Fridel Rickenbacher ist Mitbegründer, Partner, Geschäftsführer und Verwaltungsrat der MIT-GROUP, eines Total-unternehmens für «Empowering for the 4th Industrial Revolution» und Informations- und Kommunikations-management. 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

Booster-Impfung
für Cybersecurity und Digitalisierung

Beitrag von Fridel Rickenbacher

Vom Problem zur verpassten Chance

Bekanntlich hatte auch das äusserst professionelle und erfolgreiche «Business Modell CyberCrime» auf der «dunklen Seite der Macht» aber auch der mitunter erzwungene «Reifegrad der Digital Transformation oder Hybrid Cloud», in den letzten 2 Jahren von mehreren, mitunter parallel zur Covid-Pandemie verlaufenden Wellen, wiederum massive Risiken, komplexe Probleme und auch Chancen hervorgebracht. Viele dieser alten und neuen Probleme sowie Chancen sind bekannt aber mitunter noch immer ungelöst.

Nicht gemachte Hausaufgaben in dynamischen Bedrohungslagen

Die weiter voranschreitende «Massive Interconnection» im Universum von IoT «Internet of Things Dinge» bzw IoE «Internet of Everything», in der Kollaboration in Hybrid Cloud Services (z.B. Microsoft 365, speziell Microsof Teams, Microsoft Azure und anderen Cloud Services) und in der virtuellen Welt von Socialmedia, hat zu den bereits älteren Hausaufgaben viele weitere und komplexer gewordene Herausforderungen generiert. Vor allem rund um Datenschutz, Datensicherheit, ICT-Risiko Management, ICT-Strategie, zugunsten der optimierten Angriffs- und Betriebs-Sicherheit und zum «Schutz der digitalen Identität». Viele der wertstiftenden Potentiale zugunsten einer möglichen ICT-Strategie/Vision/Mission von «Secure Modern Work» (sicheres, modernes, automatisiertes und effizientes Arbeiten) sind entsprechend schwer erschliessbar, aufgrund zu vielen nicht gemachten Hausaufgaben.

Booster-Impfung zugunsten Stand der Technik, KnowHow und Halbwert-Zeit des Wissens

Eine Impfung sollte möglichst freiweillig 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». Dass dabei euch speziell das ICT-Risk Management und Aufbau/Pflege von «business contingency planning (BCP)» und «incident response planning (ICP)» schon länger Standard bzw. «Stand der Technik» ist, hält zum Glück Einzug in die ICT-Strategie, Planung, Budget und auch Verantwortung in der Führungs- und Entscheidungs-Ebene. Vorallem auch der Faktor Mensch als wichtigster Akteur und Betroffener sollte gezieltes KnowHow, 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. KnowHow-Transfer oder «Stand der

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.).

Technik», nimmt stetig ab und bedarf eine nachhaltige (Kampagnen)Planung und proaktive Förderung.

Cybersecurity und Digitalisierung Sensibilisierung zugunsten Gesamtsystem-Resilienz und Digtal-DNA-Transformation

Die massgeschneiderte Aufklärung und Informations-/Trainings-Kampagne rund um die Chancen und Risiken in den Bereichen von Cybersecurity, Datenschutz/Datensicherheit, digitaler Identität und effizienzsteigernden Digitalisierung ist essentiell, auf diesem anspruchsvollen «Hochseil-Akt» und zur gemeinsamen Meisterung eines möglichst verletzungsfreien «Spagat zwischen Security, Effizienz und moderner Anwender-Erfahrung». Mittels einer ausgewogenen Mitgestaltungsmöglichkeit kann auch ein gutes und hilfreiches Mass einer «gemeinsamen Mitverantwortung rundum Cybersecurity- Resilienz und Digitalisierung» etabliert und in die «Digital-DNA» der Organisation/Transformation verankert werden.

Der Traum der hybriden Arbeitswelt wird zur Realität und das Cybersecurity-Risiko zum gefürchtesten Albtraum

Die Covid-Pandemie und die Ukraine-Krise haben gezeigt, dass unvorhersehbare Ereignisse tatsächlich jederzeit eintreffen und jeden hart treffen können. Im dritten Jahr des unveränderten Ausnahmezustandes von ursprünglich der Covid-Pandemie und nun rund um die Auswirkungen der Ukraine-(Welt)-Krise wird hoffentlich nachhaltige Massnahmen und Lerneffektive hinterlassen. Es bleibt auch zu hoffen, dass der näher greifbare, realisierbare Traum einer möglichst effizienten und hybride Arbeitswelt bzw. «Digitalisierungs Grad» nicht zu stark verflüchtigt oder nicht verdrängt wird wegen der derzeit grössten Sorge der meisten Unternehmen, des Alptraums eines «Cybersecurity / Cybercrime Vorfalls». Man sollte bewusst «gross planen» und möglichst «unbegrenzt träumen» mit entsprechenden «best practices gemäss Stand der Technik», um das Beste auch bewusst und gezielt aus solchen Ausnahmezuständen mit viel Adaptions- und Lern-Potential rauszuholen und weiter zu entwickeln.

«start thinking, stop clicking – stop being naive, stay aware – get and stay smart»

Weiterhin gutgläubig/naiv zu bleiben und sich den bekannten Herausforderungen und Hausaufgaben nicht bewusst(er) und ernsthafter zu widmen, wird immer härter bestraft in der beschleunigten Technologie-Weiterentwicklung und deren erhöhten Komplexität.

Eine konsequent angewandte Grundsatz-Regel von «start thinking, stop clicking» (zuerst mit-denken und erst dann klicken und handeln mit gesundem Menschenverstand) kann ganz viele Cybersecurity-Risiken, speziell im beliebten und negativ «erfolgreichsten» Angriffsvektor von «Social Engineering» reduzieren oder gar verhindern helfen.

Selber sensibilisiert und vorallem «smart» zu werden und vorallem zu bleiben im Universum der «massiven Interkonnektion» bzw. «smart connected world», Internet generell, Internet der Dinge / Internet von allem, Social Media, und letztlich in der «hybriden Privat- und Arbeits-Welt» ist eine Generations-Herausforderung. Der Umgang mit der eigenen «digitalen Souveränität», einer nicht zu hoher «Systemgläubigkeit» und dem Schutz der persönlichen «digitalen Identität» – zunehmend geprägt mit auch (Sicherheits)Faktoren rund um Biometrie bis zur Verhaltens-Biometrie – wird möglichst bald «en vogue» oder gar zum «persönlichen und sozialen Verhaltens-Codex» in einem «next gen» Knigge 5.0. Naivität und Fahrlässigkeit in Wissen der persönlichen, digitalen Angreifbarkeit und auch zulasten der Organisation / Gesellschaft (z.B. Lösegeld zahlen infolge nicht gemachten Hausaufgaben in die gefährliche Kriegskasse von Cybercrime) muss entsprechend leider zunehmend auch als asozial eingestuft werden.

Internet + Internet der Dinge = Wissen / Kontrolle / Macht der Welt

Damit nicht andere Organisationen, Akteure oder gar Staaten alles Wissen, Kontrolle und Macht zu stark vereinen, ist die persönliche «digitale Souveränität» (auch von Staaten, Organisationen, Firmen etc.) im «digitalen Raum» und speziell in der eigenen «digitalen Identität» entsprechend essentiell und einer der wichtigsten Herausforderungen und übergeordneten «Hausaufgaben mit weiter noch folgenden Prüfungen» in der Zukunft.

Charles Darwin's Zitat «survival of the fittest» wird in der zunehmend rasanten (R)Evolution und mitunter hinterher hängenden Adaption der Technologie und speziell in der Digitalisierung einen neuen Stellenwert erlangen.