Cheat Sheet

Informationssicherheits-Management

«Vom Newbie-CISO bis zum INFOSEC-GURU – für jeden etwas dabei»

Passion für Transformation

Bestimmung des Schutzbedarfs von Fachanwendungen und Datensammlungen

Verfügbarkeit

- Ab welcher Ausfalldauer entsteht ein für das Business nicht mehr tragbarer Schaden?
- Maximal verkraftbare Ausfallzeit (Recovery Time Objective, RTO)
- Anforderungen an die IT in Bezug auf Redundanzen oder SLA in Verträgen

Datenverlust

- Ab welcher Dauer ist ein Datenverlust für das Business nicht mehr tragbar?
- Maximal verkraftbare Datenverlustzeit (Recovery Point Objective, RPO)
- Anforderungen an das Backup, die Disaster-Recovery-Strategie oder die SLA in Verträgen

Vertraulichkeit

- Welche Schäden entstehen bei Verletzung der Vertraulichkeit für das Business?
- Ist das Unternehmen existentiell bedroht?
- Mögliche Bereiche: Reputation, Finanzen, Personenschaden, Klage wegen Nichteinhaltung von Verträgen oder Vorgaben

Integrität

- Welche Schäden entstehen bei Verletzung der Integrität für das Business?
- Ist das Unternehmen existentiell bedroht?
- Mögliche Bereiche: Reputation, Finanzen, Personenschaden, Klage wegen Nichteinhaltung von Verträgen oder Vorgaben

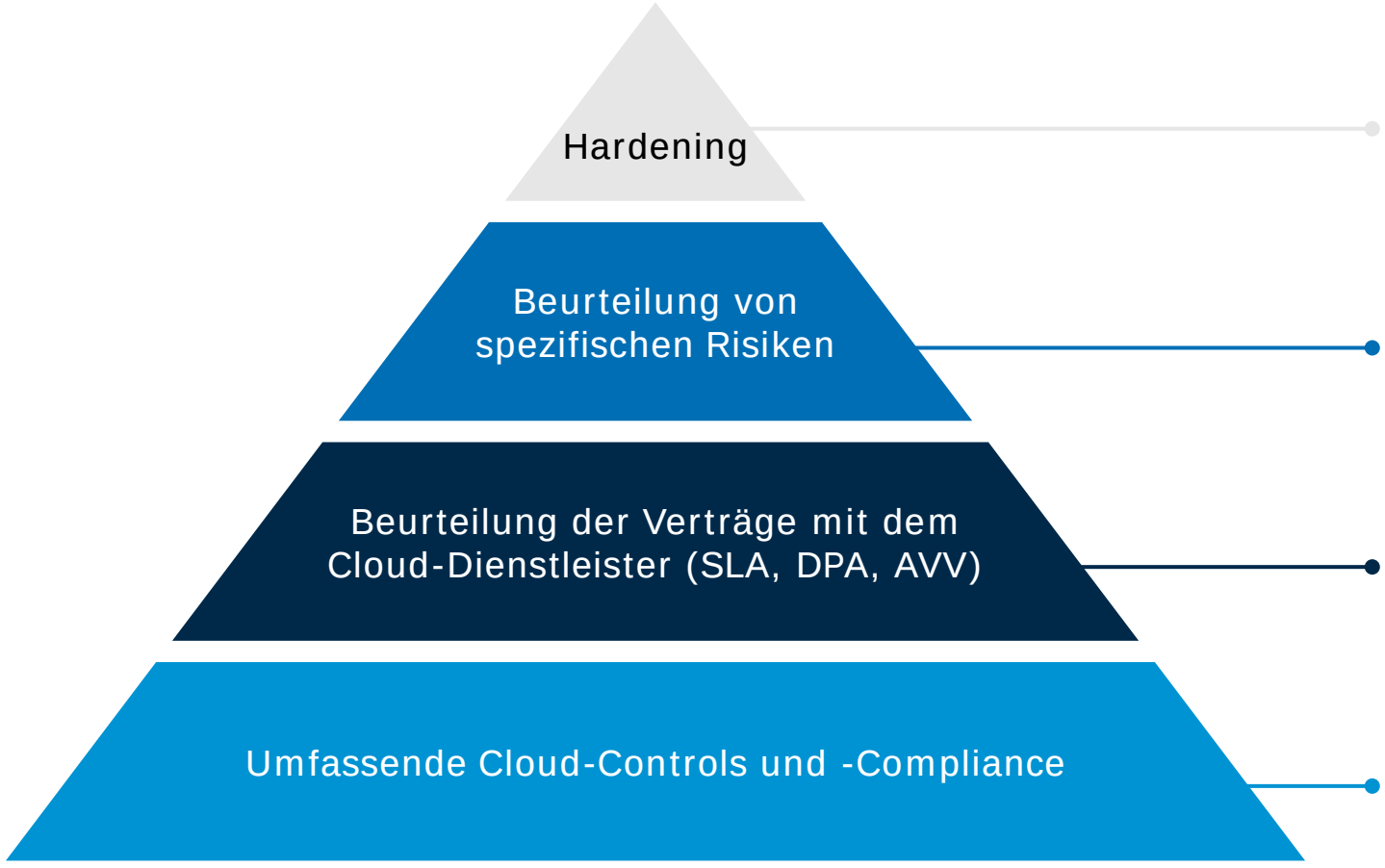
Personendaten

- Werden Personendaten oder besonders schützenswerte Personendaten gemäss DSG Art. 5 bearbeitet?
- Welche Personendaten werden in welchen Datensammlungen bearbeitet?

Erstellung eines ISDS-Konzeptes und Durchführung der Vorabkonsultation in IT-Projekten

- Erstellung der Schutzbedarfsanalyse. Bei erhöhtem Schutzbedarf in einem Aspekt ist ein ISDS-Konzept zu erstellen.
- Durchführung einer Datenschutz-Folgenabschätzung (DSG Art. 22) falls hohe Risiken für betroffene Personen vorhanden sind. Beachtung der Vorlagen der kantonalen Datenschutzbeauftragten.
- Erarbeitung einer Risikoanalyse (Datenschutz und Datensicherheit), Herleitung von Massnahmen und Restrisiken. Erstellung des ISDS-Konzeptes inklusive Beilagen wie z.B. ein Benutzer- und Rollenkonzept.
- Falls nach Reduktion immer noch erhöhte Risiken für betroffene Personen bestehen: Durchführung der Vorabkonsultation beim EDÖB (private, DSG Art. 23) bzw. bei den kantonalen Datenschutzbeauftragten (öffentliche Organe).

Anerkannte Checklisten für den sicheren Cloud-Einsatz



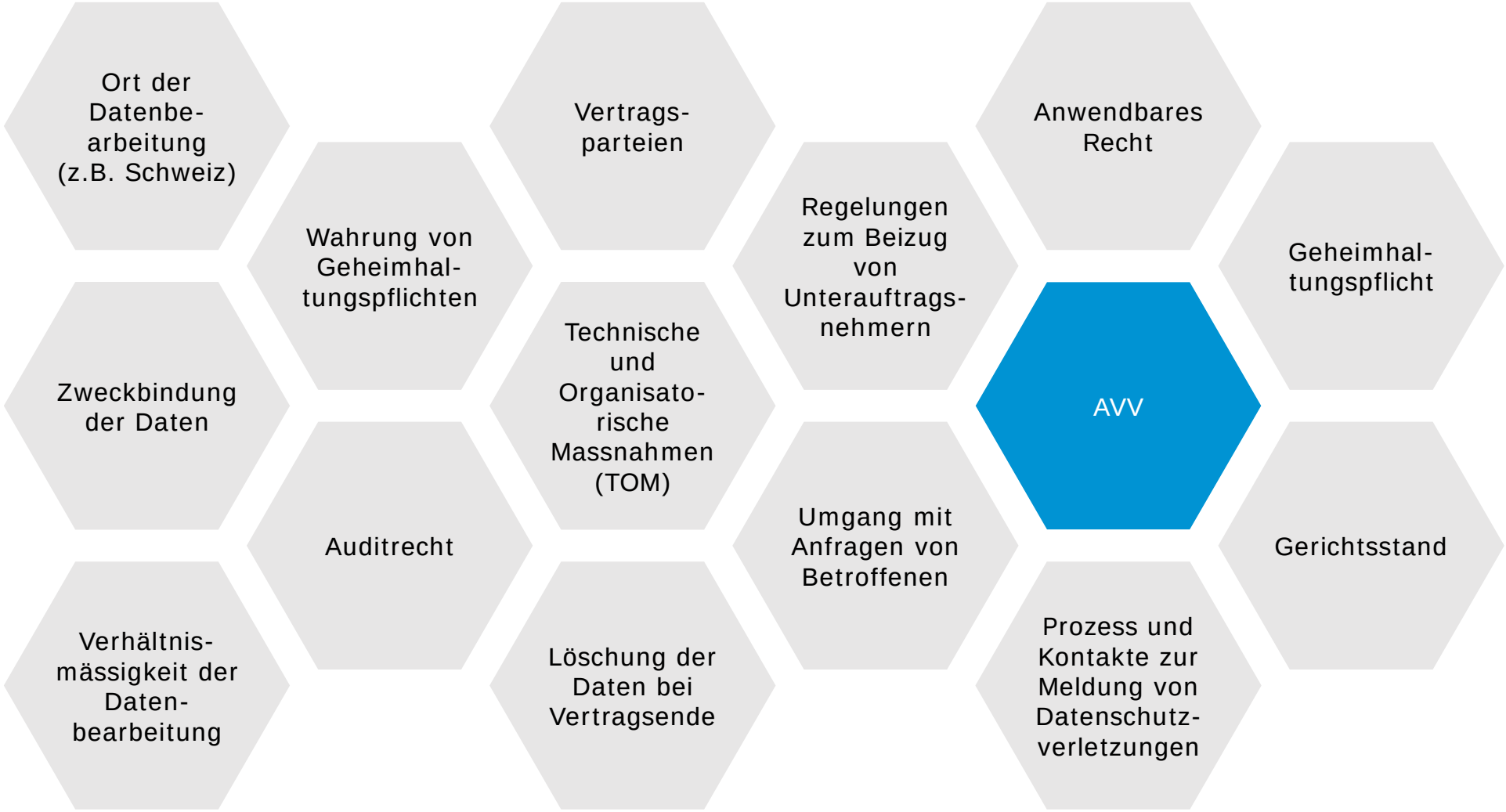
Anwendung von CIS-Benchmarks für das Hardening

Z.B. Beurteilung des Risikos eines Lawful Access gemäss der Methode von David Rosenthal

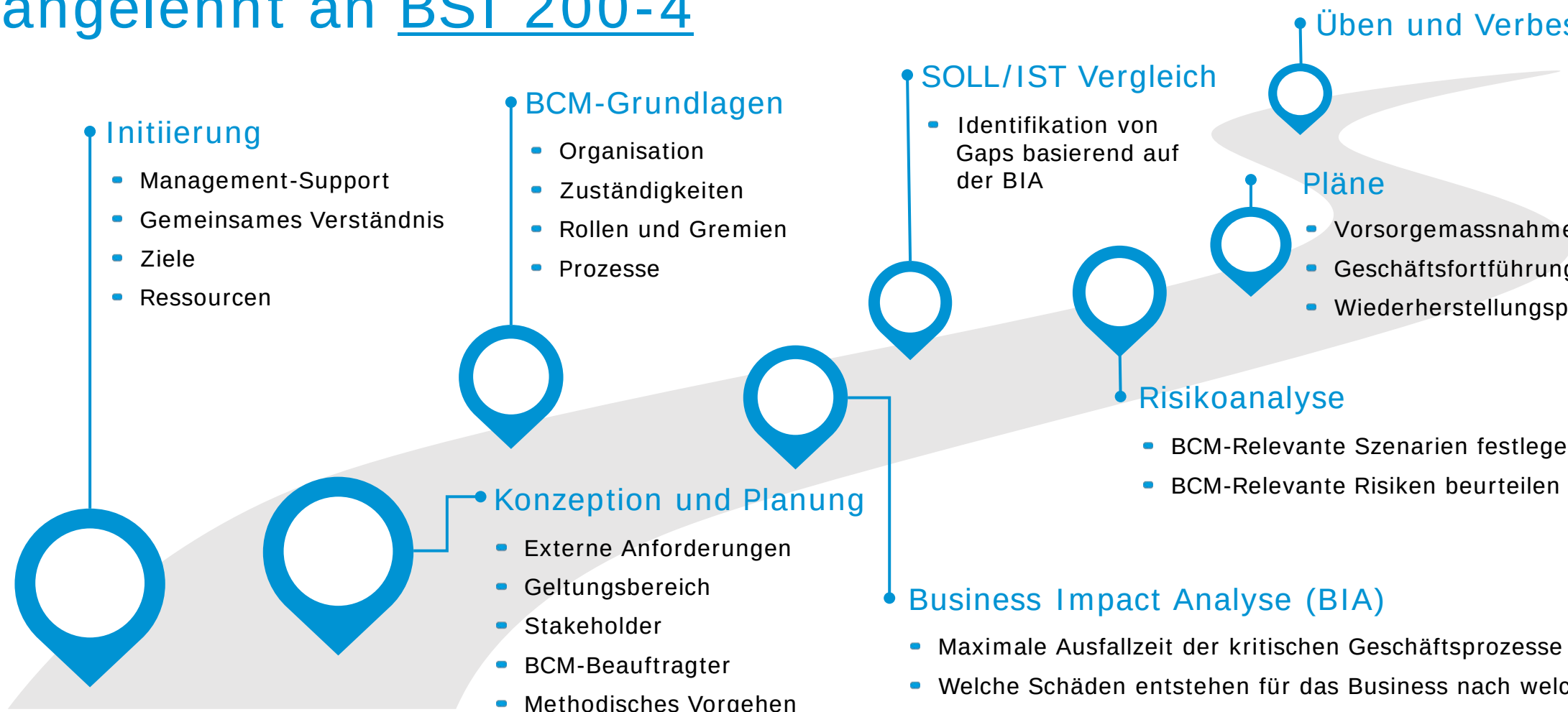
Beurteilung der Verträge in Bezug auf Datenschutz, z.B. gemäss Privatim

Auswahl der relevanten Aspekte aus BSI C5

Inhalte eines Auftragsverarbeitungsvertrags (AVV)



Aufbau eines Business Continuity Management Systems angelehnt an BSI 200-4



Initiierung

- Management-Support
- Gemeinsames Verständnis
- Ziele
- Ressourcen

BCM-Grundlagen

- Organisation
- Zuständigkeiten
- Rollen und Gremien
- Prozesse

Konzeption und Planung

- Externe Anforderungen
- Geltungsbereich
- Stakeholder
- BCM-Beauftragter
- Methodisches Vorgehen
- Flughöhe
- Phasen (Plan-Do-Check-Act)

Business Impact Analyse (BIA)

- Maximale Ausfallzeit der kritischen Geschäftsprozesse
- Welche Schäden entstehen für das Business nach welcher Zeit?
- Welches sind die kritischen Ressourcen?

Risikoanalyse

- BCM-Relevante Szenarien festlegen
- BCM-Relevante Risiken beurteilen

Pläne

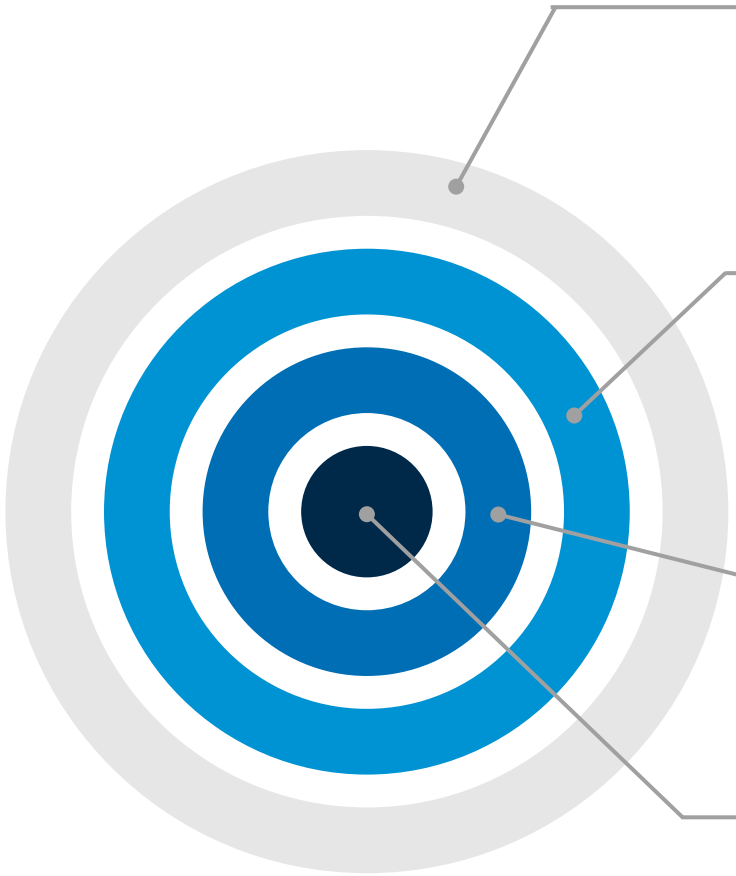
- Vorsorgemassnahmen
- Geschäftsfortführungspläne
- Wiederherstellungspläne

SOLL/IST Vergleich

- Identifikation von Gaps basierend auf der BIA

Üben und Verbessern

Planung einer Security-Awareness-Kampagne



Wiederkehrende Massnahmen und Evaluation

- Awareness ist ein Marathon, kein Sprint: Über Jahre wiederkehrende oder abwechselnde Bausteine, die aufeinander abgestimmt sind
- Evaluation, ob die Ziele erreicht wurden

Awareness-Bausteine

- Festlegen von Bausteinen, wie E-Learning, Phishing-Training, Plakate, Give Aways, Live-Hacking, Smartphone-Game, Attack-Simulation, Phishing-Kampagne, Schulungen, angepasste Logon-Screens, Brownbag-Sessions, interner Sicherheitstag, CAS für Schlüsselpersonen

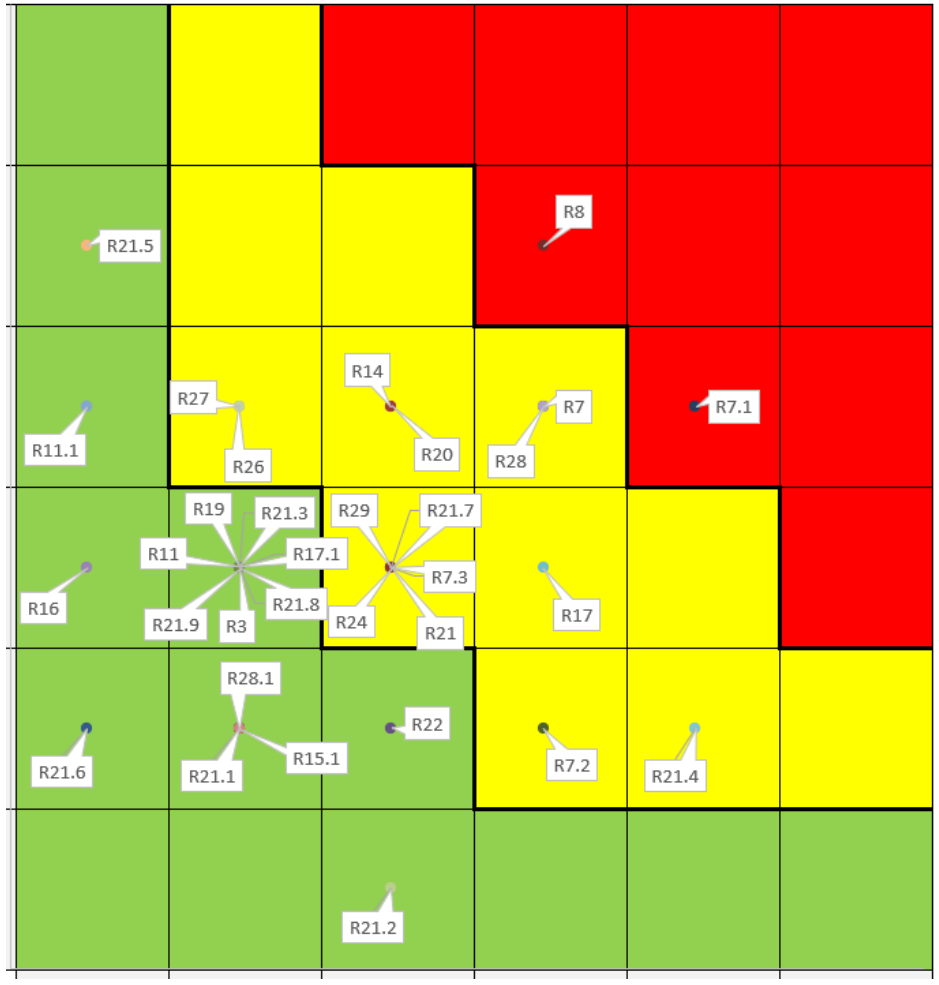
Zielgruppen und Inhalte

- Bestimmung der Zielgruppen (z.B. alle Mitarbeitenden, Management, IT-Administratoren, Lehrlinge & Praktikanten)
- Definition der zu vermittelnden Botschaften und Inhalten

IST-Analyse

- Analyse der IST-Situation im Bereich Awareness (z.B. basierend auf Phishing-Check, Umfrage, Auswertung E-Learning oder Interviews)

Risikomanagement / Risk-Register



- Verwaltung der Informationssicherheits-Risiken in einem Risk-Register, z.B. basierend auf ISO 27005
- Definition der Kategorien für Eintretenswahrscheinlichkeit und Ausmass sowie der Kriterien für die Risikoakzeptanz
- Risikobeurteilung in Bezug auf die Dimensionen Verfügbarkeit, Integrität, Vertraulichkeit, Nachvollziehbarkeit
- Zuweisung der Risiken zu einem Risk-Owner
- Risikobehandlung: Vermeidung, Reduktion durch Massnahmen, Transfer an z.B. Versicherung oder Akzeptanz
- Formelle Akzeptanz von Restrisiken durch GL
- Tracken des Umsetzungsstandes von Massnahmen
- Wiederkehrender Prozess zur regelmässigen Bewertung der Risiken

Last but not least: Verschlüsselung und Signatur

Symmetrische Verschlüsselung

Sender und Empfänger benutzen den gleichen geheimen Schlüssel. Dieser muss zuerst sicher ausgetauscht werden.

Anwendung: Vertraulichkeit von Daten z.B. Festplattenverschlüsselung, E-Mail auf dem Transportweg, Internetverkehr.

Aktuelle Algorithmen und Schlüssellänge:
AES 128bits, AES 196bits, AES 256bits

Asymmetrische Verschlüsselung

Sender und Empfänger benutzen ein Schlüsselpaar bestehend aus einem geheimen „Private“ und öffentlichen „Public“ Schlüssel. Der Sender verschlüsselt mit dem „Public Key“ des Empfängers und der Empfänger entschlüsselt mit seinem „Private Key“. Der „Private Key“ liegt geschützt beim Besitzer (z.B. Zertifikatsspeicher, Smart Card).

Anwendung: Austausch von geheimen symmetrischen Schlüsseln für E-Mail- und Webverschlüsselung

Aktuelle Algorithmen und Schlüssellänge:
RSA 3000bits, DLIES 3000bits, ECIES 250bits

Signaturverfahren

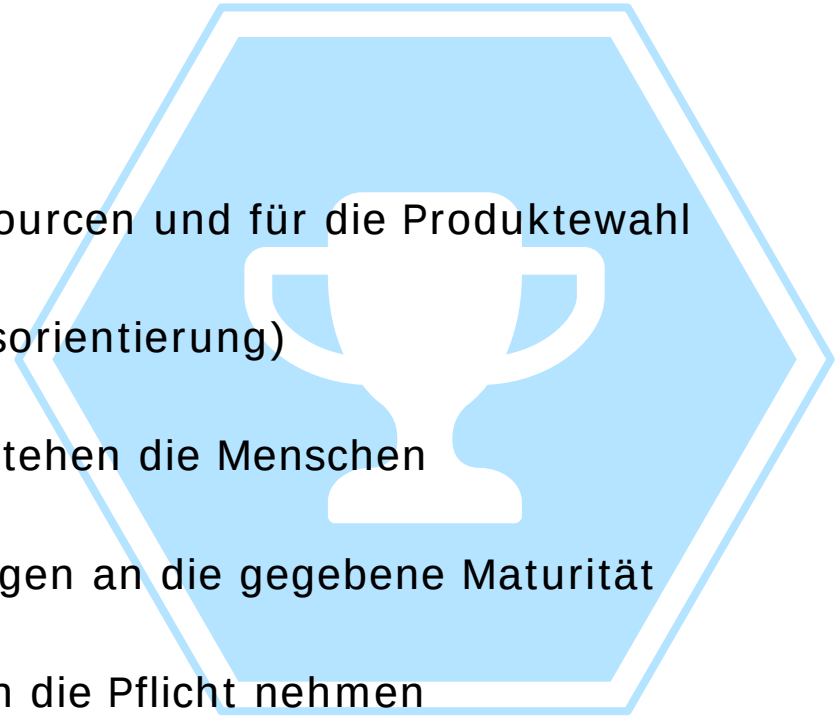
In Signaturverfahren werden die zu signierenden Daten zunächst gehasht, bevor aus diesem Hashwert die Prüfsumme beziehungsweise die Signatur mit dem „Private Key“ des Senders berechnet wird. Der Empfänger verifiziert anschliessend die Signatur mit dem entsprechenden „Public Key“ des Senders.

Anwendung: Integrität von Daten z.B. Echtheit von E-Mails und Dokumenten.

Aktuelle Algorithmen und Schlüssellänge:
RSA 3000bits, DSA 3000bits, ECDSA 250bits

Post-Quantum Encryption Standards: Kyber, Dilithium, Falcon, SPHINCS+

How to survive as a CISO



- Risikomanagement als Herzstück zur Priorisierung der Ressourcen und für die Produktewahl
- Enabler gegenüber dem Business und in Projekten (Lösungsorientierung)
- Beziehungen intern und extern aktiv pflegen: Im Zentrum stehen die Menschen
- Angemessene Flughöhe wählen: Anpassung der Anforderungen an die gegebene Maturität
- Management, Business, IT, Compliance und Mitarbeitende in die Pflicht nehmen
- Strukturiertes Vorgehen im Rahmen eines ISMS: Berücksichtigung sämtlicher Dimensionen (Identifikation, Prävention, Detektion, Reaktion, Wiederherstellung)
- Informationssicherheit ist ein Marathon und kein Sprint: Stetige Verbesserungen und langfristiges Denken über Jahre hinweg verbessern die Situation

IHRE ANSPRECHPARTNER

Jens Albrecht

Senior Security Consultant
Dipl. El.-Ing. FH / Wirtschaftsing. FH
CISSP, CISM, CRISC
jens.albrecht@csp-ag.ch
+41 44 520 33 68

Peter Flütsch

Expert Security Consultant / Partner
Dipl. Ing. FH / EMBA IT-Management
CISSP, CISM, ISO 27001 Lead Auditor
peter.fluetsch@csp-ag.ch
+41 71 508 09 72