Sicherheit. Mehrwert. Marktwirkung.

Wie ein ISMS seine Wirkung entfalten kann

Autor: Dr. Michael Wolfensberger, Joël Bühler

Die Fähigkeit, die eigenen Dienstleistungen mit angemessenen Massnahmen der **Sicherheit** zu schützen **ist** mittlerweile nicht mehr nur **Grundvoraussetzung für nachhaltigen wirtschaftlichen Erfolg,** sondern hat sich tatsächlich zu einer **Überlebenskompetenz** herausgebildet**.** Die **Vielzahl der Angriffe** auf alle nur erdenklichen Betriebe und Organisationen, die mit dem Internet verbunden sind, **hat derart zugenommen**, dass es einfach **nur eine Frage der Zeit** ist, **bis es zu einem Angriff kommt.** Wenn eine Organisation von so einem Angriff **auf dem falschen Fuss** erwischt wird, dann **kann es** nicht nur sie selbst, sondern **mit ihr auch sämtliche Kund:innendaten und -informationen treffen** und kompromittieren. Die Angst um die eigenen wie um die Kund:innendaten ist also begründet.

Die **Sicherheit der Unternehmung und ihrer Kund:inneninformationen** muss also bestmöglich sichergestellt sein. Das **Vertrauen der Kund:innen** in diesen Schutz ist eine wichtige Zielgrösse für Angebotsqualität und Absatz der Services am Markt. Damit haben das ISMS und das **ISO 27001-Zertifikat** als objektiver Nachweis der Sicherheit einen **enormen Stellenwert für jede:n Dienstleister:in und Produzent:in.**
Um einen angemessenen Schutz aufzubauen und am Markt auch nachweisen zu können, ist eine **Zertifizierung oft unverzichtbar**. Ohne sie ist der Markt oft nicht mehr bereit, Dienstleistungen bei IT-Servicedienstleistern und technischen Zulieferern einzukaufen, denn die **allgegenwärtige Verfügbarkeit von Informationen** stellt auch eine **allgegenwärtige Gefährdung** dar. Die Verantwortlichen brauchen ein **verlässliches Bild über Wirksamkeit und Zuverlässigkeit des Informationsschutzes**. Die **transparente Kenntnis** über den Stand der Systeme, Schutzobjekte, Gefährdungen und laufenden Massnahmen hilft, an den entscheidenden Stellen **gezielt Massnahmen** zu ergreifen, die **bedarfsorientiert, kostenwirksam und ergebnisorientiert** den gewünschten Stand der Sicherheit herstellen - und beibehalten. Um dies erfolgreich und gesichert umzusetzen, braucht man ein Informations-Sicherheits-Management-System, das innenwirksam Rahmen und Orientierung für die Sicherheit bildet und das aussenwirksam auch zertifiziert werden kann.

ISMS – Informationssicherheit systematisch managen

Ein funktionierendes Informations-Sicherheits-Management-System (ISMS) nach ISO 27001 bietet angemessenen Schutz. Es ermöglicht mit angemessenen, organisationsspezifischen Policies und Regelungen den Schulterschluss zwischen Führungsetage, Mitarbeiter:innen, Lieferant:innen und Kund:innen einer Organisation.

Ein ISMS schützt durch organisierte Sicherheit als Verbund-System von Massnahmen und Methoden, die - wenn sie eingehalten werden - in ihrer Gesamtheit und Kombination in allen organisatorischen Bereichen verlässlich gegen die meisten Bedrohungen im Bereich IT wirken.

Wie wirkt ein ISMS?

Das gesamte ISMS folgt dem Deming-Zyklus: Plan-Do-Check-Act (PDCA).

Mit diesem für ISO-Modelle wie auch für alle anderen gemanagten Sicherheits-Systeme (NIST, VdS, ISSS etc.) gültigen Standard wird wiederkehrend der folgende Prozess durchlaufen:

- Planen, was notwendig ist
- Umsetzen, was geplant wurde
- geprüft, ob die geplanten Ziele erreicht wurden

- und letztlich festgestellt, was man im nächsten PDCA-Zyklus besser machen könnte.

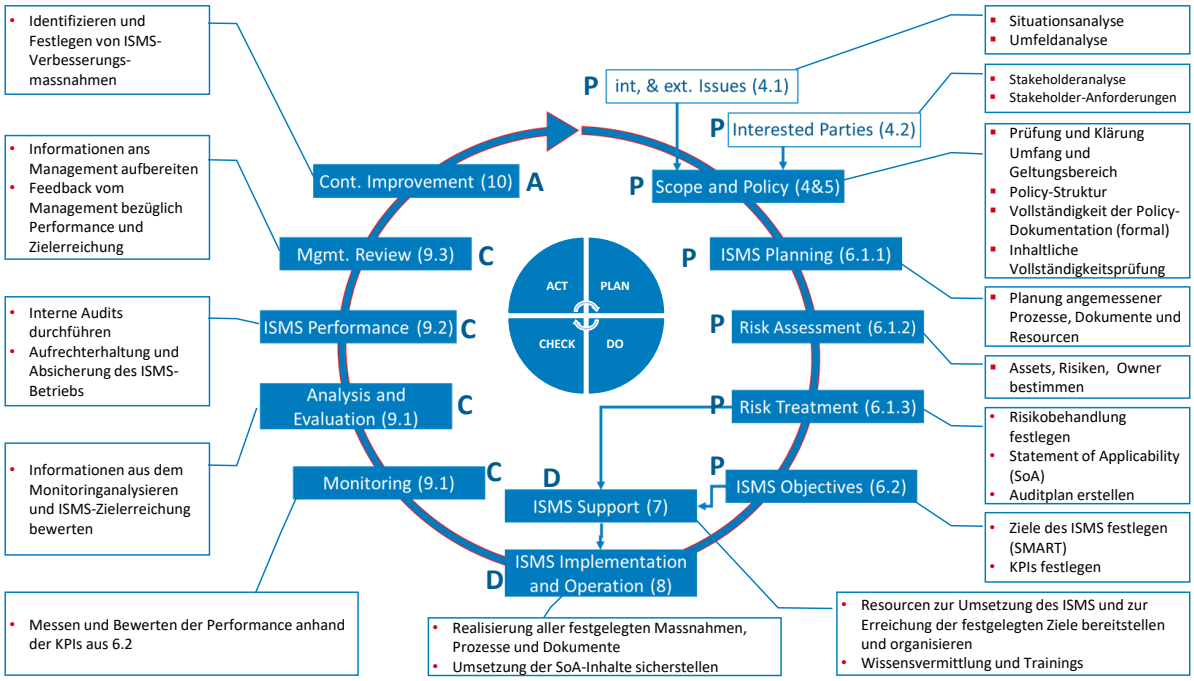
So ist kontinuierliches Lernen und Verbessern in allen Bereichen ein wesentlicher Teil eines ISMS. Die Orientierung an der Norm ISO 27001 bewirkt dabei einfach, dass kein Aspekt der Sicherheit bei Implementierung, Betrieb und Verbesserung des Systems vergessen geht. Dabei sind nicht nur technische Aspekte wesentlich, sondern auch Massnahmen, die die notwendige Disziplin aller Beteiligten im Tagesgeschäft wie auch im Notfall fördern.

Die wesentlichen Resultate des Schutzes durch ein ISMS sind:

- Hoheit über die informationelle Selbstbestimmung der Organisation
- Einhaltung von gesetzlichen Bestimmungen und branchenorientierten Obligaterien
- Wirksame Kontrolle über wichtige und (überlebens-)kritische Daten und Informationen der Organisation
- Wahrung von produkt- und verfahrensbasierten Alleinstellungsmerkmalen
- Aufrechterhaltung der Produkt- und auch der Markenqualität
- Absicherung des wirtschaftlichen Erfolgs
- und damit last, but not least: sichere Arbeitsplätze und sicheres Einkommen

Mit einem aktiven und funktionierenden ISMS erfüllt man nicht nur interne und externe Vorgaben. Es stärkt die Glaubwürdigkeit nach aussen und lässt sich beispielsweise über eine Zertifizierung durchaus als werbewirksames Aushängeschild am Markt nutzen.

Wie baut man ein ISMS auf?



Auch in Aufbau und Pflege eines ISMS führt kein Weg am Deming-Zyklus vorbei. Es wird geplant, getan, geprüft und gelernt.

[PLAN]
Bei der Planung eines ISMS ist grundsätzlich Augenmass gefordert, denn zu wenig Schutz ist nutzlos, zu viel Schutz stranguliert Tagesgeschäft und Geldbeutel. «Angemessen» und «organisationsspezifisch» sind hier die Zauberworte.

Zu Beginn wird eine Situations- und Stakeholder-Analyse gemacht, in der festgestellt wird, welche Sicherheitsansprüche überhaupt von wem an die Organisation gestellt werden.

Auf dieser Basis werden Geltungsbereich und Umfang des Sicherheitssystems festgelegt und die - für alle Stakeholder gültigen - Policies erstellt. Die Informations-Sicherheits-Policy ist dabei das Statement der Führung, Zeit und Mittel zur Verfügung zu stellen, um ein ISMS zu betreiben und so angemessene Sicherheit zu gewährleisten.

In einem nächsten Schritt werden die für die Sicherheit notwendigen Prozesse mit ihren Ressourcen und Dokumenten festgelegt.

In der Folge werden die Schutzobjekte, deren Risiken und die notwendigen Vermeidungs- und Bewältigungsmassnahmen identifiziert und geplant. Damit hat man einen Überblick über das notwendige Ausmass des Schutzes, der vom ISMS gewährleistet werden soll. Nun werden die konkreten Ziele des ISMS und die zur Kontrolle der Zielerreichung notwendigen Kennzahlen festgelegt.

[DO]
Das ISMS wird implementiert und betrieben. Alle geplanten Massnahmen im Sinne von Weisungen, Prozessen, Technik und Dokumenten werden in der Organisation verankert und im Tagesgeschäft genutzt.

[CHECK]
Die in der Planung festgelegten Kennzahlen werden zur Kontrolle der Zielerreichung im Tagesgeschäft gemessen und bewertet. Interne Audits stellen sicher, dass Weisungen, Regeln und Prozesse eingehalten werden. Die Ergebnisse der Messungen, Audits und Kontrollen werden aufbereitet und zur Information und Erfolgskontrolle dem Management weitergeleitet.

[ACT]
Die Ergebnisse der Verlaufskontrollen dienen der kontinuierlichen Verbesserung. Hier wird der Anpassungsbedarf in verschiedensten Bereichen des ISMS identifiziert, der dann in die nächste Planungsphase des PDCA-Zyklus eingeht.

Nach der Zertifizierung ist vor der Zertifizierung

Um die Sicherheit im gewünschten Masse aufrecht zu erhalten, muss der Prozess immer wieder durchlaufen werden. Das Motto ist: «dranbleiben, um den Schutz aufrecht zu erhalten.»

- Mit regelmässigen Audits für einzelne Bereiche oder das gesamte ISMS wird geprüft, ob es unbeabsichtigte Ausreisser gibt
- Awareness-Analysen und Sicherheits-Trainings sollen fortlaufend den Sinn und Zweck der Vorschriften vermitteln und so Awareness, Know-how und die stressresistente Compliance der unterschiedlichen Rollenträger:innen ermöglichen (Notfallhärtung)
- technische Überprüfungen stellen sicher, dass sicherheitskompromittierende technische Fehler weitestgehend ausgeschlossen werden können
- Es wird eine sukzessive Feinjustierung der Massnahmen und Auditpläne von Jahr zu Jahr sichergestellt und so eine kontinuierliche Verbesserung und Anpassung an die sich ändernden Gegebenheiten ermöglicht
- Und das Risiko-Management ist ebenfalls ständige:r Begleiter:in

Um den ständigen Änderungen in Technik, Struktur und Umwelt einer Organisation Rechnung zu tragen, muss die Organisation das ISMS und dessen Aktivitäten also immer wieder anpassen, nachbessern und prüfen, ob noch alles zum Besten bestellt ist.

Und das tun die Zertifizierungsstellen auch. Nach einer Erst-Zertifizierung folgen zwei Aufrechterhaltungs-Zertifizierungen und darauf wiederum eine Re-Zertifizierung. So wird sichergestellt, dass die Organisation in ihrem Bemühen nicht nachlässt.

Die Arbeit am ISMS hört also mit gutem Grund nie auf.

Und das lohnt sich. Denn ein veraltetes, schlecht gepflegtes ISMS vermittelt der Organisation und den Kund:innen einen gefährlich trügerischen Eindruck von Sicherheit.

Quo vadis, ISMS?

Allgemein gesprochen waren Mitarbeiter:innen einer Organisation früher meist in einem Gebäude- oder Bürokomplex untergebracht, mit Abteilungen, die mittels interner Post einen regen Informationsaustausch pflegten, um die Aufgaben zu erfüllen, die im Rahmen der arbeitsteiligen Grundstruktur anfielen. Und die Informationen und Daten waren auch dort, wo die Mitarbeiter:innen waren – an einem Ort. Und Einbrüche fielen hier noch auf.

Das hat sich geändert.

Mit dem aktuellen und von Corona heftig befeuerten Trend zur Digitalisierung, in die Cloud und in Richtung Industrie 4.0 virtualisiert sich auch die Firmenstruktur rasant. Die Mitarbeiter:innen

müssen nicht mehr in einem als «Firma» markierten Gebäude oder Aufenthaltsbereich ihren täglichen Aufgaben nachgehen. Auch «Home-Office» im Sinne von «daheim arbeiten» war gestern. Heute sind und arbeiten die Mitarbeiter:innen wortwörtlich überall. Und dort sind auch ihre Daten. Und die der Kund:innen. Und in dieser virtuellen Umgebung fallen Einbrüche und Diebstähle - ausser bei Ransomware-Attacken - kaum noch auf.

Die Unterstützung, Anleitung und Kontrolle im Umgang mit Daten und Informationen durch ein ISMS ist somit wichtiger denn je, denn speziell bei einer verteilten Organisation wird ein wirksames ISMS als übergeordnete und anerkannte Richtlinie und aktive Verfahrenshilfe im Umgang mit Daten und Informationen zum gemeinsamen Nenner aller Mitarbeiter:innen in Sachen Sicherheit.

Das ISMS begleitet jeden Stakeholder – egal, wohin er geht. Ganz sicher.