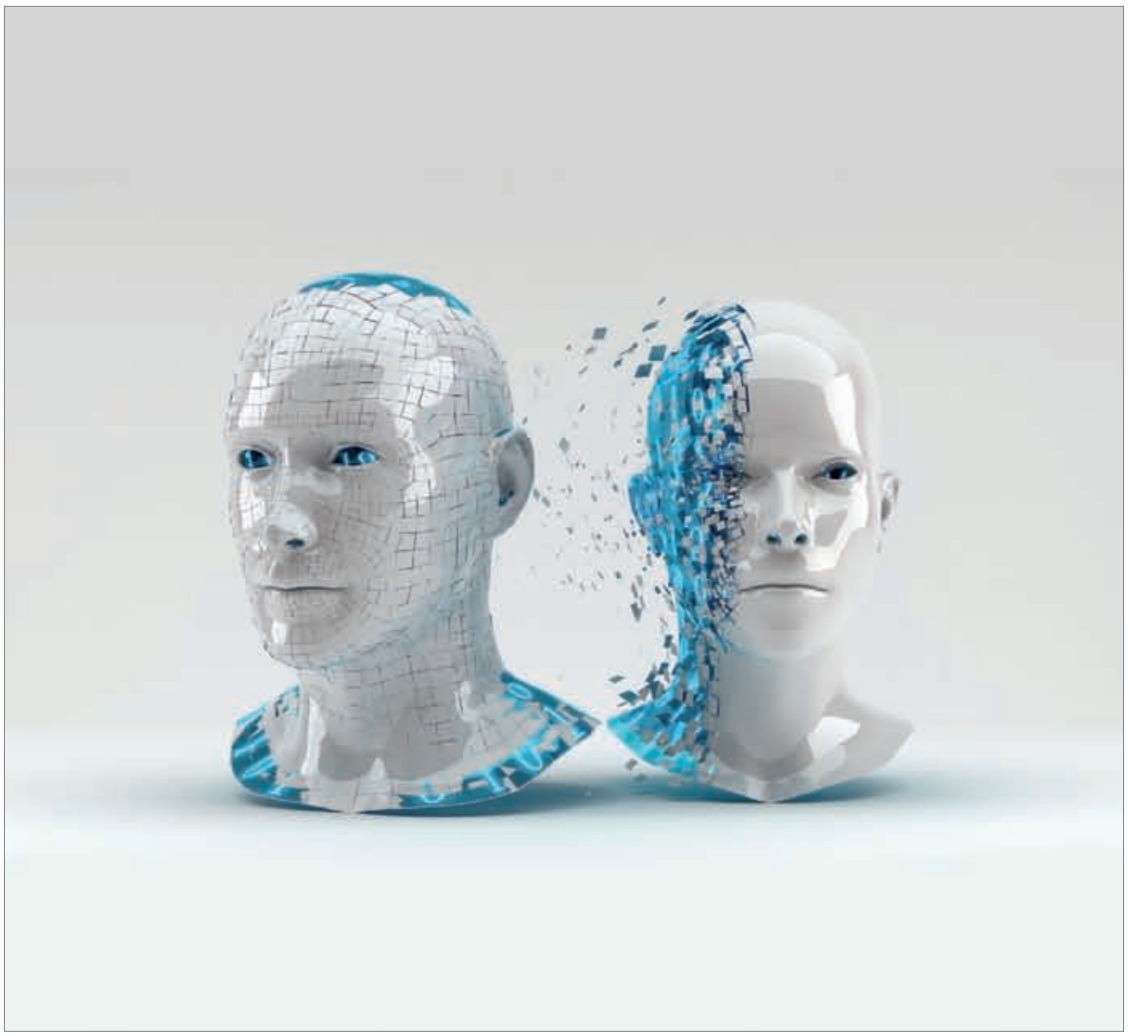


Leading Innovation

Impulse aus dem TÜV AUSTRIA Innovationsbeirat

1

Sicherheit als Wegbereiter für die Digitale Transformation

IMPULSE AUS DEM
TÜV AUSTRIA INNOVATIONSBEIRAT
BAND 1
SICHERHEIT ALS WEGBEREITER FÜR
DIE DIGITALE TRANSFORMATION
JUNI 2017

TÜV AUSTRIA GROUP
INNOVATIONSMANAGEMENT
TÜV AUSTRIA-Platz 1
2345 Brunn am Gebirge
innovation@tuv.at
www.tuv.at

Leading Innovation

Impulse aus dem TÜV AUSTRIA Innovationsbeirat

1

Sicherheit als Wegbereiter für die Digitale Transformation

Juni 2017

Textbeiträge: Franz Kühmayer | Grafiken: zukunftsinstitut | Redaktion: Christoph Schwald
Bilder: www.fotolia.com (Péter Mács, kentoh, maciek905, jamesteohart, fgnopporn, Nmedia, everythingpossible, REDPIXEL;)

Sicherheit als Wegbereiter für die Digitale Transformation

Eine Einführung von DI Dr. Stefan Haas

Wie Analysen zeigen, hat sich die Verweildauer von Unternehmen in den letzten 50 Jahren dramatisch verkürzt, von 60 Jahren zu heute nur noch ca. 18 Jahren (Quelle: Standard & Poor's 500 Index). Das sich ständige Neuerfinden ist somit keine Kür, sondern Pflicht. Wir als TÜV AUSTRIA wollen unsere Geschäftspartner dabei unterstützen und entwickeln laufend neue Services, damit die Innovationen unserer Kunden auch entsprechend sicher sind, wenn diese auf den Markt gebracht werden. Denn eines ist evident: Sicherheit wird in unserer immer rascher digitalisierten Welt zum Wettbewerbsvorteil.

Damit wir unsere Kunden auch zukünftig optimal begleiten und unterstützen können, diskutieren wir ab sofort unsere eigene Innovationsstrategie einmal jährlich mit führenden Persönlichkeiten aus Industrie, Forschung und Wissenschaft. In diesen Innovationsbeirat werden Repräsentanten der obersten Leitung von Unternehmen und Universitäten geladen, die in ihrem Bereich als Innovations- und Technologieführer gelten.Ich freue mich persönlich über die hochkarätige Besetzung des Innovationsbeirats, deren Mitglieder wir Ihnen im Folgenden vorstellen dürfen.Für die initiale Sitzung des Innovationsbeirats haben wir uns die Frage gestellt, wieviel Sicherheit die Digitale Transformation aus Sicht des TÜV AUSTRIA Innovationsbeirats überhaupt benötigt. Dabei haben wir uns, unter Moderation von Trendforscher Franz Kühmayer vom zukunftsinstitut, einem der einflussreichsten Think Tanks der europäischen Trend- und Zukunftsforschung, dieser Fragestellung nicht nur im industriellen sondern auch bewusst in einem ganzheitlichen Kontext gestellt.

Sicherheit ist nichts Absolutes, sondern definiert sich auch über gerade noch akzeptierbare Risiken, diese müssen aber in einer zunehmend digitalisierten Welt zunächst als solche erkannt werden. Unter anderem werden Softwareprogramme nicht nur im Office- oder Smartphone-Bereich laufend upgedated, auch Fahrerassistenzsysteme oder kollaborative Industrieroboter bekommen laufend neue Funktionserweiterungen. Somit bekommt der Begriff Sicherheit durch die Digitale Transformation eine völlig neue Bedeutung

„Nie war es wichtiger, als in unserer Zeit des raschen technologischen Fortschritts, durch Innovation den Unternehmenswert nachhaltig zu steigern, um auch noch morgen am Markt zu existieren.“

und wandelt sich von einem statischen Zustand zu einem hochdynamischen und kontinuierlichen Prozess.

Die Digitalisierung durchdringt sämtliche Ebenen der Industrie, Wirtschaft und Gesellschaft gleichzeitig und betrifft uns alle gleichermaßen. Die Transformation in eine hochdigitalisierte und zugleich sichere Welt wird somit nur durch einen gemeinsamen Schulterschluss sämtlicher Akteure erfolgreich sein.

Als TÜV AUSTRIA sehen wir unseren gesellschaftlichen Auftrag darin, Technologien durch die digitale Transformation aktiv zu begleiten, denn nur wenn diese sicher, beherrschbar und umweltfreundlich sind, werden sie von Wirtschaft und Gesellschaft akzeptiert werden und letztendlich den Mehrwert bringen, den wir uns alle daraus erhoffen dürfen und müssen.

In diesem Sinn freue ich mich, die Erkenntnisse der Sitzung 2017 des Innovationsbeirats mit Ihnen teilen zu dürfen und wünsche Ihnen auf den folgenden Seiten eine interessante, spannende und aufschlussreiche Lektüre.

DI Dr. Stefan Haas, CEO TÜV AUSTRIA Gruppe

TÜV AUSTRIA Innovationsbeirat

O. Univ. Prof. DI Dr. Sabine Seidler

Rektorin der TU Wien

- Seit 10/2011: Rektorin der Technischen Universität Wien
- Leiterin des Instituts für Werkstoffwissenschaft und Werkstofftechnologie, TU Wien
- Aufsichtsrat des Helmholtz-Zentrums Berlin für Materialien und Energie GmbH
- Aufsichtsrat der AMAG (Austria Metall AG)
- Stellvertretende Kuratoriumsvorsitzende des Naturhistorischen Museums Wien

- Österreichs größte naturwissenschaftlich-technische Forschungs- und Bildungseinrichtung
- 29.919 Studierende (Stand 01/2016)

Johann Christof

CEO und Eigentümer Christof Industries GmbH

- Seit 2015 CEO und Eigentümer der Christof Industries GmbH
- 1989-2015 Mitbegründer und Geschäftsführer von J. Christof GmbH; Vorstandsvorsitzender der Christof Holding AG – Christof Group
- Seit 2008: Honorarkonsul der Republik Litauen; Amtsbereich Steiermark, Burgenland und Niederösterreich
- 2011: Jahrgangscaptain des Lehrganges Innovationsmanagement an der Fachhochschule Campus02

- Global agierender Partner für die Entwicklung, Errichtung und Servicierung von Anlagen für die Industrie und Energiewirtschaft entlang des gesamten Lebenszyklus
- Technologische Entwicklungen im Bereich erneuerbare Energien
- Ca. 1.900 Mitarbeiter an 17 Standorten weltweit (Stand 2017)

DI (FH) Andreas Gerstenmayer

CEO AT&S AG

- Seit 2010 Vorstandsvorsitzender der AT&S AG
- 2003 – 2008 Siemens Transportation Systems GmbH: Geschäftsführer & CEO der Business Unit Fahrwerke Graz
- Vorsitzender des steirischen Forschungsrates

- Europäischer Marktführer und weltweit einer der führenden Hersteller von hochwertigen Leiterplatten
- 9.452 Mitarbeiter (02/2017) an sechs Produktionsstandorten in Österreich, Indien, China und Korea

Ing. Mag. Thomas Jost

Vorstand Liaunig Industrieholding AG,
CEO und Miteigentümer Waagner-Biro AG

- 03/2013 Vorstandsvorsitzender/ Miteigentümer Waagner-Biro AG
- 03/2012 Vorstand Liaunig Industrieholding
- 2005- 2012 Geschäftsführer Wild Holding GmbH
- Stellvertretender Aufsichtsratsvorsitzender der Binder+Co AG

- International tätiges Stahlbauunternehmen mit Hauptsitz in Wien
- 1.475 Mitarbeiter (Stand 2015) an rund 17 Standorten in Europa, dem Mittleren Osten und Asien

DI Dr. Peter Layr

Sprecher des Vorstandes EVN AG

- Seit 10/1999 Vorstand der EVN AG
- Aufsichtsratsvorsitzender RAG-Beteiligungs-AG und Rohöl-Aufsuchungs AG
- Aufsichtsrat der VERBUND AG

- Anbieter für Strom, Gas, Wärme, Trinkwasserver- sowie Abwasserentsorgung und thermische Abfallverwertung auf Basis modernster Infrastruktur, Betrieb von Netzen für Kabel-TV und Telekommunikation sowie Anbieter verschiedener Energiedienstleistungen für Privat- und Businesskunden sowie für Gemeinden
- 6.830 Mitarbeiter (GJ 2015/ 2016)

DI Dr. Stefan Poledna

Vorstand und Mitbegründer TTTech Computertechnik AG

- Vorstand und Mitbegründer TTTech Computertechnik AG: verantwortlich für das Automobilgeschäft, F&E-Aktivitäten, Supply Chain und Qualitätsmanagement
- 1998 Gründer TTTech Computertechnik AG
- Universitätsdozent für Technische Informatik an der TU Wien
- 2013 zum Österreicher des Jahres in der Kategorie „Unternehmertum“ gewählt (Vergabe durch „diePresse“)

- Führender Lösungsanbieter für zuverlässige Netzwerklösungen, basierend auf zeitgesteuerter Technologie und modularen Sicherheitsplattformen
- Laufende Entwicklung von Lösungen für komplexe Probleme für Embedded System Designs von cyber-physischen Systemen und dem Internet der Dinge
- über 500 Mitarbeiter weltweit (Stand 2016)

DI Armin Rau

Geschäftsführer TRUMPF Maschinen Austria GmbH + Co KG

- Seit 2004 Geschäftsführer bei TRUMPF Maschinen Austria GmbH + Co. KG.
- von 1982 bis 2003 in der TRUMPF Entwicklung tätig - verantwortlich für Steuerungstechnik, Software und Sensorik
- Aufsichtsrat Firma Engel

- Tochtergesellschaft der deutschen TRUMPF Gruppe
- 530 Mitarbeiter (2015)
- Kompetenzzentrum für Biegetechnologie der TRUMPF Gruppe
- Seit 2011 staatlich ausgezeichneter Ausbildungsbetrieb
- 2011 Fabrik des Jahres
- 2012 Staatspreis Innovation

Megatrend Digitalisierung: Sicherheit in einer zentralen Rolle

Eine Lawine in Zeitlupe

Thematische Einführung von Franz Kühmayer, zukunftsInstitut

Die Gesellschaft verunsichert, der Staat überfordert. Die allumfassende Vernetzung der Welt und der radikale Wandel, den die Digitalisierung mit sich bringt, führt uns auf den Weg in eine neue Sicherheitskultur. Mehr denn je stellt sich für Entscheidungsträger die Frage, wie sie die Ambivalenz zwischen Sicherheit und Risiko, Stabilität und Agilität meistern sollen.

Wer Digitalisierung als plötzliche Veränderung wahrnimmt, hat bereits seit längerem seine Augen vor der Realität verschlossen. Wir stehen nicht am Anfang eines Umbruchs, sondern mittendrin. Während jedoch viele Unternehmen immer noch in den Anfangsgründen des Wandels feststecken, haben Innovationsführer die transformatorische Wirkung der Digitalisierung erkannt und erschließen die Chancen der Disruption in ihrer ganzen Tragweite. Dabei nimmt die Entwicklung immer mehr Fahrt auf, die Dynamik des Wandels steigt rasant an.

Längst geht es nicht mehr darum, bestehende Prozesse effizienter zu gestalten, sondern um völlig neue Geschäftsmodelle, völlig neue Vorstellungen von den Potentialen vernetzter, lernender Maschinen, die die kognitiven Fähigkeiten des Menschen spielend übertreffen.

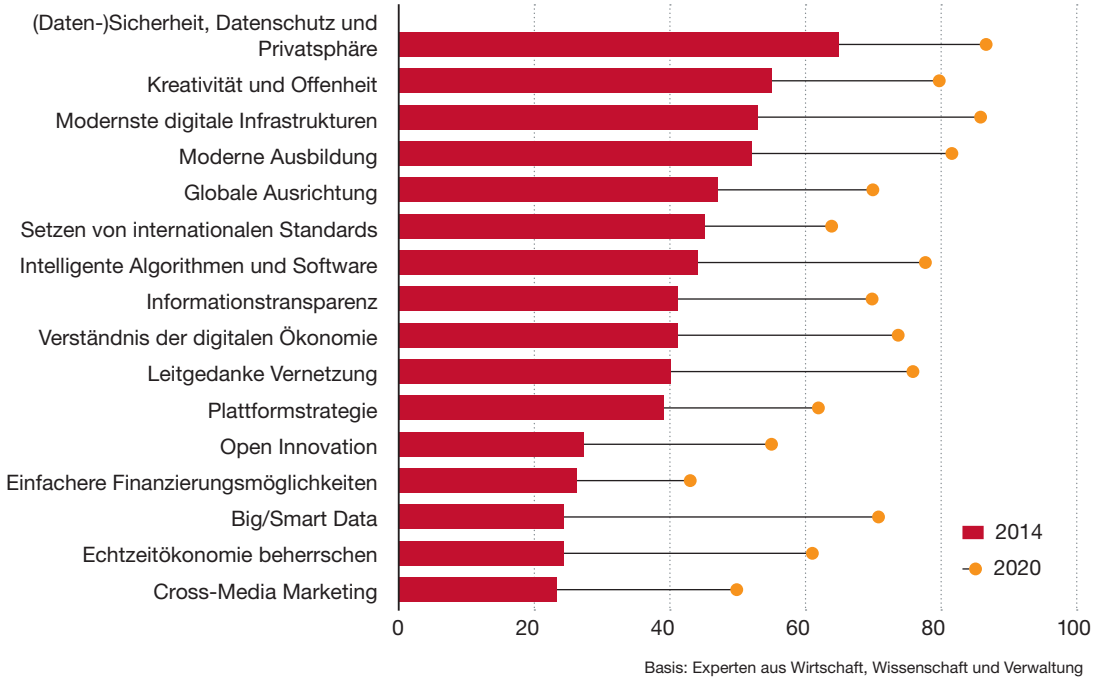
Die dadurch ausgelösten Veränderungen geschehen nicht sprunghaft, plötzlich, augenblicklich. Doch sie sind tiefgreifend und radikal. Wie eine Lawine in Zeitlupe zerrt die Digitalisierung an den Grundfesten von Wirtschaft und Gesellschaft. Und stellt uns vor neue Fragen der Sicherheit.

„Bei vielen unserer Kunden sind die digitale Transformation und das Bewusstsein, welche Chancen und Risiken damit verbunden sind, noch gar nicht angekommen. Vor allem im Bereich der IT-Security wurde hier noch wenig Vorsorge getroffen."

DI Armin Rau
Geschäftsführer TRUMPF Maschinen Austria GmbH + Co KG

Agilität: Zwischen Sicherheit und Offenheit

Wichtige Erfolgsfaktoren der Digitalisierung für die Wettbewerbsfähigkeit von Unternehmen
(Bewertung sehr starker/starker Einfluss in Prozent)



Basis: Experten aus Wirtschaft, Wissenschaft und Verwaltung

Quelle: Münchner Kreis

DI Dr. Stefan Poledna

Die digitale Transformation ist eines der ganz großen Themen unserer Zeit: Im Prinzip geht es darum, auf Basis von Daten, die gesammelt werden, Kundennutzen verfügbar zu machen. Über diese ganze Kette der Generierung und Sammlung von Daten stellt sich selbstverständlich die Frage nach der Sicherheit im Sinne der Safety und Security, die bei der Erbringung dieser Services eine zentrale Rolle einnimmt.

DI Dr. Peter Layr

Die digitale Transformation hat eine hohe Geschwindigkeit und Dynamik. Der Gesetzgeber kann nur versuchen die gröbsten Mängel zeitversetzt zu beseitigen. Hier kann sich der TÜV AUSTRIA einbringen, damit dieses System zweier Geschwindigkeiten nicht aus dem Ruder läuft und bereits in der Umsetzung der digitalen Transformation Maßnahmen getroffen werden, um mögliche spätere Sicherheitsmängel zu vermeiden.

Ing. Mag. Thomas Jost

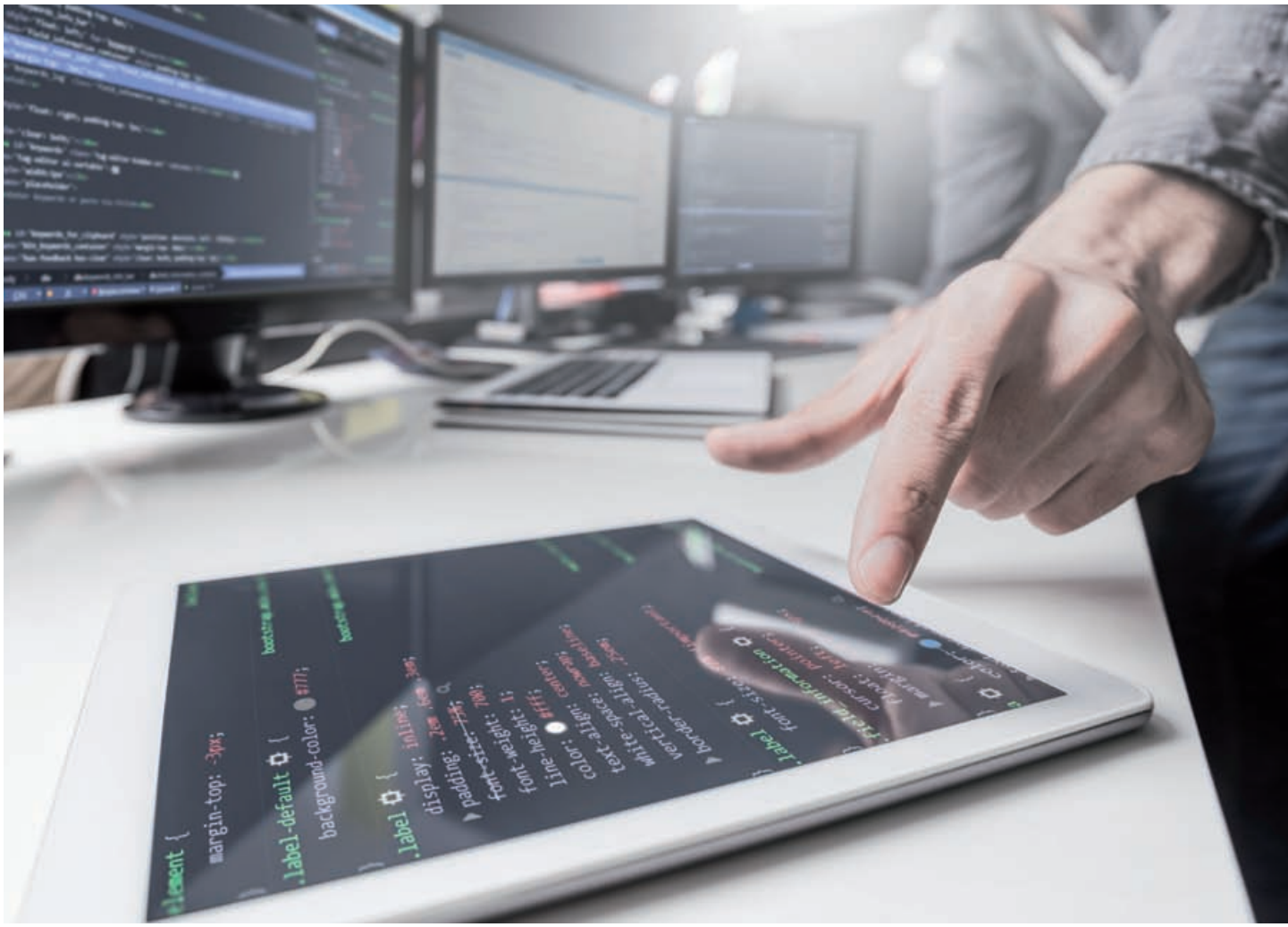
In der Baubranche ist die digitale Logistik ein großes Thema, über die Fortschrittsrechnung bis hin zur Abnahme. Digitalisierung allein löst allerdings die Grundprobleme nicht, am Ende des Tages müssen das Gebäude und die Infrastruktur auch funktionieren. Auch wird der Rücktransfer aus der digitalen in die reale Welt immer schwieriger, auch durch die mögliche Verfälschung von Daten.

DI Armin Rau

Bei vielen unserer Kunden sind die digitale Transformation und das Bewusstsein, welche Chancen und Risiken damit verbunden sind, noch gar nicht angekommen. Vor allem im Bereich der IT-Security wurde hier noch wenig Vorsorge getroffen.

Johann Christof

Sicherheit in der digitalen Transformation ist eine sich ständig ändernde und wachsende Herausforderung für jedes Unternehmen. Jegliche Art von Kommunikation und Datenaustausch ist davon betroffen, für uns insbesondere im Zuge der Bearbeitung und Bereitstellung von Datenräumen für Due Diligence oder Projekte. Für den Umgang der Mitarbeiter mit Unternehmensdaten in der mobilen Kommunikation über Voice, Whatsapp, interne Kommunikations-App, SMS/MMS, sowie die Integration von Social-Media-Plattformen wie Facebook, LinkedIn, Twitter, etc. bedarf es einer laufenden Sensibilisierung.



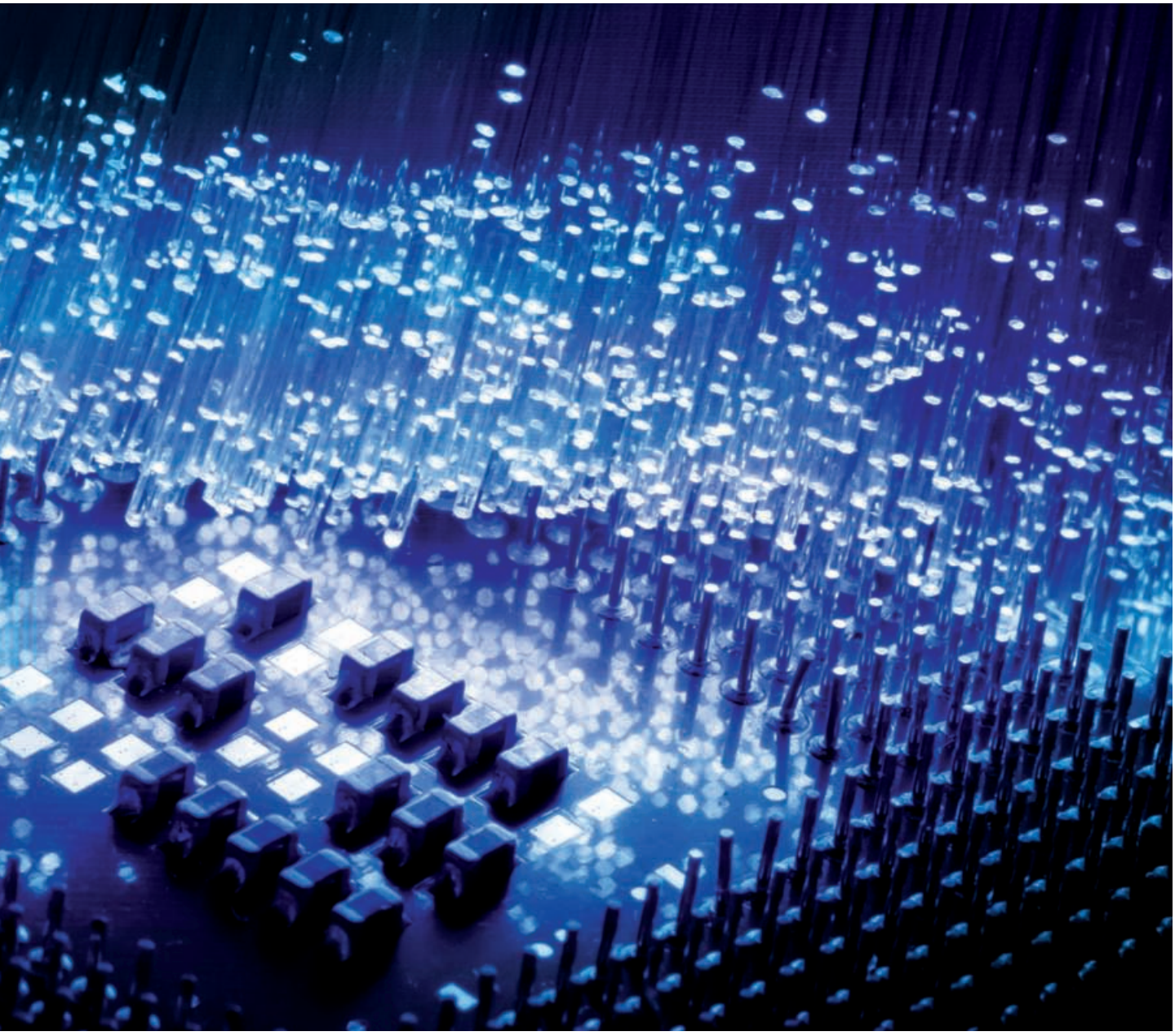
„Die digitale Transformation hat eine hohe Geschwindigkeit und Dynamik. Der Gesetzgeber kann nur versuchen die gröbsten Mängel zeitversetzt zu beseitigen.“

DI Dr. Peter Layr
Sprecher des Vorstandes EVN AG

Interaktion mit der digitalisierten Welt

„Es stellt sich auch die Frage, wie wir Maschinen etwas beibringen können, was die Menschen selbst nie gelernt haben."

Ing. Mag. Thomas Jost
Vorstand Liaunig Industrieholding AG, CEO und Miteigentümer Waagner-Biro AG



Der Mensch zwischen 0 und 1

Thematische Einführung von Franz Kühmayer, zukunftsInstitut

Digital, das ist Wissen aus Fakten, evidenzbasierte Grundlagen, klare Entscheidungen, kühle Rationalität. Zumindest scheinbar. Denn je nüchterner unser Blick auf die Welt ist, je analytischer und unbestechlicher unsere Herangehensweise, umso mehr nähern wir uns zutiefst emotionalen und moralischen Aspekten der Welt von morgen.

Schon heute pflegen viele Menschen einen geradezu fröhlich fahrlässigen Umgang mit ihren Daten und ihrer Privatsphäre. Die GAFAnomie (von Google Apple Facebook Amazon) macht sich die digitalen Spuren zunutze, die wir hinterlassen, verknüpft sie auf immer neue Art miteinander und entwickelt auf deren Basis Lösungen für Probleme, die uns gar nicht bewusst waren. Doch das ist erst der Anfang.
In der cyberphysikalischen Welt des Internet of Things potenziert sich der Sachverhalt. IT-Konzerne, Hersteller alltäglicher Produkte und Anbieter von Dienstleistungen wachsen zusammen, erfassen und vernetzen Daten und tauschen Informationen aus. Dann sammeln nicht nur Anbieter sozialer Medien oder Suchmaschinen die digitalen Krümel unseres Alltags auf, sondern auch die Hersteller von smarten Heizungen und Fahrstühlen, die Modefirma, die Wearables herstellt und die Lebensversicherung, die auf die Fitnessdaten der Smartwatch zugreift. Im Verschmelzen von real und digital verschieben sich Strukturen hin zu neuen Grenzen und bislang unberührten Fragestellungen. Wie sollen autonome Fahrzeuge reagieren, wenn sie Gefahr laufen, Menschen zu gefährden? Wo sind die Grenzen der algorithmischen Einflussnahme auf demokratische Prozesse? Ist Artificial Intelligence ein Segen für die Menschheit oder führt sie uns an den Rand des Abgrundes?

Wenn wir über digitale Sicherheit nachdenken, geht es längst nicht mehr nur darum, Menschen vor technischen Unzulänglichkeiten von Maschinen zu schützen, oder Maschinen vor fehlgeleitetem Handeln des Menschen. Wir müssen weiter denken. Lernende Maschinen verstärken diese Entwicklung nur noch: Künftig ist der Output eines Computerprogramms eben nicht mehr deterministisch vorgegeben, sondern basiert darauf, was und von wem die Maschine gelernt hat. Das führt nicht nur zu ethischen Debatten, sondern auch zur Diskussion um Sicherheit, Verantwortung und Haftbarkeit. In der rationalen Welt der Algorithmen ist der Mensch als kulturprägender Faktor mehr denn je gefragt.

O. Univ. Prof. DI Dr. Sabine Seidler

Die Art wie Automatisierung stattfindet, ändert das Verhältnis von Mensch zu Maschine dramatisch. Vollkommen neue soziale Aspekte benötigen besondere Sensibilität vor allem auch unter dem Sicherheitsaspekt. Der Roboter wird zunehmend als Mensch und nicht als Maschine gesehen werden, aber bleibt letztendlich Maschine. Sicherheit in der Mensch-Maschinen-Interaktion wird somit zunehmend ein ganzheitliches Thema. Darüber hinaus spielt durch die globale Vernetzung der Produktion, und dem dadurch wachsenden Datenvolumen und intensivierten Datenaustausch, die Informationssicherheit eine große Rolle.

„Maschinen sind gut, wo es deterministisch zur Sache geht. Dort können sie klare Entscheidungen auf Basis von Fakten treffen."

DI Dr. Stefan Haas
CEO TÜV AUSTRIA Gruppe

DI Dr. Peter Layr

Die Wirtschaft und die Gesellschaft müssen von der Digitalen Transformation langfristig profitieren können, ansonsten wird es nur einer von vielen Hypes gewesen sein: Wirtschaftlichkeit und Nutzen vor Selbstzweck. In diesem Zusammenhang werden unterschiedliche Themenfelder wie Automatisiertes Fahren und Industrie 4.0 zeitgleich diskutiert, aber die unterschiedlichen Zeitachsen zu deren Realisierung nicht berücksichtigt. Hier müssen in der öffentlichen Diskussion realistischere Zeiträume betrachtet werden, um durch überzogene Erwartungshaltungen keine negativen Enttäuschungseffekte zu bewirken. Die Datensicherheit nimmt dabei eine kritische Rolle ein und muss mit der Digitalisierung selbst Schritt halten können.

DI Dr. Stefan Poledna

Im Kundengespräch zeigt sich, dass es noch ein sehr neues Thema ist, wo noch viele Fragen offen sind. Fragen unter dem Aspekt der Security wie „wer besitzt die Daten?", „wo gehen die Daten hin?". Da letztendlich diese Daten dazu verwendet werden, um Prozesse zu steuern, ist es ein zentraler Punkt, dass diese Aktionen letztendlich auch sicher im Sinne der Safety ausgeführt werden.

DI Armin Rau

In der Vergangenheit stand die Gefährdung der Maschine Richtung Benutzer im Fokus. Durch die digitale Transformation rücken Themen wie Datensicherheit, Sicherheit im Umgang mit Assistenzsystemen wie dem Trumpf MagicShoe oder auch 3D-Brillen und Sicherheit im Umgang mit kooperierender Robotik in den Vordergrund. Im Bereich der digitalen Vernetzung gibt es heute sicher noch zu wenig Sicherheit. Nachdem vermehrt vom Eindringen in Rechnersystemen und Datendiebstählen, bis hin zu Wahlverfälschungen im politischen Umfeld berichtet wird, wird man bezüglich Datensicherheit viel sensitiver.

DI Dr. Peter Layr

Im Prinzip muss der Mensch die Grenzen der Digitalisierung definieren.
Dabei muss aber die Grenze nicht beim Nutzer sondern beim Inverkehrbringer gezogen werden, um mögliche Hemmungslosigkeiten zu vermeiden.

DI Dr. Stefan Haas

Maschinen sind gut, wo es deterministisch zur Sache geht. Dort können sie klare Entscheidungen auf Basis von Fakten treffen. Es wird dort ein großes Thema, wo es bei Entscheidungen kein Richtig oder Falsch gibt, wie zum Beispiel bei Fragen ethischer Natur, wo unterschiedliche Menschen auch unterschiedlich reagieren würden.

> *„Im Prinzip muss der Mensch die Grenzen der Digitalisierung definieren.“*
>
> **DI Dr. Peter Layr**
> Sprecher des Vorstandes EVN AG

Ing. Mag. Thomas Jost

Es stellt sich auch die Frage, wie wir Maschinen etwas beibringen können, was die Menschen selbst nie gelernt haben.

O. Univ. Prof. DI Dr. Sabine Seidler

Solche Fragestellungen werden bereits im wissenschaftlichen Kontext behandelt. Wir werden sehen welche Antworten hier kommen werden und was die Auswirkungen auf unsere Gesellschaft sein werden.

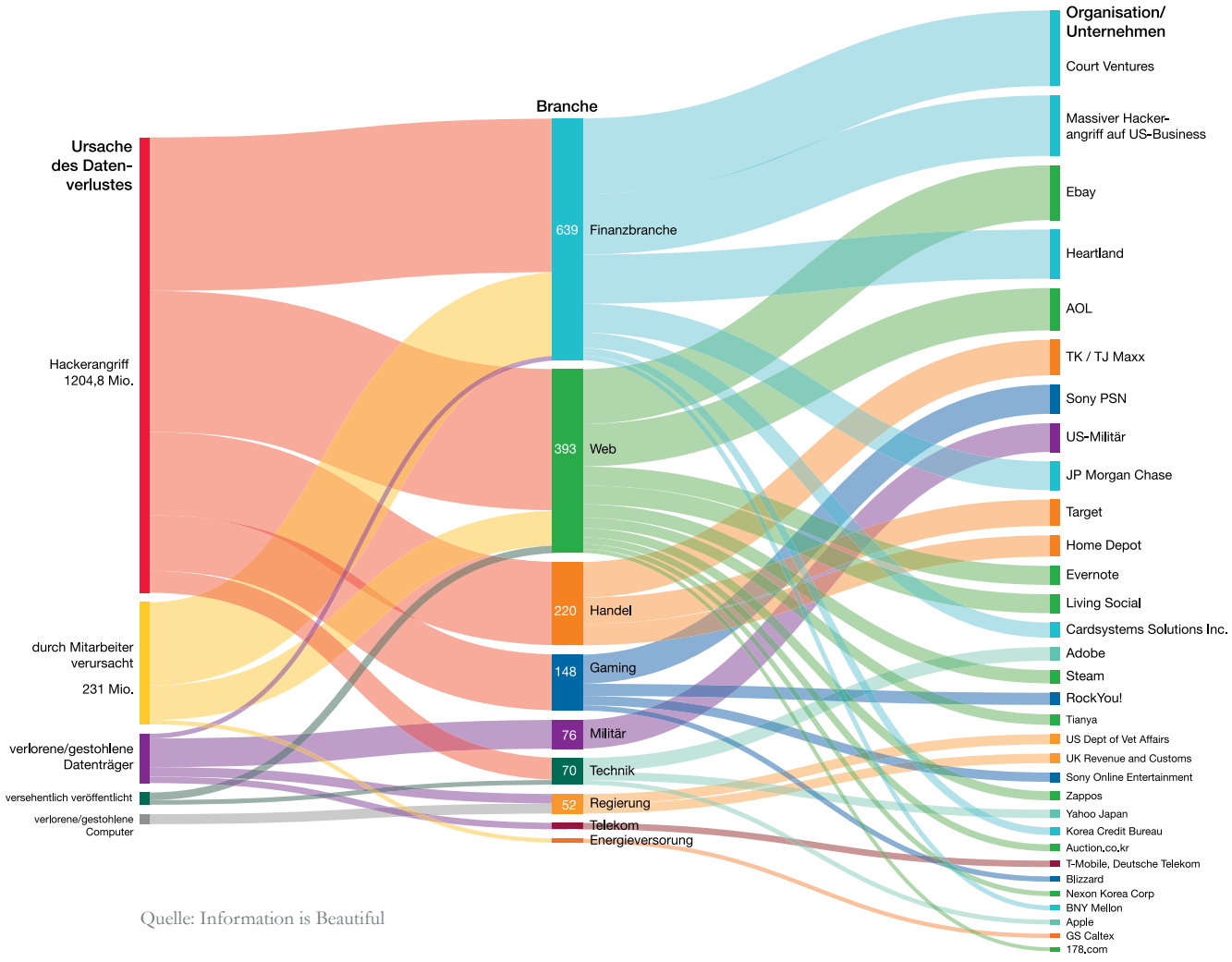
Die Hackerwirtschaft

Die größten Datenverluste und -diebstähle seit 2004 (in Millionen Datensätze)

Dargestellt sind Datenverluste und -diebstähle seit 2004 mit mehr als 10 Millionen betroffenen Datensätzen.
Die Verluste werden aufgeschlüsselt nach der Organisation, der die Daten abhanden gekommen sind, nach der Branche sowie nach der Ursache des Datenverlustes bzw. -diebstahls. Die Stärke der Linien stellt die Anzahl der betroffenen Datensätze dar. So waren beim größten Fall (Court Ventures) 200 Millionen Sozialversicherungsnummern, Kreditkarten- und Kontodaten betroffen, bei der Gaming-plattform 178.com 10 Millionen Nutzer- und Zugangsdaten.

Datenverlust in Unternehmen

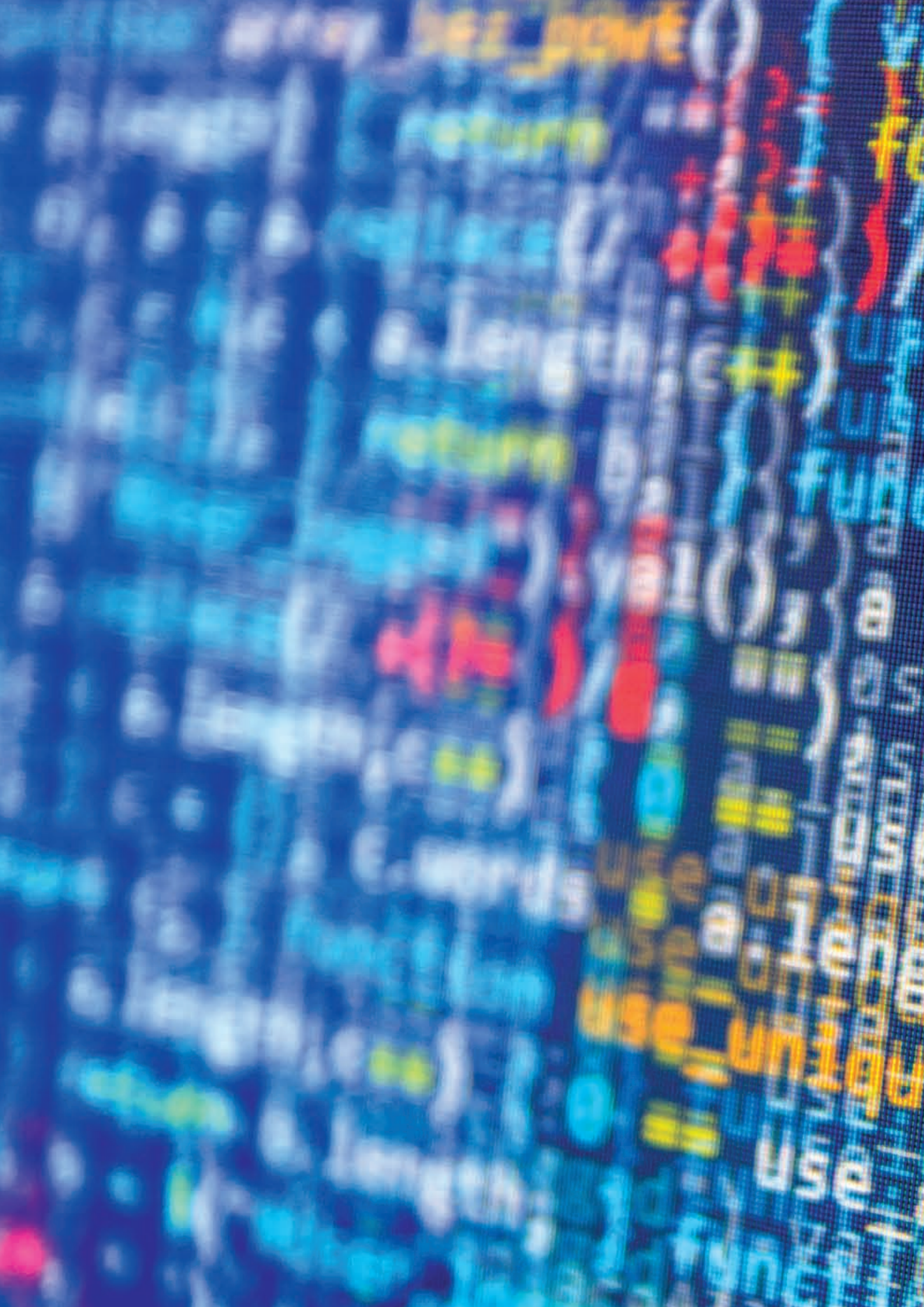
Für jedes Unternehmen ist es heute von existenzieller Bedeutung, seine Daten zu schützen. Der Schaden bei einem größeren Datenverlust ist zumeist kaum wiedergutzumachen. Selbst wenn ein Unternehmen den Datenverlust wirtschaftlich übersteht, erleidet es einen irreparablen Imageschaden. Neben spektakulären Hackerattacken kann es aber auch noch andere, wesentlich trivialere Ursachen für einen Datenverlust geben. Der am Bahnhof oder Flughafen vergessene Laptop, der auf dem Postweg fehlgeleitete Datenträger sind gar nicht so selten vorkommende Auslöser für den Verlust von Kundendaten oder von geistigem Eigentum. Auch Mitarbeiter missbrauchen ihren Zugang zu vertraulichen Kundendaten, um diese an Cyberkriminelle oder Unternehmensspione weiterzureichen. Laut einer Untersuchung des Softwarehauses Symantec ist die Verwicklung von Angestellten in Datenschutzverletzungen in den letzten Jahren massiv gestiegen.



Quelle: Information is Beautiful

„Im Kundengespräch zeigt sich, dass es noch ein sehr neues Thema ist, wo noch viele Fragen offen sind."

DI Dr. Stefan Poledna
Vorstand und Mitbegründer TTTech Computertechnik AG




Nutzen der Datenflut

Vom logischen zum systemischen Denken.

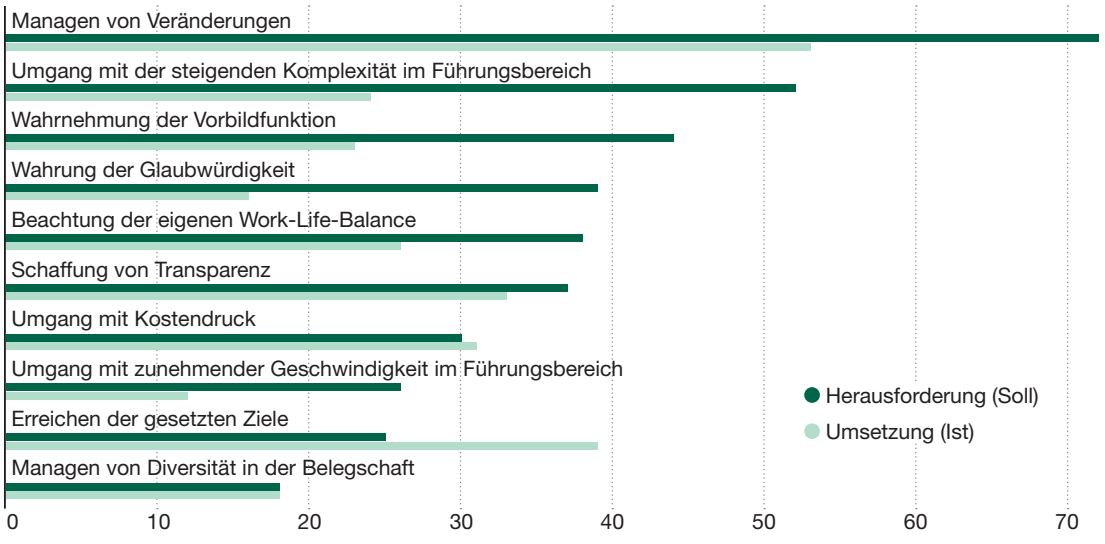
Thematische Einführung von Franz Kühmayer, zukunftsInstitut

Isolierte Betrachtungsweisen helfen uns nicht mehr weiter. Mehr als jede andere wirtschaftliche Entwicklung stülpt die Digitalisierung das Unternehmen radikal um: Was innen war, rutscht an die Außengrenze; was geheim war, wird öffentlich; was geschlossen war, wird durchlässig und offen. Denn der Erfolg der Zukunft entsteht auch für die Big Data Champions nicht in individueller Exzellenz als Unternehmen, sondern als Mitspieler auf Datenplattformen. Dort, wo Daten als neue Währung gehandelt werden, wo aus Information gegenseitiger Mehrwert wird, entscheiden sich Wachstum und Gewinn. Führungsarbeit bedeutet mehr denn je radikale Öffnung, Denken und Handeln über Grenzen hinweg und interdisziplinäres Verständnis über die digitalen Ökosysteme. Und Sicherheit ist kein Aspekt, der ein einzelnes Unternehmen betrifft, sondern stets ganze Netzwerke von Betrieben.

Dabei birgt die digitale Revolution nicht nur Risiken, sondern auch neue Methoden zur Erhöhung der Sicherheit. Schäden bereits vereiteln, bevor sie entstehen, und technische Interventionen schon vor dem Anlassfall vornehmen zu können, ist das Motto vorausschauender Maßnahmen. Mit Predictive Analytics kommt man diesem Ziel näher als je zuvor - vorausgesetzt man entwickelt ein systemisches Verständnis über die Zusammenhänge komplexer Systeme.

Management von Veränderung und Komplexität

Anteil der Entscheider, die folgende Aspekte als wichtige Herausforderung ansehen, und ihre Einschätzung der Umsetzung (in Prozent)



Quelle: Hays

Ing. Mag. Thomas Jost

Es muss gewährleistet werden können, dass im Digitalisierungsprozess sämtliche Systeme und Prozesse im Unternehmen nach wie vor vollumfänglich zur Verfügung stehen. Daten müssen in Formaten und mit entsprechenden Technologien gespeichert werden, damit sie auch nach vielen Jahren noch lesbar sind.

DI Dr. Peter Layr

Generell ist die Sicherheit aber auch die Qualität der Software eine Schlüsselfrage. Wird in Zukunft fehlerfreie Software einfach mehr kosten, wodurch man sich selbst für ein Sicherheitsniveau entscheiden kann?

DI (FH) Andreas Gerstenmayer

Open Source Modelle benötigen eine konsequente IT-Governance zur Vermeidung der Risiken. Wo es sich nicht vermeiden lässt und wo Provider professionelle Lösungen anbieten, nutzen wir heute schon Cloud-Services. Dabei gehen wir aber keine Kompromisse bei unseren internen Vorgaben zur Risikovermeidung ein.

Johann Christof

Wir verwenden bereits heute verschiedene, sorgfältig selektierte Cloud-Lösungen, um am globalen Markt konstruktiv, zeitschonend und flexibel arbeiten zu können. Da es allerdings sehr viele verschiedene Möglichkeiten und Plattformen gibt zu kommunizieren und wir global tätig sind, haben wir noch immer Schwierigkeiten alle nötigen Kommunikationswege in unsere IT zu integrieren und dabei den gewünschten Sicherheitslevel beizubehalten. Die westliche Welt verwendet zum Beispiel hauptsächlich Whatsapp, Skype und LinkedIn, im Mittleren Osten und Osteuropa aber vermehrt Telegram und Viber. Es gibt auch keine standardisierten Datenraum-Plattformen, was heißt, dass wir immer wieder mit neuen Programmen und Cloud-Lösungen konfrontiert sind um zum Beispiel auf Dokumente während eines Due Diligence Prozesses zugreifen zu können oder sicherheitskritische Dokumente für Industrialisierungen von externen Technologien auszutauschen.

DI Armin Rau

Durch die Vernetzung werden die Systeme an sich resilienter, weil man Ersatzstrategien fahren kann und mehrere vernetzte Maschinen zur Verfügung hat, die unter Umständen das Gleiche bewirken können. Wenn ein Teil einer Maschine ausfällt, kann dessen Funktion durch die Vernetzung von anderen Komponenten oder Maschinen übernommen werden. Somit wird aber auch sichere Vernetzung ein wesentlicher Aspekt.

Führung in immer komplexeren Systemen

Komplexität braucht ein neues Sicherheitsverständnis.

Thematische Einführung von Franz Kühmayer, zukunftsInstitut

Durch die gestiegene Datenmenge und die Volatilität und Mehrdeutigkeit einer immer dynamischeren Wirtschaft werden die bewährten Führungsprinzipien immer öfter in Frage gestellt. Hinzu kommt die Unübersichtlichkeit der Gesamtsituation: Zu komplex und volatil sind die Umgebungsbedingungen, um noch mit langfristiger Planung bearbeitbar zu sein. Selbst erfahrene und hochkompetente Führungskräfte müssen anerkennen, dass ihnen die Deutungshoheit über die Zusammenhänge zunehmend entgleitet: Das Schreckgespenst der Komplexität geht um. Widerstand scheint zwecklos, und vielleicht ist er sogar unangebracht. Der Erfolg der Zukunft liegt weniger darin, Komplexität zu bekämpfen, als vielmehr darin, sie freudvoll ins Unternehmen zu integrieren.
Mehr denn je wird uns klar: So wie von der Planbarkeit müssen wir uns in einer komplexen und vernetzten Welt auch von der absoluten Sicherheit verabschieden. Sie wandelt sich zu einer sozialen und technischen Konstruktion im Spannungsfeld zwischen dem Wunsch nach Kontrolle einerseits und Freiheit andererseits. Der Handlungsbedarf wird dadurch nicht geringer, im Gegenteil: Sicherheit verändert sich von einem Zustand zu einem aktiven Prozess.

Und am Ende begreifen wir: Sicherheit lässt sich nicht durch hermetisches Abschirmen gegen die Risiken der Außenwelt erzeugen, sondern im Gegenteil durch aktive Integration dieser Einflüsse. So wie eine Impfung das Immunsystem erst irritiert und dann stärkt, brauchen Unternehmen störende Einflüsse, um ihre Zukunft abzusichern.

„Auch muss man mit zunehmender Digitalisierung sehr genau wissen, welche Assets im Unternehmen überhaupt schützenswert sind. Das gesamte Management muss sich zu diesem Schutz bekennen.“

DI (FH) Andreas Gerstenmayer
CEO AT&S AG

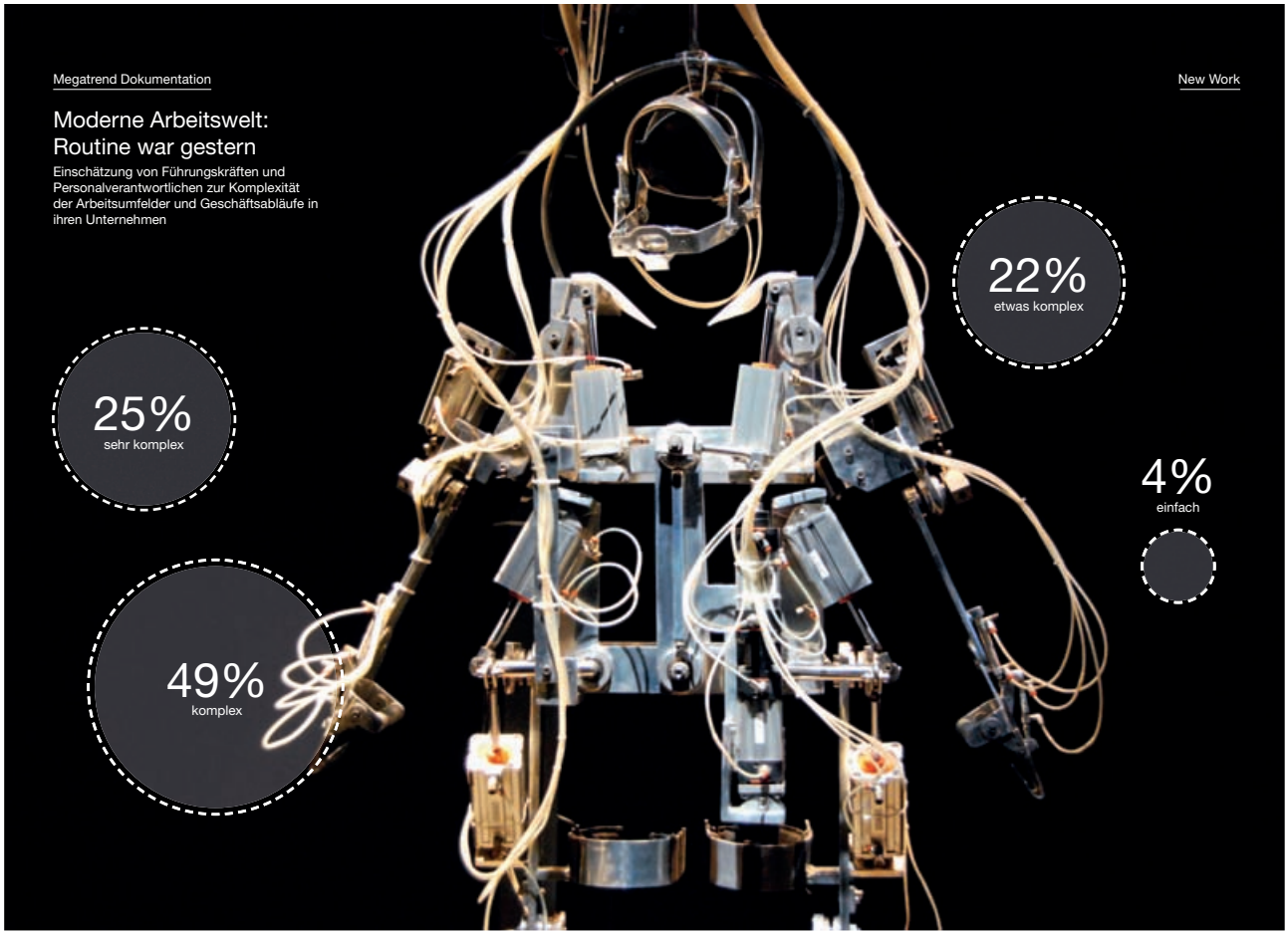


Foto: Flickr, andybient, CC BY 2.0
Quelle: Deloitte

DI (FH) Andreas Gerstenmayer

Die Vielzahl der Aktivitäten zum Thema digitale Transformation im Unternehmen zeigt, dass man Sicherheit nicht mehr anlass- und projektbezogen betrachten kann. Es müssen solide Security-Prozesse und eine Up2Date Basisinfrastruktur zum Thema Security implementiert werden, damit man auf eine solide Basis neue Projekte aber auch Versuchsanordnungen und Pilotprojekte aufsetzen kann. Hier helfen Information Security Management Systeme und auch Zertifizierungen wie ISO 27001 um nachweisbare Unternehmensabläufe zu garantieren. Auch muss man mit zunehmender Digitalisierung sehr genau wissen, welche Assets im Unternehmen überhaupt schützenswert sind. Das gesamte Management muss sich zu diesem Schutz bekennen.

„Alles was digitalisiert werden kann, wird auch digitalisiert werden. Somit findet zwangsweise die Konvergenz von Safety und Security statt."

DI Dr. Stefan Haas
CEO TÜV AUSTRIA Gruppe

DI Armin Rau

Zunächst ist bei der digitalen Transformation die Sicherheit nicht offensichtlich und direkt im Fokus. Es geht zunächst primär um Automatisierung und Vernetzung. Die Vernetzung von Sensoren und Aktoren bietet jedoch die Möglichkeit, Redundanzen zu bilden, die zu neuen Sicherheitskonzepten führen. Hier ist der TÜV AUSTRIA gefordert. Das gilt ebenso bei neuen Automatisierungstechniken wie kooperative und kollaborierende Roboter. Auf der übergeordneten Ebene der Smart Factory, in der Maschinen vernetzt sind und zukünftig ganze Prozesse gesteuert werden, muss man über neue Sicherheitskonzepte nachdenken, da nicht mehr die einzelne Maschine im Fokus steht.

DI Dr. Stefan Haas

Alles was digitalisiert werden kann, wird auch digitalisiert werden. Somit findet zwangsweise die Konvergenz von Safety und Security statt. Dadurch, dass sicherheitsrelevante Funktionen vermehrt über Software hergestellt werden, entstehen auch neue Angriffsvektoren. Schon allein aufgrund dessen muss man sich mit dieser Thematik proaktiv beschäftigen. Sicherheit muss konzeptionell von Anfang an mit hinein gedacht werden, also „Safety & Security by Design"; als Beispiel beim Automatisierten Fahren oder bei der Mensch-Maschinen-Kollaboration. Sicherheit ist nichts Absolutes; es müssen neue Methoden zur Risikobewertung entwickelt werden, um die Aussage treffen zu können, wann ein System gerade ausreichend sicher ist.

DI Dr. Stefan Poledna

Es braucht sicher vermehrt resiliente Systeme, es braucht aber auch ein proaktives Vorgehen, indem in einem regelmäßigen Intervall der Zustand des Systems überprüft wird, um möglichst schnell reagieren und auch Fehler erkennen zu können. Selbst wenn etwas nicht passiert, kann das durchaus auch ein Fehler sein.

Sicherheit wandelt sich von einem diskreten Zustand zu einem aktiven Prozess

Vom Risiko- zum Sicherheitsfaktor.

Thematische Einführung von Franz Kühmayer, zukunftsInstitut

Unter dem medialen Dauerfeuer von Krisen und Katastrophen entsteht eine Gesellschaft im Daueralarm. Schreckensbilder lähmen die Handlungsfähigkeit. Das düstere Außenbild hat dann verheerende Konsequenzen für innen. Aus dem Alarmismus der permanenten Bedrohungslage entsteht ein ängstlicher Blick auf die Zukunft und ein in sich gekehrtes Betriebsklima, das zu unbegründeten, übervorsichtigen Reaktionen führt. In diesem Klima blüht ein Führungsstil, der systemerhaltend wirkt, notwendige Veränderungen verhindert und der Innovationsbereitschaft des Betriebes diametral gegenüber steht. Das muss sich ändern, wenn Unternehmen im Wettbewerb um Wachstum und Marktanteile an die Spitze wollen. Führungskräfte brauchen jetzt vor allem eines: Mehr Mut, Richtungen vorzugeben und mehr Bereitschaft, die Zukunft aktiv zu gestalten.

Fordernde Zeiten sind immer auch ein fruchtbarer Boden für frische Ideen, in diesem Sinne leben wir in einer geradezu prototypischen Aufbruchszeit. Aus dieser Erkenntnis entsteht die Einsicht, dass wirtschaftliches Handeln immer risikobehaftet ist und es Führungsaufgabe ist, Risiko aktiv zu gestalten. Das macht den Unterschied aus zwischen einer fremd- und einer selbstbestimmten Zukunft, und ob Chancen genützt werden oder vorbeiziehen. Ausgerechnet Mut, und nicht übertriebene Vorsicht, stärkt die Resilienz von Unternehmen. Leadership bedeutet, einen Rahmen schaffen, der es ermöglicht, positiv mit den Dynamiken der Welt umzugehen, Zukunft zu gestalten und nicht gestaltet zu werden. Dazu braucht es eine frische Perspektive auf die Chancen von morgen - und einen starken Partner an seiner Seite, der Sicherheit versteht und immer wieder neu denkt.

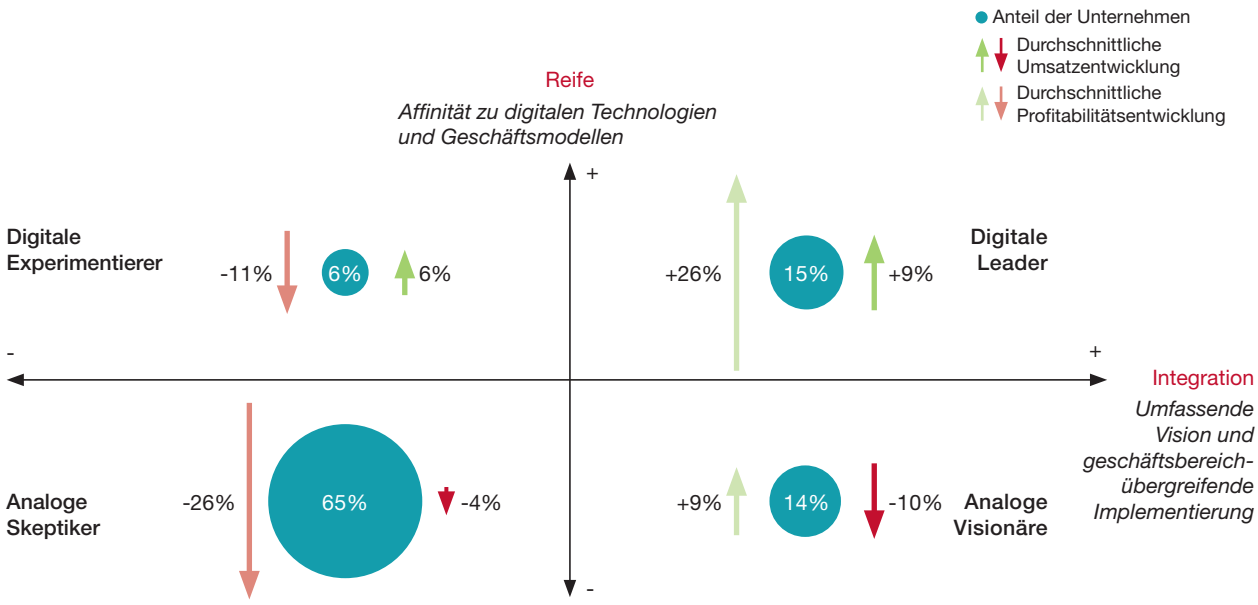
Dann wirkt auch Disruption spannend und nicht bedrohlich.

„Zunächst wird man definieren müssen, was überhaupt das passende Sicherheitsniveau ist. Es darf die Produktivität und Kreativität im Unternehmen nicht behindern – andererseits muss es uns aber adäquat schützen."

DI (FH) Andreas Gerstenmayer
CEO AT&S AG

Visionäre, Skeptiker, Experimentierer, Leader

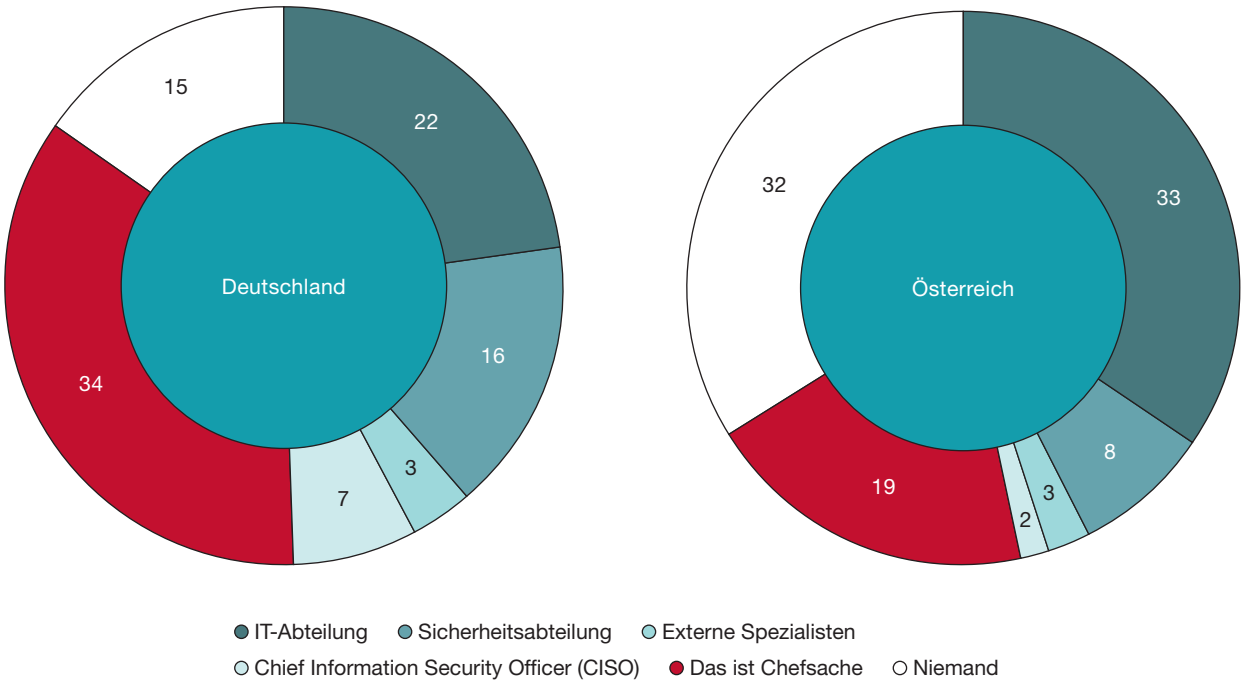
Auf dem Weg zur Digital Leadership zeigen sich beträchtliche Performance-Unterschiede



Quellen: Daten: Cap Gemini, Embracing Digital Technology, 2013; n = 1.600 Unternehmen
Darstellung: Franz Kühmayer

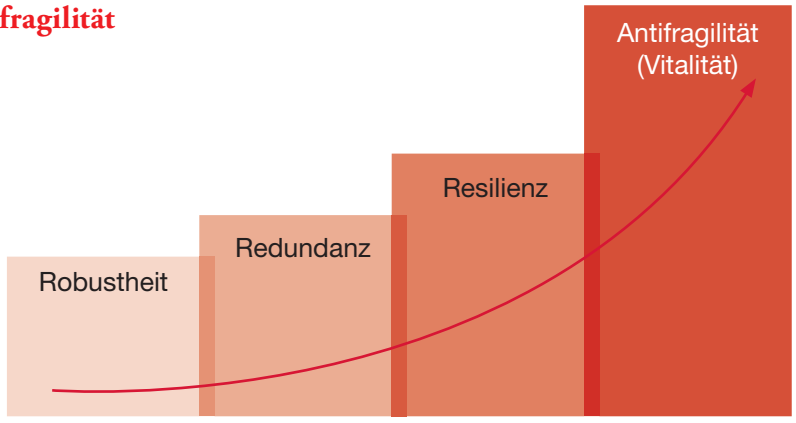
Sicherheit ist Chefsache

Wer kümmert sich in Ihrem Unternehmen um die zentralen Belange des Informationsschutzes? (Angaben in Prozent)



* Rundungsdifferenzen; Rest auf 100% = Sonstiges, keine Angabe
Quelle: Corporate Trust 2014; Befragte: 6.767 Unternehmen in Deutschland sowie 1.396 Unternehmen in Österreich

Von Resilienz zu Antifragilität



Quelle: Matthias Horx, Future Tools 2015

DI (FH) Andreas Gerstenmayer

Die Awareness zum Thema muss nicht nur beim Management der Unternehmen, sondern auch bei allen MitarbeiterInnen gesteigert werden. In den Medien werden sehr viele Vorfälle im Umfeld Security berichtet und jeder Mitarbeiter müsste sich laufend überlegen: Kann mir das auch passieren? Was würde ein solcher Vorfall für mich privat oder auch für mein Unternehmen bedeuten? Was kann ich zur Verhinderung solcher Vorfälle beitragen? Es muss ein „Sicherheits-Dialog" entstehen und für alle MitarbeiterInnen klar sein, wen sie im Unternehmen mit Fragen und Ideen dazu, aber auch bei Sicherheitsbedenken ansprechen können. Sicherheit muss heute auch als Informationssicherheit interpretiert werden, die alle Teile der Organisation betrifft. Der Begriff Sicherheit sollte untrennbar mit der Risikobetrachtung im Unternehmen verbunden werden. Zunächst wird man definieren müssen, was überhaupt das passende Sicherheitsniveau ist. Es darf die Produktivität und Kreativität im Unternehmen nicht behindern – andererseits muss es uns aber adäquat schützen.

Johann Christof

Sicherheit ist sehr wichtig, aber kann natürlich auch hohe Kosten und Inflexibilität mit sich bringen. Wir denken, dass ein wohl zu definierender Mindestlevel auf jeden Fall notwendig ist und Unternehmen darauf aufbauend versuchen sollten, ein jeweils maßgeschneidertes Sicherheitssystem zu implementieren, das sich einerseits in einem finanzierbaren Rahmen bewegt und andererseits dabei abgewogen werden muss, wie stark man seine Flexibilität einschränken kann, darf oder sollte. Speziell in unserem Geschäftsfeld kann die Menge und zeitliche Abfolge von Informationen entscheidend sein.

> *„Sicherheit ist sehr wichtig, aber kann natürlich auch hohe Kosten und Inflexibilität mit sich bringen."*
>
> **Johann Christof**
> CEO und Eigentümer Christof Industries GmbH

DI Dr. Peter Layr

Aus Unternehmenssicht wäre es wichtig, dass Sicherheit im Bezug zu Risiko adäquat abgebildet werden kann. Hier ist sicher der TÜV AUSTRIA gefragt – Unterstützung von Unternehmen über entsprechende Risikobewertungen. Letztendlich muss das Management das nötige Schutzniveau des Unternehmens definieren können.

„An das Bildungssystem werden durch die digitale Transformation immense Herausforderungen gestellt.“

O. Univ. Prof. DI Dr. Sabine Seidler
Rektorin der TU Wien

DI Dr. Stefan Poledna

Das Denken und die Einstellung zum Begriff Sicherheit haben sich in den letzten Jahren ganz wesentlich gewandelt. Dieses Sicherheitsdenken, das bereits in den 1980er Jahren in der Flugindustrie voll etabliert wurde, dringt nun ganz weit in Bereiche wie Automobil, Maschinen, industrielle Anwendungen vor. Auch aufgrund der Tatsache, dass Computer viel mehr steuern als es früher der Fall war, rückt Sicherheit in das Zentrum und spielt eine zentrale Rolle.Zu viel Sicherheit kann man nie haben. Die Fragestellung muss sein: Wie kann ich Sicherheit möglichst effizient erreichen.

DI Dr. Stefan Haas

Durch die Digitalisierung steigt die Gefahr, dass viele Grundfähigkeiten verloren werden. Der Schritt vom Stadtplan zu Google Maps kann auf die Technik übertragen werden: Wenn Ingenieure keine Pläne mehr lesen können, sondern nur mehr 3D CAD, werden sicherheitsrelevante Fehler erst möglich die es so bisher nicht gegeben hat.

O. Univ. Prof. DI Dr. Sabine Seidler

An das Bildungssystem werden durch die digitale Transformation immense Herausforderungen gestellt. Sicherer Umgang in und mit digitalen Medien und Inhalten muss gelehrt und gelernt werden. Für die digitale Welt braucht es analoge Entsprechungen – alles was digital entsteht muss auch real geschehen. Nicht Karten lesen zu können mag nicht immer sicherheitskritische Auswirkungen haben, schlimm wird es aber wenn man außer Google auf nichts mehr zurückgreifen kann.

Company Profile TÜV AUSTRIA

Company Profile TÜV AUSTRIA

Die Servicekompetenzen der vier Geschäftsfelder „Industry & Energy“, „Infrastructure & Transportation“, „Life, Training & Certification“ und „Service Providers and Public“ umfassen die Bereiche Prüfung, Überwachung, Zertifizierung, Aus- & Weiterbildung und Beratung.

Der österreichische TÜV ist ein internationales Unternehmen mit Niederlassungen in mehr als 40 Ländern der Welt. TÜV AUSTRIA beschäftigt über 1.500 Mitarbeiterinnen und Mitarbeiter und erwirtschaftet 160 Mio. Euro Umsatz.

Engagement in Forschungsprojekten

Der TÜV AUSTRIA engagiert sich in einer Reihe von Forschungsprojekten zur Digitalen Transformation. Ziel dabei ist, die Entwicklungen der Kooperationspartner mit integrierten Sicherheitskonzepten zu unterstützen, um einen zeitnahen Praxiseinsatz der Technologien zu ermöglichen. Beispielhaft dafür wird im Folgenden je ein Projekt aus den Handlungsfeldern „Industrie 4.0“ und „Automatisiertes Fahren“, vorgestellt.

Industrie 4.0 | Mensch-Roboter-Kollaboration (MRK)

Innovationsvorhaben: Integriertes Safety & Security-Konzept für MRK
Projektziel: Entwicklung eines anwendungsorientierten, integrierten Safety & Security (ISS)-Konzepts zur ganzheitlichen Berücksichtigung sicherheitsrelevanter Aspekte bei der Einführung von MRK im Produktionskontext: Theoretische Erarbeitung und praktische Erprobung anhand konkreter Applikationen in der Industrie 4.0 Pilotfabrik der TU Wien. Laufende Veröffentlichung der Erkenntnisse in einer White Paper Reihe.
Projektpartner: Fraunhofer Austria
Assoziierte Projektpartner: TU Wien Pilotfabrik Industrie 4.0, Joanneum Research Robotics

White Paper Reihe zu Safety & Security in der MRK

Automatisiertes Fahren | Autonome Autobusse

Innovationsvorhaben: auto.Bus Seestadt

Projektziel: Technologische und rechtliche Weiterentwicklung von autonomen Kleinbussen. Ziel ist die nachhaltige Erhöhung der Effizienz und der Betriebssicherheit autonomer Fahrzeuge, um letztlich eine Buslinie in der Seestadt in Aspern / Wien unter realen Bedingungen betreiben zu können – mit Haltestellen, Fahrplan und echten Fahrgästen.
Projektpartner: Wiener Linien, AIT Austrian Institute of Technology, das Kuratorium für Verkehrssicherheit, SIEMENS AG Österreich und der französische Bushersteller NAVYA

© APA/NAVYA/Pierre Salomé

innovatüv®

Die creative Community der TÜV AUSTRIA Gruppe

innovatüv® ist die Social Crowdsourcing Plattform der TÜV AUSTRIA Gruppe und ein hocheffizientes Tool zur kollaborativen Ideenfindung und Ableitung von Innovationsvorhaben. innovatüv® vernetzt die komplette TÜV AUSTRIA Gruppe zu einer Ideen-Community und nützt dabei Gamification-Elemente (Integration von spieltypischen Elementen), wodurch eine signifikante Motivationssteigerung der Teilnehmer erreicht wird. Nach nicht einmal zwei Jahren sind über 60% aller MitarbeiterInnen registriert, 545 Ideen wurden eingereicht und eine Vielzahl davon bereits umgesetzt. Zahlreiche Diskussionsgruppen werden laufend quer über die Kontinente gebildet, in denen Ideen gemeinsam global weiterentwickelt werden.

TÜV AUSTRIA GROUP
CORPORATE INNOVATION MANAGEMENT
TÜV AUSTRIA-Platz 1
2345 Brunn am Gebirge
innovation@tuv.at
www.tuv.at