

Wirtschaft

03. Jan. 2023 | 08:37 Uhr | von Siegfried Müller

Kolumne

Digitalisierung und IT-Sicherheit: So lösen Sie das Paradoxon

Je höher der Grad der Digitalisierung, desto größer sind die potenziellen Angriffsflächen. Wie Sie das Paradoxon auflösen können, erklärt unser Kolumnist Siegfried Müller.



Verläuft die Digitalisierung – insbesondere im Mittelstand – noch immer stockend? (Bild: NicoElNino - stock.adobe.com)

Ich hatte in meiner vorletzten Kolumne angekündigt, **das Digitalisierungs-Paradoxon** einmal näher zu beleuchten und was im Gesamtkontext der Digitalisierung dabei meiner Meinung nach bedacht werden müsste.

Aber, wie es manchmal eben so ist, während der letzten Vorbereitungen zur SPS kam mir irgendwann der Gedanke, es wäre doch sinnvoll umzudisponieren – aus diesem Grund habe ich dann ein Thema vorgezogen, das dedizierter auf die Messe Bezug nahm. Doch jetzt – direkt nach dem Digital-Gipfel – bietet es sich ja geradezu an, den Faden wieder aufzunehmen. Wobei das Digitalisierungs-Paradoxon dem Grund nach natürlich unmittelbar nichts mit dem Digital-Gipfel zu tun hat. **Denn in Berlin stand aktuell die Datenökonomie im Vordergrund – also, dass es die Daten sind, die „im Mittelpunkt des digitalen Wandels stehen“.** Mit dem Fokus wird verdeutlicht: diese bestimmen im Prinzip alles, sowohl unseren Konsum und unsere Lebensweise als auch unsere Produktionsprozesse sowie die Lieferketten.

In der Theorie hört sich das alles sehr gut an, aber wie sieht es in der Praxis aus – konkret, wie versiert kann insbesondere der produzierende Mittelstand in Bezug auf die Digitalisierung inzwischen tatsächlich sein?

Digitalisierung kam nicht immer gut an

Ein kurzer Rückblick könnte diesbezüglich eventuell einen Anhaltspunkt geben: Vor noch nicht allzu langer Zeit, das mag jetzt vielleicht vier Jahre her sein, standen viele Unternehmen der Digitalisierung keinesfalls durchweg zustimmend gegenüber – teilweise wurde sogar abfällig vom „Digitalisierungs-Hype“ gesprochen und entsprechende Schreckensszenarien entworfen, zum Beispiel, dass infolgedessen eine digitale Jobvernichtung zu erwarten wäre, weil die IT immer einfacher werde und dies massenweise Arbeitsplätze vernichten würde.

Vor knapp drei Jahren (und teilweise auch heute noch) fiel dann die Bewertung der Digitalisierungserfolge gar nicht durchgehend positiv aus – oftmals stand hierbei provokativ an erster Stelle die Frage im Raum, wie sich denn eine stagnierende Produktivität trotz technologischem Fortschritt erklären ließe.

Doch kann darin insgesamt die Begründung liegen, warum die Digitalisierung – insbesondere im Mittelstand – noch immer stockend verläuft? Vor allem, da ja – eigentlich allseits bekannt – eine gewisse Notwendigkeit dazu besteht, denn die hochwertigen (deutschen) Produkte müssen zu konkurrenzfähigen Kosten hergestellt werden und diese Anforderung zu erfüllen setzt eben eine hohe Effizienz der Produktionsprozesse voraus.

Digitalisierung: Es fehlen Anwendungsszenarien

Meines Erachtens gibt es zwei relevante Faktoren, die in diesem Kontext Beachtung finden müssen:

Erster Faktor: Es fehlen gute Anwendungs- und Einsatzszenarien

Da bis vor zwei Jahren das Erfordernis zur Digitalisierung noch nicht in der Form gegeben war, bestand hier kein unmittelbarer Handlungsbedarf sich mit **neuen Technologien** eingehender zu beschäftigen. Daraus resultiert jetzt die Krux, dass die Verantwortlichen mittlerweile über Projekte entscheiden müssen, obwohl für sie lediglich das erforderliche Investment in die Digitalisierung transparent ist – sie jedoch nur über wenig bis keinerlei praktische Erfahrungsberichte bezüglich der Eignung einer Technologie für einen speziellen Einsatzzweck beispielsweise im Produktionsumfeld verfügen.

Doch das ist nicht der einzige Knackpunkt: häufig erschließt sich den Verantwortlichen weder unmittelbar und bisweilen auch gar nicht, welche Vorteile der Einsatz neuer Technologien überhaupt mit sich bringen könnte. Hier gibt es meines Erachtens noch zu wenig Ansätze, um einen konstruktiven Austausch zwischen Unternehmen zu fördern und definitiv nicht genügend konkrete plastische Anwendungsszenarien.

Hinzu kommt, dass zu oft eine Diskrepanz besteht zwischen realen Problemstellungen in den Unternehmen und dem, was als ‚Must have‘ im Sinne einer fortschrittlichen Technologisierung postuliert wird. Denn abgesehen von einer hier oftmals fehlenden Interoperabilität – nein, nicht jede Technologie lässt sich barrierefrei implementieren, auch wenn dies nahezu durchweg als Standard-Versprechen kursiert – die sich dann eher als Bremsklotz für die Digitalisierung erweisen kann, lässt sich ein Projekt doch nur dann als Erfolg bewerten, wenn dadurch ein vorhandenes Problem gelöst wurde.

Zu guter Letzt zählt in diesem Kontext natürlich auch der monetäre Aspekt – also ob sich das Investition tatsächlich rechnen lässt. In diesem Punkt mangelt es ebenfalls oft an Hilfestellung für die Unternehmen: Es gibt zwar klassische Beispielkalkulationen, aber die sind eben aufgrund ihrer intendierten Allgemeingültigkeit nicht auf jedes Unternehmen anwendbar und von daher als Entscheidungsgrundlage ungeeignet.

Je mehr Digitalisierung, desto mehr potenzielle Angriffsfläche

Zweiter Faktor: Es gibt ein Digitalisierungs-Paradoxon bezüglich IT-Sicherheit

Es gibt einen logischen Widerspruch, der sich offenkundig bislang (noch) nicht leicht auflösen lässt, obwohl die Auswirkungen davon als extrem gravierend bezeichnet werden können: das mit der Digitalisierung einhergehende und gleichzeitig dieses hemmende Sicherheitsdilemma.

Denn je höher der Grad der Digitalisierung ist und je mehr digitale Werte dadurch entstehen, **desto größer sind die potenziellen Angriffsflächen**. Aufgrund dessen besteht eine latente Angst bei den Unternehmen: denn einerseits resultieren daraus mehr Einfallstore für kriminelle Angriffe und andererseits sind zusätzlich negative Auswirkungen dadurch zu erwarten, dass – bedingt durch die entstandene Transparenz – sensible Daten nach außen gelangen können.

Konsequenterweise müsste dies zur Erhöhung des Schutzniveaus führen – **also Unternehmen dazu veranlassen, mehr in IT-Sicherheitsmaßnahmen zu investieren**. Doch das geschieht nicht im erforderlichen Maße und gleichzeitig hemmt diese Angst die Motivation überhaupt Digitalisierungsprojekte anzugehen, um die Angreifbarkeit nicht zu erhöhen.

Meine Empfehlung zur Auflösung des Paradoxons

Auch wenn dieser Satz gerne als Allgemeinplatz hingestellt wird, verliert er nicht an Relevanz – denn die Aussage hat sich in den letzten Monaten immer wieder bewahrheitet: Die Digitalisierung kann nicht erfolgreich vonstattengehen, wenn die Cyber-/IT-Sicherheit nicht von Anfang als fester Bestandteil miteingeplant wird.

Bezüglich der konkreten Umsetzung hat sich meiner Erfahrung nach in den vergangenen Jahren bewährt, kompakte und somit überschaubare Digitalisierungsprojekte anzugehen – immer mit Blick darauf, dass diese geeignet sind ein vorhandenes Problem im Unternehmen zu lösen. Der Vorteil dieser Vorgehensweise besteht zudem darin, dass die erforderlichen Cyber-/IT-Sicherheitsmaßnahmen parallel dazu entsprechend mitkonzipiert werden können.

Zu guter Letzt: Ja – auch 2022 gab es einige Herausforderungen bezüglich der Cyber-/IT-Sicherheit und gerade im Dezember hat das dem ein oder anderen vielleicht ein wenig die Stimmung verdorben.

Ich hoffe, Sie hatten schöne Feiertage und wünsche Ihnen ein gutes neues Jahr!

Das ist unser Kolumnist Siegfried Müller

Siegfried Müller ist Vice-President Advanced Technologies bei der MB Connect Line GmbH Fernwartungssysteme.

In seinen ersten Berufsjahren als Steuerungstechniker für den Maschinenbau hat er den Nutzen von Fernwartung erkannt. Im Alter von 25 Jahren gründete er MB Connect Line. Unter seiner Leitung entwickelte sich das Unternehmen zum Technologieführer in den Bereichen Fernwartung, Datenerfassung und Industrial Security. Heute ist die MB Connect Line der europäische Standort der Red Lion Inc. in der Industrial Division der Spectris PLC Gruppe.



(Bild: MB Connect Line)