Neue Angriffsfläche durch Digitalisierung

Berthold Morschhäuser

Die Digitalisierung verändert die Welt. Schlagworte wie Industrie 4.0, Internet der Dinge, künstliche Intelligenz und Blockchain erreichen immer mehr die breite Öffentlichkeit und lösen dabei gleichermaßen Faszination wie Verunsicherung aus. Politiker, Wissenschaftler und nicht zuletzt die Unternehmensmanager sind für die Auswirkungen sensibilisiert. Viele sind hoch motiviert, teilweise sogar elektrisiert, in ihren Metiers neue Trends bei der Rahmengestaltung, der Erforschung neuer Lösungen oder der praktischen Umsetzung aktiv mitzugestalten. Bei allem Wettbewerbsdruck werden die Etats für Digitalisierungsprojekte vergleichsweise großzügig ausgestattet. Digitalisierung first lautet im Zweifel das ausschlaggebende Kriterium beim Gerangel um die Budgetverteilung.

Viele mögliche Folgen und Auswüchse der Digitalisierung hingegen sind den Managern wie auch dem breiten Publikum suspekt. So reizvoll gewisse Aussichten der neuen vernetzten Welt auch klingen mögen, die Einflüsse auf das Arbeitsleben, die Produktionsbedingungen und die Beschäftigungslage bleiben ebenso unklar wie die Auswirkungen auf die Sicherheit. Einen Vorgeschmack auf die Gefahrenlage einer immer stärkeren Vernetzung der gesamten Wirtschaft geben heute schon die neuen Kommunikationsdienste wie Google Earth, Google Maps, Facebook, Whatsapp und Twitter oder auch Internet- und E-Mail-Accounts. Sie erfahren zwar in aller Welt eine hohe Akzeptanz, doch die Schattenseiten der massenhaften Datenspeicherung und -auswertung mit all ihrem Missbrauchspotenzial machen auch nachdenklich. Das zeigte sich besonders deutlich an der allgemeinen Betroffenheit und Ratlosigkeit angesichts möglicher Manipulationen oder zumindest einer massiven Einflussnahme bei den US-Präsidentenwahlen.

Von nicht minderer Qualität sind großflächige Angriffe auf die (über)lebenswichtige Infrastruktur von Unternehmen oder staatliche Institutionen. Die im Verlauf dieses Jahres bekannt gewordenen Attacken von Hackern auf die Systeme von Weltkonzernen wie Fed-Ex, Merck oder Maersk haben zu Produktionsstörungen mit Millionenschäden geführt. Auch beim sogenannten Wanna-Cry-Fall Mitte Mai dieses Jahres wurde die Anfälligkeit eines zunehmend vernetzten Wirtschaftslebens offengelegt. Binnen weniger Stunden waren Hunderttausende Computer von privaten Nutzern infiziert, die Daten verschlüsselt und zur Freigabe wurde die Zahlung einer Art Lösegeld verlangt. Wiederum waren auch Systeme von vermeintlich professionellen Betreibern betroffen, etwa bei der Deutschen Bahn sowie dem Nationalen Gesundheitsdienst NHS (National Health Service) in Großbritannien.

Längst sind es nicht mehr nur Routinetätigkeiten und banale Entscheidungen, die der Maschine überlassen werden, sondern hochkomplexe Angelegenheiten. Besonders beeindruckende Beispiele aus dem Alltagsleben sind selbstfahrende Autos, die Experimente mit Paketzulieferungen durch Drohnen oder auch sprachgesteuerte Informationsdienste über automatische sprachbasierte Dialogsysteme, die sogenannten Chatbots. Was sich durch Industrie 4.0 im alltäglichen Leben und in den Wirtschaftsabläufen konkret ändern wird, wenn Beschaffung, Produktion und Vertrieb mit moderner Informations- und Kommunikationstechnik vernetzt werden, ist ein überaus spannendes Feld für Zukunfts- und Trendforscher.

Dass je nach Produktionstempo und Lagerbeständen ohne viel menschliches Zutun automatisch neue Rohstoffe beziehungsweise Vorprodukte bestellt werden und/oder gewisse Vertriebsmaßnahmen eingeleitet werden können, ist gedanklich leicht fassbar. Die Funktionen von Fenstern, Türen und Lampen per Smart-Home-Technik automatisch oder auch individuell über eine App zu steuern, wird als Erleichterung des Alltags wahrgenommen und schon fleißig geübt. Und dem Modul am Kühl- oder Vorratsschrank die Freigabe für die Nachbestellung von Gütern des täglichen Bedarfs einzuräumen – eventuell mit einer direkten Kontoabbuchung – liegt für viele Menschen zumindest im Bereich der Vorstellungskraft. Doch all das lässt sich stören.

Auch für die Kreditwirtschaft stellen Angriffe auf die IT-Struktur kein fiktives Szenario dar,

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Fritz Knapp Verlag GmbH

sondern können Realität werden. Größere Häuser wie die Commerzbank, die BNP Paribas und die ING Diba haben die massiv voranschreitende Digitalisierung längst zu ihrem wichtigsten strategischen Ziel erklärt und reklamieren eine aktive Vorreiterrolle in der Umsetzung. Die emsige Fintechbranche versteht die neuen technischen Möglichkeiten ohnehin als Basis jeglicher Markterfolge. Ihre Robo-Advisory-Lösungen boomen gerade. Aber auch für die beiden großen Verbünde der deutschen Kreditwirtschaft mit ihrer breiten Verankerung im Privat- und Firmenkundengeschäft ist der kluge Umgang mit den neuen technischen Errungenschaften buchstäblich überlebenswichtig. Ohne eine weitgehende Digitalisierung der Prozesse und der Öffnung des Vertriebs auf den Onlinekanälen einschließlich einer klugen Entscheidung über die Nutzung vorhandener Daten für eine gezielte Kundenansprache werden sie im harten Preiswettbewerb zerrieben.

All diese Einsichten und Aussichten haben unmittelbare Auswirkungen auf die Sicherheitsarchitektur der Banken. Waren in den Anfängen der Bankautomatisierung so banal klingende Themen wie die unterbrechungsfreie Stromversorgung oder ein adäquates Backup bei Ausfall eines Rechenzentrums zu lösen, bewegen sich die Sicherheitsprobleme der Kreditwirtschaft einschließlich der Abschätzung der Folgewirkungen von Digitalisierungsmaßnahmen heute in ganz anderen Dimensionen. Nahezu jede strategische Entscheidung tangiert die IT und könnte eine Gefährdung der Sicherheitslage bedeuten – im schlimmsten Fall eine totale Geschäftsblockade. Sollte man als Kreditinstitut massiv das Onlinebanking per Mobilgerät propagieren, wenn IT-Experten reihenweise Lücken bei einschlägigen Banking-Apps aufdecken? Wie reagieren die Kunden, wenn in Zeiten einer massenhaft genutzten Videoberatung dieser Beratungskanal ausfällt? Was passiert eigentlich, wenn die Bargeldversorgung an Geldausgabeautomaten nicht nur stundenweise wegen Wartungsarbeiten und kleinerer technischer Störungen, sondern tagelang mehr oder weniger flächendeckend gestört wird und so ganz nebenbei auch das Cash-Back-Verfahren, also die Geldausgabe im Händlernetz, durch kriminelle Machenschaften torpediert wird?

Solche Szenarien haben längst auch die Bankenaufseher auf den Plan gerufen – nicht zuletzt unter dem Blickwinkel der Finanzstabilität. Schon in den vergangenen Jahren haben BaFin und Bundesbank wiederholt auf die Gefahren der Cyberkriminalität hingewiesen und von der Branche angemessene Sicherheitsstandards eingefordert. Anfang November hat die Aufsicht als weiteren Baustein ihrer Prüfungstätigkeit in einem Rundschreiben die Bankaufsichtlichen Anforderungen an die IT veröffentlicht. Sie erläutert darin ihre Prüfkriterien und Vorstellungen von einer angemessenen technisch-organisatorischen Ausstattung der IT-Systeme der Banken, unter besonderer Berücksichtigung der Anforderungen an die Informationssicherheit sowie eines angemessenen Notfallkonzepts.

Die Branche selbst ist damit gefordert, an den relevanten Schnittstellen im Geschäftsverkehr die notwendigen Vorkehrungen zu treffen, um die System- und Datensicherheit zu gewährleisten. Ob dabei, einschließlich der Sensibilisierung von Mitarbeitern und Kunden für sicherheitsrelevante Verhaltensweisen, genug getan wird, ist für Außenstehende nur schwer zu beurteilen. Denn Sicherheit ist als Marketingansatz nur begrenzt geeignet. Schutzmaßnahmen gehören traditionell nicht zu den Features, über deren Ausgestaltung die Institute gerne in Einzelheiten sprechen. Und bei den Kunden wird die Sicherheit der Systeme ohnehin einfach vorausgesetzt. So bleibt bei der Einschätzung der Sicherheitslage stets ein wenig der Eindruck des Spiels von Hase und Igel. Schadenfreude im wörtlichen Sinne über sicherheitstechnische Pannen bei Wettbewerbern ist gleichwohl nicht am Platz. Denn jeder ernsthafte Vorfall trifft die ganze Branche. In diesem Sinne ist IT-Sicherheit eine Gemeinschaftsaufgabe.

Noch sind unterschiedliche Sicherheitsstandards allem Eindruck nach nicht zum entscheidenden Wettbewerbsfaktor in der Kreditwirtschaft geworden. Aber mit den Nebenbedingungen und vor allem auch Nebenwirkungen der Digitalisierung hat die Bedeutung einer wirksamen Sicherheitsarchitektur eine Dimension erreicht, die über eine Bedrohung für einzelne Häuser und Branchen hinausgeht und zu einer großen gesellschaftspolitischen Herausforderung bis hin zu einer Gefahr für die Demokratie werden kann (siehe auch Beitrag Nolting in diesem Heft). Dieser Gedanke hebt wirksame Sicherheitsvorkehrungen in den Rang einer Infrastrukturmaßnahme.

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Fritz Knapp Verlag GmbH