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 Regeln und Adaption

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.

«Rules before Tools» – Regeln bevor neue Werkzeuge zum Einsatz kommen

Bevor eine Organisation die KI implementiert und anwendet, sollte sie jedoch einige grundlegende Regeln und auch ICT Security Policy / Compliance Definitionen («know your data and rights» beachten, die den Datenschutz/Datensicherheit, die Qualität und die Nachhaltigkeit bis hin zur Ethik der KI und Digital-DNA-Transformation gewährleisten. Folgende Beispiele einer solchen Regel/Grundlage können hier helfen:

ICT Security & Dataprotection Policy

Vor der Einführung/Adoption von neuen Tools sollte man eine klare und konsistente Richtlinie für die Informationssicherheit (Datenschutz und Datensicherheit) haben, die die Ziele, die Verantwortlichkeiten, die Regeln, Weisungen, Massnahmen und die Kontrollen für den Schutz der Daten, Berechtigungen und der Systeme vor internen und externen Bedrohungen definiert. Dabei sollte sie auch die spezifischen Risiken und Herausforderungen berücksichtigen, die die KI mit sich bringt, wie z. B. die Anfälligkeit für Manipulation, die Abhängigkeit von Drittanbietern, Urheberrechtsfragen, Schutz von personenbezogenen oder firmenkritischen Informationen und bis hin zur einer Unvorhersehbarkeit (Systemgläubigkeit) des Verhaltens oder Outputs mit Folgeauswirkungen.

Sensibilisierung und Aufklärung

Das Bewusstsein und das Verständnis für die KI (und speziell hier immer wieder auch für die nicht zu vergessende «Cybersecurity Sensibilisierung») sollte bei allen Anwendern / Stakeholdern / Akteuren aktiv gefördert werden, die von der KI betroffen sind oder die KI bzw. deren Anwendung auch mitgestalten können. Dabei sollte sie nicht nur die Vorteile und die Chancen, sondern auch die Grenzen und die Risiken der KI transparent und ehrlich kommunizieren, um falsche Erwartungen, Ängste und Widerstände zu vermeiden. Erst mit einem richtigen, an die Organisation angepasstem «Mindset» (Einstellung, Richtung der Gedanken) und ausgewogenen Rahmenbedingungen (z. B. auch passendes «toolset» und «skillset) kann erst die passende KI-Anwendung und Innovation zielführend Einzug halten mittels einer sogenannten «Adoption» und auch gezieltem «Prototyping» rund um identifizierte, lohnenswerte «use cases» (Anwendungsfälle).

Critical Thinking / gesunder Menschenverstand

Das mit der fortlaufenden Digitalisierung immer kritischer werdende Denken sogenanntes «Critical Thinking» und die Urteilsfähigkeit muss bei allen Anwendern / Stakeholdern / Akteuren geprägt und sensibilisiert werden, die mit der KI interagieren oder letztlich abschliessend entscheiden müssen. Dabei sollte sie nicht nur die technischen und funktionalen Aspekte, sondern auch die ethi-

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.).

Fridel's BLOG

schen und sozialen Auswirkungen der KI berücksichtigen, um verantwortungsvolle und nachhaltige Entscheidungen (am Ende entscheidet immer noch der Mensch) zu treffen bei der Anwendung / Weiternutzung / Weitergabe von KI-Outputs.

Die mitunter gefährliche Systemgläubigkeit bei vor allem AI-Fehlinformationen/Desinformationen, aber auch bei Social Engineering / Cybercrime / Deep Fake Attacken ist mittels neuer Kompetenzen wie z. B. «Critical Thinking» oder auch durch den guten alten «gesunden Menschenverstand» zu reduzieren. -> Ein Prinzip findet hier auch Anwendung «Zero trust, always verify». Der gesunde Menschenverstand / «Common sense» ist auch kulturell und gesellschaftlich unterschiedlich geprägt über Generationen und entsprechend sehr komplex. Dieses Selbstverständnis bezüglich genau diesem Verstand für uns Menschen ist auch für die «stärkste» KI sehr schwer oder (noch) gar nicht zu verstehen.

Schulungen und neue Kompetenzen

Die sich anzupassenden Kompetenzen und Fähigkeiten bei allen Anwendern / Stakeholdern / Akteuren müssen weiterentwickelt werden, die die KI nutzen oder die KI mit-gestalten müssen oder «dürfen». Dabei sollte sie nicht nur die fachlichen und methodischen Kenntnisse, sondern auch die persönlichen und sozialen Fertigkeiten («Toolset», «Skillset») vermitteln, um die KI effektiv und effizient zu bedienen, zu überwachen, zu verbessern und zu innovieren. Speziell bei den Schulungen und Erlangen von neuen Kompetenzen muss seitens der Organisation auch entsprechend investiert werden in dedizierte (nicht nur parallele) Zeit und Prioritäten in z. B. gezieltem «Prototyping» rund um identifizierte, lohnenswerte «use cases» (Anwendungsfälle). Empfehlenswert ist auch die Definition und Aufbau von internen «PowerUsers» («Influencer»), welche das Wissen möglichst intern auf- und ausbauen und auch der ganzen Belegschaft (potenzielle «Followers») als Erstansprechpartner zur Verfügung stehen beim Aufbau und Ausbau vom möglichst am besten passenden «Toolset» / «Skillset» / «Mindset».

Menschen werden nicht einfach so durch die KI ersetzt, jedoch werden Menschen eher mal «ersetzt» mit Menschen, welche mit KI/Tools umgehen und interagieren können mittels eines «smarten Dialogs und Interaktion» anstelle «statischem Anwenden von beschränkten Tools und unstrukturierten Daten». Wie früher erwähnt: 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

Fortsetzung Seite 31

im «Mindset» der betroffenen Akteure.

LowCode/NoCode
Die Zugänglichkeit, Qualität und die Benutzerfreundlichkeit der KI bzw. Tools sollte optimiert und trainiert werden, indem Plattformen, Werkzeuge, Apps, Vorlagen angeboten werden, die es den Anwendern / Stakeholdern / Akteuren ermöglichen, KI-basierte Tools ohne oder mit wenig Programmierkenntnissen (LowCode) zu nutzen, erstellen, zu konfigurieren und zu modifizieren. Genau hier braucht es aber mitunter ein sehr vertieftes, «menschliches» Grundverständnis und genaue Analyse-/Beschreibungskompetenz des zu lösenden Problems oder zur z. B. erreichenden Optimierung / Automatisierung / Effizienzsteigerung.
Dabei sollte die Organisation aber auch die Qualität und die Zuverlässigkeit sicherstellen, indem sie Standards und Richtlinien für die Entwicklung, die Prüfung und die Freigabe solcher KI-Anwendungen auf Basis von «NoCode»/«LowCode» festlegt.

Compliance
Eine Organisation sollte die Rechtmässigkeit und die Konformität der KI gewährleisten, indem sie die geltenden Gesetze, Vorschriften, eigenen Organisationsrichtlinien, ICT Security & Dataprotection Policy («know your data») und Normen einhält, die die KI regulieren oder beeinflussen. Dabei sollte sie auch die Anforderungen und Erwartungen der Anwender / Stakeholder / Akteure erfüllen, die die KI bzw. deren Outputs überwachen oder bewerten, wie z. B. die Behörden, die Kunden, die Partner und die Gesellschaft.

Business Continuity Planning
Die businesskritische Verfügbarkeit und die Widerstandsfähigkeit (Resilienz) und letztlich die Angriffs- und Betriebssicherheit der IT/KI bzw. den darauf basierten Tools / Apps / Schnittstellen muss sichergestellt werden, indem entsprechende Pläne und Massnahmen (z. B. «Business Contingency Planning») für den Fall von Störungen, Ausfällen, Katastrophen und auch Datenschutz-/Cybercrime-Vorfälle vorbereitet (inkl. auch Krisen-Kommunikationskonzept), die die KI beeinträchtigen oder unterbrechen können. Dabei sollten auch die Alternativen und die Notfalllösungen (z. B. Notfall-Betrieb während Incident Response / Business Recovery, halb-automatischer Betrieb usw.) bereitgestellt und getestet werden, die die KI/Tools überbrücken, ersetzen oder ergänzen können, wenn die KI nicht oder «falsch» funktioniert oder nicht verfügbar ist.

Datenschutz-Folgenabschätzung
Die zu schützende Privatsphäre und die Persönlichkeitsrechte der Anwender / Stakeholder / Akteure / Kunden / Mitarbeiter haben höchste Priorität, indem auch z. B. die potenziellen Auswirkungen der KI auf die Verarbeitung personenbezogener oder firmenkritischen Daten analysiert und bewertet werden mit entsprechenden Massnahmen und Szenarien in einer Datenschutz-Folgenabschätzung und auch z. B. Auftragsdatenverarbeiterverzeichnis / Kernapplikationsverwaltung. Dabei sollten auch Massnahmen / Prinzipien definiert und ergriffen werden können, die die Risiken und die Nachteile der KI/Cybersecurity generell minimieren oder beseitigen, wie z. B. Security by design, security by default, privacy by design, privacy by default, die Anonymisierung, die Pseudonymisierung, die Verschlüsselung und die Löschung der Daten.

Digital-DNA-Codex -> Effizienz als gemeinsames Ziel
Zusammengefasst aus allen diesen Regeln und Massnahmen sollte auch ein Digital-DNA-Codex/ICT-Weisungen entstehen und verabschiedet werden aus einem gemeinsamen und für die Organisation passenden Verständnis für die möglichst effiziente und sichere Zusammenarbeit. Dieses Regelwerk fasst dann die best passenden Anwendungen, Standards und Qualitätsanforderungen zusammen im orchestrierten «Toolset», «Skillset» und «Mindset» der Organisation zugunsten der Fokussierung auf «Effizienz» bis hin zum strategischen Ziel einer «Hyperautomation».

Ein solcher «echt gelebter und angewandter» Digital-DNA-Codex/Digitalisierungs-Maturität kann ja zukünftig gar als Gütesiegel und Unterscheidungs-Merkmal kommuniziert und beworben werden im Wettbewerb.

Das kann mitunter auch bei der diesbezüglich zunehmend relevanten Arbeitgeber-Attraktivität, Rekrutierung im Fachkräftemangel und strategischem Talentmanagement hilfreich sein.

Teil 3
in der nächsten Ausgabe