Grundlagen
Informationssicherheit und Datenschutz

Laiks GmbH

- Datenschutzberatung (keine Rechtsdienstleistungen i. S. d. § 2 Rechtsdienstleistungsgesetz)
- Stellung des externen Datenschutzbeauftragten
- Informationssicherheitsberatung
- Stellung des externen Informationssicherheitsbeauftragten
- Notallkonzepte (Planung und Umsetzung)
- Informationssicherheitsmanagementsystem (ISMS) Einführung
- KRITIS (§ 8a BSIG)
- Krisenmanagement im Schadensfall
- Coaching & Supervision
- Training in Gewaltfreier Kommunikation nach Marshall B. Rosenberg

Lars Christiansen

zertifizierter Datenschutzbeauftragter (udiszert, CIPP/E)

zertifizierter Informationssicherheitsbeauftragter

Lead Auditor ISO/IEC 27001

Prüfer für Kritische Infrastrukturen nach § 8a BSI-Gesetz (KRITIS)

Coach DGfC

Warum Informationssicherheit?

Gesetzliche Verpflichtung:

- EU-Datenschutzgrundverordnung (DSGVO)
- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
- NIS2-Richtlinie der EU, bis Ende 2024 Umsetzung in nationales Recht
  (Quickcheck: https://www.reuschlaw.de/news/nis2-richtlinie-quickcheck/)
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
- Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)
- Telemediengesetz (TMG)
- Telekommunikationsgesetz (TKG)
- Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)
- IT-Strafrecht im Strafgesetzbuch (StGB)

Informationssicherheit ist Schutz von Unternehmenswerte

Daten und Know-How sind wertvoll.

Verlust von Daten führt fast immer zu wirtschaftlichen Schäden.

Die Nichtverfügbarkeit von Daten kann die Existenz eines Unternehmens bedrohen.

Küchenhersteller insolvent durch Totalausfall der IT-Server

Der deutsche Küchenhersteller „rational einbauküchen“ hat Insolvenz angemeldet. Zuvor kam es durch einen Totalausfall der IT-Server zu einem Datenverlust, der nicht wiederhergestellt werden konnte.

Der deutsche Küchenhersteller Rational einbauküchen solutions GmbH hat bei dem zuständigen Gericht einen Antrag auf Eröffnung des Insolvenzverfahrens gestellt. Wie das Nachrichtenmagazin „Unternehmer Edition“ in seiner jüngsten Ausgabe berichtet, kam es zuvor zu einem Totalausfall der IT-Server, was zu erheblichen Schäden und somit zu einem irreparablen Datenverlust führte. Der vorläufige Insolvenzverwalter Pluta Rechtsanwalts GmbH teilte mit, dass die Produktion derzeit ruht, da die Serversysteme vollständig ausgefallen sind.

Nach knapp 60 Jahren meldet das Unternehmen rational einbauküchen Insolvenz an. Das bereits im Jahr 1963 gegründete Küchenunternehmen aus Osnabrück beschäftigt aktuell etwa 64 Mitarbeiter. Zum Sortiment des Herstellers gehören Küchen in verschiedenen Designs und mit unterschiedlichen technischen Ausstattungen. Die Produktion selbst erfolgt durch ein extern beauftragtes Unternehmen. Der Verkauf der Küchen erfolgt bundesweit und international in etwa 50 Ländern.

Der Betrieb des Unternehmens soll trotz Insolvenzverfahren zunächst einmal weitergeführt werden. Insolvenzverwalter Stefan Meyer von Pluta sagte dazu: „Wir werden gemeinsam mit der Geschäftsführung und der hochqualifizierten Belegschaft schnellstmöglich nach Lösungen suchen, damit für das Traditionsunternehmen nach der unumgänglichen Unterbrechung von Vertrieb, Planung, Produktion und Verkauf eine Zukunftslösung gefunden werden kann.“

Quelle: https://www.freihoff-gruppe.de/2022/10/04/kuechenhersteller-insolvent-durch-totalausfall-der-it-server/

Wie kann so etwas verhindert werden?

Durch Informationssicherheit!

Begriffsdefinitionen

Was ist Informationssicherheit?

Informationssicherheit ist ein Zustand von ***technischen*** oder ***nicht-technischen*** Systemen zur Informationsverarbeitung, -speicherung und -lagerung, der die Schutzziele ***Vertraulichkeit***, ***Verfügbarkeit*** und ***Integrität*** sicherstellen soll. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der ***Vermeidung von wirtschaftlichen Schäden*** und der ***Minimierung von Risiken***.

Was ist Datenschutz?

Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.

Schutz vor der missbräuchlichen Verarbeitung personenbezogener Daten.

In Deutschland auch das Recht auf informationelle Selbstbestimmung.

Datenschutz ist ein Schutzrecht des einzelnen Menschen gegenüber öffentlichen und nicht öffentlichen Stellen.

Was ist Sicherheit?

Die Norm IEC 61508 definiert Sicherheit als:

„Freiheit von unvertretbaren Risiken.“

Achtung!

Security = Sicherheit

Safety = Sicherheit

Security ≠ Safety

Security: **Schutz eines Systems vor beabsichtigten Angriffen.**

Safety: **Zuverlässigkeit eines Systems, speziell in Bezug. auf dessen Ablauf- und Ausfallsicherheit.**

Risikomanagement

- **Risiken identifizieren**
- **Risiken bewerten**
- **Risiken handhaben**

Risikomanagement als messbare Grundlage für Informationssicherheit und Datenschutz.

Schutzziele der Informationssicherheit

- **Vertraulichkeit**
- **Integrität**
- **Verfügbarkeit**

Zusätzliche Schutzziele aus dem Datenschutz

- Nichtverkettbarkeit
- Intervenierbarkeit
- Transparenz

Vertraulichkeit

Unter **Vertraulichkeit** versteht man, dass Daten nur von den Personen **eingesehen** oder **offengelegt** werden dürfen, die dazu **berechtigt** sind.

Beispiele für eine Verletzung der Vertraulichkeit

- Phishing Angriffe
- Zugang über unzureichend gesicherte Anmeldungen bei Cloud bzw. Onlinedienste
- Gestohlener Master-Key von Microsoft (06.2023)
https://www.security-insider.de/gestohlener-master-key-von-microsoft-a-e13eabefaeb7354292ddd63dfae063d0/
- Microsoft AI-Forscher verlieren 38 TByte an internen Daten (09.2023)
https://www.borncity.com/blog/2023/09/19/datenleck-microsoft-ai-forscher-verlieren-38-tbyte-an-internen-daten-ber-github-azure-cloud-speicher/

Integrität

Integrität bedeutet, dass es nicht möglich sein darf, Daten **unerkannt** bzw. **unbemerkt** zu ändern.

Beispiele für eine Verletzung der Integrität

- Verschlüsselung von Daten durch Ransomware.
- Unbeabsichtigte Übertragungsfehler
- Insider-Bedrohungen
- Cyberangriffe

Verfügbarkeit

Verfügbarkeit bedeutet, das Daten jederzeit **zugänglich** seien müssen, wenn sie benötigt werden.

Beispiele für eine Verletzung der Verfügbarkeit

- Kein ausreichendes Backup.
- Keine unterbrechungsfreie Stromversorgung.
- Nicht ausreichende Klimatisierung der Serverräume.
- Keine Redundanz wichtiger Systeme.

Risiko Dienstleister, Prüfung von zwei Dienstleistern aus den HR-Bereich:

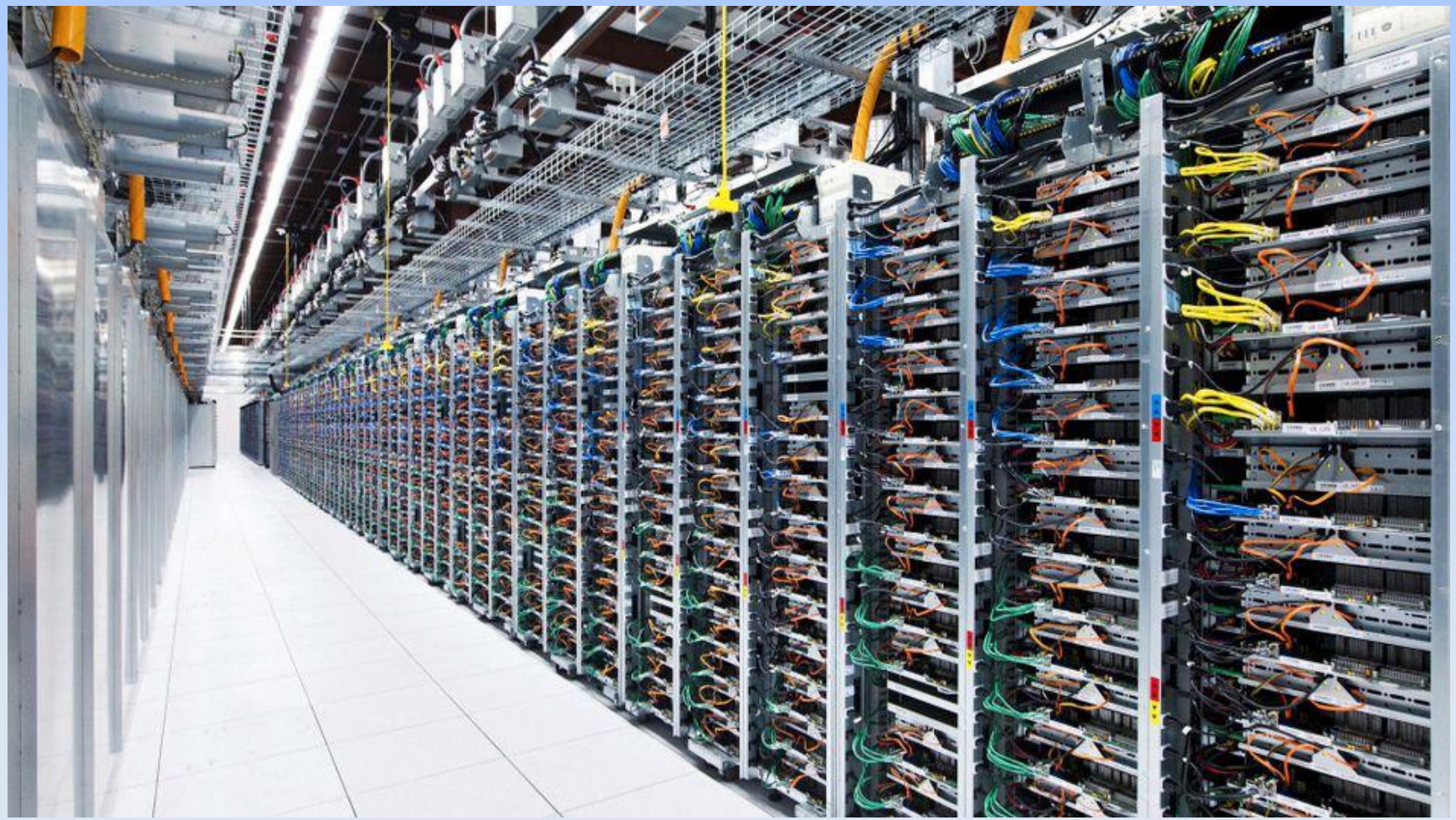
Frage nach dem Backup.

Antwort Firma 1: Wir nutzen iCloud.

Antwort Firma 2: Wir nutzen AWS, da kann es keinen Datenverlust geben.

Cloud garantiert nicht automatisch eine Verfügbarkeit der Daten!

Was ist eine Cloud?



Quelle: https://cloud.google.com

Straßburg 10.03.2021

Ein Rechenzentrum vollständig zerstört, ein weiteres RZ teilweise zerstört. Zwei RZ heruntergefahren.

30 % der betroffenen Daten nicht wiederherstellbar.

Lessons learned

Backup auf eigenen Systemen.

Regelmäßige Tests des Backups.

Ausreichend lange Speicherzeiten.

PS: Das ist kein gutes Backup ☺

Umsetzung von Informationssicherheit

ISMS

Informationssicherheitsmanagementsysteme

benötigen einen

kontinuierlichen Verbesserungsprozess

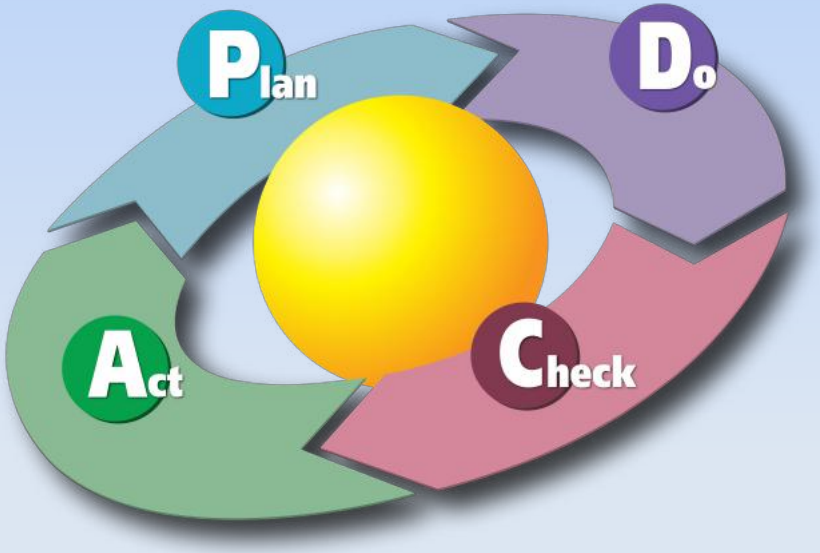


Diagram by Karn G. Bulsuk (http://www.bulsuk.com)

Normen der Informationssicherheit

ISO/IEC 27001:2022

Spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der IT-Risiken innerhalb der gesamten Organisation.

BSI IT-Grundschutz-Kompendium (Edition 2023)

„Das IT-Grundschutz-Kompendium ist die grundlegende Veröffentlichung des IT-Grundschutzes. Zusammen mit den BSI-Standards bildet es die Basis für alle, die sich umfassend mit dem Thema Informationssicherheit befassen möchten.“

DIN EN ISO 22301:2019

Anforderungen für die Erstellung und den Umgang mit dem Business Continuity Management System.

„Wo Fehler sind, da ist auch Erfahrung.“

(Anton Pawlowitsch Tschechow)

Aus der Praxis

Bei 74 % der Angriffe wurden menschliche Schwächen ausgenutzt, zum Beispiel in Form von Bedienfehlern, Missbrauch von Nutzerrechten, Nutzung gestohlener Anmeldedaten oder Social Engineering.

83 % der Angriffe wurde von Außenseitern verübt und finanzielle Bereicherung ist mit 95 % nach wie vor das weitaus häufigste Motiv.

Quelle: Verizon, Data Breach Investigations Report 2023

Aus der Praxis

- Gefälschte Anmeldeseiten von Cloud-Diensten sind ein hohes Risiko.
- Eine Anmeldung über Benutzername und Kennwort bietet keinen ausreichenden Schutz. Auch nicht bei komplexen Kennworten.
- Mehrfaktorauthentifizierung bietet einen deutlich höheren Schutz.
- Allerdings nur mit Hardware-Token, nicht mit Softwarelösungen!

Aus der Praxis

Durch die neue Cloud Synchronisation kann z. B. aus dem Google Authenticator eine Single-Faktor-Authentifizierung werden.
https://retool.com/blog/mfa-isnt-mfa/

Nur Hardware-Token als Multifaktor-Authentifizierung bieten vor solchen Angriffen einen ausreichenden Schutz.

Werbung von Youbikey mit Rachel Tobac, SocialProof Security
https://www.youtube.com/watch?v=UwPK_ietuxg

Best Practice

Was ist minimal umzusetzen?

- Usertraining / Awareness Training
- Firewall
- Netztrennung
- Antivirusprogramm
- **Backup**

Informationssicherheit und Datenschutz

Verantwortlich für Informationssicherheit und Datenschutz ist die Unternehmensleitung.

Beides ist **nicht** Aufgabe der IT-Abteilung.

Betrachten Sie bei der Risikobewertung neben der Informationstechnologie (IT) auch unbedingt die operative Technologie (OT).

IT-Grundschutz-Bausteine, IND: Industrielle IT

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

Und der Datenschutz?

Rechtliche Grundlagen

- EU-Datenschutzgrundverordnung (DSGVO)
- Bundesdatenschutzgesetz (neu) (BDSG n. F.)
- Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)
- Schweizer Datenschutzgesetz (DSG)
- California Consumer Privacy Act (CCPA)

Informationssicherheit in der DSGVO

Art. 32 DSGVO, Sicherheit der Verarbeitung

„ Unter Berücksichtigung des ***Stands der Technik***, der ***Implementierungskosten*** und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und ***Schwere des Risikos*** für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete ***technische und organisatorische Maßnahmen***, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein: die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
die Fähigkeit, die ***Vertraulichkeit***, ***Integrität***, ***Verfügbarkeit*** und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
ein ***Verfahren zur regelmäßigen Überprüfung***, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“

Informationssicherheit in der DSGVO

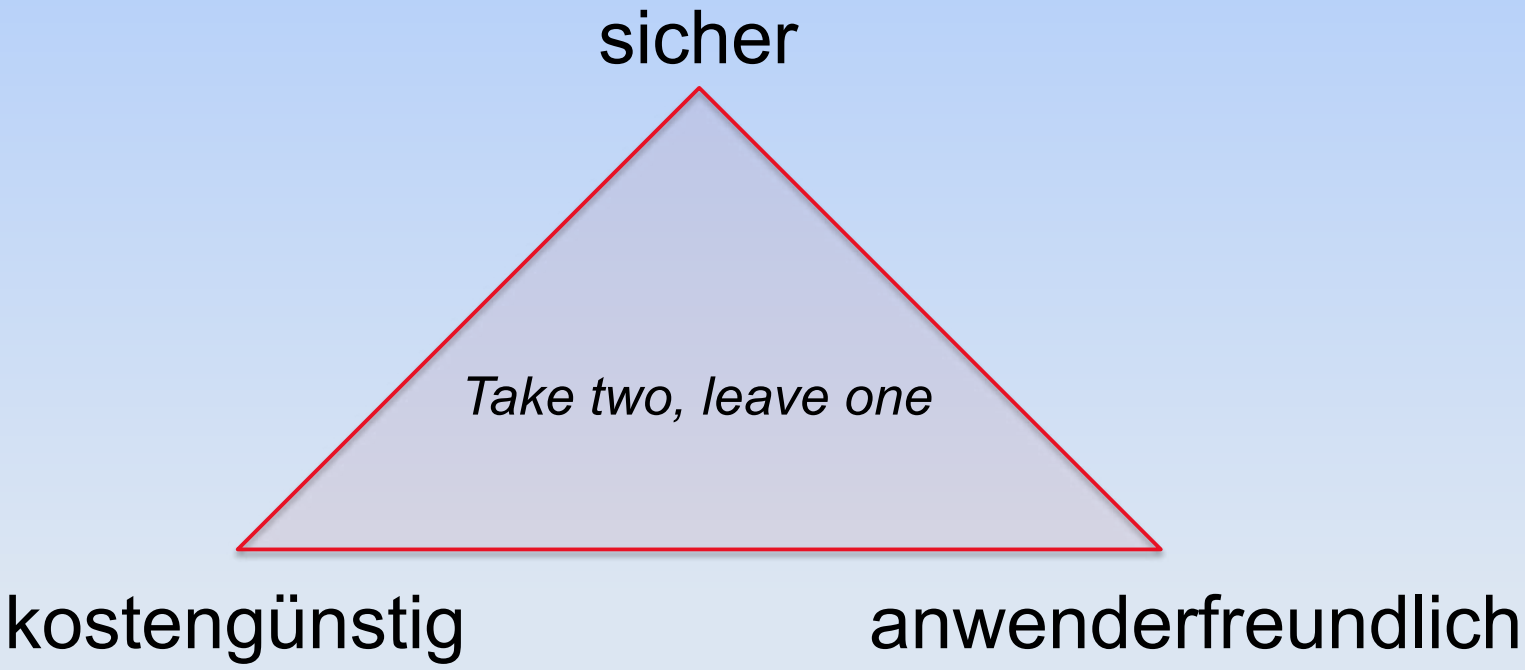
Was bedeutet Stand der Technik?

Handreichung „Stand der Technik“ des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT)

https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

Informationssicherheit in der DSGVO

Implementierungskosten



Datenschutz in Deutschland

Warum ist Datenschutz in Deutschland so unbeliebt?

- Mangelnde Kommunikation zur DSGVO durch den Gesetzgeber und die Aufsichtsbehörden für den Datenschutz.
- Fehlerhafte Kommunikation zur DSGVO durch Medien und Wirtschaftsverbände (z. B. Thema Einwilligung).
- Uneinheitliche Aussagen der deutschen Aufsichtsbehörden für den Datenschutz.
- Mangelnde Durchsetzung der eigenen Aussagen der deutschen Aufsichtsbehörden für den Datenschutz.
- Panikmache durch Verweis auf die hohen Bußgelder der DSGVO.
- Europarechtswidrige Regelungen im neuen BDSG (z. B. § 4 BDSG, Videoüberwachung)
- Umsetzung der ePrivacy-Richtlinie aus 2009 durch das TTDSG Ende 2021

Informationssicherheit durch Datenschutz

- Jedes Unternehmen verarbeitet personenbezogene Daten.

- Datenschutz gilt vollumfänglich unabhängig von der Größe des Unternehmens oder einer Benennungspflicht für einen Datenschutzbeauftragten.

- Wenn die Prozesse, mit denen personenbezogene Daten verarbeitet werden, dokumentiert werden müssen, dann gleich alle Prozesse der Datenverarbeitung aufnehmen.

- Eine Risikobewertung auch für nicht personenbezogene Daten durchführen und entsprechende Schutzmaßnahmen umsetzten.

Informationssicherheit durch Datenschutz

Work smart not hard.

- Ein Managementsystem lässt sich auch schlank aufbauen.
- Wenn schon Managementsysteme im Unternehmen etabliert sind, können Datenschutz und Informationssicherheit i. d. R. dort angegliedert werden.
- Risikobewertungen müssen durchgeführt werden, z. B. Arbeitssicherheit. Einheitliche Methoden des Risikomanagements können verwendet werden.
- KPIs auch für Datenschutz und Informationssicherheit definieren.
- Datenschutz und Informationssicherheit zusammen denken und Synergien nutzen.
- Datenschutz und Informationssicherheit frühzeitig in Projekte einbinden. Nachträglich funktioniert das nicht.

Und KI, oder Maschinelles Lernen?

„KI“ wirft viele Fragen in Bezug auf Informationssicherheit und Datenschutz auf.

- Wo findet die Datenverarbeitung statt?
- Wer hat Zugang zu den Systemen und den verarbeiteten Daten?
- Nach welchen Kriterien wurden die Systeme trainiert?
- Wer trainiert die Systeme?

Künstliche Intelligenz (KI) imitiert menschliche kognitive Fähigkeiten.

Bei **maschinellen Lernverfahren** erlernt ein Algorithmus durch Wiederholung selbstständig eine Aufgabe zu erfüllen. Die Maschine orientiert sich dabei an vorgegebenen Kriterien und dem Informationsgehalt der Daten. Ein Lösungsweg wird nicht vorgegeben.

Eine „KI“ ist aktuell nicht kreativ. Schöpfung/Kreation erfolgt nach wie vor ausschließlich durch den Menschen

Und KI, oder Maschinelles Lernen?

Spotlight auf Funktionsweise: GPT 3.5 mit Reinforcement Learning

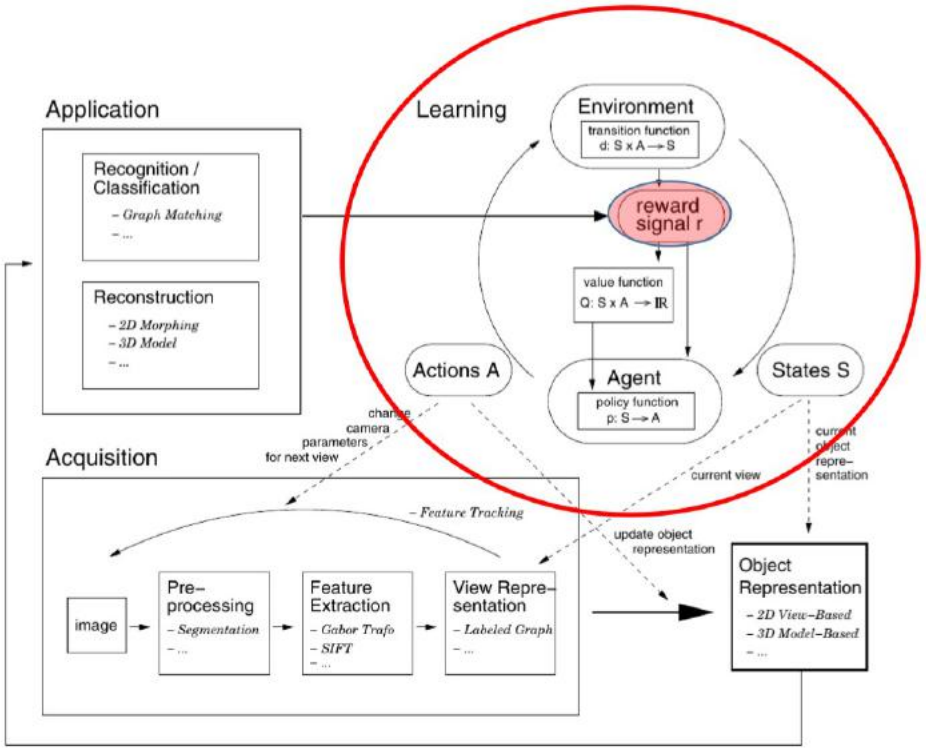


Figure 3. Architecture of a vision system that learns object representations.

aus: Gabriele Peters, *A Vision System for Interactive Object Learning*, 4th IEEE International Conference on Computer Vision Systems (ICVS 2006), New York, 2006.

GPT 3.5: Frage-Antwort-Sprachmodel für ChatGPT, wie DALL-E von Open AI

Reinforcement Learning entspricht operanter Konditionierung, Behaviorismus, Verhaltenstherapie

Lernen durch Belohnung und Bestrafung

Belohnung: positives reward signal r
Bestrafung: negatives reward signal r

Und KI, oder Maschinelles Lernen?

Rechtliche Regelungen zu KI?

„Am 14. Juni 2023 haben die Abgeordneten ihre Verhandlungsposition zum Gesetz über künstliche Intelligenz angenommen. Nun beginnen die Gespräche mit den EU-Mitgliedstaaten im Rat über die endgültige Ausgestaltung des Gesetzes.

Ziel ist es, bis Ende des Jahres eine Einigung zu erzielen.“

Quelle: https://www.europarl.europa.eu/news/de/headlines/society/20230601STO93804/ki-gesetz-erste-regulierung-der-kunstlichen-intelligenz

Vielen Dank für Ihre Aufmerksamkeit!

Laiks GmbH

Datenschutz und Informationssicherheit

Echternstr. 76
32657 Lemgo

Fon: +49 5261 / 2172591
Fax: +49 5261 / 2172593
Mobil: +49 170 5301383

https://www.ds-christiansen.de

info@ds-christiansen.de

IT-Sicherheitsbeauftragter

IRCA CERTIFICATED AUDITOR
INFORMATION SECURITY MANAGEMENT SYSTEMS