AVENIQ

Sicherheit im Public & Education Sektor

Den Wald trotz den vielen Bäumen als Ganzes sehen

IT-Grundschutz

Impulsreferat

Sicherheit als Ganzes sehen mit Fokus auf Risk-Management, Governance und Compliance

In einem zunehmend komplexen Geschäftsumfeld kann man im Dschungel aus Cyber-Risiken, Regulatorien und Lieferanten rasch den Überblick in der Informations-sicherheit verlieren und wesentliche Risiken übersehen.

In diesem Impulsreferat werden die essenziellen Aspekte eines Konzepts für Public- & Education-Organisationen beleuchtet, um Informationssicherheit als Ganzes zu sehen basierend auf Prozesse in Kombination mit einem risikobasierten IT-Grundschutz.

Anschliessend folgt eine tiefgründige Diskussion, um die Implikationen und Herausforderungen zu erörtern.

Werner Stocker
CISO

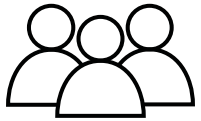
+41 43 233 34 63
werner.stocker@aveniq.ch

Herausforderungen Informationssicherheit

Der tägliche Dschungel

Cyber-Risken

- Der klassische Perimeter existiert nicht mehr
- Die Angriffslandschaft ist breiter und dynamischer geworden
- Daten sind das neue Gold, auch für Angreifer



Lieferanten

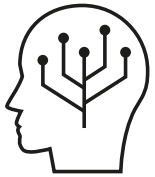
- Wandel zur Cloud
- Sammelsurium an Lieferanten
- Ländergrenzen verschwimmen
- Datenflüsse werden zunehmend komplexer

Regulatorien

- Vielfalt nimmt national & international zu
- Viele sind unübersichtlich und komplex
- Blinde Flecken

Herausforderungen Informationssicherheit

Aktuelle Beispiele



KI

- Angreifer nutzen KI ohne «Gewissen»
- Angriffe sind schneller und professioneller
- Imitationen sind kaum mehr vom Original zu unterscheiden

Microsoft M365

- On-Premise Dienste werden durch Cloud-Dienste ersetzt ohne Alternative
- Nicht alle Dienste sind mit Datenhaltung Schweiz erhältlich

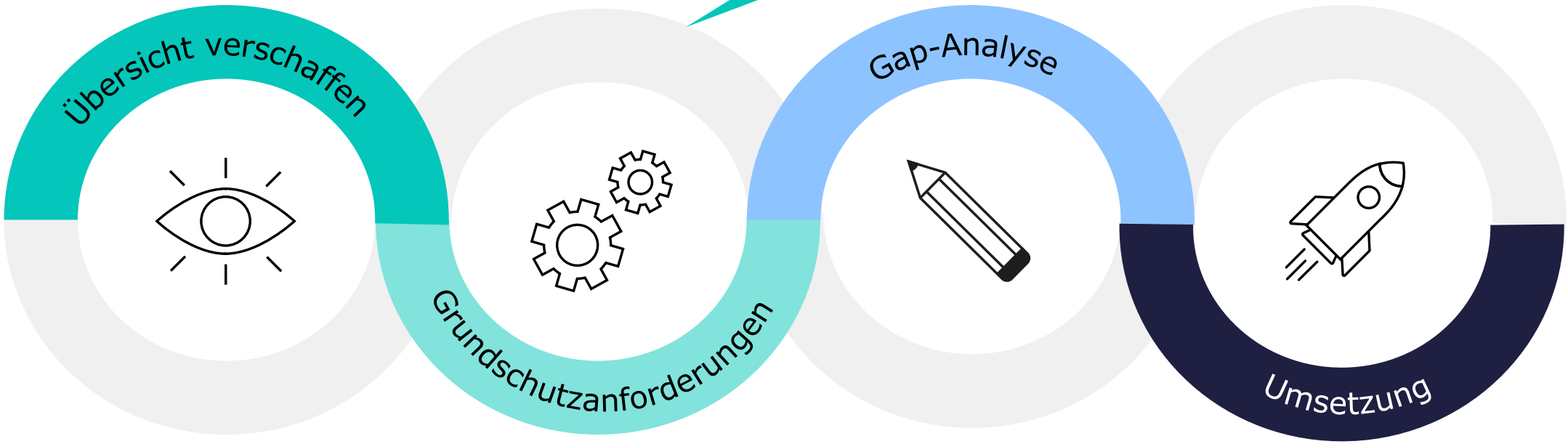
CH DSG vs. EU DSGVO

- Privatbussen CH DSG bis CHF 250’000.-
- Eine Person mit EU/EWR-Bezug zwingt in die EU DSGVO
- Inventar versus Liste der Bearbeitungstätigkeiten

Risikobasierter Ansatz

Sicherheit als Prozess

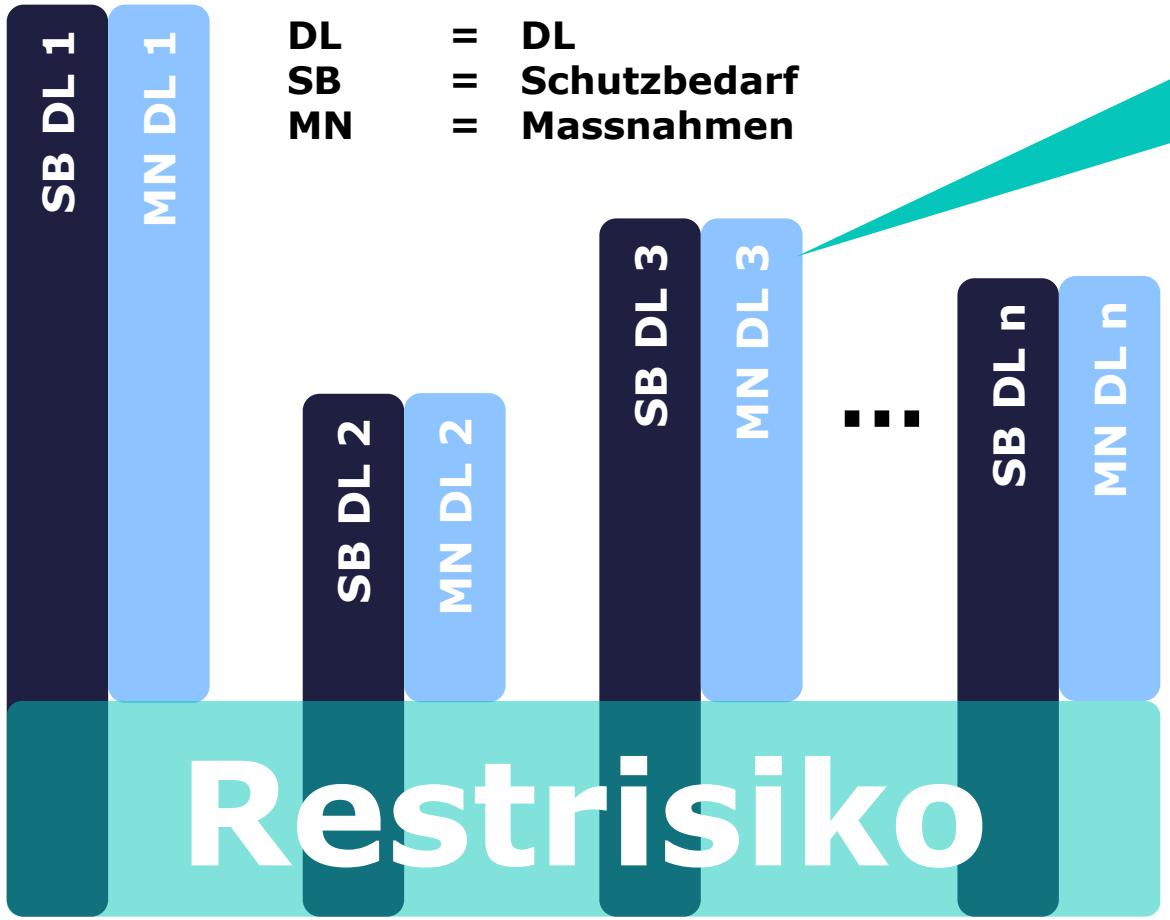
Dieser Prozess ist anwendbar für bestehende wie neue Dienstleistungen



Risikobasierter Ansatz

Strukturierter Ansatz

Die Herausforderung liegt darin, dies effizient zu strukturieren



(1) Angebotene Dienstleistungen identifizieren

(2) Schutzbedarf Daten und Prozesse festlegen

(3) Risiken identifizieren

(4) Schutzmassnahmen definieren

(5) Schutzmassnahmen umsetzen

Risikobasierter Ansatz

Ein möglicher strukturierter Prozess

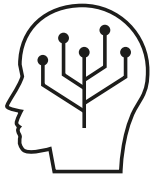
Liefert auch Grundlage für Lieferantenmanagement

Jährliche Wiederholung stellt Aktualität sicher

Inventar	**Review**	**Risiko-bewertung**	**Massnahmen**	**Proaktivität**
In einem zentralen Register werden die Dienstleistungen inklusive Schutz-bedarfsniveau und Regulatorienbindung dokumentiert.	Ein regelmässiger Review ergänzt das Inventar und trägt Veränderungen nach.	Basierend auf dem Schutzbedarfsniveau und den gebundenen Regulatorien werden Risiken mit einem standardisiertem IT-Grundschutz bewertet.	Zum IT-Grundschutz abweichende Risken sollten über Mass-nahmen behoben oder müssen vom Datenbesitzer als Restrisiko getragen werden.	Bei wesentlichen Veränderungen in den Dienstleistungen oder der Regulatorien können über das Inventar Risiken proaktiv gemanagt werden.

Herausforderungen Informationssicherheit

Wie werden aktuelle Beispiele mit dem risikobasierten Prozess behandelt



KI

Der IT-Grundschutzes stellt sicher, dass Massnahmen regelmässig an die sich verändernde Angriffs-Landschaft angepasst wird.
→ Aber KI kann auch als Service genutzt werden.

Microsoft M365

Der IT-Grundschutz ist so flexibel gestaltet, dass sich Massnahmen verändern, je nachdem ob Dienst-leistungen On-Premise oder in der Cloud betrieben werden.

CH DSG vs. EU DSGVO

Ein aktuelles Inventar stellt sicher, dass alle auf eine Dienstleistung wirkenden Regulatorien mit entsprech-enden Massnahmen abgedeckt sind.

Impulse zur Sicherheit im Public & Education Sektor

Sicherheit als Ganzes sehen

Impuls 1 – IT-Grundschutz

- Stellt ein ausgewogenes Restrisiko über alle genutzten Services sicher.
- Ein aktuelles Service-Inventar inkl. Mapping von Schutzbedarf und Regulatorien stellt sicher, dass eine solide Grundlage für die Umsetzung eines IT-Grundschutzes vorhanden ist zur Verhinderung von blinden Flecken.

Impuls 2 – Regulatorien

- Es muss regelmässig geprüft werden, welche nationalen und internationalen Regulatorien Anwendung finden.
- Ein aktuelles Service-Inventar inkl. Mapping von Schutzbedarf und Regulatorien stellt sicher, dass eine solide Grundlage für die Umsetzung aller notwendigen regulatorischen Anforderungen vorhanden ist zur Verhinderung von blinden Flecken.

Impuls 3 – Weg in die Cloud / KI

- Cloud und KI sind nur eine neue Art von Services.
- Kennt man seine Services inkl. deren Schutzbedarf und Regulatorien, so hat man die benötigten Grundlagen:
  - Ist ein Weg in die Cloud möglich und wenn ja in welche?
  - Sicherheitsleitplanken, um die Planung und Umsetzung gemäss Geschäftsbedürfnissen und Regulatorien richtig auszuführen.

Impuls 4 – Strukturierter Ansatz

- Führt man das Service-Inventar und den IT-Grundschutz über einen strukturierten Prozess bei Einführung und Betrieb fortlaufend weiter, so hat man seine Informationssicherheit im Griff und unter Kontrolle.
- Investitionen können gezielt da angesetzt werden, wo die Restrisiken am höchsten sind.