NN investment partners

bisher ING INVESTMENT MANAGEMENT

Kolumne

von Nina Hodzic, ESG-Spezialistin bei NN Investment Partners

Datenschutz vs. Datenklau – Sicherheit im Cyberspace und die Folgen für ESG*

Weltweit werden persönliche und geschäftliche Daten zunehmend in digitaler Form auf offenen und global miteinander verknüpften Technologieplattformen gespeichert. Das birgt erhebliche Risiken für Datensicherheit und Datenschutz. Tatsächlich vergeht kaum ein Tag ohne Schlagzeilen über eine neuartige Cyber-Bedrohung oder eine massive Datenschutzverletzung. Hacker, Kriminelle und ausländische Regierungen verlagern ihren Aktionsradius – ob Diebstahl, Betrug oder Sabotage – in diese zunehmend vernetzte Welt.

Durch die Aktionen des amerikanischen Whistleblowers Edward Snowden hat Datenschutz bei Unternehmen jetzt als Frage unternehmerischer Verantwortung höchste Priorität. Snowden hat der Öffentlichkeit vor Augen geführt, in welchem Ausmaß Regierungen die private Kommunikation ihrer Bürger über das Internet belauschen. Konzerne wie Facebook und Google sahen sich urplötzlich an den Pranger gestellt, als sich zeigte, dass sie auf behördliche Anordnungen hin Nutzerdaten an die US-Regierung weitergegeben hatten.

Glücklicherweise gibt es nicht nur schlechte Nachrichten. Der Cyberspace entwickelt sich kontinuierlich weiter und bietet immer wieder neue Chancen und Gelegenheiten. Unternehmen sind generell für neue Technologien (Stichwort: Internet, Cloud) offen, bedeuten sie doch, dass sich so neue Geschäftskanäle öffnen. Doch sie bringen auch ungeahnte Risiken mit sich. Der Bereich Cybersecurity wächst rapide, und Unternehmen mit genügend Weitsicht, um diese Trends zu nutzen, können sich hier einen deutlichen Vorsprung in puncto Wertschöpfung sichern.

Stand der Dinge

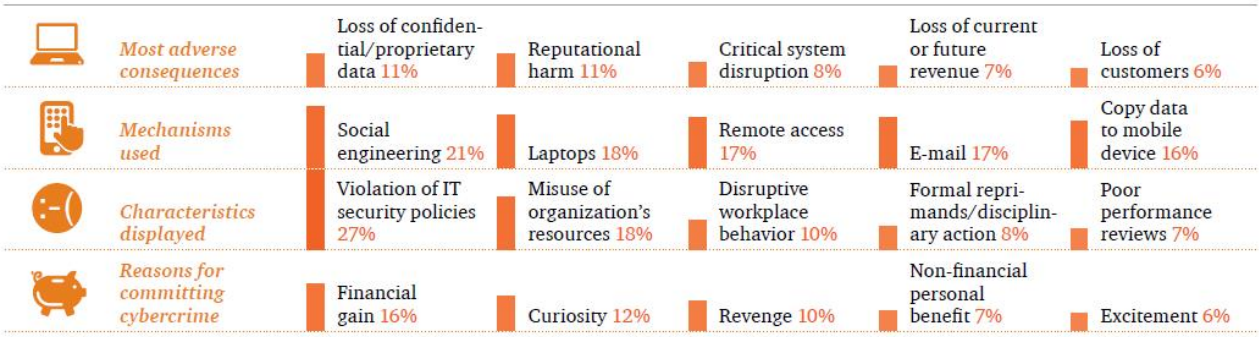
Datensicherheit – auch Cybersecurity – bezieht sich auf den Schutz von Informationen und Daten (Systemen) vor unbefugtem Zugriff, das schließt auch Nutzung, Weitergabe, Unterbrechung, Verfälschung und Vernichtung ein. Datenschutz bezieht sich demgegenüber auf die rechtmäßige Nutzung von Informationen. Datenschutz bedeutet, dass Daten nur zum beabsichtigten Zweck genutzt und nicht ohne Einwilligung der betroffenen Person an Dritte weitergeben werden. Datensicherheit und Datenschutz werden häufig synonym verwendet. Ohne angemessene Datensicherheitsprogramme lässt sich Datenschutz nicht zuverlässig darstellen. Umgekehrt mag die Datensicherheit technisch und prozessual zuverlässig gesichert sein, doch mangels unzureichender administrativer Maßnahmen haben externe Dienstleister unbefugten Zugang zu den Daten.

Die Motive von Cyberkriminellen liegen auf der Hand. Weniger offensichtlich ist, was Hacker antreibt. Als mögliche Motive kommen finanzieller Nutzen durch Betrug, Identitätsdiebstahl oder Missbrauch geistigen Eigentums, politi-

sche Gründe oder einfach die Lust am Sabotieren von Wirtschaftsunternehmen in Frage. Ein weitverbreiteter Irrglaube ist, dass die Angreifer Außenstehende seien. Tatsächlich finden diese Angriffe häufig von innen heraus statt: durch gegenwärtige oder ehemalige Beschäftigte, Dienstleister, befugte Nutzer eines internen Systems oder Auftragnehmer. Von diesen Insider-Angriffen bekommen wir in der Regel nichts mit, weil mit ihnen häufig intern verfahren wird und sie daher nicht an die Presse gelangen. Dadurch unterschätzen wir ihre Tragweite.

Die von der Wirtschaftsprüfungsgesellschaft PwC durchgeführte Umfrage 2014 US State of Cybercrime Survey ergab, dass fast ein Drittel der Befragten Insider-Kriminalität als teurer bzw. schädlicher ansieht als von Außenstehenden begangene IT-Attacken. Je größer das Unternehmen, desto wahrscheinlicher werden Insider-Attacken als teurer und schädlicher wahrgenommen. Dennoch gaben nur 49 Prozent der Befragten an, einen Plan für den Umgang mit Insider-Bedrohungen zu haben. Über 500 leitende Angestellte von US-Unternehmen sowie hochrangige Vertreter der Strafverfolgungsbehörden und anderer staatlicher Stellen nahmen an dieser Umfrage teil. Das nachfolgende Diagramm illustriert die Ursachen und Folgen der von Insidern verübten Cyberkriminalität. [1]

Ursachen und Folgen der von Insidern verübten Cyberkriminalität



Source: PwC 2014 US State of Cybercrime Survey

Schlimmste Konsequenzen	Verlust vertraulicher / proprietärer Daten **11 %**	Reputationsschäden **11 %**	Kritische Systemstörung **8 %**	Gegenwärtige oder zukünftige Umsatzverluste **7 %**	Verlust von Kunden **6 %**
Genutzte Technik	Social Engineering **21 %**	Laptops **18 %**	Remote Access **17 %**	E-mail **17 %**	Kopieren von Daten auf mobiles Gerät **16 %**
Merkmale	Verletzung von IT-Sicherheitsregeln **27 %**	Missbrauch von Ressourcen **18 %**	Störendes Verhalten am Arbeitsplatz **10 %**	Offizielle Warnung / Disziplinarmaßnahmen **8 %**	Schlechte Leistungsbewertung **7 %**
Gründe für Cyberverbrechen	Finanzieller Nutzen **16 %**	Neugier **12 %**	Rache **10 %**	Nicht-finanzieller persönlicher Nutzen **7 %**	Nervenkitzel **6 %**

Quelle: PwC 2014 US State of Cybercrime Survey

Das Center for Strategic and International Studies (CSIS) gab im Juni 2014 einen Bericht heraus, wonach die Vereinigten Staaten, China und Deutschland zusammen einen Schaden in Höhe von jährlich geschätzt 200 Milliarden Dollar durch Cyberkriminalität erlitten haben.

[1] *ESG ist die englische Abkürzung für „Environment Social Governance“, also Umwelt, Soziales und Unternehmensführung. Der Begriff ist international in Unternehmen als auch in der Finanzwelt etabliert, um auszudrücken, ob und wie bei Entscheidungen von Unternehmen und der unternehmerischen Praxis sowie bei Firmenanalysen von Finanzdienstleistern ökologische und sozial-gesellschaftliche Aspekte sowie die Art der Unternehmensführung beachtet beziehungsweise bewertet werden. Quelle: Lexikon der Nachhaltigkeit https://www.nachhaltigkeit.info/artikel/esg_1609.htm

Im Unternehmenssektor sind insbesondere die Finanz- und die Telekommunikationsindustrie bevorzugte Ziele für Angriffe von Cyberkriminellen. Die Finanzindustrie ist einem breiten Spektrum von Risiken ausgesetzt, darunter Diebstahl sensibler Kundendaten, Bedrohung des Geschäfts und das Durchsickern vertraulicher geschäftlicher Daten. Telekommunikationsanbieter kontrollieren, verarbeiten, übertragen, empfangen und speichern elektronische Daten und sind daher für das Funktionieren kritischer Telekommunikationsinfrastrukturen (wie beispielsweise im Bereich Verteidigung) von maßgeblicher Bedeutung. Sie gehen mit wertvollen Informationen um und müssen in allen Ländern, in denen sie tätig sind, datenschutzrechtliche Bestimmungen beachten.

Tatsächlich ist es aber so, dass die meisten Wirtschaftsunternehmen bei der Entwicklung ihrer Expertise zum Umgang mit Cyberrisiken immer noch in den sprichwörtlichen Kinderschuhen stecken. Diesen Unternehmen geht es darum, ein klareres Verständnis dafür zu entwickeln, welche Informationsgüter zu schützen sind, wer die Angreifer sind und wie man sie am wirksamsten abwehrt. Als effektive Maßnahme hat sich dabei die Ernennung eines Cyber-Beauftragten bewährt, wie beispielsweise eines Director of Cybersecurity oder eines Chief Digital Officer (CDO), um sämtliche Aktivitäten im Cyberspace zu überwachen und den Vorstand entsprechend zu beraten. Eine der wichtigsten Fragen zum Datenschutz lautet: Sind Unternehmen zu schnell bereit, Daten an Regierungen weiterzugeben? Vodafone hat sich in dieser kontroversen Debatte besonders hervorgetan, indem der Mobilfunkanbieter sämtliche staatlichen Anfragen nach Kundendaten – nach Ländern aufgegliedert – offenlegt. Danach gehen die Regierungen in 29 Ländern das Unternehmen um Kundendaten an.

Was sind die nächsten Schritte?

Zwar haben die wichtigsten Akteure bereits Schritte in die richtige Richtung unternommen, es gibt aber noch viel zu tun. Sicherheit beruht auf Profilaxe, Erkennen der Gefahr und dem Ergreifen entsprechender Maßnahmen. Die größte Herausforderung besteht darin, dass die technischen Systeme immer komplexer werden. Das erschwert die lückenlose Absicherung. Hier sind u. a. vereinfachte Prozesse und ein Abbau der wechselseitigen Abhängigkeiten vonnöten, um den Übergang zu eher lose gekoppelten Strukturen und Systemen zu schaffen. Kurzfristig besteht zudem dringender Handlungsbedarf, auf Unternehmensseite die Robustheit gegenüber Cyber-Attacken zu verstärken. Die Geschäftsführungen sind hier gefordert. Das würde zudem nach und nach die Zusammenarbeit der Unternehmen mit Partnern an allgemeingültigen bzw. internationalen Richtlinien sowie gemeinschaftlichen und systemischen Vorgaben für den Umgang mit Cyberkriminalität verbessern.

Unternehmen sind auf das Vertrauen ihrer Kunden angewiesen. Ohne Vertrauen kein Geschäft. Sowohl die Privatwirtschaft als auch der öffentliche Sektor müssen beim Kampf gegen die Cyberkriminalität in weitaus größerem Umfang in den Nachwuchs investieren. Eine strategische Möglichkeit wäre zum Beispiel, die „bösen“ kriminellen Black-Hat-Hacker zu „guten“ White-Hat-Hackern zu resozialisieren, die ihr Wissen ausschließlich im gesetzlichen Rahmen einsetzen.

Bei NN Investment Partners sehen wir Cyber-Sicherheit als wichtiges Thema, dem Unternehmen besondere Aufmerksamkeit schenken sollten. Daher raten wir Unternehmen, all die sensiblen Daten, die ihre Kunden ihnen anvertrauen, wirksam zu schützen.

Wie wir dieses Thema im Rahmen unserer ESG-Aktienstrategie nutzen können

Bei NN Investment Partners nutzen wir dieses Thema, indem wir in Unternehmen investieren, deren Geschäftsmodelle eindeutig an Bereiche wie Verbraucherschutz, Content-Sicherheit, kritische Infrastruktur, Datenverschlüsselung, Unternehmenssicherheit, Firewalls, Systeme zur Aufdeckung und Verhinderung unerwünschter Netzwerkzugriffe, mobile Sicherheit, Web-Sicherheit usw. anknüpfen. Innerhalb unseres ESG-Portfolios ist Cyber-Sicherheit ein zentra-

les Thema, dem Unternehmen besondere Aufmerksamkeit schenken sollten. Daher stehen wir im Dialog mit Unternehmen aus den verschiedenen Sektoren, um zu ergründen, inwieweit sie auf Cyber-Attacken vorbereitet sind und welche Initiativen sie für Datensicherheit und Datenschutz ergreifen.

Presse Kontakt

NN Investment Partners Deutschland

Birgit Stocker

-Head of PR D/A/CH-

T: +49 69 50 95 49 -15

M: + 49 160 989 63164

E: birgit.stocker@nnip.com

www.nnip.com

Über NN Investment Partners

NN Investment Partners (NN IP)* ist der Asset Manager der NN Group N.V., einer an der Börse gehandelten Aktiengesellschaft. NN IP hat seinen Hauptsitz in Den Haag, in den Niederlanden und verwaltet weltweit ca. Euro **186** Milliarden** (USD **227** Mrd.**) Assets under Management für institutionelle Kunden und Privatanleger. NN IP beschäftigt mehr als **1.100** Mitarbeiter und ist in **16** Ländern in Europa, im Nahen Osten, Asien und den USA vertreten.

Am 7. April hat ING Investment Management zu NN Investment Partners umfirmiert. NN IP ist Teil der NN Group N.V., einer an der Börse gehandelten Aktiengesellschaft. 54,6% der NN Group sind derzeit im Besitz der ING Group. Sie und ihre Tochtergesellschaften verwenden den Namen „ING" und damit zusammenhängende Warenzeichen der ING Groep N.V. (ING Group) mit einer entsprechenden Genehmigung.

**NNIP/NN Investment Partners ist der Markenname von ING Asset Management B.V. (ab 7. April NNIP Asset Management B.V.) Frankfurt Branch.*

***Stand: Q4 2014, 31. Dezember 2014*

Weitere Informationen erhalten Sie unter www.nnip.com und www.nn-group.com