mabuco GmbH

Informationssicherheit- und Datenschutz für KMU

Wollen Sie Informationssicherheit und Datenschutz systematisch managen?

Sind Sie sicher, dass Ihre Daten bei Ihnen sicher sind?

Rechtliche Grundlagen

Rechtliche Grundlagen - Begriffe

Informationen

Aufzeichnungen auf Informationsträgern und mündliche Äusserungen.

Informationsträger

Träger von Informationen irgendwelcher Art, namentlich Schriftstücke und Träger von **Text-, Bild-, Ton- oder andere Daten** - Zwischenmaterial, namentlich **Entwürfe**, gelten ebenfalls als Informationsträger.

Quelle: Informationsschutzverordnung, SR510.411 – Personen fehlen in der Definition

Rechtliche Grundlagen - Begriffe

Informationssicherheit (IS)

- Informationssicherheit hat den Schutz von Informationen als Ziel.

- Dabei können Informationen sowohl auf **Papier**, in **Rechnern** oder **auch in Köpfen** gespeichert sein.

Quelle: Bundesamt für Sicherheit in der Informationstechnik Glossar (Deutschland)

Datenschutz (DS)

Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.

Quelle: Bundesgesetz über den Datenschutz (DSG)

Rechtliche Grundlagen - Übersicht

Datenschutzgesetze

Für Unternehmen:

- Art. 13 der Bundesverfassung
- Bundesgesetz über den Datenschutz (DSG)
- Verordnung zum Bundesgesetz über den Datenschutz (VDSG)
- Art. 28-28l Zivilgesetzbuches (ZGB)
  (Schutz der Persönlichkeit)

Für Unternehmen,
welche Daten im Auftrag von Behörden (Kanton Bern) bearbeiten:

- Kantonales Datenschutzgesetz (KDSG)

Die Risiken von aussen

7. Februar 2018 - Swisscom meldet, dass Unbekannte im letzten Herbst Zugriff auf Daten von 800'000 Kunden hatten. Dabei soll es sich um "nicht besonders schützenwerte Personendaten" gehandelt haben.

IT-Konferenz zeigt, wie in Minuten ein Spital gehackt wird

Krankenhäuser sind lukrative Ziele für Hacker. In IT-Sicherheit wird oft nicht investiert. Dabei stehen aber Menschenleben auf dem Spiel. Die Konferenz des Health Tech Cluster in Rotkreuz suchte Lösungsansätze.

Spezialisten des Bundes entdeckten Russen-Muster

Hacker-Angriff auf das VBS!

Die Bundesverwaltung ist erneut Opfer eines Cyber-Angriffs geworden. Das hat der Bundesrat heute bekannt gegeben. Nach seinen Angaben galt der Angriff dem Verteidigungsdepartement VBS. Es wurden zwei Strafanzeigen gegen Unbekannt eingereicht.

Was ist der Nutzen?

Die Risiken von innen

BUNDESSTRAFGERICHT

Mehrjährige Freiheitsstrafe für Datenklau: UBS-Banker verkaufte Kundendaten an Nordrhein-Westfalen

Da staunte Datenschutz-Anwalt Martin Steiger

Migros verschickt fremde Cumulus-Informationen

Pascal Tischhauser — 20:02 Uhr 09.04.2018 — 01:14 Uhr 01.10.2018

Internetanwalt Martin Steiger wollte wissen, was für Daten die Migros über ihn im Cumulus-Bonusprogramm gesammelt hatte. So forderte er diese beim orangen Riesen an. Doch die Migros schickte ihm nicht bloss seine Daten, sondern auch die einer wildfremden Person.

Datenklau beim NDB

20 Monate bedingt für Ex-Computerexperten

Ein Computerexperten, der im Nachrichtendienst des Bundes (NDB) grosse Mengen an gehei
bedingt verurteilt worde
Jahre Haft.

Der Informatiker hat **grosse Mengen von geheimen Daten kopiert** und zu sich nachhause geschafft.

Als er ein Nummernkonto bei einer Bank eröffnen will und erwähnt, dass er eine Million Franken wegen eines **Datenverkaufs** erwartet, fliegt er auf.

WikiLeaks

Integrale Sicherheit

Integrale Sicherheit

Personen-Sicherheit

Informations-Sicherheit

Sicherheit von Sachwerten (Assets)

Umweltsicherheit

A) Informationsschutz
- Klassifizierung und Schutzbedarf
- Zugang, Zutritt, Zugriff
- Verfügbarkeit, Integrität
- Prüfung, Kontrolle, Nachweise

B) Informatik-Sicherheit
- Sicherheitszonen
- Schutz der IKT-Mittel
- Umgang mit IKT-Mittel
- Test, Prüfung, Nachweise

C) Datenschutz
- Einhaltung der Rechte Betroffener
- Verbindlichkeit, Vertraulichkeit
- Prüfung, Kontrolle, Nachweise

powered by mabuco GmbH

Ihr Nutzen?

Mit der Umsetzung einer angemessenen Informationssicherheit sind Sie fit für

- die Umsetzung einer wegweisenden Digitalisierungsstrategie und Transformation, welche bestehende Geschäftsfelder unterstützt.
- die Implementierung neuer Geschäftsfelder und Arbeitsformen in Ihrer Unternehmung.

➢ weil Sie wissen, **wo, wann, welche, wie und in welcher Form Ihre Informationen** verfügbar und verarbeitbar sind.

Ihr Nutzen?

Mit der Umsetzung einer angemessenen Informationssicherheit sind Sie fit für

- die konsequente Nutzung der vorhanden Verbesserungspotentiale sowie zur Vermeidung und Schliessung von Schwachstellen.
- die Verbesserung bei der Anforderungsdefinition für neue Anwendungen und damit einer Erhöhung der Qualität bei ICT-Beschaffungsverfahren.

➢ **weil Sie wissen, wo Ihre Stärken und Ihre Schwächen sind und sich dadurch kontinuierlich verbessern können und somit "FIT für die Unternehmung 4.0" sind.**

Ihr Nutzen?

Mit der Umsetzung einer angemessenen Informationssicherheit sind

- Sie sich der Kritikalität der Daten und Informationen in Ihrer Unternehmung bewusst, was für künftige Umsetzungen von Digitalisierungsprojekten von enormen Vorteil ist.
- Sie für Ihre Partner und für neue Dienstleister bezüglich der Vertraulichkeit der (externen) Datenbearbeitung eine verbindliche und berechenbare Unternehmung – heute und morgen.

➢ **weil Sie wissen, welche Massnahmen Sie wo umsetzen müssen, damit sich Kunden und Partner auf Sie verlassen können**

Ihr Nutzen?

Mit der Umsetzung eines anerkannten Schutzes der Privatsphäre (Datenschutz) sind Sie fit für

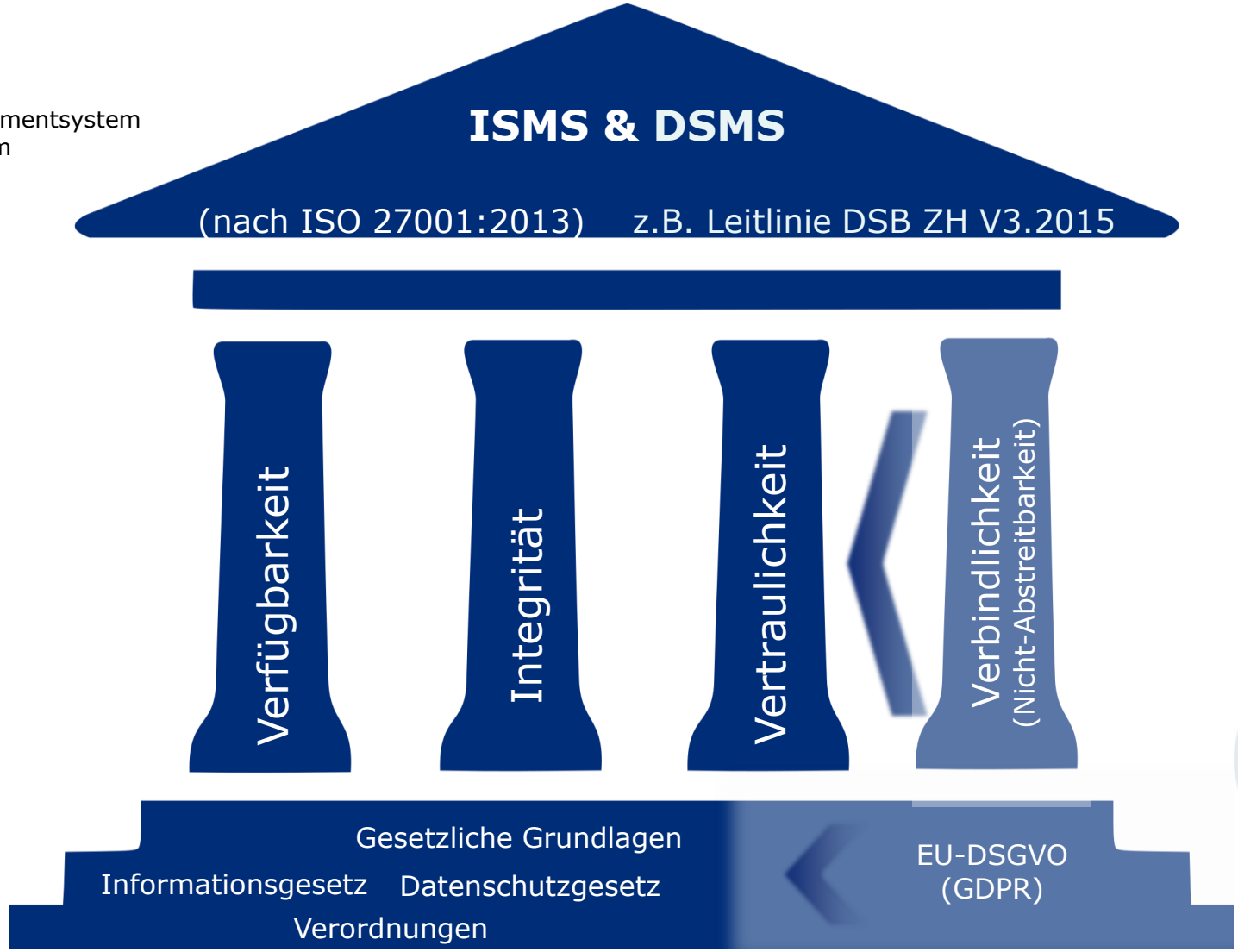
- die Umsetzung einer wegweisenden Digitalisierungsstrategie und Transformation, bei welcher Datenschutz zukunftweisend und transparent für Ihre Kunden umgesetzt wird.
- neue Geschäftsfelder und Arbeitsformen, welche auch im europäischen Raum denkbar und rechtssicher umsetzbar werden.

➢ **Weil Sie sich mit kommenden Fragestellungen zur Privatsphäre frühzeitig befassen und somit in bestehenden wie auch zukünftigen Märkten an Rechtssicherheit gewinnen**.

Säulen von Schutzkonzepten

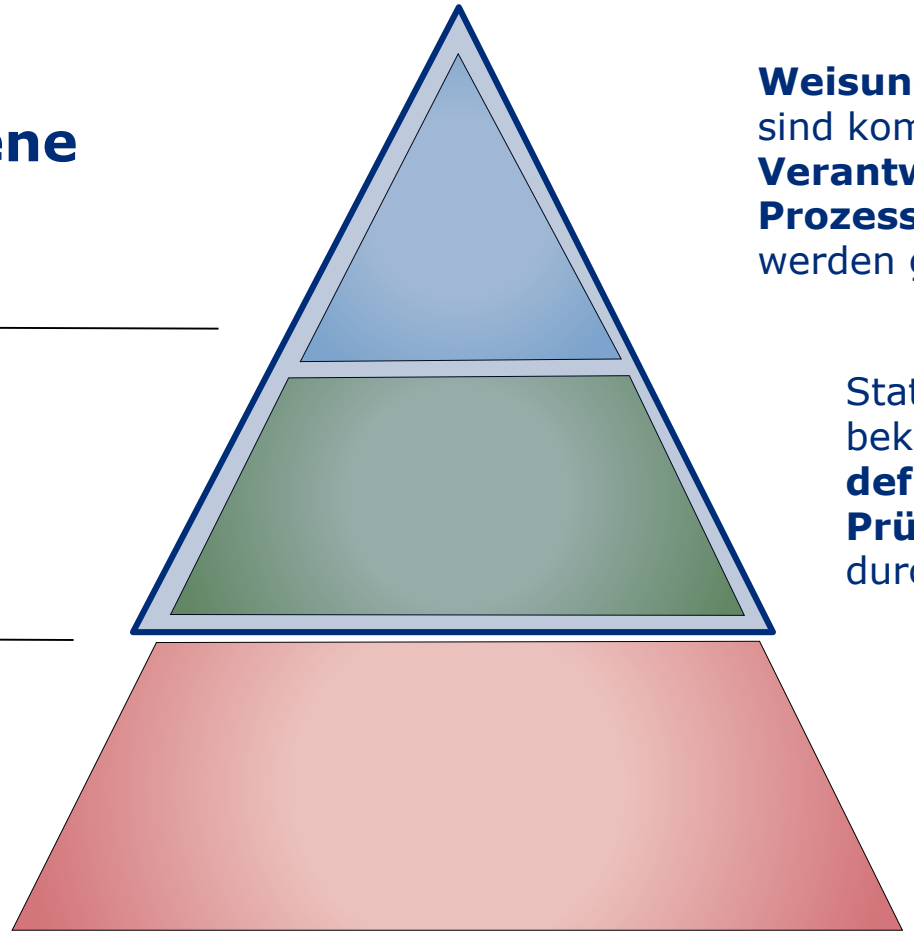
Neu durch DSGVO

DSGVO: Datenschutz- Grundverordnung
ISMS: Informationssicherheits- Managementsystem
DSMS: Datenschutz- Managementsystem



Aufbau und Betrieb

Sicherheitsarchitektur



Strategische Ebene

Sicherheitspolitik
Sicherheitsstrategie

Weisungen und **Richtlinien** sind kommuniziert, **Verantwortlichkeiten** und **Prozesse** sind bekannt und werden gelebt.

Taktische Ebene

Sicherheitsdispositiv
Sicherheitskonzeption

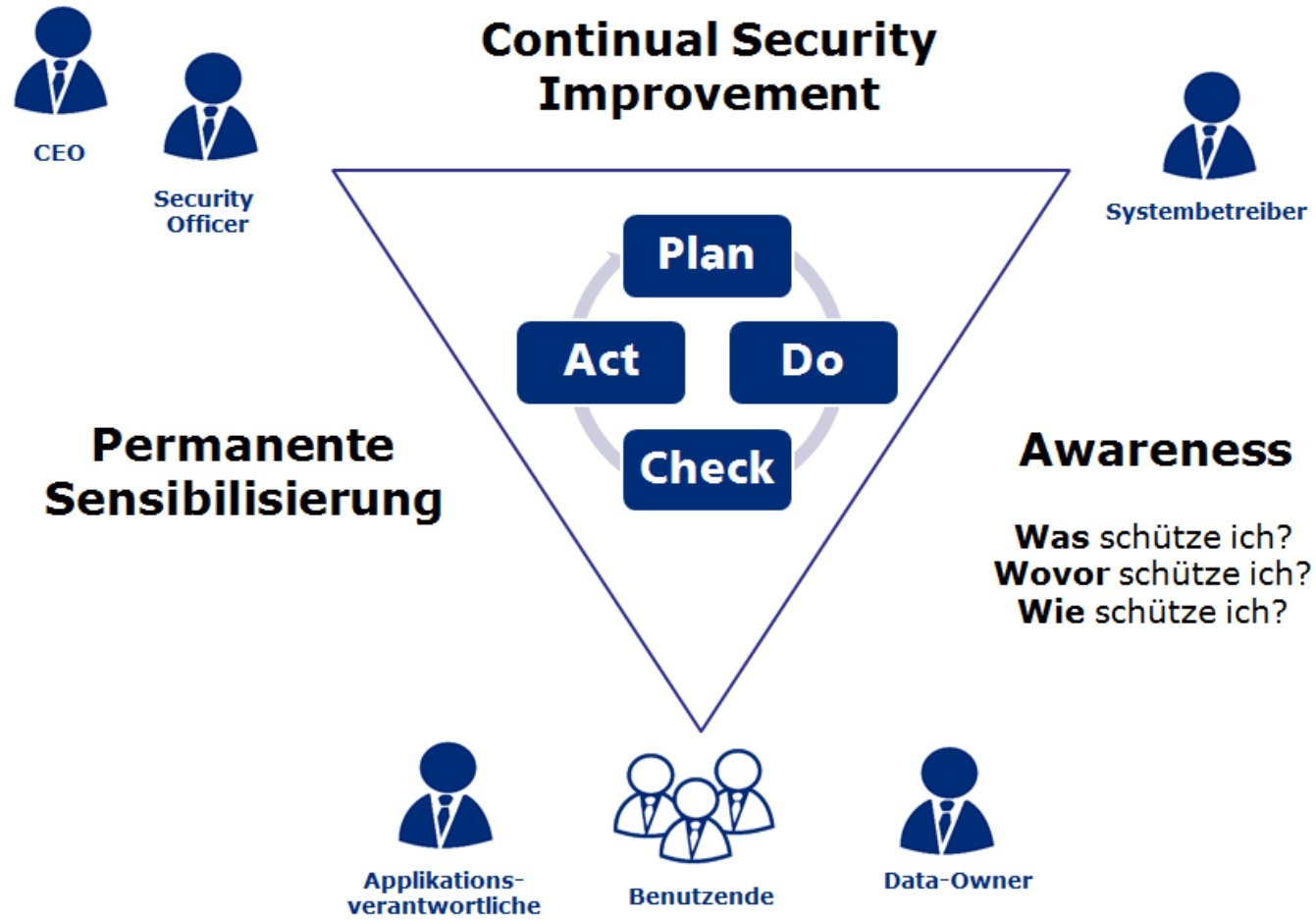
Status und Lücken sind bekannt, **Massnahmen** sind **definiert** und priorisiert, **Prüfungen** werden durchgeführt.

Operative Ebene

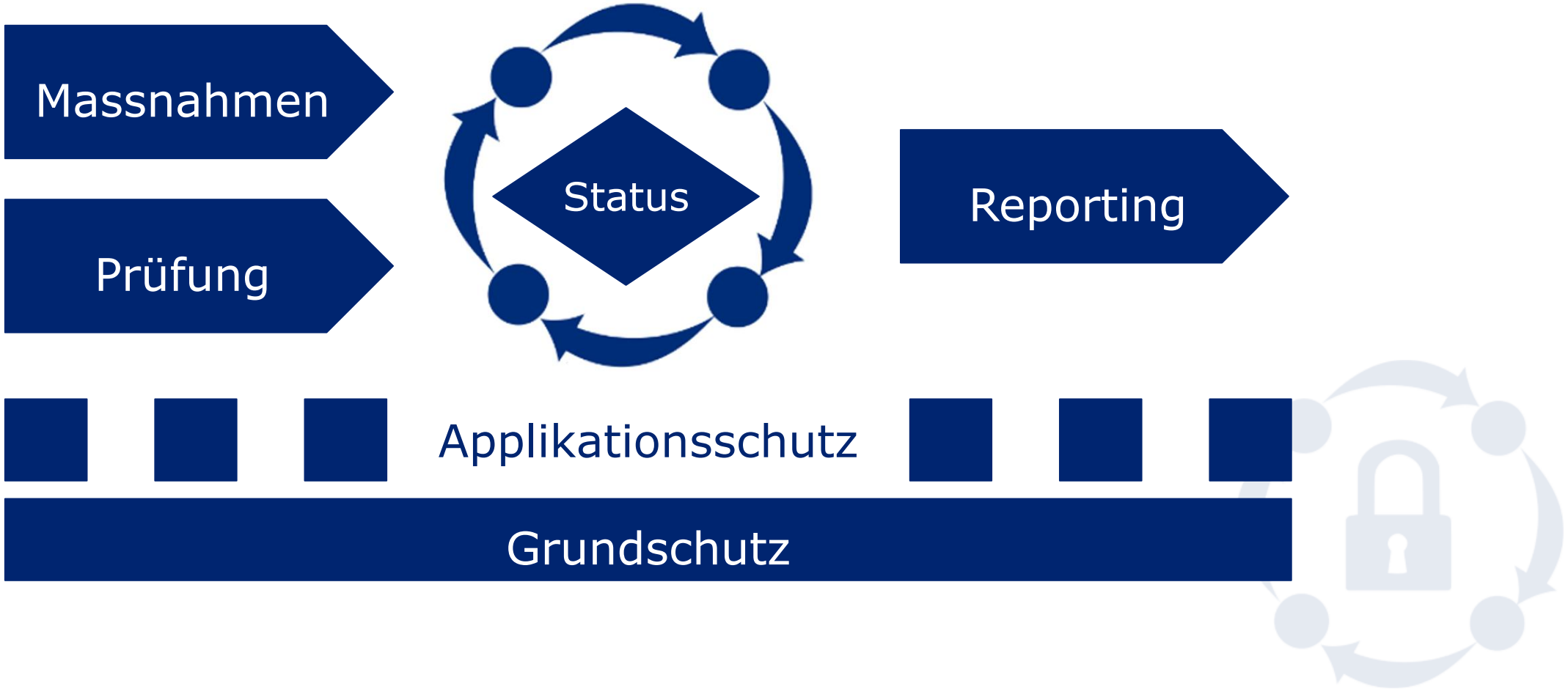
Umsetzung

Definierte, prüfbare **Aufträge** mit klarer **Verantwortlichkeit** für die umzusetzenden Massnahmen und erwarteter Ergebnisdokumentation.

Informations- und Datenschutz: unsere Sichtweise

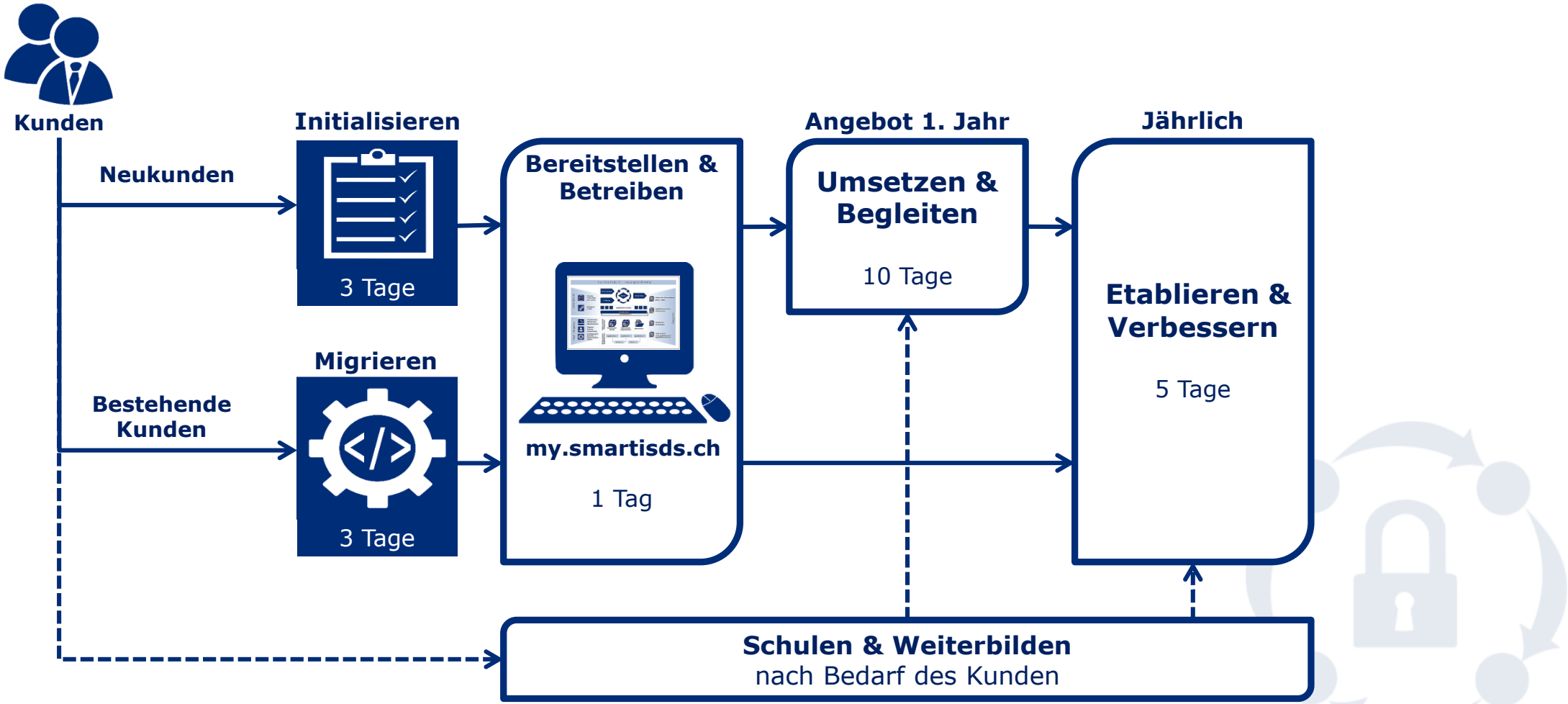


smartISDS Lösungsübersicht



Aufbau und Betrieb – smartISDS in 5 Schritten

Eine konforme Lösung für Ihre KMU in 14 Tagen



Eine Lösung basierend auf internationalen Standards

my.smartisds.ch basiert auf dem ISO/IEC 27001:2013 Framework. Das Tool zeigt pro Kapitel und ISO-Prüfpunkt den Stand der Massnahmenumsetzungen und die Lücken in der Unternehmung auf.

smartISDS, die Web-Applikation für die Verwaltung von InformationsSicherheit und DatenSchutz!

- Referenzieren Sie die gesetzlichen und Ihre eigenen, internen Vorgabedokumente
- Erstellen Sie für Ihr Unternehmen relevante Massnahmen auf Basis der Prüfpunkte ISO 27001:2017
- Stützen Sie sich bei der Erstellung von Massnahmen auf den Code of Practices aus ISO 27002:2017
- Führen Sie definierte Sicherheits-Prüfungen durch und referenzieren Sie diese mit Nachweis- und Vorgabe-Dokumenten
- Mehrere Grundschutzdefinitionen sind möglich (z.B. intern, SaaS, Cloud, usw.)
- Besitzen Sie eine grosse Anzahl von Applikationen? In smartISDS können diese bei Bedarf in "Cluster" strukturiert und gebündelt werden
- Jederzeit den Gesamtstatus auf einen Blick durch die Unterstützung eines ISMS nach ISO 27000:2017
- Management-Reports zu Grund- und Applikationsschutz (Erweiterungen auf Wunsch)
- Andere Kataloge zur Informationssicherheit möglich (z.B. ISO 27001:2013; VdS, usw.)
- Gehostet in der Schweiz

Haben Sie hierzu noch Fragen?

www.mabuco.ch/isds

Oder erfahren Sie mehr über unsere Dienstleistungen!

www.mabuco.ch

Dienstleistungs- und Produktportfolio

Beratungsdienstleistungen

- ICT-Governance und –Compliance
- Informationssicherheit und Datenschutz (ISDS)
- ICT-Servicemanagement
- Prozess- und Organisationsentwicklung
- Change Management

Projektdienstleistungen

- Programm- und Projektmanagement
- Business Analyse und Requirements Engineering
- Evaluation und Beschaffung

Interims-Fachkräfte

- Kader- und Schlüsselrollen
- Teamergänzungen

Coaching und Begleitung

- Einzel- und Gruppen Coaching
- Mentoring
- Begleitung und Moderation von Gruppenprozessen

Was ist smartISDS?

- Grundschutz & Applikationsschutz
- Massnahmen
- Prüfung
- Reporting
- my.smartisds.ch

Was ist smartAssesment?

- Überprüfung der Informatik
- Beurteilung auf Basis von Good Practices
- Fundierte, unabhängige Einschätzung der aktuellen Situation der Informatik
- Konkrete Angaben zum Handlungsbedarf

Firma

mabuco GmbH
Oberfeldweg 1
3072 Ostermundigen

+41 (0)31 305 05 50
info@mabuco.ch
www.mabuco.ch
www.linkedin.com/company/mabuco-gmbh