Fridel Rickenbacher ist ehemaliger Mitgründer, Co-CEO, Partner, Verwaltungsrat und nun beteiligter «Unternehmer im Unternehmen» / «Senior Consultant» bei der Swiss IT Security AG / Swiss IT Security Group. Auf Bundesebene ist er als Experte und Akteur vertreten bei «Digital Dialog Schweiz» + «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS». Er ist in seiner Mission «sh@re to evolve» seit Jahren als Redaktionsmitglied, Experten-Gruppen-

AI Readiness Strategie – «Un-Hype the Hype» mit Fokus auf «Compliance & Security»

Der Hype rund um die künstliche Intelligenz (KI/AI) und der sogenannten, inflationär referenzierten «AI Readiness/AI Strategie» zeigen bei vielen Organisationen auch nicht gemachte Hausaufgaben auf. Wie schon länger die «Digital Transformation» ist auch die «künstliche Intelligenz (KI/AI)» bzw. die entsprechende «AI Readiness» letztlich eine forcierte, immer dynamisch werdende Komponente / Weiterentwicklung gemäss «Stand der Technik». Nebst der technischen Dynamik bezüglich «Stand der Technik» ist die organisatorische Dynamik in Zukunft kaum mehr zu schaffen, wenn eine Zukunfts-Kompetenz wie z. B. die «Wandlungsfähigkeit» fehlt im «Mindset» der betroffenen Akteure.

Strategisches Daten- und App-Management – «know your data and apps»

Die KI ist stark abhängig bzw. aufbauend von den Daten und den Anwendungen, die sie speist, die sie nutzt und trainiert. Daher ist es für eine Organisation unerlässlich, ein strategisches Daten- und App-Management aufzubauen und weiterzuentwickeln. Dieses soll die Qualität, die Sicherheit, die Compliance und die Nachhaltigkeit der Daten und der Anwendungen gewährleisten in einer möglichst nachhaltigen Weiterentwicklung und Spezialisierung mit der diesbezüglich unterstützenden KI. Ein strategisches Daten- und App-Management sollte folgende Beispiel-Aspekte umfassen:

Datenschutz

Eine Organisation sollte die Einhaltung der Datenschutzgesetze/Regulationen und -richtlinien sicherstellen, welche die Verarbeitung personenbezogener oder firmenkritischen Daten regeln oder beeinflussen. Dabei sollte sie auch die Rechte und Interessen der Betroffenen respektieren und schützen, wie z. B. das Recht auf Auskunft, Berichtigung, Löschung, Widerspruch, Datenminimierung und Datenübertragbarkeit. Dazu gehören auch Konzepte und Ansätze von z. B. «privacy by design» oder «privacy by default». Die sogenannte «Datenschutzfolgenabschätzung» (DPIA) als ein unumgängliches Verzeichnis bzw. Instrument zur Risikobewertung von Datenverarbeitungen nach der EU-Datenschutz-Grundverordnung (DSGVO) ist hier ebenso ein wichtiges Element zur Vorabbewertung bestimmter Verarbeitungsvorgänge, um das Risiko von besonders schützenswerten, personenbezogenen Daten zu erkennen, zu bewerten und zu bewältigen.

Datensicherheit

Ebenso muss die Sicherheit der Daten und der Anwendungen gewährleistet werden, welche die KI speist und nutzt. Dabei sollte die Organisation geeignete technische und organisatorische Massnahmen ergreifen, um die Daten und die Anwendungen vor unbefugtem Zugriff, Verlust, Beschädigung, Manipulation oder Missbrauch bis hin zu auch z. B. Erpressung durch Cybercrime-Organisationen zu schützen. Dazu gehören wiederum z. B. «Security by design», «security by default», die Verschlüsselung, die Authentifizierung, die Zugriffskontrolle und die Überwachung bzw. das Monitoring.

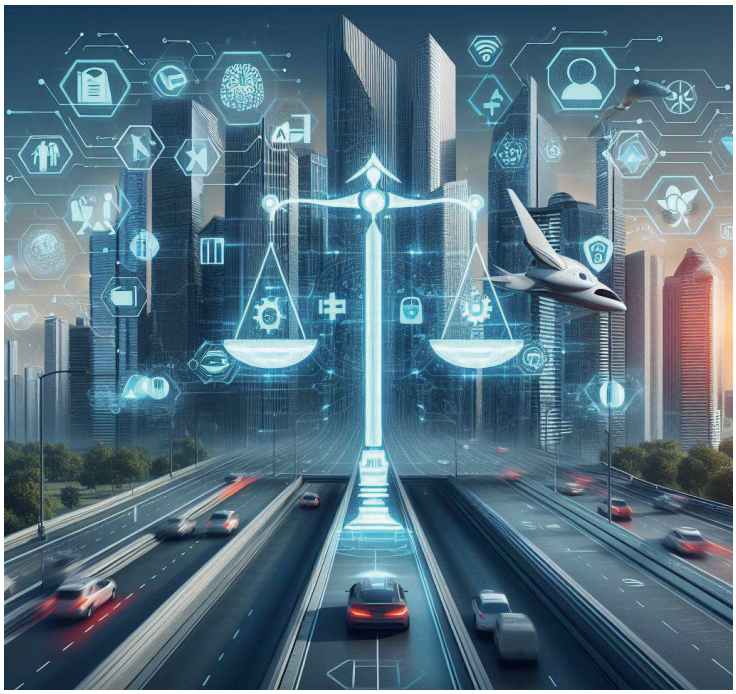
Compliance

Es ist wichtig, Prozesse zur Auswahl und Qualität von KI- und Cloud-Systemen, Risikoklassifizierung, Dokumentation, Einhaltung von Regulatorien, Informations- und Transparenzpflichten zu etablieren. Zunehmend ist speziell die möglichst automatisierte Überwachung und bei Bedarf Erzwingung der Einhaltung datenschutz-, datensicherheits-technischer, rechtlicher und ethischer Rahmenbedingungen zu etablieren und sicherzustellen. Bei den zunehmenden Komplexitäten bei Berechtigungen, Zugängen, Datenablagen, Freigaben/«Oversharing», Schnittstellen bis hin zu auch kritischen Datenabflüssen mit Folgeschaden-Potenzial usw. sind entsprechende organisatorische und technische (bei Bedarf auch automatisiert erzwingbare) Richtlinien mitunter unumgänglich gemäss «Stand der Technik» und «best practices».

und Verbands-Aktivist tätig bei z. B. SwissICT, s-i.ch, isss.ch, isaca.ch, bauen-digital.ch rund um Digitalisierung, Engineering, Clouds, ICT-Architektur, Security, Privacy, Datenschutz, Audit, Compliance, Controlling, Information Ethics, in entsprechenden Gesetzes-Vernehmlassungen und auch in Aus- und Weiterbildung (CAS, eidg. dipl.).

Auftragsverarbeiter- und Kernapplikations-Verzeichnis

Nicht nur aus regulatorischen Notwendigkeiten sollte ein Verzeichnis geführt werden, welches allen Auftragsverarbeiter/Kern-Applikations-Lieferanten und entsprechende relevante Partner auflistet, die im Rahmen der KI-Nutzung personenbezogene oder firmensensitive Daten – auch speziell entwickelte Algorithmen / Codes / Scripts / Apps usw. – im Auftrag der Organisation verarbeiten, speichern oder auch supporten. Dabei sollte sie auch die Art, den Umfang, den Zweck und die Dauer der Datenverarbeitung sowie die Gewährleistungen für die Einhaltung der Datenschutzvorschriften, «Stand der Technik» oder akzeptierte «best practices» / «good practices» dokumentieren. Diese Verzeichnisse sind ebenso einzelne, wichtige Bestandteile für eine «Business Kontinuitäts-Planung» (BCP) bzw. hilfreich bei Vorfällen und Massnahmen im Rahmen vom sogenannten «Incident Response Management/Planning».



Know-how-Management

Speziell das Wissen/Dokumentation und die spezialisierten Fähigkeiten über die Daten und die entwickelten Anwendungen/Algorithmen/Modelle, die die KI speist und nutzt, sollte dokumentiert, intern auf möglichst mehrere Know-how-Träger/Keyuser/Poweruser verteilt und gepflegt werden. Dieses Know-how-Management sollte je nach Abhängigkeit auch gar auditierbar sein von Dritten oder neuen Partnern. Dabei sollten auch die Kompetenzen und die Verantwortlichkeiten für die Daten- und App-Verwaltung klar definiert und verteilt werden auf «mehrere Know-how-Träger», bei Bedarf und je nach Kritikalität auch unterstützt durch externe Spezialisten. Dazu gehören z. B. auch die erweiterte Daten- und App-Modellierung, -Bereinigung, -Anreicherung, -Analyse, -Visualisierung/Dokumentation und -Aktualisierung bei kritischen Kernapplikationen. Solche speziellen Massnahmen sind mitunter sehr relevant auch bei speziell schützenswerten Anwendungen und Methoden gegenüber Mitbewerbern (Intellectual Property/geistiges Eigentum).

Evaluationen von neuen Systemen / Tools / ERP

Eine Organisation sollte die Eignung und die Auswirkungen von neuen Systemen, Tools oder ERP, die die KI speisen oder nutzen, sorgfältig prüfen und bewerten. Dabei sollten auch die Anforderungen und die Erwartungen aller Stakeholder und vor allem internen Akteuren/Anwender berücksichtigt und einbezogen werden. Dazu gehören z. B. die Integration in KI-/Cloud-Systemen, Kompatibilität (zu z. B. Cloud-Lösungen), Schnittstellen-/API-Unterstützung, App-Verfügbarkeit auf diversen Plattformen, Funktionalität, Benutzerfreundlichkeit, Kompatibilität, Skalierbarkeit, Automatisierungsoptionen, Kosten bis gar hin zur messbaren Leistung und Nachhaltigkeit des zukunftsorientierten Nutzens. Diese Evaluation muss entsprechend in mehreren Aspekten weiter gehen bis hin zur auch z. B. Unterstützung der maximierten Angriffs- und Betriebssicherheit, Datenschutz, Datensicherheit, Compliance in der dynamischen Bedrohungslage gemäss «Stand der Technik». Speziell im Trend von «LowCode»/«NoCode» werden immer mehr Fragen und Anforderungen gestellt in den Evaluationen in Richtung von «make or buy» in der Kombination von neuen Lösungen («buy») mit einzelnen selber oder unterstützt erstellten Apps, KI-Tools, Automatisierungen und Optimierungen («make»).