# Information Security Management

Eine kleine Zusammenfassung der HSLU.I Vorlesung *Managementaspekte der Information Security* (MANSEC), basierend auf den Folien von *Prof. Dr. Bernhard M. Hämmerli Security Experte* and friends.

Geschrieben von mir, in InfoSec-Denglisch.

# Einführung

## CIA

Grundziele IT-Security:

- **Confidentiality**: Vertraulichkeit
- **Integrity**: Integrität
- **Availability**: Verfügbarkeit

## Triple A

Triple A (_Authentication, Authorization, Accounting)

## Dimensionen von IT-Sicherheitsfragen

- Rechtlich
- Organisatorisch
- Menschlich
- Technisch

## Management

Ziele und Aufgaben des Managements:

- **POSDC** (Traditionell): *planning, **organizing**, staffing, directing, controlling*
- **POLC** (Wichtig für CISO): *planning, organizing, **leading**, controlling*

Die Planung erfolgt auf *strategischer*, *taktischer* und *operativer* Ebene.

## Entwicklung

Aufgaben und Trends in der Information Security:

- **bis 1985**: Verfügbarkeit optimieren. man war froh, wenns läuft
- **bis 1992** : IT Security = Encryption, ein Problem der Techniker
- **bis 1995**: Sache des Security Officers, Delegation von Tasks
- **bis 1999**: IT-Security ist Chefsache (Risk Owner)
- **ab 2000**: Risiko Management
- **ab 2003**: Sparmassnahmen, IT-Security reduziert auf gesetzliche Anforderungen; digitale Forensik kommt auf

- **ab 2008**: Konstante Attacken
- **ab 2011**: Cyber defense plans
- **ab 2012**: Outsourcing, Cloud computing; Rolle des CISO muss neu definiert werden

## Conclusions Folien SW01

- IT Security hat sich verändert mit neuen Technologien
- Standards und Frameworks gewinnen an Bedeutung
- Organisatorsche Probleme: **Risk Management**, **Governance** und **Compliance**
- Technische Probleme: Komplexere Tools, Integration ins Gesamtsystem
- Aufgaben Security Officer: coach, communicator, promoter and police
- Security Officer wird vom Technokraten zum Manager
- Rechtliche Aspekte gewinnen an Bedeutung
- Outsourcing wird unvermeidbar für KMUs und teilweise auch grössere Unternehmen
- Messbarkeit auch von "soft factors" wichtig für Erfolg
- Rolle des CISO ändert sich mit cloud computing, mehr menschliche und organisatorische Aufgaben

# Information Security Policy

## Lernziele

### ***Information Security Policy*** **definieren können:**

- Sicherheitsrichtlinie, beschreibt den angestrebten Sicherheitsanspruch in einer Organisation.
- Policies sind eine Sammlung von organisatorischen Richtlinien, die das Verhalten in einer Organisation vorgeben.
- Bestimmen, **was** gemacht werden darf, andere Dokumente befassen sich eher mit dem **wie**
- Damit sie effektiv sind müssen Policies *definiert*, *verstanden*, *anerkannt* und *durchgesetzt* werden
- Policies müssen ständig angepasst werden

### **Die drei Arten von *Information Security Policies* beschreiben können:**

1. **EISP**: Enterprise Information Security Programm Policy

High-Level, bestimmt die strategische Ausrichtung, den Umfang und den allgemeinen Grundton aller Sicherheitsmassnahmen. Wird auch als *InfoSec Policy* oder *Security Program Policy* genannt.

Weist Verantwortungen zu und regelt die Entwicklung, Einführung und Managementansprüche an die Informationssicherheit.

Die EISP beinhaltet einen Überblick über die Grundeinstellung der Unternehmung im Bezug auf IT-Security, Informationen zur Struktur und Personen der IT-Security, Verantwortungsbereiche für Angestellte, Kunden usw.

2. **IISP**: Issue-specific Information Security Policy

- Werden auch *fair and responsible use policy* genannt
- Eine Richtlinie mit detaillierten Anweisungen für die Verwendung einer bestimmten Ressource oder Technologie.
- Beinhaltet Informationen zu der erwarteten Verwendung und der Kontrolle eines eingesetzten Systems.

Beispiele: E-Mail, Whatsapp und andere Kommunikation; Verwendung des Internets; Persönliche Verwendung von Unternehmensgeräten; Zugangsberechtigungen; ...

3. **SISP**: System-specific policies

Anweisungen des Managements zur Implementation und Konfiguration von Systemen, wie beispielsweise Zugriffsberechtigungen (ACLs, Firewall-Konfiguration).

Werden definiert für Technologien, welche die CIA von Informationen betreffen und informieren über die Absichten des Managements

- **Konfiguration** und **Zugriffsrechte** als Liste oder Matrix. Regelt das *wer*, *was*, *wann*, *wo* & *wie*

### Erklären, was für eine erfolgreiche Policy notwendig ist:

Damit eine Policy effektiv sein kann muss sie:

- definiert
- gelesen
- verstanden
- akzeptiert
- einheitlich durchgesetzt werden

### Prozess der Entwicklung, Umsetzung und Unterhalt von *Information Security Policies*:

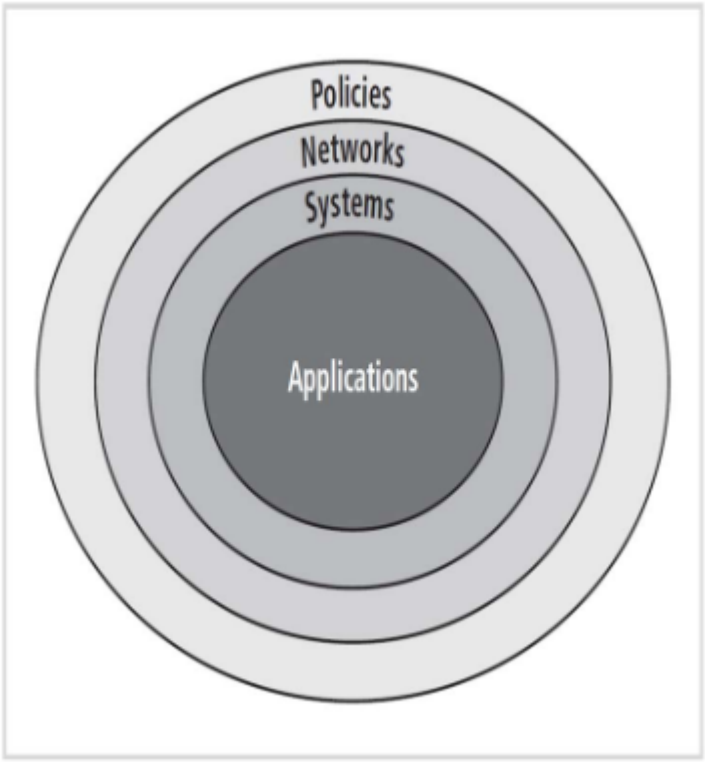
```
TODO
```

## Gründe für Policies

Policies sind der Grundstein effektiver Informationssicherheit. Eine gute Policy sollte:

- Zum Erfolg des Unternehmens beitragen
- Sinnvolle Aufteilung der Verantwortung vornehmen
- Benutzer sollten bei der Festlegung von Policies involviert werden

## The Bullseye Model




## Begriffe

- **Policy**: Policies sind eine Sammlung von organisatorischen Richtlinien, die das Verhalten in einer Organisation vorgeben.
- **Standard**: Detaillierte Beschreibung aller Tätigkeiten, die notwendig sind, um eine Policy zu erfüllen.
- **Richtlinie**: Nicht zwingende Empfehlung, dient als Referenz für das Verhalten der Angestellten
- **Prozeduren**: Schrittweise Anleitungen mit dem Ziel, Angestellten zu helfen, den Policies zu folgen
- **Praktiken**: Beispiele von Handlungen, die Übereinstimmung mit den Policies demonstrieren

## Effektive Policies

Anforderungen für effektive Policies:

1. Entwickelt mit Instriestandard / akzeptierten Praktiken und vom Management abgesegnet
2. Verteilt und bekanntgemacht werden mit allen angemessenen Mitteln
3. Von allen Angestellten gelesen
4. Formelles Einverständnis der Angestellten
5. Einheitlich angewendet und durchgesetzt werden.

### Entwicklung

Policy-Development wird oft als Prozess mit drei Schritten betrachtet:

1. **Designen und Schreiben** (oder Umschreiben) einer Policy
2. **Review** durch einen Chef / Senior Manager und formale Absegnung
3. Managementprozesse zur **Festlegung und Umsetzung**

Der erste Schritt benötigt gutes *Projektmanagement*, die anderen zwei gute *Business Practices*.

### Verteilung

Erfolg *physisch* oder *elektronisch*. Die Verteilung der Policy ist wichtig, da sie nicht durchgesetzt werden kann, wenn nicht nachgewiesen ist, das diese dem Endbenutzer bekannt war. Vertrauliche Policies erfordern besondere Massnahmen wie besondere Kennzeichnung, Zerstörung von Vorgängerversionen und so weiter.

### Lesen

- Sprachkenntnisse und Analphabeten berücksichtigen
- Sehbehindertenfreundliche Versionen
- Übersetzungen

Eventuell prüfen mit Tools und Test (Flesch Reading Ease Tests). Leseniveau eines Oberstufenschülers ist das Maximum.

### Verstehen

- Sinnvolles Sprachniveau (siehe oben), minimale Verwendung technischer Fachbegriffe und *Manager Slang*
- Assessments durchführen, um das Verständnis zu prüfen über das grundlegende Ziel der Policy
- Mittels Tests den Schulungsbedarf einzelner Mitarbeiter ermitteln

### Policy Compliance

Muss entweder **Agreed by confirmation**sein oder **Agreed by act**: Eine Handlung ist erforderlich, mit der das Verständnis einer Policy bestätigt wird bevor eine Technologie oder Ressource verwendet werden kann.

Das Verweigern des Einverständnisses wird als Arbeitsverweigerung ausgelegt und ist somit **Grund zur Terminierung**.

### Durchsetzung

Die Durchsetzung von Policies muss einheitlich und unparteiisch erfolgen und auch externer Überprüfung standhalten. Strafen und andere Massnahmen, die aus Missachtungen resultieren müssen diesen auf diese Aspekte überprüft werden können.

## Automatisierung mit Tools

Es existieren Tools zur Hilfe bei der Entwicklung, Implementation und Unterhalt von Policies, beispielsweise zur sicheren, passwortgeschützten Bereitstellung oder zur Überwachung, welche Mitarbeiter die Policies gelesen und akzeptiert haben.

Beispielsweise *VigilEnt Policy Center* (VPC) Server, welche Dokumente, Quizzes und Informationen zur Verfügung stellen.

## SecSDLC

Wie bei anderen Projekten ist auch bei der Policy Entwicklung eine rigorose Planung wichtig. Eine Möglichkeit, dies zu erreichen ist die Verwendung eines *System Development Life Cycles* (SDLC). Dies definiert sechs

Phasen:

1. **Investigation Phase**: Unterstützung von Management, IT-Management sicherstellen, Ziele definieren, Beteiligte und Betroffene ermitteln und einbeziehen, Scope und Kosten festlegen
2. **Analysis Phase**: Ein aktuelles Risikoassessment oder ein Audit, welches die aktuellen InfoSec-Bedürfnisse der Organisation dokumentiert, wichtiges Referenzmaterial sammeln (beispielsweise bestehende Policies)
3. **Design Phase**: Dokumententwurf erstellen, Reviews und Anpassungen bis *Manager Approval* ™
4. **Implementation Phase**: Plan zur Verteilung und der Überprüfung der Verteilung erstellen, Bestätigungen einholen (z.B. Unterschrift und Datum)
5. **End User License Agreement**
6. **Maintenance Phase**: Überwachung, Aufrechterhaltung und Anpassungen der Polices, Mechanismen zum Melden von Problemen (idealerweise anonym), periodische Reviews

## Policy Administrator

Policies brauchen einen _Champion_und einen und Manager. Werden diese beiden Positionen kombiniert, nennt man das Ergebnis **Policy Administrator**. Dieser ist Verantwortlich für die Erstellung, Revision, Verteilung und Aufbewahrung der Policy.

# Review Schedule, Procedures & Practices

### Schedule

Periodische Überwachung zur Sicherstellung der Effektivität. Folgende Punkte sollten geprüft werden:

- Aktualität
- Genauigkeit
- Vollständigkeit

Diese Reviews sollten im vornherein festgelegt werden und mindestens ein mal jährlich durchgeführt werden.

### Prozeduren und Praktiken

Der **Policy Administrator ©** sollte dafür sorgen, das einfach Rückmeldungen gemacht werden können mittels Mail und anonymer *drop box*. Diese Rückmeldungen sollten idealerweise auch gelesen werden.

Eine Policy sollte immer ein Veröffentlichungsdatum und die Daten der Revisionen enthalten, um Unklarheiten bezüglich Aktualität und Gültigkeit zu vermeiden. Je nach Inhalt ist es auch sinnvoll, das Ende der Gültigkeit festzuhalten, sofern dies vorhersehbar ist (*sunset clause*).

## Conclusions Security Policy

Policies dienen hauptsächlich dazu, Angestellte zu informieren, welches Verhalten akzeptabel ist und welches nicht. Die *meisten* Angestellten wollen sich korrekt verhalten. Deshalb sich Informationen und Schulung das effektivste Mittel zur Sicherstellung der Policies.

- InfoSec beginnt und endet mit Policies

- Policies sind ein Management-Problem, die technischen Aspekte kommen erst nach der Festlegung der Policies
- Policies sind die günstigste, aber die Massnahme die am schwierigsten zu implementieren ist.
- Policies dürfen nicht mit dem Gesetz in Konflikt stehen und müssen vor Gericht *verheben*, falls angefochten.
- Endbenutzer sollten in die Erstellung einbezogen werden.
- Sollten beschreiben was gemacht werden muss, nicht gemacht werden darf und was die Konsequenzen bei Fehlverhalten sind.
- Policies müssen **geschrieben, verteilt, gelesen, verstanden, zugestimmt UND durchgesetzt** werden
- Drei Arten: Enterprise InfoSec Policy, Issue-Specific Policy, System-specific Policy

# Audits

## Begriffe

- **Audit**: Untersucht, ob Prozesse, Anforderungen und Richtlinien die geforderten Standards erfüllen, oftmals im Rahmen eines Qualitätsmanagements. Audits werden von dem speziell hierfür geschulten *Auditor* durchgeführt.

- **Enterprise Governance**: Unternehmensführung & -lenkung, ein Set von Verantwortungen und Massnahmen des Managements zur Festlegung der *strategischen Ausrichtung*, Sicherstellung der *Zielerreichung*, *Risikomanagement* und *Ressourcenverwaltung*.

## COBIT

COBIT (Control Objectives for Information and Related Technologies) ist ein *good-practice* Framework der ISACA für IT Management und IT Governance. Darin werden *Steuerungsziele* basieren auf Unternehmenszielen festgelegt. Es wird vor allem das *was* geregelt, und nicht vorrangig das *wie*.

COBIT hat 34 kritische Prozesse definiert und in 4 Domains eingeteilt. Dazu gibts 318 detaillierte *Control Objectives*. Beipiele for *Detail Controls*:

**DS11 Manage Daten**

- Unternehmensanforderungen an Datenmanagement
- Speicherungs- und Aufbewahrungsvorkehrungen
- Entsorgung
- Backup und Wiederherstellung
- ...

## Definitionen

> **Kontrollen (Definition)** Der Begriff Kontrollen (*controls*) ist definiert als die Konzepte, Verfahren, Praktiken und Organisationsstrukturen, welche eine angemessene Gewissheit verschaffen, dass die Geschäftsziele erreicht und dass unerwünschte Ereignisse verhindert oder erkannt und korrigiert werden.

> **Kontrollziel (Definition)** Ein _Kontrollziel (*control objective*) ist eine Aussage zum gewünschten Resultat (Zweck), das mit der Implementierung von Kontroll(verfahr)en in einer bestimmten Aktivität

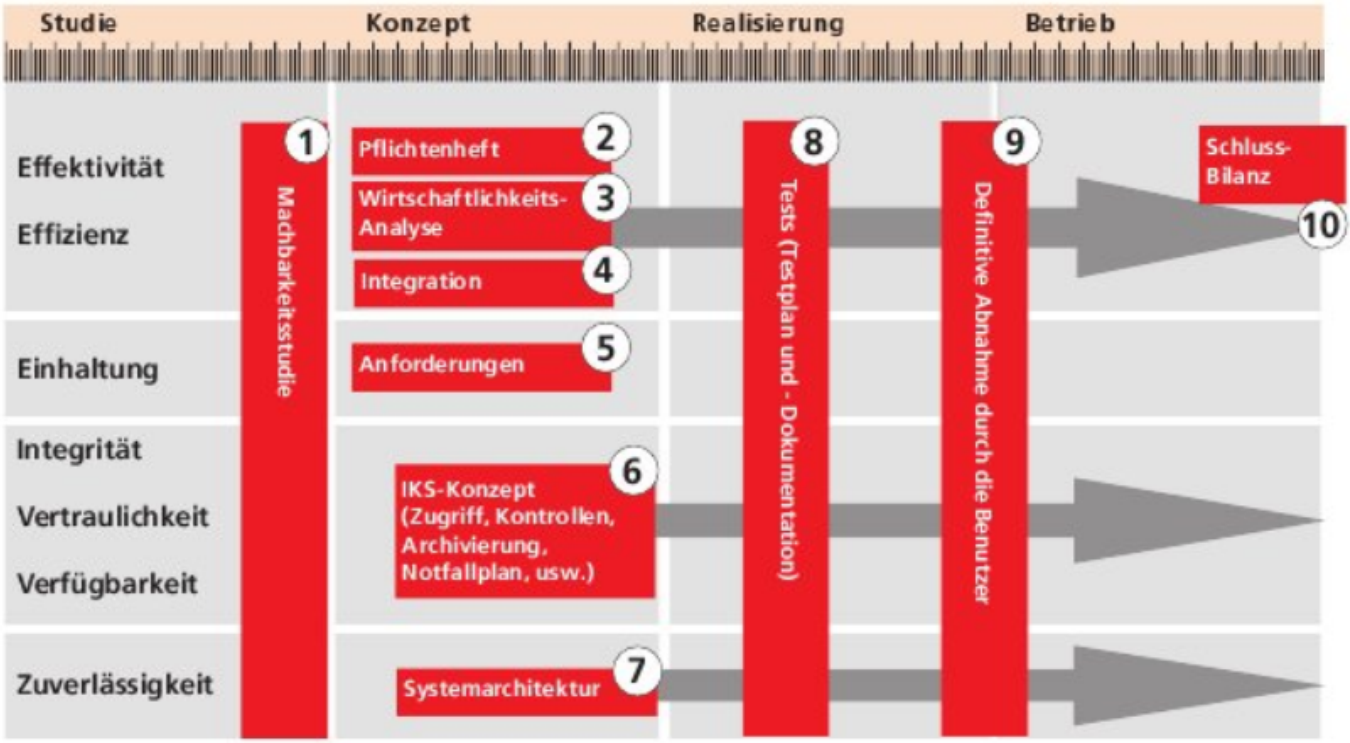
> erreicht werden soll.

## Projektzyklus

Die wichtigsten Ziele, die erreicht werden sollten:

- **Effektivität / Effizienz**: Zielerreichung, Ressourcenverwendung
- **Einhaltung**: Gesetze, Verträge, Reglemente
- **CIA**: Sicherstellung
- **Zuverlässigkeit**: Bereitstellung zuverlässiger Informationen

Die 10 Schlüsseldokumente eines Projektzyklus:




Der Projektverlauf wird von vielen Einflüssen geprägt: *Systemsicherheit, Risikobeurteilung, Normen und Standards, Strategiedefinition, Konfigurationsmanagement, Betriebsmanagement, Change Management usw. usf.*

## Genereller Ablauf eines IS-Audits

Um IS-Audits machen zu können braucht man folgendes:

- die Sicherstellung des Management-Supports,
- die Festlegung der verwendeten Standards und
- die Definition der Ziele und des Umfangs
- eine Geheimhaltungserklärung
- Sicherstellung des Budgets / Vertrags

Wenn man das alles hat, kann ein Audit geplant werden:

- Zielbereiche
- Personal

- Ablauf / Zeitplan
- Kickoff-Meeting
- Notwendige Hilfsmittel
- Zugriffsberechtigungen
- Interne Absprachen
- Kaffeepause
- Interview-Listen
- Sammlung von Evidents
- Auswertung von Informationen
- Vorschläge zur Verbesserung
- Periodische Risikoanalyse
- Regelmässiges Reporting
- Supervision
- Endbericht / Präsentation

# Human Factor

W5: https://elearning.hslu.ch/ilias/goto.php?target=file_3675384_download&client_id=hslu

Organisationen sind im Wandel von stark strukturierten, von internen Beziehungen *Maschinen* zu schwächer strukturierten, mehr von externen Beziehungen geprägten Beziehungen geprägten *Organsimus*.

## Security Culture

Charakteristiken für eine gesunde Sicherheitskultur:

- Empowerment
- Trust
- Openness
- Responsibility
- ...

### Awareness, attitude & behaviour

- **Awareness**: ist auf kreative Kommunikation angewiesen
- **Behavior**: ist geprägt von Wahrnehmung, Erfahrungen
- **Attitudes**: sind langfristig und schwer zu ändern

**Awareness** kann Zwischenfälle verhindern. Massnahmen zur Verbesserung (*sticky factors*):

- Ansprechende / provokante Bilder
- Einbeziehung des Publikums
- Einfache und klare Kommunikation
- Beschränkung auf das Wesentliche
- Kontinuierliche Verbesserung

Ein Awareness-Programm beginnt mit einer Vision und dem Messen der aktuellen Situation Anschliessend müssen Prozesse zur Generierung neues Wissens, Einstellungen, Verhalten, Rollen, Umgebungen, Systeme

usw. geschaffen werden. und mit *sticky factors* versehen werden. Anschliessend muss der neue Status gemessen werden, damit Aussagen über die Effektivität der Massnahmen getroffen werden können.

**Verhalten** kann von vielen Faktoren geprägt werden:

- Medienberichte
- Erfahrungen
- Umfeld, Umwelt & Umgebung
- Regeln und Prozeduren
- Beobachtungen
- Konsequenzen, Belohnungen & Bestrafung

Eine veränderte Welt mit steigender Mobilität, IoT und Clouds führt zu einer ständigen Vernetzung und somit auch zu Veränderungen in der InfoSec:

- Das Ende der Privatsphäre
- Identitätsbestimmung per Verhaltensanalyse im *Cyberspace*™
- Security mehr *probabilistisch* statt *deterministisch*
- Benutzer sind mächtiger, aber auch verwundbarer
- *We must learn to harness the power of the community* - Bernie Hammers

Das verlangt eine mobilere, abstraktere und vielfältigere IT-Security und andere Adjektive in denen *Security Dudes* traditionellerweise nicht so besonders stark sind.

## Corporate Security Model

1. Vision /Strategie
2. Security Policy
3. Bedrohungsanalyse, Risikoanalyse
4. Gegenmassnahmen, einzelne Sicherheitsvorkehrungen

Elemente der Dokumentation:

- Vision, Mission, Strategie
- Bedrohungs- und Verwundbarkeitsprofil
- Verschiedene Risikoanalysen, Risikomanagement
- Aufgabenbeschreibung *Information Security Officer*
- Management: Sicherheits-Policies, -Konzepte, -Kultur...
- Technologie: Disaster Recover, Firewall, Backup...
- Rechtliches: Verträge, relevante Gesetze, Nachweisbarkeit...
- Sicherheitsprojekte definieren

Die Dokumentation sollte sich an Frameworks und Normen orientieren wie ISO 2700x, CObIT etc.

# Risikomanagement und ISMS

## Lernziele

**Sie wissen, was unter Risiko, Risiko-Management und Risiko-Prozess verstanden wird und welche Ziele damit verfolgt werden**

> - Risiko = Potentieller Schaden
> - Risikomanagement = Umgang mit Risiken
> - Risiko-Prozess = R-Identifikation, R-Analyse, R-Bewertung, R-Behandlung, begleitende Aufgaben (Kommunikation, Kontrolle etc.)

**Sie erkennen den Zusammenhang von Governance, Risk und Compliance**

> TODO

**Sie kennen wichtige GRC Organisationen, Standards und Frameworks**

> - ISO 27001: ISMS (Information Security Management Systems)
> - BSI-Standards

##Risikomanagementprozess

1. Risikoidentifikation: *Assets (Schutzobjekte) festlegen, Abhängigkeiten definieren*
2. Risikoanalyse: *Existierende Massnahmen, Bedrohungen, Auswirkungen usw. tabellarisch erfassen in einem Riksikokatalog*
3. Risikobewertung: *Risikokatalog ergänzen mit Risiko-Bewertungen*
4. Risiko-Behandlung: *Risikokatalog ergänzen mit Massnahmen (Priorisierung, Termin, Budget, Status, Verantwortung*

# Disaster Recovery Planning & Data Backup Strategies

## Disaster Recovery Plan

ein DR-Plan besteht aus Richtlinien und Verfahren, die beschreiben was zu tun ist, wenn die IT-Services gestört sind, beispielsweise aufgrund von Naturkatastrophen, Sabotage oder *Cybercrime*.

Ziel ist es, die Geschäftsprozesse so schnell wie möglich wiederherzustellen durch erneute Inbetriebnahme der Systeme oder durch Ausweichen auf ein Notsystem.

Das **Business Continuity Management (BCM)** beschreibt Prozesse, welche das Weiterlaufen essentieller Geschäftsfunktionen nach einem Notfall und die schnelle Rückkehr zum Normalbetrieb sicherstellen. **DRP** sind Teil des BCM: technisch orientierte Dokumente, die es erlauben, verschiedene Systeme möglichst schnell wieder zum ordnungsgemässen Betrieb zu bringen.

Ein DRP umfasst folgende Aspekte:

- IT-Services: Welche Prozesse benötigen werlche Systeme?
- Akteure: Wer muss was machen beim Disaster Recovery Prozess?
- Lieferanten: Wer muss kontaktiert werden?
- Orte: Wo sind die Ersatzarbeitsplätze?
- Training: Welche Schulungen und Dokumentation stehen zur Verfügung?

## KPIs von DRPs

- **Recovery Point Objective (RPO)**: Zeitraum zwischen zwei Datensicherungen
- **Recovery Time Objective (RTO)**: Die maximale Zeitdauer zwischen Wiederherstellung und Normalbetrieb

## DR-Plan erstellen

- Einführung: Zusammenfassung der Ziele, abgedeckte Services, RTOs & RPOs
- Rollen und Verantwortlichkeiten
- Ereignisreaktion: Wann sollte der Plan ausgelöst werden, wer soll informiert werden
- DR-Prozesse: Welche Akteure starten welche Prozesse
- Anhänge: Listen, Formulare, relevante Dokumente

## DR-Plan leben

- Schulungen
- Verantwortlichkeiten vergeben
- Überprüfen
- Teilweise und dann auch komplett testen

# Data Backup

Daten sind auch für kleine Unternehmen oder Privatpersonen ein wichtiges Asset und deshalb schützenswert. Ein sinnvolles Backup sollte geplant werden:

1. Kritische Datensysteme identifizieren
2. Abhängigkeiten identifizieren
3. RTO und RPO festlegen
4. Benötigte Kapazitäten ermitteln
5. Ort für Offsite Storage festlegen

Backups gibts in verschiedenen *Flavors*:

- Full: Wiederherstellung simpel, braucht viel Speicher
- Full + Incremental: Wiederherstellung komplizierter, weniger Speicher
- Full + Differential: Öppis dazwischen
- Virtualisierung + Snapshots
- Continuous Data Protection: Änderungen loggen mittels dedizierter Hardware
- Replication: Duplikaton des System: Braucht viel Bandbreite

Die Aufbewahrungszeit und das Speichervolumen bestimmen, welches Speichermedium verwendet wird:

- Band
- CD / DVD
- Offsite / Internetbasiert
- Hybrid-Lösungen

Bei der Implementierung sollte folgendes beachtet werden:

- Überlast, Fehler, fehlende Daten

- Bandbreite, Kapazität
- Auswirkung auf Systemleistung
- Testen
- Strategie regelmässig prüfen / anpassen
- Dokumentation

# Datenschutz

## Persönliche Daten

Als **persönliche Daten** bezeichnet man *alle* Informationen, die eindeutig einer bestimmten Person zugewiesen werden können (direkt und indirekt via Identifikationsnummer). Insbesondere umfasst dies Angaben zu physischen, mentalen, sozialen, ökonomischen und kulturellen Merkmalen.

Dazu gehören beispielsweise:

- Sozialversicherungsnummer, Kontonummer, Führerschein
- Alter, Geschlecht, Grösse, Gewicht, Kleidergrösse
- Religionszugehörigkeit, Parteimitgliedschaft
- Geburtsdatum, Name, Wohnort
- Location data, Stromverbrauch

> Personal data is the new oil of the internet

-- *Scrooge McDuck*

### Kategorisierung von Kunden

Basierend auf den erhobenen Daten werden Kunden in Kategorien eingeteilt. Facebook beispielsweise ermittelt Zielgruppen anhand von 98 Datenpunken wie Ort, Sprache, Bildung, Einkommen, Beziehungsstatus, Automarke etc.

Solche Kategorien heissen dann beispielsweise *Elite Suburbs*, *Working Town* oder *Avec-Kunden*.

## Tracking und Targeting

Targeting (im Sinne von targeted advertising) geschieht mit verschiedenen Techniken:

- Browser- und Providerinformationen
- Os, Bildschirmauflösung und Bandbreite
- Geo-Targeting, GPS, IP-Adresse
- Cookies, Flash cookies, count pixels
- URL-Parameter
- JavaScript
- Social Media Plugins, z.B. Facebook Like Button

Als **fingerprinting** bezeichnet man die Identifizierung eines Benutzer anhand einer Kombination aus vielen Merkmalen, die zusammen eine eindeutige Identifikation ermöglichen.

Bsp: Treiberversionen + Systemschriftarten + installierte Browser-Plugins + Bildschirmauflösung + viele weitere Faktoren ermöglichen eine eindeutige Identifikation

## Smartphones

Inhalte werden vermehrt über Apps abgerufen. Diese verwenden kein HTTP, sondern eigene Kommunikationskanäle und haben oft Zugriff auf sehr viele persönliche Informationen wie Kontakte, Kalender, Lokation usw.

Schutzmöglichkeiten:

- vertrauenswürdiger App-Marks
- Kontrolle / Analyse von unabhängigen Parteien
- Apps mit integrierten Sicherheitsmechanismen

## Erkennungs- und Ortungstechniken

Lokationsdaten mit Zeitangaben reichen aus, um 95% aller Individuen zu identifizieren.

- Access Point vom Internet Service Provider
- WLAN
- Mobile Radio
- GPS
- Kreditkarte
- Kameras
- ...
-

Einfache Personenzähler und Gesichtserkennungssoftware sind weitere Arten Personendaten zu erfassen. *Computer Vision* kann beispielsweise das Geschlecht, Alter, Gemütszustand, aber auch Tracking durch Erkennen von *Landmarks* ermöglichen.

Massnahmen, um die Gesichtserkennung zu erschweren sind:

- Das Gesicht modifizieren (beispielsweise mit Farbe -> *CV Dazzle*)
- Anti-Photo-Massnahmen (*Camoflash*, Sensoren die bei für Autofokus typischen Infrarot-Signalen ein zu leuchten beginnen, um den Kontrast zu verhunzten).
- *Privacy Visor* - Brillen, die near-infrared Signale transmitten.
- Bildmanipulation mit *Photoshop©*. Other brands are available.

## Zusammenfassung

Es gibt viel verschiedene Arten, Waren und Menschen zu *tracken*. Gesichtserkennung wird wichtiger, es werden vermehrt Personen überwacht.

# Privacy

Der **Code of Fair Information Practices (1973)** sagt, es braucht:

- Benachrichtigung / Awareness bezüglich Datenerhebung
- Consent (opt-in vs. opt-out)
- Security
- Enforcement (Regeln, Gesetze)

Die **OECD** sagt, man muss folgendes definieren:

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguard
- Openness
- Individual Participation

## Purpose

Die Absichten hinter der Datenerhebung sollten ersichtlich sein.

## Consent

Das *Data Subject* muss (freiwillig) eine Einwilligung geben, oder anderweitig erkennbar man das *es* sein Einverständnis gibt, die Daten zu erheben und auszuwerten. Dies kann irgendeine Form haben, muss aber eine positive Aktion (?) sein und das *Data Subject* sollte verstehen, zu was es da zustimmt.

## Datenschutzrichtlinien

Datenschutzrichtlinien (*Privacy Policies*) informieren den Benutzer über die Datenschutz-Praktiken einer Website, damit diese entscheiden können ob sie das akzeptieren, ob sie opt-ins & opt-outs machen wollen usw.

Das ist zwar gut und richtig, in der Realität sind diese aber oft mangelhaft umgesetzt:

- schwer zu finden
- schwer zu verstehen
- zu lang
- werden geändert ohne zu informieren

Datenschutzrichtlinien sollten folgende Komponenten enthalten:

- Identifikation von Seite, Umfang, Kontaktinformationen
- Zugriffsinformationen
- Sicherheitsbestimmungen
- Erhobene Daten inkl. Cookies
- Verwendungszweck
- Datenaufbewahrungszeiten
- Verwendung und Weitergabe der Daten
- Infos zu opt-in/opt-out

Das sind zwar viele Infos, es sollte aber trotzdem kurz und einfach zu lesen sein.

# Datenschutz-Managementsysteme

Regeln und Verfahren für Organisationen, um Datenschutz (Gesetze EU, Bund, Kantone, Verträge und Standards) mit Prozessen zu erfüllen.

Planung, Entwicklung, Anwendung, Kontrolle und Verbesserung von organisatorischen und technischen Massnahmen und die Ermittlung des aktuellen Datenschutz-Niveaus.

Beschreibt was (nicht *wie*) zu tun ist, um Informationssicherheit (CIA, Nachvollziehbarkeit...) und Privatsphärenschutz (Erkennbarkeit, Einwilligung, Anonymisierung...) sicherzustellen.

## Die sechs Fragen des Datenschutzes

- Welche personenbezogenen Daten verarbeiten wir?
- Warum verarbeiten wir personenbezogene Daten?
- Wann können wir die personenbezogenen Daten vernichten?
- Wer wird Zugang haben und rechenschaftspflichtig sein?
- Wo werden wir die persönlichen Daten verarbeiten und speichern?
- Werden wir eine legitime Grundlage für die Verarbeitung haben?

# Anonymisierung

Oft übersehen: Testdaten sind meist eine direkte Kopie der Produktivumgebung und müssen deshalb gleich geschützt werden. Bei Auslagerung von Tests müssen also Vorkehrungen getroffen werden.

- Maskierung sensitiver und nicht-sensitiver Daten, wenn mit ihnen sensitive Daten wiedergestellt werden können
- Daten verfälschen, Rauschen hinzufügen aber Aggregatstatistik erhalten.
- Daten nicht verfälschen: Generalisierung durch Zusammenfassen in Wertebereiche (Alter: 20-29)
- Unterdrückung: Daten(sätze) entfernen

Anonymisierte Daten fallen (in Europa (mit Ausnahmen)) nicht mehr in den *scope of data protection legislation*.

## Bewertung der Attribute

- **Identifikator**: Attribut, das eine Person eindeutig bestimmt
- **Quasi-Identifikator**: Untermenge der Attribute, deren Kombination eine Person bestimmbar machen könnte
- **Sensitive Attribute**: Attribute, die nicht mit einer Person verknüpfbar sein sollten.

# *k*-anonymity

*k* Datensätze bilden eine Äquivalenzklasse bezüglich eines Quasi-Identifikators. Das führt zu einem Schutz mit Konfidenz 1/*k* vor einer korrekten Verknüpfung einer Person mit ihren sensitiven Attribut.

In einer *k-anonymous* Tabelle ist jedes Tupel vom mindestens k-1 anderen Tupeln nicht unterscheidbar (ausser in den sensitiven Attributen).

- Das Ziel des ganzen ist nicht der direkte Schutz von *sensiblen* Daten, sonder von *charakteristischen* Daten

Das ganze kann versagen, wenn die sensitiven Werte zu wenig Vielfalt haben, oder wenn der Angreifer Hintergrundwissen hat.