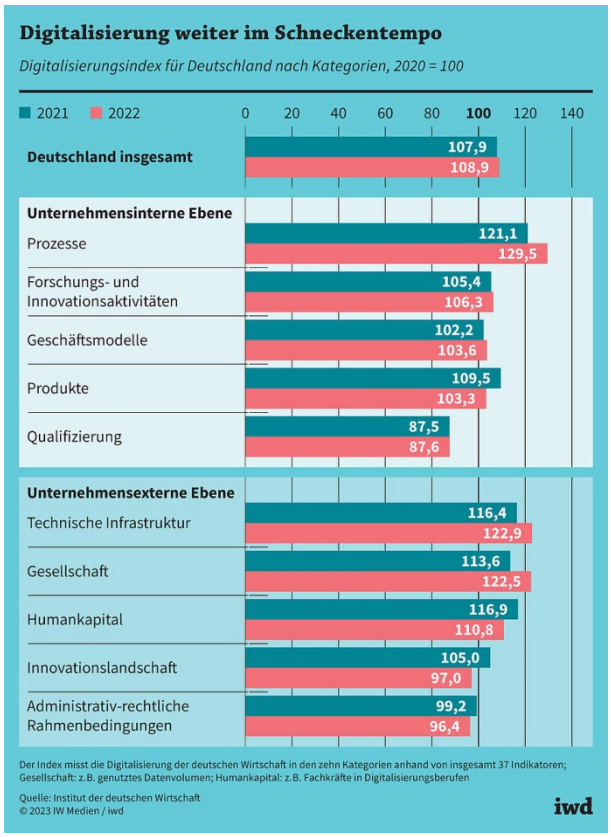
Digitale Transformation und Cybersicherheit

BCCG Brit Chamber Talks am 5. September 2023

Digitale Transformation und Cybersicherheit, ein Thema, das häufig in den Mund genommen wird, aber – so die Auffassung und Erfahrung der Experten von EY – nicht immer die Bewertung und Berücksichtigung erhält, die zwingend erforderlich ist.
Grund genug, sich im Rahmen des Hamburger BCCG-Formates Brit Chamber Talks dieses Sujets anzunehmen, um aus berufenen Mund eine Übersicht zum Stand der Dinge zu erhalten.

Den Zuhörern wurde das komplexe Themenfeld in zwei Keynotes anschaulich präsentiert. Olaf Riedel, EY Office Manager Hamburg und Lead Partner Technology übernahm den Part, den gegenwärtigen Stand der digitalen Transformation Deutschlands aufzuzeigen und einen Überblick über die auf die europäischen Unternehmen zukommenden Regularien im Reporting zu geben.
Grundsätzlich ist festzustellen, dass in Sachen Digitalisierung die Umsetzungsdynamik in Deutschland im Vergleich zu 2020 reichlich an Schwung verloren hat.

Indiziert auf 2020 (Index 100) ist für Deutschland insgesamt 2021 der Index auf 107,9 gestiegen und 2022 auf nur 108,9. Man kann durchaus von Schneckentempo sprechen. Schlimmer sieht es im Segment administrativer und rechtlicher Rahmenbedingungen aus. Hier sank der Index von 99,2 auf 96,4.und im Bereich Innovation fiel der Index auf 97,0. Auf Unternehmensebene zeigt sich ebenfalls kein gutes Bild. Geschäftsmodelle sind gegenüber 2022 um 3,6 Indexpunke mehr digitalisiert als 2020. Nur bei den Unternehmensprozessen ist der Digitalisierungsgrad um 29,5 Punkte höher als 2020 (siehe auch Grafik unten).



Die Anforderungen, insbesondere an börsennotierte Unternehmen, werden in den kommenden Jahren noch weiter steigen, so dass die Bezeichnung eines 'regulativen Tsunamis' nicht so ganz unpassend ist.

Scheinen in erster Linie nur große Unternehmen betroffen zu sein, ist jedoch davon auszugehen, dass die Welle auch auf den Mittelstand überschwappt. Große, nicht-kapitalmarktorientierte Unternehmen (auch gehobener Mittelstand) fallen ab 2025 verpflichtend in den Anwendungsbereich der Corporate Sustainability Reporting Directive (CSRD). Allein bei den KMU gibt es ab 2026 die zusätzliche Erfordernis einer Börsennotierung, um unter die Berichtspflicht zu fallen. Im Mittelstand betrifft dies auf europäischer Ebene anstelle der bisher ca. 11.600 Unternehmen dann über 50.000 Unternehmen. Die Auswirkungen werden branchenunabhängig in besonderer Weise vor allem die großen Zulieferer in der Lieferkette zu spüren bekommen.

Zu bemerken ist auch, dass selbst nicht-europäische Institutionen sowie Banken und Versicherungen schon heute das regulative Rahmenwerk der EU teilweise als zukunftweisend betrachten und ähnliche Prozesse in ihren eigenen Jurisdiktionen anschieben oder zumindest erwägen.

Dies alles bedeutet, dass sich die Industrie insgesamt mittel- und langfristig auf die an sie gestellten Anforderungen vorbereiten muss – egal von wo aus die Geschäfte gelenkt werden.

Letztlich wird die verlangte Auditierbarkeit relevanter Prozesse eine Datenqualität erfordern, die neben der angepassten analogen Infrastruktur umfangreiche Digitalisierung unabdingbar macht.

Was die Daten und ihre Sicherheit und Sicherung betrifft, so lernten die Zuhörer von Sven Bartheidel, EY Lead Partner, Technology Risk-Europe West, wo die spezifischen Risiken liegen und womit sich Unternehmen auseinander setzen sollten, um sich vor Cyber-Angriffen zu schützen und sich gegebenenfalls auch zu wehren; dieses können, wie Sven Bartheidel ausführte, teilweise sehr einfache Schutzmechanismen sein.

Die gegenwärtigen geopolitischen Disruptionen und das Einkommensgefälle zwischen westlichen Industrienationen und Entwicklungsländern zeigen, dass mit recht wenig Aufwand und einem gewissen Grad an krimineller Energie sich im Bereich Cyber Extortion (Erpressung) bereits probate 'Geschäftsmodelle' entwickelt haben. Es sei noch nicht einmal erforderlich, die Angriffe selbst zu programmieren. Im Dark-Net bieten Hacker-Organisationen die komplette Umsetzung von Cyber-Attacks gegen moderate 'Gebühren' an.

Wichtig sei in diesem Zusammenhang, dass Unternehmen sich tunlichst vorbereiten sollten, wie sie mit Erpressungsversuchen umgehen können. Ein Weg sei jedenfalls, eine etablierte Backup-Struktur zu schaffen, die es ermöglicht, das ganze System herunter zu fahren und mit den gesicherten Daten neu zu starten.

Automatisierte und analoge Sicherungsprozesse sowie laufende Notfallübungen seien bedauerlicherweise noch nicht praktizierter 'Stand der Unternehmensführung', sind aber mit Blick auf die zunehmenden Cyber-Angriffe eine dringende Notwendigkeit, genauso wie der unternehmensinterne Umgang mit dem Thema. Das Wissen und die Einstellung der Mitarbeiter zu Cyber-Angriffen muss geschärft werden.
Sven Bartheidel: "Die Trojaner fühlten sich hinter ihren Mauern sicher – und wurden letzten Endes Opfer ihrer Unaufmerksamkeit"

Alles in Allem ein gelungener BCCG Brit Chamber Talk mit lots of food for thought.

Das BCCG Committee Northern Germany dankt dem Veranstalter EY und den Referenten, Olaf Riedel und Sven Bartheidel, für die umfangreichen Einsichten und die Gastfreundlichkeit.

Rainer M. Giersch, Founding Partner,
Accordo Partners Ltd. &
BCCG Regional Chairman Hamburg/Norddeutschland

File: E/RMG/BCCG/Reg/HHev/BCCG230906-Brit Chamber Talks - Digitale Transformation und Cybersicherheit