**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-

# Auch das «digitale» Wasser findet seinen Weg

### Der «Stand der Technik» und die «zunehmende Regulation» findet seinen Weg – wie Wasser

Bei der Digitalisierung und speziell in Bereichen Cybersecurity und Künstlicher Intelligenz (KI/AI) ist es ähnlich wie beim Wasser. Es wird seinen Weg irgendwie finden und zum Ziel vor- oder/und eindringen. Es liegt weiterhin und fortwährend an uns, den Weg dieses grösser werdenden Flusses mitzugestalten oder gar möglichst passend zu leiten.

Der weiter stark angestiegene «Hacktivismus» (diese finden ihren Weg ebenfalls wie das Wasser …) der höchst professionell agierenden und leider sehr «erfolgreichen» Cybercrime-Organisationen war entsprechend auch dazu passend wieder im Fokus des halbjährlichen NCSC-Berichtes (Nationale Zentrum für Cybersicherheit).

Akzentuiert geprägt seit dem Jahre 2018 mittels der Europäischen Datenschutz-Grundverordnung und nun auch teilweise adaptiert und nun definitiv in Kraft getreten seit dem 1. September 2023 mittels des neuen schweizerischen Datenschutz-Gesetzes finden sich juristische und natürliche Personen mit weiteren Regulationen und Herausforderungen konfrontiert.

### Nicht gemachte Hausaufgaben in «Stand der Technik» und dynamischen Bedrohungslagen

Vor allem rund um Datenschutz, Datensicherheit, ICT-Risikomanagement, ICT-Strategie, zugunsten der optimierten Angriffs- und Betriebs-Sicherheit und zum «Schutz der digitalen Identität» ergeben sie weitere technische und organisatorische Hausaufgaben.

Viele der wertstiftenden Potenziale zugunsten von «Secure Modern Work» (sicheres, modernes und effizientes Arbeiten) bei möglichst passendem «Automatisierungs-Grad» sind entsprechend noch komplexer geworden und nur effektiv erschliessbar mit entsprechenden Prioritäten und Budget (Zeit und Geld).

Die hohe Dynamik von Umweltfaktoren wie z. B. Wirtschaft, Gesellschaft, Cybersecurity, Geopolitik, Stand der Technik verlangt entsprechend auch eine hohe Agilität und Flexibilität in entsprechenden organisatorischen und technischen Massnahmen bis hin zu einer immer agiler werdenden ICT-Planung/ICT-Strategie.

### Die Künstliche Intelligenz (KI/AI) – Fluch oder Segen / Evolution oder Revolution?

Künstliche Intelligenz (KI) ist ein Thema, das mitunter viele Fragen aufwirft. Es gibt sowohl Befürworter als auch Kritiker. Einige glauben, dass KI mehr als eine Evolution bzw. eine regelrechte Revolution in der Technologie darstellt, während andere befürchten, dass sie zu einem gar schlimmeren und noch schlechter berechenbaren Fluch als bisherige «Dunkle Seiten der Macht» (wie eben z. B. Cybercrime) werden könnte. Die effektiv eintretende Wahrheit und Realität in unserem Privat- und Geschäftsleben liegt wahrscheinlich irgendwo dazwischen.

Was aber definitiv wie beim Datenschutz/Datensicherheit und diesbezüglich speziell beim «Schutz der digitalen Identität» eine weitere Hausaufgabe sein wird, ist möglichst ein guter Schutz und Kontrolle von sogenannten «AI/KI Assets».

Ein Ansatz besteht darin, einen Rechtsrahmen für KI zu schaffen, der die Verwendung von KI-Systemen regelt und sicherstellt, dass sie sicher und ethisch möglichst einwandfrei sind. Ein weiterer Ansatz besteht darin, die Sicherheit von KI-Systemen durch die Verwendung von Sicherheitsmechanismen wie Verschlüsselung, Zugriffskontrollen, Authentifizierung und entsprechendem Monitoring zu erhöhen. Hierbei kommen auch Grundsatzprinzipien wie z. B. «security & privacy by default / by design» und entsprechenden ICT-Security Policies / Anwendungsrichtlinien zum Einsatz, welche dann hoffentlich auch «good und best practices» gemäss jeweiligem «Stand der Technik» mitprägen und möglichst breite und akzeptierte Anwendung finden.

### Booster-Impfung zugunsten Stand der Technik, Know-how und Halbwert-Zeit des Wissens

Eine Impfung sollte möglichst freiwillig sein und bleiben. Regulatorische Vorgaben und anerkannter «Stand der Technik» / «Best Practices» rund um den Datenschutz und Datensicherheit in Hybrid Cloud-Umgebungen zwingen jedoch zunehmend zu einer «Impfung mit neuem Wissen in technologischen und prozessualen Standards».

Spezielle (R)Evolution-Stufen wie z. B. das «plötzlich sehr nah greifbare

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.).


und nutzbare Universum von KI/AI» mit deren Chancen und Risiken und weitere «Regulationen rund um Datenschutz/Datensicherheit» im Zuge der dynamischen Bedrohungslage der Cybersecurity sollten möglichst allen Akteuren per fortwährender Sensibilisierung noch näher gebracht werden.
Vor allem auch der Faktor Mensch als wichtigster Akteur und Betroffener sollte gezieltes Know-how, Sensibilisierung und den höchsten Stellenwert erhalten, als Mitgestalter einer solchen Forcierung oder Weiterentwicklung in der «Digital Transformation».
Die Halbwerts-Zeit einer solchen «Digital-DNA-Booster-Impfung» mittels z. B. Know-how-Transfer oder «Stand der Technik», nimmt stetig ab und bedürfen einer nachhaltigen (Kampagnen)Planung und proaktiven Förderung.

**Es gibt nicht DIE EINE «Digital-DNA» in einer Organisation – aber irgendeine muss es sein**

«Digital DNA» ist ein Begriff und auch eine Methodik in einer Digital Transformation, der sich auf die Fähigkeiten und Kompetenzen bezieht, die für die Arbeit in einer digitalen und möglichst schlanken/automatisierten Organisation erforderlich sind. Es gibt drei diesbezügliche Hauptkomponenten des «Digital DNA»: Mindset, Skillset und Toolset. Eine solche «Digital DNA» ist speziell immer relevanter geworden bezüglich der mitunter laufenden technologischen Weiterentwicklungen (speziell derzeit auch KI/AI), Herausforderungen und «nicht mehr verschiebbaren Hausaufgaben».
Daraus kann ein regelrechtes Framework/Methodik (bis hin zur Verankerung im QMS) entstehen für die Effizienzsteigerung im Rahmen der Digital Transformation durch intelligente Orchestrierung und seitens Akteuren mitentwickelter Kombination von Cloud-/ICT- und AI-Lösungen und internen und externen Anwendungen/Anweisungen.

*Mindset:* Das Mindset bezieht sich auf die Einstellung und Richtung der Denkweise, die erforderlich ist, um in einer digitalen Umgebung erfolgreich zu sein – speziell auch im Teamwork. Ein digitales Mindset erfordert Offenheit, Flexibilität und die Fähigkeit, schnell zu lernen und sich an Veränderungen anzupassen, welche man auch mitgestalten und mitprägen kann.

*Skillset:* Das Skillset bezieht sich auf die Fähigkeiten und Kenntnisse, die erforderlich sind, um in einer digitalen Umgebung erfolgreich zu sein – in z. B. der Selbstorganisation oder auch im Teamwork. Dazu gehören technische Fähigkeiten wie Grundlagenverständnis, Fachbegriffskenntnisse, erweiterte Anwendungskenntnisse bis hin zu gar einfachen modularen, vorlagenbasierten Programmierung / App-Erstellung / Flow-Generierung, Datenanalyse und Cybersicherheit sowie Soft Skills wie Kommunikation, Zusammenarbeit, Problemlösung und Prototyping.

*Toolset:* Das Toolset bezieht sich auf die Werkzeuge und Technologien, die in einer digitalen Umgebung verwendet werden. Dazu gehören Softwareanwendungen, Apps, Vorlagen, Flows, Cloud-Plattformen, aber auch soziale Medien, mobile Geräte und Security-Technologien.

Es ist wichtig und mitunter auch beinahe gar unumgänglich geworden, alle drei Komponenten des «Digital DNA» passend für die eigene Organisation zu entwickeln, um in einer digitalen Umgebung und im globaler werdenden Wettbewerb (spez. beim Fachkräftemangel können entscheidende Unterschiede entstehen bei z. B. Rekrutierung in eine Organisation mit einer «hohen und attraktiven DIGITAL-DNA-Maturität» im Vergleich zu anderen Arbeitgebern) erfolgreicher zu werden und zu bleiben. Dabei gibt es eben für jede Organisation zu berücksichtigende, unterschiedliche Rahmenbedingungen und angestrebte/erreichbare Maturitätsstufen (Reifegrade) je nach auch z. B. Arbeitsplatz / Jobprofil / Arbeitsumfeld / Branche / Automatisierung-Potenziale und Regulationsvorgaben.