Fridel Rickenbacher ist Mitbegründer, Partner, Geschäftsführer und Verwaltungsrat der MIT-GROUP, einem Totalunternehmen für «Empowering for the 4th Industrial Revolution» und Informations- und Kommunikationsmanagement. 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

Der Reifegrad / Monetization von «data driven» Business Modellen kann gefördert werden mit Involvierung der Mitarbeiter und robusten und innovativen ICT-Prozessen

Dies vorallem als Initial-Impuls auch durch stufengerechter Involvierung und Verständnisförderung der Mitarbeiter mittels massgeschneiderten Informationen wie z. B. mittels einfachen Begriffserklärungen, ICT Glossars, Sensibilisierung und Trainings.

Beitrag von Fridel Rickenbacher

ICT-Glossar, Teil 1

Industrie 4.0, Digitalisierung

Mit der «inflationären» Bezeichnung «Industrie 4.0» soll das Ziel zum Ausdruck gebracht werden, eine vierte industrielle Revolution einzuleiten. Die technische Grundlage hierfür sind intelligente und digital «massiv» vernetzte Systeme bis hin zu «cyber physical» Systemen mit (teil)eigenständigen Entscheidungen.

Business Modell Maturity mit Data Data Science / Monetization

Je nach Branche kann durch eine frühzeitige und nachhaltige Strategie und Innovation zur Verbesserung des Reifegrades des eigenen, vielfach zunehmend «data driven» Geschäftsmodells mit auch ausgebauten Analyse und Verwertung von Daten («Data Science / Data Monetization») weitere Wettbewerbsvorteile/-Vorsprünge erreicht oder erst gar erhalten werden. Dies kann je nach Branche, Business Modell und Mitbewerber auch mitunter existenzielle Auswirkungen prägen.

CyberSecurity, CyberRisk

Präventive und/oder reaktive Massnahmen gegen Risikofaktoren wie z. B. Mensch (als «schwächstes Glied der Kette» welches u.a. mittels sogenanntem «Social Engineering» angegriffen wird) / Systemen / Prozessen zugunsten der Angriffs- und Betriebs-/Informations-Sicherheit. Trotzdem kann nie eine «100% Sicherheit» erreicht und letztlich in ähnlicher Reihenfolge provoziert / angegriffen werden von internen (Mitarbeiter) und externen Angreifern. Methodische, technologische und prozessuale Ansätze in Richtung von «security by design» / «security by default» und auch überwachte Automatisierung mit gleichzeitiger Reduktion der «human interaction» sind mittlerweile unumgängliche Hilfs-Strategien.

ICT Security Policy

Das sind einfach gesagt Weisungen und Spielregeln in der Nutzung und Umgang mit der Informationstechnologie (verbunden mit ICT Sensibilierungs-Massnahmen / «Awareness-Programm»), teilweise bewusst als Arbeitsvertrags-Bestandteil. Diese regeln z. B. den Umgang der seitens Firma zur Verfügung gestellten ICT-Werkzeugen zur aktiven Mithilfe seitens Mitarbeiter für die Maximierung der Angriffs- und Betriebs-Sicherheit der vitalen Firmen-Systemen, Firmen-Daten, Firmen-Know How oder auch personensensitiven (Kunden)Daten.

Phishing, Spoofing, Spam-Mails

Unter dem Begriff Phishing (von fishing, engl. für «Angeln») versteht man (leider zunehmend erfolgreiche) Versuche, über manipulierte Webseiten, clever gefälschte E-Mails (inkl. Name, Absender, Emailsignatur oder gar internen Informationen in den Emails) oder Kurznachrichten an persönliche Daten eines ICT-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Ziel des Betrugs ist es, mit den erhaltenen Daten beispielsweise Kontoplünderung zu begehen, Zugang zu Firmensysteme oder sensitiven Daten zu erhalten. Es handelt sich dabei um eine Form des Social Engineering.

Social Engineering

Einfach erklärt handelt es sich hierbei um eine (teilweise) sehr clevere Manipulation der Verhaltenweise (z. B. Herausgabe von sensitiven Informationen oder Durchführen sicherheitsgefährdenden Handlungen) und zwischenmenschliche Beeinflussung eines Menschen auf der mitunter skrupellos ausgenutzten Basis der Gutgläubigkeit und menschlichen Tendenz des Vertrauens. Siehe auch Phishing als ein Beispiel. Häufig dient Social Engineering der Vorbereitung und Vorstufe vor dem Eindringen oder Angreifen in ein Computersystem, Programm oder Netzwerk, um vertrauliche Daten zu

Jahren als Redaktionsmitglied, Experten-Gruppen- 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.).

erhalten (z. B. auch Spionage) oder zu manipulieren; man spricht dann auch von Social Hacking.

Datenschutz, Privacy by design / by default
Neue Regulationen (z. B. CH-DSG, EU-DSGVO / GDPR) und Standards haben zum anspruchsvollen Ziel, die Persönlichkeitsrechte / Datenschutz / Datenhoheit / Haftungsfragen und Schutz der Privatsphäre mittels Prozessen / Standards wie z. B. voreingestellten Sicherheits-Mechanismen (privacy / security by design oder by default), Datenschutzfolgenabschätzungen und zu definierenden Rollen eines Datenschutzbeauftragten / «Data Protection Officer DPO» zu fördern und schützen. Solche Datenschutzthemen sind auch wichtige Bestandteile rund um das Risk-Management / Incident Response Management und auch Haftungsfragen in Geschäftsführung / Verwaltungsrat und letztlich dem ICT-Auditing.

Datenklassifizierung, Metadaten
Bei der Klassifizierung von Daten, Dokumente können basierend auf z. B. Dokumente- oder Email-Inhalten, Keywords, Dokumenttypen, Titeln, Betreffs, Metadaten weitergehende automatisierte Prozesse / Workflows angestossen werden. Hier werden Ziele in folgende Richtungen angestrebt: vollautomatische, integrierte Daten-/Dokumente-/Email-Verschlüsselung, Dokumenten-/Projekte-/Dossier-Workflows bzw. auch Dokumentenlenkung, Dokumentenrechteverwaltung / Informationsrecheverwaltung DRM/IRM, Email-/Dokumenten-Archivierung, Filterung, Blockaden auf Ebenen wie Email / Internet / Firewall / Speicherung / Synchronisation, Alarmierung (siehe auch folgend DLP).

Informations Ethik
Die Informationsethik ist eine philosophische Disziplin, genauer gesagt eine Bereichsethik, die sich mit dem Umgang mit Informationen und mit Informations- und Kommunikationstechnologien unter moralischen und ethischen Gesichtspunkten beschäftigt. Hierbei liegt auch ein spezielles Augenmerk bei Risiken / Chancen und Grenzen bei der Verwendung oder Verwertung von personensensitiven Daten oder auch der informationellen Selbstbestimmung als ein angestrebtes Grundrecht.

Informationskompetenz, Coding
Um die «data driven» Zukunft und digitale Gesellschaft 4.0 mitgestalten zu können braucht es erweiterte Kompetenzen rund um Informatik, Coding / Programmierung, Mathematik bzw. Informationsmanagement. Sozusagen das Erlernen der «5. Landessprache» der Schweiz.

ShadowIT, Schatten Informatik
Mangels echter Alternativen wurden die Geschäftsanforderungen im Bereich IT in der Vergangenheit jahrzehntelang mit lokalen, meist eher starren EDV-Support-Prozessen abgebildet. Diese teilweise dynamisch, unkontrollierbare gewachsenen EDV-Infrastrukturen (im ungewissen Schatten), die durch die System- und Softwarelieferanten stark mit geprägt waren und vielfach auf «Best Practices» basierten, stellten lange ein durchaus robustes und auch funktionierendes Rückgrat des Unternehmens dar (Business-Support durch IT). Derzeit verändern die neuen sogenannten Hybrid-/Cloud-basierten Technologien und Trends jedoch diesen Bereich – auch über Systemgrenzen hinweg – zugunsten der Transparenz. (Licht in die Schatten-Informatik).

Data Loss / Leak Prevention DLP
Sämtliche Bemühungen in technischer und prozessmässiger Hinsicht zur „beinahen« Verhinderung oder eher „nur« Behinderung von Datenverlust / «Daten-Lecks» bzw. Entwendung, Manipulation, Löschung oder Nutzen-Veränderung von firmen- oder personen-sensitiven Daten.

Intrusion Prevention System IPS, Intrusion Detection System IDS
Als Intrusion-Prevention-Systeme (kurz: IPS) werden Intrusion-Detection-Systeme (kurz: IDS) bezeichnet, die über die reine Generierung von Ereignissen (Events, Alerting) hinaus Funktionen bereitstellen, die einen entdeckten Angriff auf die Angriffs- und Betriebs-Sicherheit einschränken oder abwehren (z. B. gegen Hacker, DDoS-Attacken, Bot-Netze, Viren, Schadsoftware/Malware, Crypto-Trojaner, Erpressungssoftware / Ransomware oder künftig auch gefährliche Algorithmen / Artificial Intelligence AI). Alle entsprechenden Massnahmen in einem Gesamtsystem – und komplexitätsbedingt meist von spezialisierteren Anbietern als Gesamtlösung bzw. «managed service» angeboten – können auch im Rahmen des Reporting und Monitorings als Trend-, Analyse- und Risk-Management-Basis verwendet werden in der zunehmend dynamischen Bedrohungslage rund um die Cyber-Security. Aufgrund auch der Komplexität von Angriffen und CyberTerrorismus werden (müssen …) zunehmend auch Technologien und Stärken von Artificial Intelligence AI und Machine Learning ML unterstützend eingesetzt.

Teil 2 in der Januar-Ausgabe