Chancen und Risiken der Digitalisierung

Aufsichtsräte im Spannungsfeld zwischen Wertigkeit und Cybersicherheit von Daten als immaterielles Wirtschaftsgut

Dr. Edgar Bernardi, Inhaber der avant ag, Agno (Schweiz)

„Digitalisierung" ist fast schon ein Hype, der allseits für Unternehmen gefordert wird. Zu sehr stehen jedoch die Chancen im Vordergrund, ohne die Risiken ausreichend in Betracht zu ziehen, die mit der Datenerfassung, -speicherung und -verarbeitung verbunden sind und auf deren Diebstahl Cyberangriffe abzielen. Der Aufsichtsrat steht daher zunehmend im Spannungsfeld zwischen digitaler Transformation und Abschätzung der damit verbundenen Risiken. Der folgende Beitrag soll aufzeigen, dass zunehmend komplexere und weitreichendere unternehmerische Aspekte auf den Aufsichtsrat mit der Digitalisierung zukommen.

I. Die neue Wertigkeit: Daten

Google hat heute eine Marktkapitalisierung von ca. 750 Mrd. US-Dollar (Mai 2018). Worin besteht der Wert dieses Unternehmens? Daten! Und wie viel wäre Google wert, wenn in einem hypothetischen Horror-Szenario plötzlich alle Daten oder der Suchalgorithmus unwiederbringlich gelöscht würden? 0 US-Dollar!

Daten und deren Verarbeitung als immaterielles Wirtschaftsgut sind inzwischen wertvoller als materielle Wirtschaftsgüter wie Maschinen oder Gebäude. Während eine Maschine vom ersten Tag der Investition über die Abschreibung an Wert verliert, werden Daten hingegen nach Beschaffung dank Analyse oder iterativ lernender Systeme (Künstliche Intelligenz) immer wertvoller.

Nicht nur Datenbesitz und deren Inhalt wie Kundenverhalten, Mess- oder Überwachungsdaten machen den Wert aus, sondern die Generierung von Mehrwert aus diesen Daten wie Vorschläge in Form von Produktempfehlungen oder Prognosen für Verschleiß und Ersatz von Maschinenkomponenten. Während der Verlust einer Maschine durch eine Ersatzinvestition verkraftbar erscheint, entzöge der Verlust von Daten den Unternehmen die Grundlage, die ihr Geschäftsmodell auf der Datenanalyse, Wartungsvorhersagen (predictive maintenaince) oder künstlicher Intelligenz aufgebaut haben. Digitalisierung, digitale Transformation oder Industrie 4.0 sind die Schlagwörter, welche diese sog. 4. industrielle Revolution umschreiben.

Jeder industrielle Fortschritt hat aber auch Risiken, insbesondere eine neue Art von Kriminalität mit hervorgebracht. Die mit der Digitalisierung aufkommende neue Wirtschaftskriminalität konzentriert sich nicht mehr auf Ideen-Diebstahl, sondern vermehrt auf alle Art von Daten-Diebstahl. Zum begehrten Diebes-Gut zählen nicht nur objektive Daten wie z.B. Produktionsdaten von Wettbewerbern, sondern insbesondere personenbezogene Daten, die über eine individuelle Persönlichkeit und deren persönliches Verhalten Auskunft geben. Hinzu kommt, dass Angriffe auf Daten nicht nur von außen, sondern auch durch Mitarbeitern von innen erfolgen, wie z.B. der Diebstahl und Verkauf von Bankkundendaten, um Steuerhinterzieher zu ermitteln. Inzwischen sind selbst Verhaltensdaten von Wählern in sozialen Netzwerken oder sensible politische Daten der Bundesregierung sehr begehrt, womit die Cyberkriminalität nicht bei Unternehmen halt macht, sondern sogar politische und gesellschaftspolitische Dimensionen erreicht. „Hacking wird Teil der Außenpolitik", hat der Sicherheitsexperte Adam Segal jüngst in einem Interview konstatiert.[1]

INHALT

Keywords
Cybersicherheit; Daten; Digitalisierung

1 Siehe DER SPIEGEL Nr. 14 / 31.3.2018.

Während Firmengeheimnisse früher in Form von Blaupausen im Tresor verschlossen wurden, kreisen heute vertrauliche Firmendaten durch das Internet, nachdem sich die Unternehmen inzwischen auf smart working, home office, mobiler Arbeitsplatz und cloud services eingerichtet haben.

Wie also schützt man als Unternehmer seine Daten bei zunehmender Wertigkeit, aber gleichzeitig verstärkter und risikobehafteter Nutzung durch Mitarbeiter, Lieferanten, etc. innerhalb und außerhalb des Firmengeländes?

Und wie sorgen Unternehmen und Gesetzgeber dafür, dass in der vernetzten Welt auch andere Unternehmen, Lieferanten oder vernetzte Geschäftsbeziehungen eigene und gemeinsame Daten schützen? Bei aller Notwendigkeit von Sicherheitsmaßnahmen muss deren Umsetzung praktikabel sein und die Unternehmen müssen dabei arbeits- und wettbewerbsfähig bleiben.

Angesichts dieses unternehmerischen Spannungsumfeldes kommt dem Aufsichtsrat die zusätzliche Aufgabe zu, das unternehmensweite Chancen-Risiken-Management um das Wirtschaftsgut „Daten" und deren interner wie externer Nutzung, Speicherung und Transfer zu erweitern. Dies beinhaltet aktive Beratung bei der Definition und Etablierung von digitalen Produkteigenschaften oder Maßnahmen zur Cyber-Sicherheit von operativen IT-gestützten Prozessen bis zur permanenten Überwachung der Einhaltung. Und das unter unternehmerischen Aspekten, also Abwägen von Chancen gegen Risiken sowie Aufwand gegenüber Nutzen.

II. Die neue Begehrlichkeit: Datendiebstahl

Warum werden Daten gestohlen, was ist die Motivation der Diebe? Dies kann alles sein: Schadenfreude, Gott spielen, Religion, der Glaube an Initiativen, der Wunsch, Menschen eines Besseren zu belehren, eine finanzielle Motivation, einfach „weil man es kann", weil man sich einen wirtschaftlichen Vorteil erarbeiten möchte oder letztendlich Spionage.

Seit es Cyber-Kriminalität gibt, hat sich das Verhalten der Hacker und deren Motivation in den letzten Jahren dramatisch verändert: im Jahre 2014 waren laut Umfrage unter 127 selbstidentifizierten Hackern (Thycotic Black Hat 2014 Survey) deren Motivation Spaß, Reiz (51 %), politisch-moralische oder soziale Einstellungen (29 %), Geld, finanzieller Anreiz (19 %) oder nur notorisches Handeln (1 %). Damals gingen 86 % der Hacker davon aus, nicht erwischt zu werden. Attacken konzentrierten sich auf die IT-Administration (30 %), Vertragspartner (40 %), die Administration auf Executive Level (8 %), Mail-Konten des Executive Levels selbst (6 %) und der nichtexekutiven Mitarbeiter (16 %). 99 % der Hacker waren der Meinung, dass ‚phishing' (‚Angeln' von nutzerspezifischen Daten durch gefälschte E-Mails, Webseiten, etc.) noch immer eine sehr effektive Methode ist, aber rund 50 % der Hacker gaben an, dass Nutzer stetig dazu lernen, um solche Taktiken zu verhindern.

Vor Jahren war der durchschnittliche Hacker ein einsam agierender Jugendlicher, der sich beweisen und anderen zeigen wollte, dass er irgendwo ein System hacken und interessante und wirkungsvolle Malware (Schad- oder Spionage-Software) kreieren konnte. Selten haben diese Gruppe von Hackern größere Schäden angerichtet.

Heute gehören die meisten Hacker zu professionellen Gruppen, die Systeme und Werte angreifen oder Daten stehlen und dabei meistens größere Schäden anrichten.

Ihre Malware ist so strukturiert, dass sie verdeckt und geheim eingeschleust wird und vor der Entdeckung möglichst viele Daten und Werte abgreift.

Demzufolge sind laut jüngster Untersuchung von ‚CSO from IDG' (5.4.2018) Hackerangriffe inzwischen anders motiviert und priorisiert:

1. finanzielle Gründe
2. regierungsunterstützte Attacken (‚cyberwar'), Meinungs- und Wahlbeeinflussung
3. Unternehmensspionage: Strategien, F&E-Vorhaben, Kalkulationen, Kundendaten, etc.
4. Protestmittel, Verbreitung politischer Anschauung
5. Ressourcen-Diebstahl: Personendaten zur Abwerbung, Einkaufspreise für Lieferantenverhandlung, etc.
6. Spieler-Mentalität ohne Schädigungsabsicht, aber Befriedigung des Suchtverhaltens.

Unabhängig von der Motivation dringen Hacker und ihre Malware oft auf gleiche Art und mit gleicher Methode in ein IT-System ein (Reihenfolge nach Häufigkeit):

1. „Social engineering", d.h. Ausnutzen menschlicher Schwäche; Vertrauen oder Unachtsamkeit (z.B. gefälschte E-Mails (fakes), auf die Mitarbeiter ahnungslos reagieren; sich als Servicetechniker der Fernwartung ausgeben und sich Zugang ins IT-System verschaffen; mithilfe ahnungsloser Reinigungskraft in den Datenraum gelangen),
2. nicht „gepatchte" Software (SW), d.h. temporäre Lösung eines bekannten SW-Fehlers nicht eingespielt, verletzbare oder unterdimensionierte Hardware, Leistungsschwäche oder Speichermangel, so dass ein Überlastungs-Ausfall provoziert werden kann.
3. „Zero-Day" Lücken, d.h. SW-Fehler, die dem SW-Hersteller unbekannt sind bis zum Tag Null, an dem sie zufällig entdeckt werden. Entdeckt der Hacker diesen Fehler vor dem SW-Hersteller, nutzt er ihn so lange aus, bis auch der SW-Hersteller darauf aufmerksam wird. Zusätzlich bedarf es weiterer Zeit für die Entwicklung / Bereitstellung eines Patches (temporä-

re Lösung) oder „workarounds" (Umgehung des Problems). In diesem Zeitraum greift der Hacker an und installiert eine Malware, die im Hintergrund unentdeckt und ungehindert arbeitet. Je schneller er angreift, umso erfolgreicher und nachhaltiger ist er. Nur wenige „Zero-Day"-Attacken werden pro Jahr entdeckt, bevor sie analysiert und temporär repariert werden (patches). Weit mehr „Zero-Days" als bekannt arbeiten bereits unentdeckt im Hintergrund und nutzen dies aus, besonders bei regierungsunterstützten Attacken. Da sie sehr spärlich und sporadisch genutzt werden, sind sie auch kaum gezielt zu entdecken und können immer wieder von Hackern genutzt werden. Folglich sind Tag-Null-Attacken sehr ernste Störungen.

Beispiel ‚Zero-Day'-Lücke: Schadsoftware ‚WannaCry'

- weltweiter Angriff auf das Microsoft-Betriebssystem WINDOWS am 12.5.2017
- über 230.000 private und geschäftliche Computer in ca. 150 Ländern waren betroffen
- Sicherheitslücke war amerikanischem Auslandsgeheimdienst seit mehr als 5 Jahren bekannt
- Dieser nutzte dies zu eigenen Zwecken mit eigens entwickelter Spezial-SW, aber ohne Microsoft zu informieren
- Microsoft wurde erst informiert nach Diebstahl des Wissens über Spezial-SW
- Microsoft erstellte am 14.3.2017 einen Patch, jedoch nur für noch unterstützte Windows-Versionen
- einen Monat später machte eine Hackergruppe Sicherheitslücke und Spezial-SW öffentlich
- Motivation des Angriffs war finanzieller Art: Erpressung eines Lösegeldes in Kryptowährung ‚Bitcoin'.

4. Browserattacken: durch „Datenabhören" finden Hacker heraus, welche Webseiten Firmenmitarbeiter häufig besuchen. Diese Seiten werden dann so manipuliert, dass Hacker darüber an Zugangsdaten gelangen (bekannt als ‚Watering hole', angelehnt an Naturverhalten von Giraffen, die Wasserstellen in Steppen aufsuchen, wo bereits Löwen im Gebüsch lauern und bei deren Auftauchen zum Angriff übergehen).
5. Passwort-Attacken: Unsichere Passwörter wie „123456", die leider noch immer häufig genutzt werden.
6. „Abhören", d.h. Einfangen kleiner Datenpakete im Netz, die über Nutzerverhalten Rückschlüsse zulassen, einen Zugangscode oder vertrauliche Informationen enthalten.
7. ‚Denial of Service', d.h. Nichtverfügbarkeit eines Dienstes durch Überflutung eines Dienst-Servers mit Anfragen, der so überlastet wird und abschaltet.
8. physikalische Attacken auf Speicher oder Festplatten.

Der größte Teil der Cyber-Attacken erfolgt über das Internet und bedarf zur Initialisierung einer Aktion durch den Nutzer: Auf Link klicken, etwas runterladen und die Datei ausführen, „phishing", d.h. gefälschte Datenabfragen wie Name und Passwort. Oft sind Standard-Browser und gängige E-Mail-Programme wegen ihrer weiten Verbreitung beliebte Träger von Malware, die stillschweigend, vom Benutzer unbemerkte Attacken durchführen, wenn er eine Webseite besucht oder eine E-Mail öffnet.

Der wirksame Schutz gegen Cyber-Angriffe kann nur präventiv, aber dennoch recht wirksam ansetzen, indem man das IT-System software- und hardwareseitig stets aktuell und leistungsfähig hält, die Schwachstelle „Mensch" permanent sensibilisiert und trainiert, externe Zugänge zur IT-Infrastruktur streng überwacht, protokolliert oder eliminiert (z.B. USB-Sticks) sowie das IT-System regelmäßigen Belastungs- und Angriffstests unterzieht.

Ein erfolgter und entdeckter Cyber-Angriff ist sorgfältig und akribisch zu analysieren und jede dadurch gefundene Schwachstelle systematisch zu eliminieren. Laut einer statistischen Erhebung in Unternehmen in Deutschland, USA, Spanien, Niederlanden und UK, die einen Cyberangriff in 2017 erlitten haben, gibt es noch immer eine große Anzahl Mehrfach-Angriffe, also noch immer ungenügende oder ineffiziente Gegenmaßnahmen nach dem Erstangriff (s. Abb. 1).

III. Unternehmenskommunikation in Zeiten des smart workings

Die topvertrauliche Kommunikation zwischen CEO und Board findet in vielen Fällen noch immer über kostenlose Mail-Konten statt, die Nutzerverhalten zu Werbezwecke analysieren oder hinsichtlich Datenschutz, Löschen von Daten, etc. erhebliche Lücken aufweisen.

So fand z.B. der Sonderermittler Robert Mueller im Zuge der Ermittlung zur Beeinflussung des Wahlkampfs in den Vereinigten Staaten heraus, dass die Phishing-E-Mails „von Konten des Anbieters GMX und eines weiteren Freemail-Providers" versendet wurden".[2]

Die vertrauliche Kommunikation zwischen Vorstand und Aufsichtsrat von innerhalb nach außerhalb des Unternehmens, insbesondere der Austausch vertraulicher Dokumente, sollte nie per E-Mail erfolgen. Stattdessen sollten Aufsichtsratsmitglieder in ein eigenes dafür vorgesehenes unternehmensinternes Kommunikations- und Dokumenten-

2 Siehe Spiegel online, unter: www.spiegel.de/netzwelt/netzpolitik/hillary-clinton-wurde-im-wahlkampf-mithilfe-deutsche-e-mails-gehackt-a-1199566.html, vom 24.3.2018.

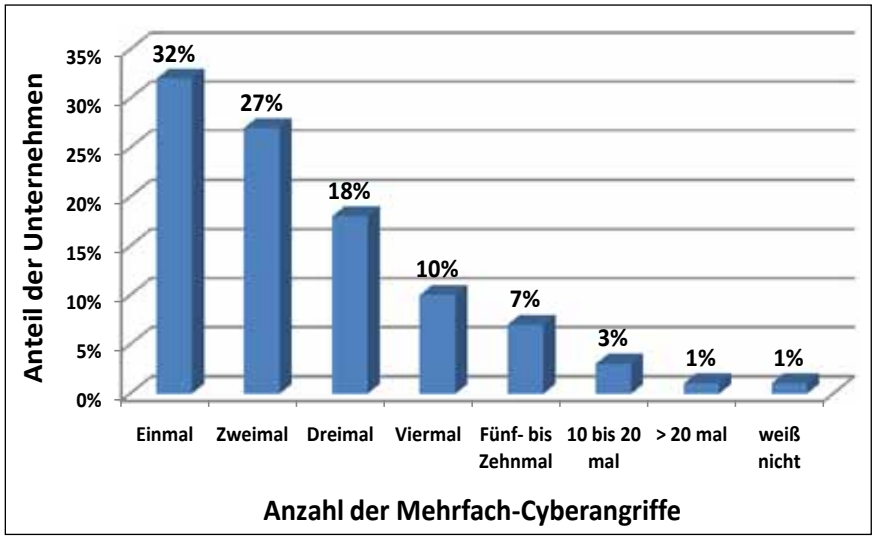

Abb. 1: Anzahl der Cyber- Angriffe auf Unternehmen in 2017; Quelle: Statista 2018

Management-System eingebunden sein („elektronischer Board Room").

Ein solches vertrauliches und verschlüsseltes Kommunikations-System ist inzwischen state-of-the-art und von verschiedenen Anbietern mit unterschiedlichen Leistungsmerkmalen verfügbar (s. Tab. 1, beispielhafte, unvollständige Auswahl).

Das Internet hat einerseits zu einer wesentlichen Veränderung der Arbeitswelt hinsichtlich Art, Zeit und Ort der Arbeit geführt, anderseits hat die damit verbundende Kommunikation und der Dokumententransfer außerhalb des Firmengeländes das Risiko für kriminelle Zugriffe auf diesen Datenaustausch enorm erhöht. Die Heimarbeitsplätze der externen Mitarbeiter sollten mindestens über ein virtuelles privates Netzwerk (Virtual Private Network: VPN), d.h. ein abgesichertes Netzwerk für eine geschlossene Nutzergruppe standardmäßig verbunden sein.

Verschiedene Firmenstandorte sollten über eine eigene Mietleitung (Multiprotocol Label Switching: MPLS-Netzwerk) statt des öffentlichen Internets verbunden sein.

IV. Digitale Transformation: Risiken steigen mit den Chancen

Die Digital-Technologie bietet unzählige programmierte und automatisierte Möglichkeiten zur Optimierung und Effizienzsteigerung von Prozessen, insbesondere im Bereich Internet der Dinge (IoT), und eröffnet mit e-commerce, Künstlicher Intelligenz, Blockchain, Big-Data, Data Analysis, Predictive Maintenance, etc. neue, innovative Entwicklungs- und Anwendungsfelder.

Da nahezu alle Einsatzmöglichkeiten der Digitalisierung mit interner und externer Vernetzung einhergehen, steigt mit jeder neuen Anwendung / Entwicklung im Bereich der Digitalisierung auch das Risiko von Cyber-Angriffen mit entsprechenden Folgen.

Jede im Internet aufrufbare Web-Seite oder jedes im Internet angeschlossene registrierte Gerät ist durch eine spezifische Adresse ähnlich einer Postanschrift oder Telefonnummer eindeutig gekennzeichnet, erreich- und ansprechbar (z.B. Domain oder Uniform Ressource Locator (URL): www.beispiel.com, IP-Adresse: 192.168.1.255; MAC-Adresse: 01-20-41-ae-fe-7e). Im Gegensatz zur Postanschrift oder Telefonnummer sind die Internetadressen allerdings nicht örtlich zugeordnet, so dass man bestimmte Geräte oder Geräteserien unabhängig vom Standort, aber je nach Motivation, Aufgabe oder Nutzung weltweit adressieren, im Angriffsfall also mit Schadsoftware versehen kann. Somit birgt das Internet der Dinge die enorme Gefahr in sich, dass jedes im Internet angeschlossene Gerät für die Außenwelt über diese Adressen völlig transparent ist, d.h. von der Heizungs- und Lichtsteuerung zu Hause über die internetgesteuerte Videokamera auf öffentlichen Plätzen oder U-Bahnen bis zur Steuerung der Produktionslinie im Betrieb oder des Kraftwerkes zur Stromversorgung.

Bei der geforderten Umsetzung der Digitalisierung muss man unbedingt im gleichen Atemzug auch die Cyber-Sicherheit mit bis zu Ende denken

Anbieter	Brainloop	Diligent	DISO AG
Produkt	Board Suite	Boards	Desktop as a Service Swiss Cloud Workplace
Produkt-Art	Applikation	Applikation Dokumenten-Management	Virtuelle Desktop über Browser (VMWare)
Benutzer-oberfläche	proprietäre Nutzeroberfläche	proprietäre Nutzeroberfläche	Gleicher Desktop, virtuelles 1:1-Abbild
Prinzip	Work-Flow-Prozess	Work-Flow-Prozess	Daten und Applikationen in der Cloud
Sicherheit	– Daten verschlüsselt auf Server und im Transfer	– Daten verschlüsselt auf Server und im Transfer – Zertifizierte Sicherheit	– übertragene Informationen sind Pixel, keine Daten („Team-Viewer"-Interface) – persistente Speicherung aller Desktops – damit: Sicherheit durch „bring-your-own-device"

Tab. 1: Beispielhafte Aufzählung von Board-Portal-Anbietern

und implementieren, um sich nicht gleichzeitig mit Einführung einer solch neuen Technologie auch wieder neue Risiken ins Haus zu holen. Dies sind nicht nur rein technische oder operative Aspekte, welche die Entwicklungs- oder Serviceabteilung durchdeklinieren muss, sondern es sind vor allem auch strategische Fragestellungen, die auf die Agenda von Aufsichtsratssitzungen gehören und mit dem Management und dem Cyber-Verantwortlichen durchdiskutiert und entschieden werden müssen.

Inzwischen gibt es Versicherungen gegen Cyberattacken, nachdem Cyber-Angriffe weltweit einen Schaden von 445 Mrd. US-Dollar verursachen laut einer Erhebung der Allianz-Versicherung (FAZ, 7.6.2018).[3]

V. Cyber-Sicherheit und Datenschutz

Der derzeitige Hype der Digitalisierung sollte um das Bewusstsein der gleichzeitig damit steigenden Risiken relativiert werden. Dies darf nicht derart zur Übertreibung führen, dass vor lauter Sicherheitsaspekten im Bereich Cyber-Security und Datenschutzrichtlinien wie die neue EU-Datenschutz-Grundverordnung (DS-GVO) neueste Entwicklungen und Geschäftsideen im Keim erstickt werden.

Die neue DS-GVO wurde mit langer Vorlaufzeit in Kraft gesetzt und muss seit dem 25. Mai 2018 verbindlich von allen in der EU tätigen Unternehmen angewendet werden. Sie ist eine einheitliche EU-weite Regelung, die nicht in nationales Recht umgesetzt werden muss. U.a. sind das „Recht auf Vergessen" festgelegt (Datenlöschung von Personendaten im Netz), oder der „one-stop-shop-Ansatz" (Datenschutzverletzungen unmittelbar im Mitgliedstaat des Betroffenen geltend machen ungeachtet des Mitgliedstaates, indem die Datenschutzverletzung stattfand).

Weiterhin gibt es verschärfte Regelungen, z.B. Information der Betroffenen über die Verarbeitung ihrer Daten, unbedingte Einholung der Zustimmung der Betroffenen, Inhalt der vertraglichen Regelung bei der Datenverarbeitung durch Dritte (Auftragsdatenverarbeitung) sowie Voraussetzungen zur Übermittlung von Personendaten in EU-Drittländer.

Verstöße gegen die DS-GVO können mit einer Geldstrafe bis zu 20 Mio. € bzw. 4 % des Jahresumsatzes sanktioniert werden.

Somit ist die Einhaltung der DS-GVO in dem zu beaufsichtigen Unternehmen ein wesentlicher Teil der zusätzlichen rechtlichen Verpflichtung, damit auch der Risiko-Betrachtung und der Cyber-Sicherheit des Unternehmens.

Wie jede zusätzliche rechtliche Verpflichtung mit Sanktionen muss auch die verschärfte Datenschutzverordnung in jede unternehmerische Entscheidung mit einbezogen bzw. in eine Produktentwicklung bzw. in Betriebskosten mit eingepreist werden. Die geringe Erfahrung mit der jüngst begonnenen Umsetzung der DS-GVO reicht allerdings noch nicht aus, um die konkreten quantitativen Konsequenzen daraus abzuleiten. Insbesondere wird es – wie in vielen dieser breit angelegten gesetzlichen Verordnungen – sicher noch Korrekturbedarf geben hinsichtlich der Umsetzbarkeit und der Machbarkeit.

VI. Fazit

Daten sind zu wertvollen Grundbausteinen der digitalen Transformation in Unternehmen, Behörden, Regierungen und der Gesellschaft geworden. Die Verflechtung der Datennutzung, -speicherung und des -transfers über das weltweite Internet macht es notwendig, den Schutz der Daten nicht nur gesetzlich sinnvoll zu regeln, sondern sie in jede unternehmerische Entscheidung mit einzubeziehen. Die Chancen, die sich durch die Digitalsierung ergeben, dürfen nicht durch die Risiken und die Absicherung dagegen erstickt werden. In diesem Spannungsfeld, das sich durch die digitale Transformation neu auftut, müssen der Aufsichtsrat zusammen mit dem Management zunehmend komplexere und weitreichendere unternehmerische Entscheidungen treffen.

3 Siehe FAZ.NET, unter: www.faz.net/aktuell/wirtschaft/unternehmen/nach-wanna-cry-versicherungen-gegen-cyberkriminalitaet-15105015.html, vom 14.7.2018.