ODDO BHF
ASSET MANAGEMENT

Cybersicherheit: Für den Schutz unserer Daten!

MAI 2018

Inhalt

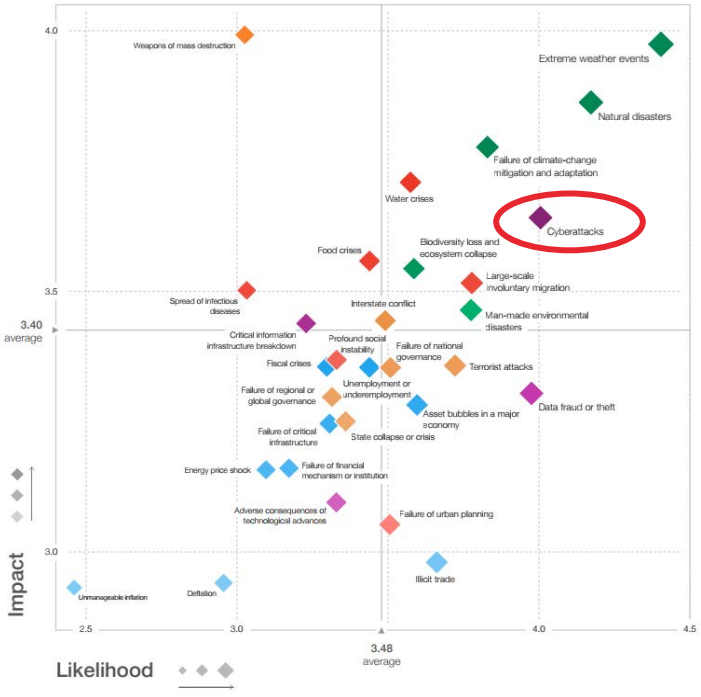
Vorwort

In den letzten zwanzig Jahren hat die Digitalisierung der Wirtschaft die Arbeitswelt und das Konsumverhalten wie auch die Beziehungen zwischen Privatpersonen und/oder Organisationen gründlich auf den Kopf gestellt. Hierdurch wurden neue Maßstäbe in Sachen Schnelligkeit, Mobilität, Konnektivität oder Virtualisierung gesetzt, auf die sich die Unternehmen einstellen mussten. Heutzutage trägt die digitale Wirtschaft mehr als 30% zum BIP-Wachstum in den entwickelten Ländern bei. **Damit sind Daten zu einem strategischen Gut geworden, das sich verwerten lässt, das es aber auch zu schützen gilt.**

> *„Die mit Cyberkriminalität verbundenen Kosten für die Weltwirtschaft könnten sich bis 2022 auf 8.000 Mrd. USD belaufen“*

Angesichts rund 3,9 Mrd. Internetnutzern weltweit und 8,4 Milliarden vernetzter Objekte ist Cybersicherheit innerhalb weniger Jahre zu einer großen Herausforderung für Unternehmen geworden, wie die aktuelle Studie[1] des Weltwirtschaftsforums zur Risikokartierung für 2018 zeigt.

Risikokarte für 2018



Quelle: Weltwirtschaftsforum

1 http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Nach Schätzungen von Experten des Weltwirtschaftsforums könnten sich die mit Cyberkriminalität verbundenen Kosten für die Weltwirtschaft bis 2022 auf 8.000 Mrd. USD belaufen. Das entspricht knapp der Hälfte des BIP der Europäischen Union. Allein im Jahr 2017 gab es zwei große Angriffe – WannaCry (300.000 infizierte Computer in 150 Ländern) und NotPetya (von dem diverse Unternehmen in der Ukraine, Russland, Europa und den USA betroffen waren). Laut einer im Januar 2018 veröffentlichten Deloitte-Studie gaben **75% der befragten Unternehmen an, nach diesen beiden Attacken neue Sicherheitsmaßnahmen ergriffen zu haben**. Cyberkriminalität verursacht Unternehmen daher nicht nur zunehmend hohe interne Kosten (vor allem IT- und Personalinvestitionen), sondern auch vermehrt schwer quantifizierbare externe Kosten (Datendiebstahl, Umsatzeinbußen, Betriebsausfälle, Reputation).

Die Ziele von Cyberkriminalität sind vielfältig. Sie reichen von geistigem Eigentum bis zu Finanzdaten. Im Fokus der meisten Angriffe stehen jedoch persönliche Daten. Die exponenziell wachsende Zahl der im Umlauf befindlichen vernetzten Objekte eröffnet ein Handlungsfeld mit außergewöhnlichen Möglichkeiten.

Bereits vor 50 Jahren wurden die ersten Regelungen zum Schutz personenbezogener Daten getroffen (1970 in Hessen, 1973 in Schweden, 1978 in Frankreich). Mittlerweile gibt es hierzu in mehr als 100 Ländern Gesetze. In dieser Hinsicht markiert das Jahr 2018 **mit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) am 25. Mai** eine wichtige Entwicklung in Europa. Sie löst die Verordnung der Datenschutzrichtlinie (DSR) aus dem Jahr 1995 ab.

> *„Angesichts der wachsenden Cyberrisiken und deren Auswirkungen auf Unternehmen ist Cybersicherheit ein wichtiges Thema bei unserem Dialogansatz“*

Die Digitalisierung der Wirtschaft eröffnet unbestreitbar in zahlreichen Wirtschaftssektoren neue Entwicklungschancen, birgt aber auch neue Risiken, deren Ausmaß und Auswirkungen ungewiss sind und sich ständig wandeln.

Der Anstieg der Cyberrisiken, die mit dem digitalen Wandel der Wirtschaft unausweichlich sind, macht das Thema zu einem unverzichtbaren Bestandteil der Analyse von Unternehmen, bei der finanzielle und nichtfinanzielle Aspekte betrachtet werden. ODDO BHF Asset Management trägt diesem bereits in seinem ESG-Analysemodell Rechnung. So ist Cybersicherheit eines der Themen, das wir in unserem Dialog mit den Unternehmen immer wieder aktiv ansprechen.

Nicolas Jacob
Leiter ESG Research bei ODDO BHF Asset Management SAS

Daten – ein schützenswertes Gut

„Daten sind das neue Öl. Sie sind unglaublich wertvoll, aber unverarbeitet können sie nicht wirklich verwendet werden. Das Öl muss erst umgewandelt werden, um es effizient nutzen zu können. Das Gleiche gilt für Daten, die erst zerlegt und analysiert werden müssen, um hieraus Nutzen zu ziehen.“

Clive Humby, britischer Mathematiker und Big-Data-Pionier, 2006

Im Jahr 2017 fragten in einer Minute 18 Millionen Personen die Wettervorhersage im Internet ab, 3,6 Millionen starteten eine Suche über Google, 4,1 Millionen schauten sich YouTube-Videos an, es wurden 527.760 Photos über Snapchat geteilt bzw. 103 Mio. Spam-Mails durch die Welt geschickt[2].

Neue Chancen, neue Bedrohungen

Die Menge der gesammelten Daten ist in den letzten 10 Jahren im Durchschnitt um über 50% pro Jahr gewachsen und eröffnet Unternehmen entlang der gesamten Wertschöpfungskette ein riesiges Analysefeld. Dieses Datenuniversum, auch „Big Data“ genannt, zeichnet sich dadurch aus, dass immer mehr verfügbare und gesammelte Daten unstrukturiert sind, d.h. in Mobilgeräten, Internetforen, sozialen Medien oder auch vernetzten Objekten anfallen. Heute liegen mehr als 90% der Daten im digitalen Universum in unstrukturierter Form vor. Dies verdeutlicht sehr gut den Multiplikator-Effekt von Big Data.

„Dreifache Herausforderung für Unternehmen: Erhebung, Speicherung und Verarbeitung von Daten“

Über eine kompetente Verarbeitung dieser Datenflut lässt sich Mehrwert generieren. So kann sich laut einer im November 2013[3] veröffentlichen Schätzung von McKinsey eine gute digitale Strategie über einen Zeitraum von fünf Jahren signifikant positiv im Unternehmensergebnis niederschlagen. Sie veranschlagen den positiven Effekt bei durchschnittlich 20% über ein kräftigeres Umsatzwachstum und bei durchschnittlich 36% durch Kostenoptimierungen (Produktivitätssteigerungen).

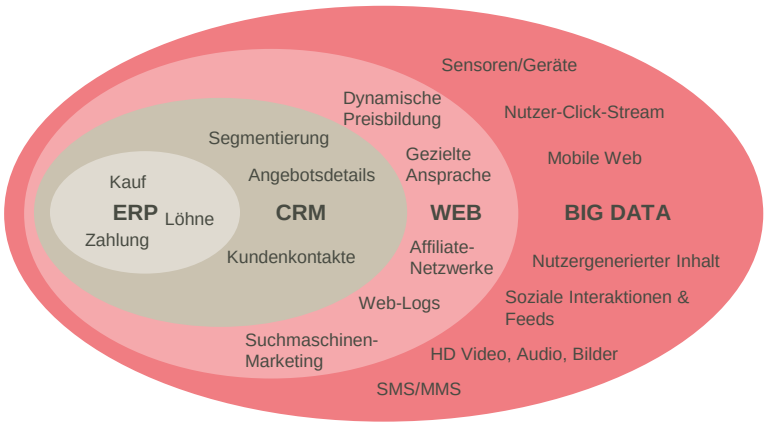
Im digitalen Transformationsprozess sind Daten für Unternehmen zu einem wichtigen Vermögenswert geworden. Bevor sie diese nutzen können, ist zunächst jedoch eine dreifache Herausforderung zu bewältigen: Die Erhebung, die Speicherung und die Verarbeitung der Daten.

Organisationen, die Daten für sich zu nutzen wissen, können hierdurch einen Wettbewerbsvorteil erlangen.

2 Quelle : Byothe.fr

3 “Finding your digital sweet spot”, McKinsey, November 2013

Das wachsende Datenuniversum



Quelle: Teradata, ODDO BHF Asset Management

Das wirtschaftliche Gewicht der Daten macht sie auch zu einem zunehmend begehrten Gut und folglich zum Ziel böswilliger oder gar krimineller Angriffe. **Allein im Jahr 2017 wurden rund 700 Millionen Cyberangriffe vermeldet – eine Verdopplung seit 2015.** So gaben beispielsweise laut dem von Thales und 451 Research[4] veröffentlichten Datensicherheitsbericht 2018 67% der 1.200 befragten IT-Sicherheitsmanager an, in der Vergangenheit schon einmal Opfer von Datendiebstahl gewesen zu sein.

> *„Durch die Entwicklung vernetzter Objekte und künstlicher Intelligenz wird sich die Zahl externer Angriffe erhöhen“*

Die Cyberbedrohungen können sehr unterschiedlicher Natur sein. Entsprechend komplex ist es für jede Organisation, diese zu antizipieren und abzuwehren. Der erste Analyseschritt besteht daher in der Differenzierung zwischen – häufig noch unterschätzten – firmeninternen Bedrohungen und Gefährdungen von außen. Zwar unterscheiden sich beide Arten von Cyberangriffen in Hinblick auf die zu ergreifenden Gegenmaßnahmen und ihre Auswirkungen. Insgesamt wächst aber ihre Zahl mit dem technologischen Fortschritt. Konkret heißt das zum einen, dass sich durch vernetzte Objekte und künstliche Intelligenz die Zahl externer Angriffe erhöhen wird. Zum anderen stellt die zunehmende Praktik, es Mitarbeitern zu erlauben, über ihre privaten Geräte auf Unternehmensdaten zuzugreifen („bring your own device“), eine große Herausforderung für die Sicherheit der IT-Systeme dar.

4 “2018 Thales data threat report”, Thales et 451 Research, Januar 2018

Vielfältige Cyberbedrohungen

Quelle: ODDO BHF Asset Management

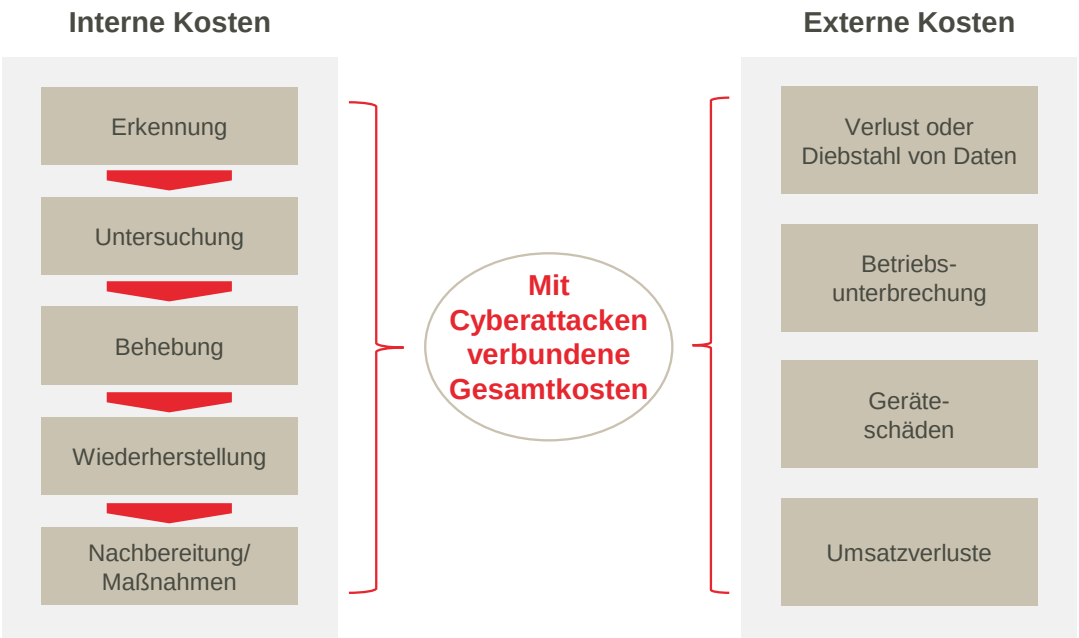
Die Entwicklung mobiler Technologien und das Internet der Dinge haben in den letzten Jahren ein hohes Maß an **persönlichen Daten generiert, die zu bevorzugten Zielen von Cyber-Angreifern geworden sind**. Es überrascht nicht, dass die am stärksten betroffenen Bereiche endverbrauchernahe Sektoren sind, wie Information und Kommunikation (96% der externen Angriffe haben persönliche Daten zum Ziel), Einzelhandel (91%) und Finanzdienstleistungen (42%)[5].

5 Quelle : IBM X-Force Threat Intelligence Index 2017

Auswirkungen nur schwer kontrollierbar

Die mittlerweile berühmt-berüchtigten Cyberangriffe aus 2017 (Wannacry und NotPetya) haben gezeigt, dass es nicht nur um den Diebstahl oder den Verlust von Daten geht, **sondern auch die Reputation eines Unternehmens auf dem Spiel steht und Kosten durch Betriebsunterbrechung oder Ausfälle kritischer Infrastrukturen entstehen**. NotPetya, eine im Juni 2017 in Umlauf gebrachte Ransomware[6], hatte schwerwiegende Folgen und setzte in der Ukraine zunächst ukrainische Verwaltungs- und Infrastrukturen außer Gefecht, bevor es diverse in der Region tätige private Unternehmen als auch Unternehmen außerhalb der Ukraine mit örtlichen Niederlassungen traf. Zu denen, die sich öffentlich zu dem Vorfall geäußert haben, zählten die dänische Firma A.P. Moeller Maersk und das britische Unternehmen Reckitt Benckiser, die Einbußen in Höhe von 250 bzw. 100 Mio. USD oder 4 bis 10% ihres operativen Ergebnisses hinnehmen mussten.

Potenzielle Kosten einer Cyberattacke für Unternehmen



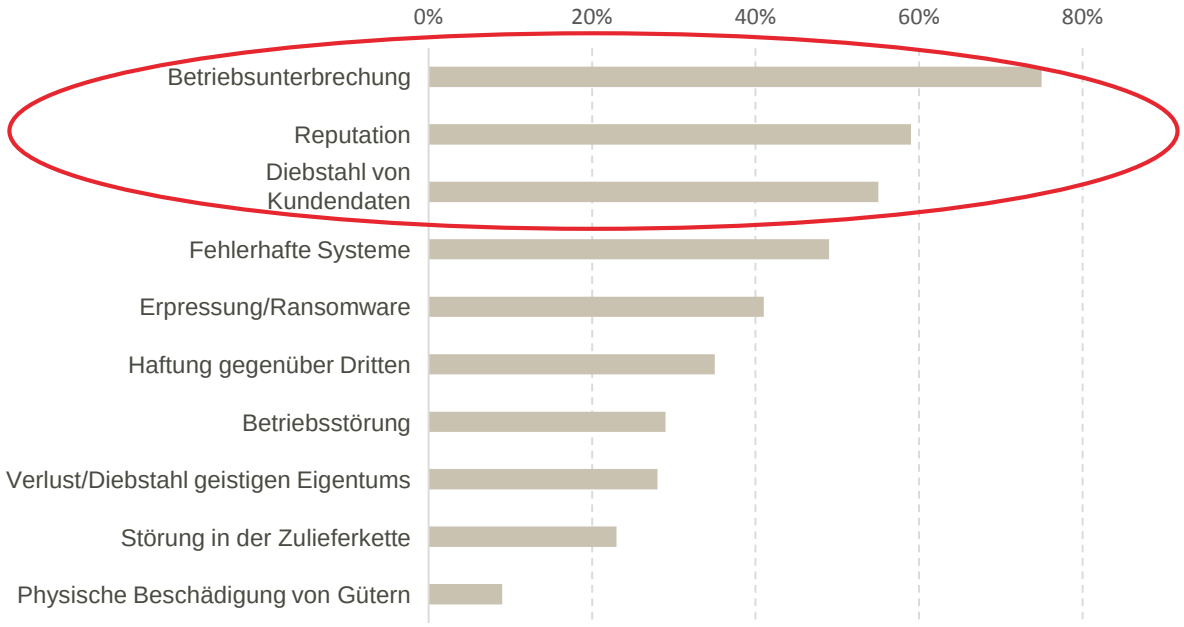
Quelle: Accenture, Ponemon

Diese Entwicklung wird von den Unternehmen mit Besorgnis beobachtet. Im Februar 2018 veröffentlichte Marsh in Zusammenarbeit mit Microsoft die Ergebnisse einer Studie zur Wahrnehmung von Cyberrisiken, an der 1.300 Entscheider aus der Geschäftswelt aus fünf Kontinenten teilgenommen haben. Bei den Themen, die den Befragten Sorgen bereiten, zeigt sich eine deutliche Verlagerung weg von internen Faktoren (z.B. IT-Management) hin zu potenziellen Auswirkungen entlang der gesamten Wertschöpfungskette des Unternehmens (Betriebsausfall, Reputationsschäden, Diebstahl von Kundendaten).

6 Siehe Glossar

„Potenzielle Auswirkungen entlang der gesamten Wertschöpfungskette“

Von Unternehmen am meisten gefürchtete mögliche Szenarios einer Cyberattacke



Quelle: Umfrage von Marsh und Microsoft zur Wahrnehmung von Cyberrisiken, 2018

Der im März 2018 öffentlich gewordene Skandal um Facebook/Cambridge Analytica[7] stellt Grundlage und Gültigkeit eines Geschäftsmodells in Frage, das ausschließlich auf der Erhebung, Speicherung und Verwertung personenbezogener Daten basiert. Der Fall hat gezeigt, dass die Nutzung von Benutzerdaten ohne deren Wissen zu einem Vertrauensverlust führen und die Reputation des Unternehmens nachhaltig beschädigen kann.

> *„Wir haben die Verantwortung, Ihre Daten zu schützen - und wenn wir dies nicht können, verdienen wir es nicht, Ihnen zu dienen“*
>
> **Mark Zuckerberg**, Gründer und Chef von Facebook, März 2018

Noch lassen sich die Gesamtkosten schwer abschätzen. Zumal der **Anteil immaterieller Vermögenswerte an der Bewertung von Unternehmen zunimmt,** was jeden Versuch einer kurzfristigen Schätzung noch komplexer macht.

7 Cambridge Analytica, ein US-Unternehmen für strategische Kommunikation, hat zwischen 2014 und 2016 persönliche Daten von mehr als 50 Millionen Menschen über das soziale Netzwerk Facebook abgegriffen

Die langsamen Mühlen der Regulierung

Technologische Durchbrüche geben zwar immer starke Wachstumsimpulse, schaffen aber oft auch neue Risiken, die von der Regulierung zunächst ignoriert wurden. Die Digitalisierung ist keine Ausnahme, und die Gesetzesmühlen mahlen langsamer als die Entwicklung betrügerischer oder krimineller Praktiken.

Cyberrisiken haben Anfang 2010 ein exponentielles Wachstum erfahren und waren ein steter Begleiter der rasch fortschreitenden Digitalisierung der Wirtschaft. **In diesem Zusammenhang hat das Europäische Parlament im April 2016 einen Gesetzesentwurf zur Überprüfung und Verschärfung der** (nach Maßgabe der Richtlinie von 1995 in Landesrecht umgesetzten) **Datenschutzmechanismen verabschiedet**. Diese Datenschutz-Grundverordnung (DSGVO) entfaltet – anders als eine Richtlinie, die erst noch in nationales Recht umgesetzt werden muss – sofort mit ihrem Inkrafttreten im Mai 2018 Wirkung.

Datenschutz-Grundverordnung (DSGVO)

Die DSGVO steckt den gesetzlichen Rahmen für den **Schutz personenbezogener Daten** auf Ebene der Europäischen Union ab**.** Dieses Regelwerk ersetzt einen früheren Text aus dem Jahr 1995 (Richtline 95/49/EG), der dem sich rasch wandelnden digitalen Umfeld nicht länger gerecht wird.

Alle (öffentlichen oder privaten) Organisationen, die ihren Sitz in der Europäischen Union haben oder aber außerhalb der EU ansässig sind, aber personenbezogene Daten von in Europa ansässigen Personen verwalten, müssen bis zum 25. Mai 2018 **der DSGVO entsprechen**.

Übersicht über maßgebliche Bestimmungen:

- **Ausdrückliche Einwilligung:** Öffentliche Organisationen und private Unternehmen müssen die ausdrückliche Einwilligung der Nutzer vor der Erhebung ihrer personenbezogenen Daten sicherstellen;
- **Recht auf Löschung** (oder auch „Recht auf Vergessen"): Jeder EU-Bürger hat das Recht, die Löschung aller oder eines Teils seiner personenbezogenen Daten durch den für die Verarbeitung Verantwortlichen zu verlangen, und zwar aus verschiedenen Gründen (z.B. bei unrechtmäßiger Verarbeitung oder Widerruf der Einwilligung);
- **Datenübertragbarkeit**: Jeder hat das Recht, seine personenbezogenen Daten von der Organisation, die sie gesammelt hat, in einem strukturierten und gängigen Format zu erhalten, um diese Daten an jegliche andere datenverarbeitende Organisation seiner Wahl zu übermitteln;
- **Meldung von Sicherheitsverletzungen**: Im Falle von Hackerangriffen muss der für die Datenverarbeitung Verantwortliche die nationale Datenschutzbehörde sowie die betroffenen Nutzer hierüber in Kenntnis setzen;
- Pflicht öffentlicher Einrichtungen (sowie von Unternehmen mit mehr als 250 Mitarbeitern), einen **Datenschutzbeauftragten** (oder Data Protection Officer) zu ernennen;
- **Einbeziehung des Datenschutzes bereits in der Konzeptionsphase**: Datenschutzanforderungen müssen von öffentlichen Stellen oder privaten Unternehmen bereits in der Konzeptionsphase ihrer Produkte, Dienstleistungen und Systeme berücksichtigt werden. Zweck dieser Bestimmung ist es, **die Daten der Nutzer so zu schützen**, dass sie nicht an Dritte weitergegeben werden können oder es diesen ermöglichen, alles über das Privatleben der Nutzer zu erfahren.

Die Umsetzung der DSGVO ist eine komplexe, zeitintensive Aufgabe, die für Unternehmen bedeutende Änderungen mit sich bringt. Ab dem 25. Mai 2018 müssen die Unternehmen nachweisen, dass sie die Bestimmungen der DSGVO und insbesondere die sich daraus ergebenden Änderungen in Bezug auf die Verfolgbarkeit und Abbildung personenbezogener Daten einhalten.

Bei Nichteinhaltung dieser Vorschriften riskieren Unternehmen eine Geldstrafe in Höhe von bis zu 20 Mio. € oder 4% des weltweiten Jahresumsatzes.

Fragen an den Experten: Interview mit Wordline zum Thema Cybersicherheit

Mit der Digitalisierung der Wirtschaft ist die Welt in eine Ära der großen Datenmengen eingetreten. Parallel zu dieser Entwicklung hat sich auch die Cyberkriminalität stetig weiterentwickelt und perfektioniert und betrifft immer mehr Organisationen und Einzelpersonen. Jüngste Ereignisse wie der Fall Facebook/Cambridge Analytica zeigen uns, dass Cybersicherheit eine Grundvoraussetzung für Vertrauen ist.

Wir danken Wordline, führender Akteur im Bereich elektronischer Zahlungsverkehr und Transaktionsdienste, der uns tiefe Einblicke in das Thema Cybersicherheit vermittelt.

ODDO BHF AM: Sie als führender Anbieter von Software für elektronische Zahlungen – wo stehen wir Ihrer Ansicht nach in Sachen Cyberrisiken in fünf bis zehn Jahren?

Worldline: Cybersicherheit nimmt eine zentrale Rolle in unserem Geschäftsmodell ein und ist in den letzten Jahren zum sensibelsten Thema auf unserer Risikokarte geworden, sowohl was die möglichen Auswirkungen auf unsere Geschäftsfelder als auch die Eintrittswahrscheinlichkeit betrifft. Das Thema steht somit jeden Monat bei Vorstandssitzungen auf der Tagesordnung und wird anhand von bestimmten KPI diskutiert. Der elektronische Zahlungsverkehr ist per se sehr sensibel, unterliegt aber auch strengen Standards, genauer dem PCI DSS (Payment Card Industry Data Security Standard). Dieser wurde 2004 von führenden Anbietern von Zahlungskarten geschaffen, um eine stärkere Kontrolle über die Karteninhaberinformationen zu erreichen und den Missbrauch von Zahlungsinstrumenten zu verringern. Konkret geht es dabei im Wesentlichen darum, die Daten so zu splitten und zu verschlüsseln, dass niemandem in der Zahlungskette mehr Daten als notwendig offengelegt werden. In diesem Bereich ist Datendiebstahl zwar noch möglich, gestaltet sich aber schwierig. Zu den schwieriger zu erfassenden (da viel einfacher umzusetzenden) Gefahren gehören sogenannte DDoS-Angriffe (Distributed Denial of Service), bei denen ein Server mittels einer Flut von Anfragen überlastet und damit unerreichbar gemacht wird. Der Angreifer versucht durch das Außergefechtsetzen der Dienste, einer Firma oder einer Marke finanziell zu schaden oder deren Ruf zu schädigen. Das Feld der Cyberbedrohungen ist daher sehr weit. Am beunruhigendsten sind wahrscheinlich diejenigen, die auf die Destabilisierung von Organisationen, Unternehmen oder öffentlichen Einrichtungen abzielen.

ODDO BHF AM: Neue technologische Bedrohungen mit technologischen Mitteln zu bekämpfen – das scheint die Lösung zu sein. Wie sehen Sie die Entwicklung der Kryptographie?

Worldline: Im elektronischen Zahlungsverkehr werden alle ausgetauschten Daten verschlüsselt. Diese Technik ist gemäß dem PCI DSS fester Bestandteil der in diesem Bereich eingesetzten Verfahren, auch wenn dieser erst ab bestimmten Umsatzsschwellen anwendbar sind. Aufgrund der kontinuierlich weiterentwickelten Verschlüsse-

lungstechniken gibt es in der Interaktion mit Kunden zuweilen Probleme, da bestimmte Sektoren nicht auf dem Stand der Technik sind. Die ständige Aktualisierung auf die neuesten Verschlüsselungstechnologien ist mit hohen Kosten verbunden und kann insbesondere für kleinere E-Commerce-Unternehmen eine große finanzielle Hürde darstellen und bei der Zusammenarbeit mit ihren wichtigsten Partnern zu operativen Problemen führen. Somit ist die Technologie zwar effizient und inzwischen weitgehend erprobt. Ihrem großflächigen Einsatz stehen jedoch von Sektor zu Sektor sehr unterschiedliche wirtschaftliche Umstände und Zwänge entgegen.

ODDO BHF AM: Kann auch die Entwicklung der Blockchain-Technologie Antworten auf Fragen der Cybersicherheit liefern?

Worldline: Durch den Wegfall von Intermediären ist die Blockchain-Technologie von Natur aus sicher. Da es sich hierbei um eine Kette von Datenblöcken handelt, die von den Benutzern selbst zerlegt und verifiziert wird, wird jeder Angriff von außen zumindest im Falle privater Blockchains deutlich erschwert. Gleichwohl ist diese Technologie noch keineswegs ausgereift. So wird sie in ihrer Entwicklung oftmals ausgebremst, z.B. durch das Fehlen einer Verarbeitung in Echtzeit, die Implementierungskosten oder auch den sehr hohen Energieverbrauch (je größer die Blockchain, desto höher ist der IT-Ressourcen-Einsatz und desto höher auch der Energieverbrauch). Noch liegt eine großflächige Anwendung im E-Commerce angesichts der Größe der Datenbasis und deren ständiger Entwicklung in weiter Ferne. Andererseits hat sich diese Technologie in einer geschlossenen Umgebung bereits bewährt. Dementsprechend hat beispielsweise Bureau Veritas im März 2018 in Zusammenarbeit mit Worldline das erste, auf der Blockchain-Technologie basierende Verfolgbarkeitsetikett im Lebensmittelsektor vorgestellt. Dieses ermöglicht Verbrauchern, jeden Schritt in der Fertigung eines Produkts nachzuvollziehen. In diesem Fall sind die Daten klar definiert und repetitiv.

ODDO BHF AM: Das Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) in der Europäischen Union scheint von vielen (insbesondere kleinen) Unternehmen unterschätzt oder von der Mehrheit der Bürger kaum beachtet zu werden. Angesichts des bei vielen Verbrauchern herrschenden Misstrauens gegenüber der Verarbeitung personenbezogener Daten – was ist Ihrer Meinung zufolge die wichtigste Neuerung gegenüber der aktuellen Gesetzgebung?

Worldline: Die DSGVO wirkt sich auf die gesamte Wertschöpfungskette aus. In vielen Fällen ist der Austausch von Daten heute nicht vertraglich geregelt. Die Stärkung der Verantwortung jedes einzelnen Akteurs bei der Erhebung und Verarbeitung von Daten wird zu erheblichen Veränderungen in der Arbeitsweise, der Datenstruktur und Kontrolle führen. Für BtoC-Geschäftsmodelle kommt die Pflicht hinzu, die ausdrückliche Zustimmung der Verbraucher einzuholen und neuen Rechten Rechnung zu tragen, wie z.B. dem Recht auf Vergessen, Datenübertragbarkeit oder Widerspruch gegen bestimmte Aktivitäten bei der Verarbeitung personenbezogener Daten. Jedes Unternehmen

wird zudem für die Verarbeitung personenbezogener Daten seiner Mitarbeiter verantwortlich sein, was vermutlich eine Komplettüberarbeitung vieler Prozesse im Personalbereich zur Folge haben dürfte.

ODDO BHF AM: Glauben Sie, dass die DSGVO zur Stärkung der Cybersicherheit beitragen wird, insbesondere durch eine bessere Nachverfolgbarkeit und eine eindeutige Inpflichtnahme der Dateninhaber?

Worldline: Ja, zweifellos. Es ist wichtig zu bedenken, dass zwei Drittel der sich aus der Umsetzung der DSGVO ergebenden Verpflichtungen Risikokontrolle und -steuerung zum Gegenstand haben. Das verbleibende Drittel sieht operative Maßnahmen vor, die sich direkt auf Informationssysteme beziehen. Der Wandel weg vom Prinzip der Konformität hin zum Prinzip der Verantwortung und mögliche abschreckende Geldstrafen machen es zu einem für jedes Unternehmen relevanten übergeordneten Thema, das eine Beteiligung aller hierarchischen Ebenen erfordert. Einer der Grundpfeiler dieser neuen Verordnung besteht darin, das Vertrauen in die Erhebung und Verarbeitung von Daten wiederherzustellen, und die einzusetzenden Mittel sind eindeutig auf eine bessere Kontrolle von Cyberrisiken ausgerichtet.

Cybersicherheit – ein zentraler Aspekt in unserem Dialogansatz

In unserem internen ESG-Unternehmensanalysemodell wurde der Untersuchung von immateriellen Vermögenswerten und immateriellem Kapital, wie z.B. Personal, Innovation oder auch Organisationskapital (Kunden, Marke, Zulieferer, Technologie), bereits in der Vergangenheit großes Gewicht beigemessen. In letzterem Analysefeld **integrieren wir einen systematischen Ansatz zur Betrachtung der digitalen Strategie von Unternehmen – eine Quelle für Chancen, aber auch für mittelfristige operative Risiken.**

Vermehrte Cyberrisiken sind ein die Führungskräfte zunehmend beschäftigendes Thema. Auch für Investoren spielen deren Auswirkungen verstärkt eine Rolle. Dementsprechend **ist Cybersicherheit auch ein zentraler Aspekt in unserem Dialog mit Unternehmen.**

Strukturierte Betrachtung der Digitalstrategie von Unternehmen

Der Einsatz neuer Technologien bedeutet aufgrund der Multiplikation von Interaktionen und extrem verkürzter Datenbearbeitungszeiten einen radikalen Wandel der traditionellen Arbeitsweise von Unternehmen unabhängig von der Branche. Die digitale Strategie der Unternehmen kann (und muss) hier konkrete Antworten sowohl für vorgelagerte (Kostenmanagement, Verarbeitung, Personal, Lieferanten) als auch nachgelagerte Prozesse (Marketing, Vertrieb) finden.

Bei einigen Unternehmen steht die Strategie für nachgelagerte Prozesse im Mittelpunkt und sollte in erster Linie auf den Kunden ausgerichtet sein. Bei vielen Unternehmen jedoch liegt die digitale Priorität auf den vorgelagerten Prozessen und der Prozessoptimierung auf den Ebenen Produktion, Lieferkette und Personalmanagement.

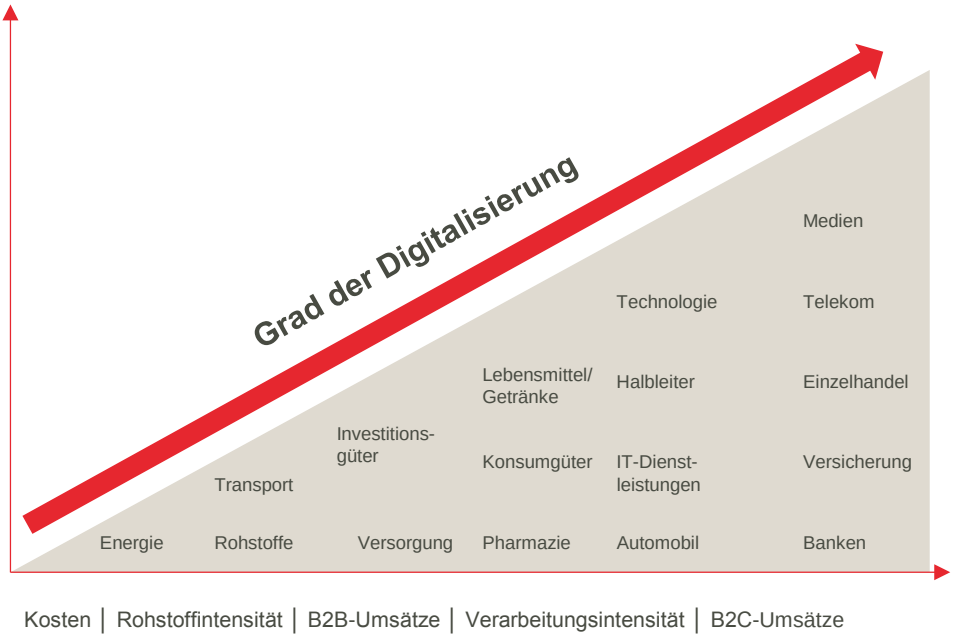
Die Umsetzung einer digitalen Strategie hängt daher von der Positionierung der einzelnen Unternehmen in der Wertschöpfungskette ab.

„Erster Schritt: Definition des Digitalisierungsgrad jedes Sektors“

In unserem ESG-Analysemodell besteht der erste Schritt darin, jeden Sektor nach der Dimension der digitalen Herausforderungen zu gewichten:

- Verhältnis Kosten / Umsätze
- Verhältnis B2B und B2C
- Rohstoffintensität vs. Verarbeitung (Personal, Back-Office-Funktionen usw.).

Digitalisierungsgrad der Sektoren



Quelle: ODDO BHF Asset Management

„Zweiter Schritt: Analyse der Digitalstrategie jedes Unternehmens“

In einem zweiten Schritt analysieren wir Unternehmen unter drei Gesichtspunkten:

- **Leadership**: Beleuchtet wird, wer im Unternehmen für die digitale Strategie und damit für das Thema Cybersicherheit verantwortlich ist (CEO, Vorstand, Expertise im Verwaltungsrat).
- **Implementierung**: Betrachtet werden bestimmte Indikatoren, wie z.B.:
  - Entwicklung der IT-Ausgaben
  - Vorhandensein eines digitalen Teams und dessen Aufgaben
  - Durchführung spezieller Schulungen für die Mitarbeiter
  - oder Zertifizierung nach ISO 27001 (Sicherheit von Informationssystemen) oder ISO 20000 (Produktion und Betrieb von IT-Systemen)
- **Risikomanagement**: Wir führen eine eher qualitative Analyse der eingesetzten Schutzmechanismen (Einsatz von Datenverschlüsselungstechnik oder starke Authentifizierungsverfahren[8]; Cyberversicherung) und der Historie möglicher Datenschutzzwischenfälle durch.

8 Siehe Glossar

Einbeziehung der digitalen Strategie in unser ESG-Analysemodell

Quelle: ODDO BHF Asset Management

Cybersicherheit – auch Gesprächsthema im Dialog mit Unternehmen

Im Rahmen seines ESG-Integrationsansatzes setzt ODDO BHF Asset Management bevorzugt auf den Dialog mit Unternehmen anstatt auf Ausschluss. Die Digitalisierung der Wirtschaft eröffnet zweifellos neue Entwicklungschancen in vielen Geschäftsfeldern, bringt aber auch neue Risiken mit sich, deren Ausmaß und Folgen noch ungewiss sind und sich ständig wandeln.

Wir ermutigen unsere Fondsmanagement-Teams, dieses Thema bei ihren regelmäßigen Gesprächen mit Emittenten zu adressieren. **Das Thema Cybersicherheit findet nun systematisch und entsprechend der Relevanz für den betreffenden Sektor Eingang in unseren aktiven Dialog mit Unternehmen zu ESG-Fragen.**

Glossar

Botnet: Der Terminus setzt sich aus den beiden englischen Begriffen „robot“ und „net“ zusammen und bezeichnet eine große Zahl an Computern, auf die Hacker eine Schadsoftware eingeschleust haben, um sie für ihre Zwecke zu nutzen. Botnets übernehmen die Kontrolle über Hunderte oder Tausende Computer und werden in der Regel dazu eingesetzt, Viren zu verbreiten, persönliche Daten zu stehlen oder Denial-of-Service-Angriffe durchzuführen. Sie gelten aktuell als eine der größten Internetbedrohungen.

Verschlüsselung: Methode, die es einer Person und/oder einem System, das nicht über den entsprechenden Verschlüsselungsschlüssel verfügt, unmöglich macht, ein Dokument einzusehen. Dieses Prinzip ist in der Regel mit dem Prinzip des bedingten Zugangs verbunden.

Persönliche Daten: Darunter wird jede Information verstanden, mittels derer eine natürliche Person direkt oder indirekt identifiziert werden kann (Name, Kennzeichen, Telefonnummer, Foto, Geburtsdatum, Wohnort, Fingerabdruck).

Hacking: Das Suchen und Ausnutzen von Schwächen eines IT-Systems oder Netzwerkes, häufig um einen finanziellen Vorteil zu erlangen

Social Engineering: Psychologische Manipulationstechnik, mittels derer Menschen zur Offenlegung vertraulicher Informationen verleitet werden sollen

Malware: Abkürzung für „malicious software“, bezeichnet Programme, die zur Infizierung und Beschädigung von Computern entwickelt wurden

Phishing: Versuch der Erlangung sensibler Daten durch Vortäuschen eines vertrauenswürdigen Absenders in einer elektronischen Kommunikation

Starte Identifizierungsverfahren: Identifizierungsverfahren, das eine Kombination von mindestens zwei Elementen (oder Zeichenfolgen) zur Authentifizierung vorsieht

Ransomware: Bösartige Software, die den Zugriff auf ein Computersystem oder Daten blockiert, bis ein Geldbetrag („Lösegeld“) bezahlt wird, oft in Kryptowährung

Quellenangaben

„Guide sur le Règlement Européen relative à la protection des données personnelles“, Bird&Bird, April 2017

„Enjeux Cyber 2018 : L’évolution de la menace Cyber“, Deloitte, Januar 2018

„Faire face aux menaces cyber“, Lloyd’s of London, September 2016

„2018 Thales data threat report”, Thales et 451 Research, Januar 2018

„2017 Cost of Cybercrime Study”, Accenture et Pnemom Institute, 2017

„The Global Risks Report 2018”, Weltwirtschaftsforum, Januar 2018

„EU-Verordnung 2016/679 des des Europäischen Parlaments und des Rates“, Amtsblatt der Europäischen Union, Mai 2016

Über ODDO BHF Asset Management

ODDO BHF Asset Management ist Teil der 1849 gegründeten, unabhängigen deutsch-französischen Finanzgruppe ODDO BHF.

ODDO BHF AM ist ein führender unabhängiger Vermögensverwalter in Europa. Das Asset Management der ODDO BHF Gruppe umfasst ODDO BHF AM SAS in Frankreich, ODDO BHF Private Equity in Frankreich sowie ODDO BHF AM GmbH in Deutschland, die zusammen knapp 61 Mrd. € verwalten.

ODDO BHF AM bietet seinen institutionellen und privaten Kunden eine attraktive Auswahl an leistungsfähigen Anlagelösungen in den wichtigsten Anlageklassen, d.h. europäische Aktien, quantitative Strategien, Renten- und Multi-Asset-Ansätze.

Auf konsolidierter Basis entfallen 70% des verwalteten Vermögens auf institutionelle Kunden, 30% auf Vertriebspartner. Die Teams operieren aus Investmentzentren in Düsseldorf, Frankfurt und Paris sowie an weiteren Standorten in Luxemburg, Mailand, Genf, Stockholm und Madrid.

Oberste Priorität von ODDO BHF AM ist es, den Kunden ein langfristiger Partner zu sein. Die Unabhängigkeit von ODDO BHF AM ermöglicht es den Teams, schnell und flexibel zu agieren und innovative Lösungen zu entwickeln, die passgenau auf die Anforderungen der Kunden zugeschnitten sind.

Disclaimer

ODDO BHF Asset Management ist die Vermögensverwaltungssparte der ODDO BHF-Gruppe. Es handelt sich hierbei um die gemeinsame Marke von drei eigenständigen juristischen Einheiten: ODDO BHF Asset Management SAS (Frankreich), ODDO BHF Private Equity (Frankreich) und ODDO BHF Asset Management GmbH (Deutschland).

Vorliegendes Dokument wurde durch die ODDO BHF ASSET MANAGEMENT SAS (ODDO BHF AM) zu Werbezwecken erstellt. **Die Aushändigung dieses Dokuments liegt in der Verantwortlichkeit jeder Vertriebsgesellschaft, Vermittlers oder Beraters. Potenzielle Anleger sind angehalten, vor Investition in eine Strategie oder einen Fonds einen Anlage- und oder Steuerberater zu konsultieren.** Es wird ausdrücklich darauf hingewiesen, dass die genannten Strategien bzw. Fonds nicht in jedem Land zum (öffentlichen) Vertrieb zugelassen sind. Im Falle einer Investition sind die Anleger angehalten, sich mit den Risiken der Anlage, insbesondere des Kapitalverlustes, vertraut zu machen. Der Wert der Kapitalanlage kann Schwankungen sowohl nach oben als auch nach unten unterworfen sein, und es ist möglich, dass der investierte Betrag nicht vollständig zurückgezahlt wird. Die Investition muss mit den Anlagezielen, dem Anlagehorizont und der Risikobereitschaft des Anlegers in Bezug auf die Investition übereinstimmen. ODDO BHF AM übernimmt keine Haftung für Verluste oder Schäden jeglicher Art, die sich aus der Nutzung des gesamten Dokuments oder eines Teiles davon ergeben. Alle in diesem Dokument wiedergegebenen Einschätzungen und Meinungen dienen lediglich zu Veranschaulichung. Sie spiegeln die Einschätzungen und Meinungen des jeweiligen Autors zum Zeitpunkt der Veröffentlichung wider und können sich jederzeit ohne vorherige Ankündigung verändern, eine Haftung hierfür wird nicht übernommen. Eine Wertentwicklung in der Vergangenheit darf nicht als Hinweis oder Garantie für die zukünftige Wertentwicklung angesehen werden. Sie unterliegt im Zeitverlauf Schwankungen. Es wird keine – ausdrückliche oder stillschweigende – Zusicherung oder Gewährleistung einer zukünftigen Wertentwicklung gegeben.

Bitte beachten Sie, dass wenn ODDO BHF AM ab dem 3. Januar 2018 Anlageberatungsdienstleistungen erbringt, es sich hierbei um nicht-unabhängige Anlageberatung nach Maßgabe der europäischen Richtlinie 2014/65/EU (der so genannten „MIFID II-Richtlinie“) handelt. Bitte beachten Sie ebenfalls, dass alle von ODDO BHF AM getätigten Empfehlungen immer zum Zwecke der Diversifikation erfolgen.

ODDO BHF
ASSET MANAGEMENT

ODDO BHF Asset Management SAS
12 boulevard de la Madeleine
75440 Paris Cedex 09 France
am.oddo-bhf.com