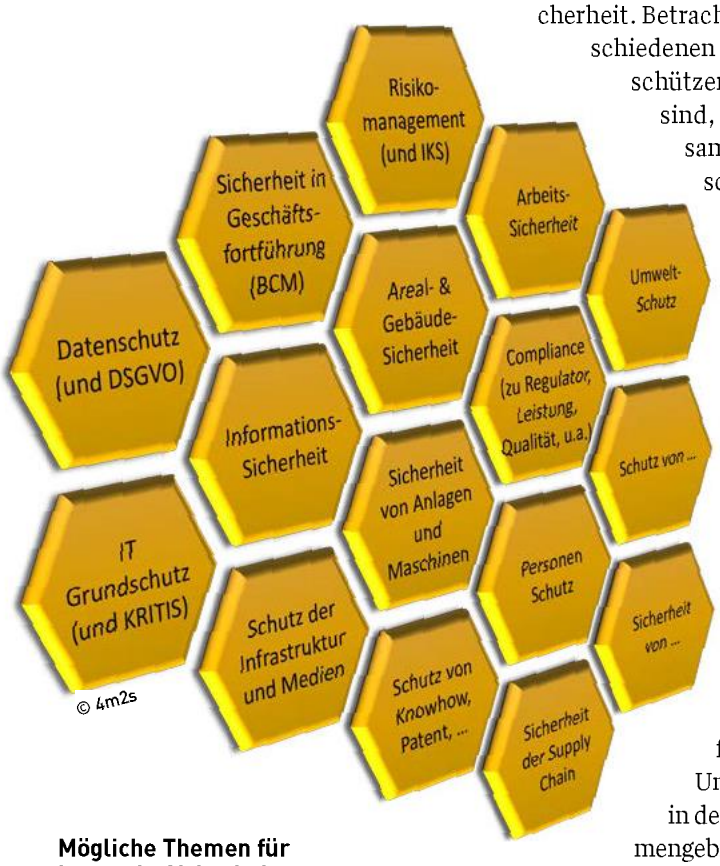
**Almut Eger**

Integrale Sicherheit ist ein starker Begriff. Aber auch schwammig, wenn der Begriff Sicherheit inflationär verwendet wird. Denn erstens: Alles zu integrieren löst Probleme nicht. Und zweitens: Was gehört denn zur Sicherheit, was nicht? Wann kann integrale Sicherheit Probleme lösen helfen?

Sicherheit bedeutet den Zustand eines Nicht-bedroht-Seins und Geschütztseins vor Gefährdung respektive der Freiheit der ungestörten Eigenentwicklung (vgl. Duden). Es geht also einerseits um die materiell via Personaleinsatz oder technische Mittel herstellbare Sicherheit (=Security), andererseits um eine betrieblich herstellbare Sicherheit via Verhalten, Prozesse und Vorkehrungen (=Safety).

## Einheit gesamthaft, umfassend schützen

Integral bedeutet gemäss Duden «zu einem Ganzen dazugehörend und es erst zu dem machend, was es ist». So haben wir die starke Anforderung für integrales Sicherheitsverständnis: Der Begriff integrale Sicherheit steht für ein integrales Verständnis der Anforderungen an Sicherheit. Betrachtet werden also die verschiedenen Aspekte, die für eine zu schützende Einheit wichtig sind, da diese Einheit gesamthaft, umfassend geschützt werden soll. Oder anders ausgedrückt – wir möchten die Themen kennen, die zur Unsicherheit dieser Einheit führen.




**Mögliche Themen für integrale Sicherheit.**

Die integrale Sicherheit einer Unternehmung kann sich also aus den unterschiedlichsten Themen zusammensetzen – mit dem Hauptziel: Sie leisten einen Beitrag zur effektiven und nicht nur zur gefühlten Sicherheit in der Unternehmung. Und wenn in der Folge beispielhaft Themengebiete genannt werden, die des Öfteren der integralen Sicherheit zugeordnet werden, so bedeutet dies, dass in diesen Themen die Frage nach der Kritikalität gestellt werden muss: Weshalb und wo ist Sicherheit so wichtig? Und sprechen wir von sicherem Funktionieren eines Prozesses? Vom immer vollständigen Vorhandensein einer Ressource? Und so weiter. Anzumerken gilt: Die effizienteste Methodik, um diese Fragen zu klären, ist die erste Stufe eines Business-Continuity-Management-Systems: Kritikalität eruieren auf der Stufe der strategischen Unternehmens- und Prozesseinheiten, Ressourcen und kritischen Abhängigkeiten.

## Beispiel Infrastrukturbereich

Welche Sicherheit braucht beispielsweise der Standort L? Die erste Frage im Sinne der integralen Sicherheit ist nun: Was macht den Standort L kritisch und weshalb? Die Antwort: Der Standort L ist kritisch wegen der spezifischen Fertigungseinheit, die in eine Just-in-time-Produktion gegenüber den Kunden eingebunden ist. Die Maschinen zu transferieren bedeutet einen Aufwand von drei Tagen – das ist mit dem Kundenversprechen nicht vereinbar.

Folglich verdient der Standort L eine Betrachtung im Sinne der integralen Sicherheit, um alle Ebenen der baulichen Sicherheit, Organisation (Prozesse, Maschinen, Personen, Know-how, Zulassungen etc.) und Compliance richtig kombiniert verstehen und bearbeiten zu können.

## Beispiel ICT, Informations- und Kommunikationstechnologie

Welche Sicherheitsvorkehrungen braucht die ICT-Infrastruktur in der Firma S? Ihre IT-Infrastruktur ist so ausgestaltet, dass

der Zugang zu Daten remote gesichert ist. Das heisst, ein Ausfall einer Datenleitung oder eines Internet-Providers blockiert keine Arbeit mehr. So viel zur Theorie.

Die Praxis zeigt ein anderes Bild: Ein Cyberangriff hat den Server 1 befallen, worauf Server 2 sich wie geplant aus der Update-Kette rausnahm, um nicht auch infiziert zu werden. Der Informationszufluss für die Verarbeitung von Aufträgen erfolgte aber nach wie vor auf Server 1, die Verarbeitung der Lieferungen auf Server 2. Nur kommunizierten die beiden nicht mehr miteinander. Die Folge waren falsch konfektionierte Aufträge (was von den Mitarbeitenden nicht bemerkt wurde), vertauschte Kunden- und Produktdaten (wurde ebenfalls nicht bemerkt), unterbrochene Lieferketten (bereits nach drei Stunden, wurde von Kunden und Mitarbeitenden gleichzeitig bemerkt).

Das Unschöne und Kritische an der Situation war somit nicht nur der Tatbestand der Fehllieferungen, sondern auch derjenige, dass es so spät und nicht vor den Kunden bemerkt wurde. Nötig waren also Massnahmen auf mehreren Stufen – und somit wurde auch das Thema Sicherheit neu definiert: Die Sicherheitsanforderungen an die Informationstechnologie wurden in Koordination mit den Anforderungen an die Organisation und Abläufe, an Anforderungen zur sicheren Verarbeitung (Qualitäts- und Vendor-Management) gekoppelt. Dabei wurden auch Prozesse mit Controlling-Funktionen in der Verarbeitung von Aufträgen angepasst. Weiter wurden Compliance-Fragen bearbeitet, damit die Verarbeitung der Lieferungen auch aus dieser Sicht sicher, weil rechtens abläuft.

Integrale Sicherheit vereint also nicht immer nur Themen gleicher Gattung (wie beispielsweise physische Sicherheit mit Gebäude- und Areal- und Brandschutzfragestellungen), sondern es gilt der umgekehrte Blickwinkel: Welche unterschiedlichen Sicherheitsanforderungen müssen ineinandergreifen können, damit der Schutz einer Leistung rundum als gesichert gelten kann?

## Beispiel Arbeitssicherheit

Reicht es aus, die gesetzlichen Vorgaben zum Schutz der Mitarbeiter vor Unfällen den Teamleitern meiner Unternehmung T mitzuteilen und sie auf ihre Führungsaufgabe zu deren Einhaltung anzusprechen?

Man sollte meinen, das sei ausreichend. Die Praxis zeigt aber, dass alle Vorkehrungen zur Arbeitssicherheit nur so gut sind, wie sie auch von der Belegschaft akzeptiert und respektiert werden. «Eine PSA (Persönliche Schutzausrüstung) zu tragen ist zwar Ehrensache und es steht im Arbeitsvertrag respektive in der Arbeitsanweisung – aber die PSA ist nervig und viel zu heiss und unbequem. Also lasse ich sie ausnahmsweise weg.» Welche Führungskraft kennt diese Ausreden nicht?!

Antwort: Das Tragen einer PSA ist keine Ehrensache, sondern die persönliche Rückversicherung, dass im Falle eines Fehlverhaltens der Person, des Materials, der Maschine etc. keine allzu gravierenden Verletzungen entstehen. Dass die PSA getragen wird, ist also definitiv eine Führungsaufgabe und hat sehr viel mit Vorbildfunktion, Führungs- und Feedback-Kultur zu tun. Wer Arbeitssicherheitsmassnahmen wirkungsvoll umsetzen will, muss also bei der Führungskultur und dem Verständnis der Aufgaben einer Teamleitung ansetzen. Es ist eine Führungsaufgabe zu erreichen, dass jede und jeder ihren/seinen persönlichen Beitrag zu unfallfreiem Arbeiten kennt. Und somit liegt der Fokus auf der bestimmungsgemässen und unfallfreien Ausführung einer Arbeit.

Unter dem Aspekt der integralen Sicherheit kommen noch weitere Punkte dazu:

*Recht und Compliance:* Die aus rechtlicher Sicht nötige Sicherheit, dass eine Arbeit ausgeführt werden darf. Beispielsweise schreibt der Regulator vor: a) eine bestimmte Ausbildung; b) dass bestimmte Sicherheitszertifikate für Material, Mensch und Maschinen vorliegen müssen; c) dass für einen Arbeitsschritt immer eine bestimmte betriebsinterne Person vor Ort sein muss etc.

*Gesundheitsschutz:* Das Einhalten von Ruhezeiten bedingt einen anderen betrieblichen Aufbau (z.B. Schichtbetrieb, aktives Bearbeiten von Stressmanagement, Monotonie u.a.)

*Zutrittsschutz:* «Unbefugten ist das Betreten der Baustelle untersagt.» Zu definieren, wer «unbefugt» ist, bedingt die Absprache aller Beteiligten, das ist der einfachere Teil. Das Durchsetzen der definierten Einschränkungen ist meist kostspielig und mit weiteren Aufwänden und Absprachen verbunden, die dann zur Frage zurückführen: Weshalb soll ich wann und wo was schützen? Und wovor – vor Unfällen, Diebstahl, Spionage, Fehlleistung oder gar Manipulation?

Und die Anschlussfrage lautet: Wer ist für welchen Schutz verantwortlich und was kostet es, was bringt es? Warum sollte ich etwas tun respektive sollte ich nichts tun?

## Beispiel Datenschutz

Der Aspekt DSGVO war vor allem 2019 in aller Munde – es wurde diskutiert, wie viel Datenschutz wo und wann und wozu angebracht sei.

Deshalb die Frage: Bezieht sich Datenschutz in meiner Unternehmung V nur

### MIT METHODIK INTEGRALE SICHERHEIT ERLANGEN

Ereignisse wie ungeplante IT- und Telekommunikationsausfälle, Cyberattacken, Datenlecks oder Covid-19 werden Unternehmen immer wieder stark beschäftigen. Das Auftreten solcher Ereignisse kann immer weniger gesteuert werden, die Auswirkungen hingegen sehr wohl. Was es dazu braucht, ist die Kenntnis zu den unternehmenseigenen Stärken und heiklen Punkten in den Prozessen, Ressourcen und Abhängigkeiten intern und extern.

Mit der Methodik des Business Continuity Managements (BCM) kann die geforderte Klarheit im Sinne der integralen Sicherheit erlangt werden:

1. Über Kritikalitätsanalysen die möglichen risikobehafteten Prozesse und Ressourcen, unabhängig von Risikofaktoren, kennen (wo ist das Unternehmen verletzlich und zu wenig geschützt?)
2. Mit der Ausarbeitung von entsprechenden Business-Impact-Analysen die Gründe und Abhängigkeiten kennen (weshalb und wann ist das Unternehmen verletzlich resp. zu wenig geschützt)
3. Mit Business Recovery und Continuity entsprechende Pläne für Resilienz bereithalten (Aufrechterhalten der Leistung), Reaktion (Notfallpläne) und Wiederanlauf (wie schützt sich die Firma vor Leistungsabfall resp. wie gestaltet man den Wiederanlauf?)
4. Mit Tests und Übungen und einem Review im Zyklus des Plan-Do-Check-Act (Demingkreis von W.A. Shewhart) für die regelmässige und kontinuierliche Überprüfung (ist am richtigen Ort das Richtige getan respektive vorbereitet?)

auf Personendaten oder muss ich das weiter fassen – wozu ich keine gesetzlichen Vorgaben sehe?

Integrale Sicherheit für Datenschutz bedeutet, die adäquate Kombination aus Umgang mit Daten, Compliance in Verträgen und im Verhalten, Kenntnis zu den internen und externen Einheiten, die heikle Personendaten beziehen, generieren oder verwalten, zu kennen. Somit muss ich zur Klärung der Frage erkennen, weshalb wo Informationen zugänglich sein sollen oder eben nicht. Das betrifft bezüglich DSGVO, also der rechtlichen Vorgaben, wohl nur die Personendaten; die Umsetzung in den Unternehmen verlangte aber nach einer breiteren Betrachtung: Beispielsweise ist allgemein bekannt, dass mit einer guten Zutrittskontrolle zu Büroräumlichkeiten und Fertigungseinheiten die im Unternehmen vorhandenen respektive generierten Informationen vor direkten Zugriffen geschützt werden können. Firewalls, Passwortschutz, richtiger Umgang mit Daten etc. sind die Pendants dazu für die digital vorhandenen Informationen. Somit gehören alle diese Themen zur integralen Sicherheit für den Schutz von Daten.

Antwort: Die Unternehmung V hat für die integrale Sicherheit von Daten folgende Themen zusätzlich involviert:

*Erstens:* Datenschutz und Informationssicherheit sind für die Unternehmung V nicht sinnvoll trennbar. Das heisst: Die gesetzlichen Vorgaben zum Schutz von Personendaten sind vollumfänglich einzuhalten. Ergänzend ist der Unternehmung daran gelegen, den Umgang mit Daten und personen-, da kundenbezogenen Daten generell besser abzusichern, um alle Compliance-Vorgaben einzuhalten, nicht nur jene der DSGVO. Somit hat das Unternehmen V ein Informationssicherheitsmanagementsystem nach ISO 27001 eingeführt. Die Fehler, wie sie in den Jahren davor immer wieder aufgetaucht sind und zu heiklen Situationen, auch für die Kunden, geführt hatten, sind seither nicht mehr passiert.

*Zweitens:* Clean Desk Policy für alle oder nur, wo nötig? Würde die Clean Desk Policy nur für einen Teil der Arbeitsplätze eingeführt, hätte das ergänzende bauliche Massnahmen zur Folge. Es hat sich deshalb als sinnvoller und pragmatischer erwiesen, die Clean Desk Policy flächendeckend einzuführen.

> «Integrale Sicherheit heisst verstehen, wofür spezifische Sicherheitsvorkehrungen nötig sind, welche das sind und wie sie koordiniert gemanagt werden können.»

*Drittens:* Das Unternehmen V hat es zur Führungsaufgabe der Teamleitungen gemacht, eine positive Feedback-Kultur zu leben. Es wurde ein Melde-Tool eingeführt, mit dem alle Mitarbeitenden melden, wenn ihnen heikle Situationen auffallen. Das Tool wird auch zwei Jahre nach der Einführung immer noch genutzt – weil man es geschafft hat, dass die Teamleitungen gute Feedback-Kultur zu ihrer Aufgabe zählen; das bedeutet aktiv gelebte Sicherheit.

## Querverbindungen zwischen einzelnen Disziplinen herstellen

All diese Beispiele machen klar, dass integrale Sicherheit heisst, Querverbindungen zwischen den einzelnen Disziplinen herzustellen, die sonst je für sich ihren guten Beitrag zur Sicherheit leisten. Denn kombiniert erbringen diese Disziplinen einen Skaleneffekt, der zum Nutzen aller mehr Effizienz und Effektivität in die gelebte Sicherheit im Alltag einbringt.

Der Beispiele gäbe es viele. Sie alle haben folgende Grundsätze und Anforderungen gemeinsam:

1. *Wo ein Schutzbedarf nötig ist, sollte über integrale Sicherheit nachgedacht werden:* Doch erst muss eine Unternehmung kennen, was kritisch und heikel ist, wo und warum deshalb ein Schutzbedarf hergestellt werden soll und welche Themen und Einheiten für diesen Schutzbedarf koordiniert werden sollen.
2. *Adressieren an involvierte Unternehmenseinheiten:* Die «eierlegende Wollmilchsau» war gestern. Integrale Sicherheit kann nicht von einer (1) Stelle geleistet werden, sondern bedeutet, die relevanten Know-how-Träger koordiniert wirken zu lassen: Erwartungen an einen Schutzbedarf abgleichen und integral entwickeln, Schutzmassnahmen koordiniert umsetzen.

## Fazit

Für die integrale Sicherheit einer Unternehmung müssen also die Risiken einerseits, die kritischen Erwartungen an die Leistungserbringung mit den dazu zwingend erforderlichen Prozessen, Vorgaben sowie internen und externen Ressourcen andererseits bekannt sein.

Aus diesen Erkenntnissen leitet sich dann der Schutzbedarf ab und damit das Wissen, wo, was, warum und mit welchen Mitteln respektive Massnahmen und Akteuren geschützt werden soll.

Das Management der integralen Sicherheit kann gesamthaft, quasi als Schirm über alles, sowie fokussiert auf den spezifischen Schutz von Werten, kritischen Prozessen, Ressourcen und Abhängigkeiten betrieben werden. Der Nutzen: ein schlank aufgestellter Schutz, mit dem die relevanten Themen koordiniert, organisiert und gesteuert werden können. ■

ALMUT EGER

Senior Consultant und Trainerin für Notfall-/Krisenmanagement, BCM und ISMS bei 4m2s – 4 Management 2 Security, Zürich und Frankfurt. Auditorin für TÜV Rheinland Cert.