

Cybersecurity –

Was wir von Dodos und Karl Marx lernen können ...

An der Digitalisierung kommt heute kein Unternehmen mehr vorbei, wenn es nicht aussterben möchte wie einst der Dodo. Aber bevor die Digitalisierung von Geschäftsprozessen beginnt, muss sich der Blick auf die Sicherheit richten.



Industrie 4.0, Digitalisierung – die Aufbruchstimmung und die Bereitschaft, die damit verbundenen Herausforderungen anzugehen, sind in der deutschen Wirtschaft spürbar. Chancen vernebeln den Blick auf Risiken und so wird schnell übersehen, dass Digitalisierung einer Grundvoraussetzung bedarf: der Cybersicherheit. Schon in der Schlacht um die Sicherheit

unserer klassischen Informationstechnik (IT) stehen wir mit dem Rücken an der Wand. Jetzt heißt es gleichzeitig eine neue Front eröffnen.

Morgen drohen uns – wenn wir nicht die richtigen Konsequenzen ziehen – Risiken ganz anderen Ausmaßes, wie ein Blick in die Vergangenheit verdeutlicht. Ende des 17. Jahrhunderts starb auf der Insel Mauritius der letzte Dodo, ein flugunfähiger Vogel. Gerade 100 Jahre hat es von seiner Entdeckung bis zu seinem Aussterben gedauert. Die europäischen Entdecker und ihre mitgebrachten Hunde und Katzen machten aus der Idylle ein gefährliches Biotop, gegen das der Dodo keine Abwehrmechanismen hatte.

Idyllisch ist auch die klassische Fabrikationsumgebung vor der Industrie 4.0. Cyberrisiken scheinen von einem anderen Planeten zu sein, die Unternehmensgrenzen schützen vor unbekanntem Gefahren. Hier kommt dann der Philosoph aus Trier ins Spiel: Karl Marx schrieb bekanntlich „Geschichte wiederholt sich – das eine Mal als Tragödie, das andere Mal als Farce“. Leider in diesem Fall in umgekehrter Reihenfolge – dies mag der Dodo allerdings anders sehen.

Entgegen dem gesunden Menschenverstand erleben wir derzeit, wie sehenden Auges Maschinen, Infrastrukturen, ja ganze Geschäftsprozesse in eine feindliche Umgebung ausgesetzt werden, auf die sie nicht ausreichend vorbereitet sind: das Internet. Im Glauben, in einer beherrschbaren, kontrollierten Umgebung betrieben und durchgeführt zu werden, wurde nie ein Augenmerk auf den Schutz gelegt. Warum sollte ein Dodo fliegen müssen, wenn er doch keine Feinde hatte?

Notdürftig wird nun oft versucht, mit technischen Hilfsmitteln im Nachgang ausreichenden Schutz zu erzielen. Ein Unterfangen, das oft genug zum Scheitern verurteilt ist. Ist es schon in der „klassischen“ IT schwer, die zentralste aller Sicherheitsmaßnahmen, etwa die Aktualität der Systeme durch Updates, zu gewährleisten, so ist dies bei Produktions- und Steuerungsanlagen noch viel schwieriger. So verbieten etwa bis dato Hersteller

jegliche Konfigurationsänderung an Maschinen mit der Androhung des Verlusts der Gewährleistung und die Anlagen sind mit einer Lebensdauer geplant, in der die IT mehrere Produktgenerationen erlebt.

In einer Welt, die einerseits mutwillig revolutionär agiert und sich andererseits nicht einmal evolutionär weiterentwickelt, drohen relevante Elemente unserer industriellen Basis zum Dodo 2.0 zu werden. Dummerweise werden wir als führende Industrienation aber erst recht das Schicksal des Dodos teilen, wenn wir den Weg der Digitalisierung nicht gehen.

Das schon berühmte Wahlplakat der FDP mit dem Slogan „Digitalisierung first, Bedenken second“ darf nur nicht missverstanden werden! Ein „Denken first, Digitalisierung second“ sollte daneben gestellt werden. Ein Denken von Anfang an auch an die Risiken, die Integration der Sicherheit in strategische Überlegungen. In der IT setzt sich immer stärker die Philosophie des „Security by Design“ durch, was zu nachhaltig besseren Lösungen führt. Dieser Ansatz muss auch in die Strategie- und Prozessgestaltung von Beginn an einziehen. Ja, vermutlich dauert dies ein paar Tage länger. Ja, definitiv wird es sicherere Lösungen nicht zum Nulltarif geben und: Ja, eventuell wird so auch die eine oder andere Idee wie eine Seifenblase platzen. Aber wann will ich als Unternehmer erfahren, dass die Ertragschancen in toto niedriger sind als die Kosten für eine angemessene Risikobegrenzung, wenn nicht ganz am Anfang?

„Security by Design“ als ursprünglich technisches Konzept ist aber gerade keine technische Herangehensweise. Wer glaubt, dass „sich unsere Techies schon um die Sicherheit kümmern werden“, hat den entscheidenden Schritt für ein Scheitern schon getan.

Sicherheit und Digitalisierung sind so eng verzahnt, dass beides strategisch und aus gesamtunternehmerischer Perspektive gedacht und gesteuert werden muss. Gerade weil Sicherheit auf den ersten Blick nichts zum Unternehmenserfolg beisteuert – und ihn scheinbar sogar reduziert,

sind der Blick und die Unterstützung vom ersten Tag und von oben von höchster Bedeutung.

Aber auch auf staatlicher und gesellschaftlicher Seite muss das Thema breiter, verzahnter und proaktiver betrachtet werden. Ein Beispiel hierfür wäre ein nationaler, privatwirtschaftlich gefüllter und gesteuerter Venture

Prof. Timo Kob

Professor für Wirtschaftsschutz und Cybersecurity, FH Campus Wien; Vorstand HiSolutions AG



Foto: Privat

„Wir dürfen Christian Lindners ‚Digitalisierung first, Bedenken second‘ nicht missverstehen! Ein ‚Denken first, Digitalisierung second‘ sollte daneben gestellt werden.“

Capital Fonds, der mit aktiver Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik und unter Einbeziehung der hervorragend aufgestellten deutschen Forschungslandschaft gleich mehrere strategische Grundübel beheben kann: Erstens, Selbsthilfe der Wirtschaft bei der Entwicklung nationaler, gegebenenfalls europäischer Lösungen an aus Sicherheitssicht neuralgischen Punkten. Zweitens, Umgehung der durch EU-Beihilfe-Regeln bei der klassischen staatlichen Förderung erforderlichen Marktferne der Forschung und drittens, strategischer Schutz der entwickelten Lösungen vor einem Verkauf ins Ausland ohne marktwirtschaftlich stets heikle Eingriffe und Verbote durch den Staat.

Auch hier gilt wie beim Selbstschutz der Unternehmen: Je früher die verschiedenen Aspekte aktiv zusammengeführt und strategisch angegangen werden, desto mehr Sicherheit können wir erreichen für einen dann definitiv tragbaren Mehraufwand. □