




Cybersecurity im medialen Diskurs

Risikoeinschätzung als Herausforderung für Unternehmen

Eva-Maria Griesbacher · Martin Griesbacher 

Eingegangen: 30. Oktober 2019 / Angenommen: 11. April 2020 / Online publiziert: 28. April 2020
© Der/die Autor(en) 2020

Zusammenfassung Die Digitalisierung hat in den letzten Jahren ein komplexes, sich scheinbar ständig veränderndes Feld möglicher Risiken hervorgebracht, dessen Ausmaße für Unternehmen zunehmend schwer erkennbar sind. Entsprechend wichtig wird die Frage, wie EntscheidungsträgerInnen und MitarbeiterInnen Gefahren im digitalen Raum besser erkennen, adäquat einschätzen und auf diese reagieren können. Da sich EntscheidungsträgerInnen in kleineren KMU meist über Internet-recherchen oder in der Tagespresse über Cybersecurity informieren, hängt ihre Risikoeinschätzung und Maßnahmensetzung davon ab, wie Cybersecurity-Themen in diversen Medien dargestellt und diskutiert werden. Basierend auf einer Diskursanalyse von 504 Medienberichten zum Thema Cybersecurity in Unternehmen zwischen 2010 und 2019 kommt der Beitrag zu dem Ergebnis, dass sich die Medien weniger an langfristig bestehenden Bedrohungslagen orientiert haben, sondern vielmehr an den spektakulärsten Zwischenfällen und typischen Rollenverteilungen zwischen „Gut“ und „Böse“. Insgesamt wurde der Cyberspace als ein unsicherer Raum für Unternehmen dargestellt – teilweise aufgrund des Verhaltens ihrer eigenen MitarbeiterInnen. Für IT-Unternehmen, Polizeibehörden und die Forschung bedeutet der Nachvollzug des medialen Cybersecurity-Diskurses eine verbesserte Einsicht in die selektive und situative Behandlung von Bedrohungslagen durch Medien und die damit verbundenen Verzerrungen unternehmerischer Risikoeinschätzungen. Zentral für die unternehmerische Cybersecurity ist zudem die Kompetenz der MitarbeiterInnen, die Gefahren akkurat erkennen zu können.

Schlüsselwörter Awareness · Cyberkriminalität · Cybersicherheit · Diskurs · Risikoeinschätzung

E.-M. Griesbacher · M. Griesbacher (✉)
Center for Social Research, Karl-Franzens-Universität Graz, Graz, Österreich
E-Mail: m.griesbacher@uni-graz.at

Cybersecurity in Media Discourse

Risk Perception as a Challenge for Companies

Abstract In recent years, digitization has created a complex, seemingly ever-changing field of possible risks. The extent of these risks is increasingly difficult for companies to identify. Accordingly, the question of how decision-makers and employees can recognize, assess and react to dangers from cyberspace becomes increasingly important. Since decision-makers in smaller SMEs usually obtain information about cybersecurity through Internet research or through daily press, their risk assessment and measures depend on how cybersecurity issues are presented and discussed in various media. Based on a discourse analysis of 504 media reports on the topic of cyber security in companies between 2010 and 2019, the article comes to the following conclusion: The media has focused less on long-term existing threats and more on the most spectacular incidents and typical role distribution between “good” and “evil”. All in all, cyberspace was portrayed as an insecure space for companies—partly due to the behaviour of their own employees. For IT companies, police authorities and research, the understanding of the media cybersecurity discourse means an improved insight into the selective and situational treatment of threat situations by the media and the associated distortions in corporate risk assessments. Finally, the competence of the employees to accurately recognize the risks is central to corporate cybersecurity.

Keywords Awareness · Cybercrime · Cybersecurity · Discourse · Risk Assessment

1 Einleitung

Die Digitalisierung hat in den letzten Jahren ein komplexes, sich scheinbar ständig veränderndes Feld möglicher Risiken hervorgebracht, dessen Ausmaße für Unternehmen zunehmend schwer erkennbar sind. Es ist auch deshalb schwierig dieser Bedrohungslandschaft effektiv entgegen zu treten, da rein technische Lösungen für die Sicherheit von Informationstechnologien aufgrund der hohen Relevanz menschlichen Verhaltens nicht mehr ausreichen (Evans et al. 2016). Entsprechend wichtig wird die Frage, wie EntscheidungsträgerInnen und MitarbeiterInnen Gefahren im digitalen Raum besser erkennen, adäquat einschätzen (im Folgenden auch „Awareness“ genannt) und auf diese reagieren können. Besonders in kleinen und mittleren Unternehmen (KMU) ist die Awareness für Cybersecurity-Risiken jedoch häufig eher gering ausgeprägt, obwohl über 90% der KMU wesentliche Geschäftsprozesse über PC-Arbeitsplätze mit Internetzugang abwickeln (Hillebrand et al. 2017, S. 39). Akkurate Risikoeinschätzung stellt somit eine aktuelle kritische Aufgabe in Unternehmen dar, welche aber im wesentlichen Teil nur auf unsystematisch über diverse Medien aufgegriffene digitale Bedrohungslagen beruht. So informieren sich EntscheidungsträgerInnen in Deutschland in kleineren KMU mit weniger als 50 Angestellten meist über Internetrecherchen oder in der Tagespresse über Cybersecurity (vgl. Hillebrand et al. 2017, S. 71).

Welche Risiken wahrgenommen und welche Maßnahmen gesetzt werden, hängt aus diskurstheoretischer Sicht maßgeblich von medialen *Diskursen* ab, also wie Cybersecurity-Themen in den diversen Medien dargestellt und diskutiert werden. Trotz der potenziell starken Auswirkungen dieser Diskurse auf die unternehmerische Risikoeinschätzung liegen darauf fokussierte Analysen für den deutschsprachigen Raum nicht vor. Der vorliegende Beitrag bearbeitet diese Forschungslücke und zeichnet die diskursive Entwicklung im Themenbereich *Cybersecurity im Unternehmenskontext* auf Basis von Daten aus österreichischen Medien nach, wobei im nachfolgenden Abschnitt zur Methodik auch Hinweise für deren Relevanz in Deutschland erläutert werden. Es erfolgt eine Darstellung der im medialen Diskurs geschilderten Themen, Bedrohungen und der zentralen Akteure im Zeitverlauf, sowie eine Analyse der *diskursiven Konstruktion* von Sicherheit und Unsicherheit im Kontext von Cybersecurity für Unternehmen. Abschließend geht der Artikel auf die möglichen Implikationen für die Praxis ein, insbesondere hinsichtlich der Bedeutung von medialen Diskursen für die Risikoeinschätzung von Bedrohungen aus dem digitalen Raum.

2 Methodik und Datengrundlage

Als Grundlage für die Diskursanalyse wurden systematisch alle zwischen 01.01.2010 und 01.04.2019 in ausgewählten Medien erschienenen Artikel, welche gleichsam Nennungen von „Cybersecurity“ und „Unternehmen“ bzw. entsprechende äquivalente Begriffe enthielten, gesammelt. Der Korpus der Diskursanalyse umfasst insgesamt 504 Artikel, die in 17 in Österreich am häufigsten von betrieblichen EntscheidungsträgerInnen gelesenen Medien (siehe IFES 2018) veröffentlicht wurden (siehe Abb. 1). Diese Dokumente wurden zur Textanalyse in die Software MaxQDA transferiert und dort lexikalisch vercodet. Codes sind als Zuordnung von allgemeineren Begriffen zu einzelnen Wörtern, aber auch umfassenderen Textstellen zu verstehen. Für die Textanalyse wurde zuerst durch offenes Codieren einer Stichprobe aus dem gesamten Korpus ein Grundstock an Codes erstellt. Anschließend wurde dieser Grundstock an Codes mittels eines aus Experteninterviews und dem einschlägigen Stand der Forschung gewonnenen Codierschemas ergänzt und entsprechende Textstellen vercodet. In der Folge wurden sie mittels Häufigkeitsauszählungen und Kreuztabellen ausgewertet. Für die Codes mit den höchsten Häufigkeiten wurde eine qualitative Inhaltsanalyse durchgeführt, um weitere Muster und ggf. Bedeutungsveränderungen innerhalb dieser Codes über die Jahre hinweg feststellen zu können.

Zwischen 2010 und 2017 ist das mediale Interesse am Thema Cybersecurity stetig angestiegen (siehe Abb. 1). Dabei stechen die Jahre 2016 und 2017 besonders hervor. Wurden ansonsten durchschnittlich 50 Artikel zu dem Thema veröffentlicht, so liegen die Artikelzahlen mit ca. 80 bzw. 120 hier deutlich höher. Dieser Anstieg an Publikationen ist der verstärkten Publikationstätigkeit der drei meistgelesenen Printmedien in Österreich, also der Kronen Zeitung, dem Standard und dem Kurier zuzuschreiben. Besonders der Kurier veröffentlichte im Jahr 2017 dreimal so viele Artikel zum Thema Cybersecurity in Unternehmen wie zuvor.

Zur Frage der Reichweite der hier behandelten Studie muss hervorgehoben werden, dass Diskurse grundsätzlich mehr oder weniger klare zeitliche, räumliche und

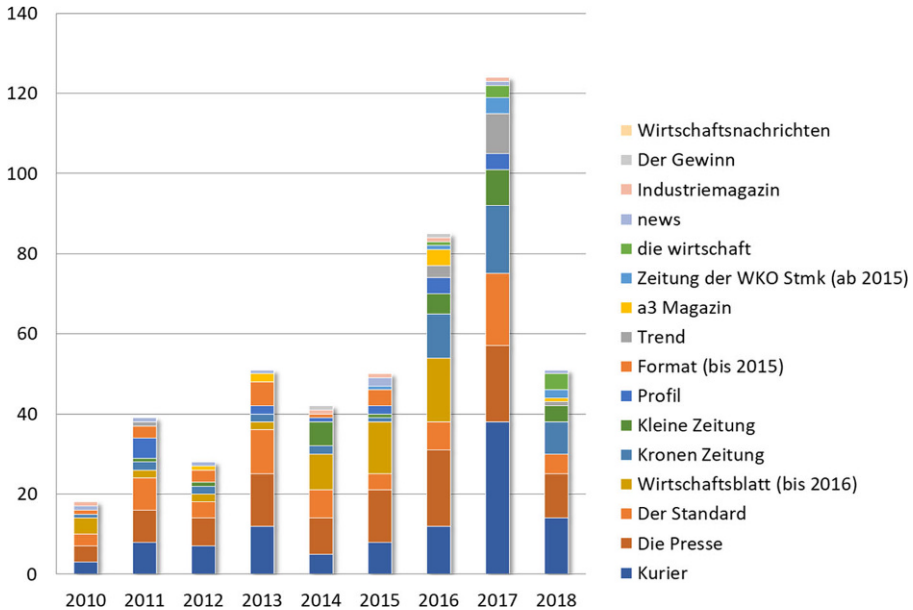


Abb. 1 Absolute Anzahl von Artikeln zum Thema „Cybersecurity in Unternehmen“ nach analysierten Printmedien. (Quelle: Eigene Erhebung)

soziokulturelle Grenzen aufweisen. Insofern wäre zunächst anzunehmen, dass der mediale Diskurs in Österreich kaum über dessen Landesgrenzen hinaus wirksam ist. Im Falle des Cybersecurity Diskurses weisen Umfragedaten aber darauf hin, dass insbesondere Österreich und Deutschland ein relativ ähnliches Meinungsspektrum aufweisen (siehe z. B. die Daten in Reichmann und Griesbacher 2017). Ein besonders auffälliger Hinweis findet sich auch in einer Eurobarometer Umfrage, die Anfang 2015 durchgeführt wurde (Eurobarometer 2015). Dort wurde – eineinhalb Jahre nach dem Beginn der Berichterstattung um die so genannte NSA Affäre¹ – die Frage gestellt, ob die Befragten schon einmal von jüngsten Enthüllungen zur Sammlung von personenbezogenen Daten durch Regierungsbehörden gehört haben. Österreich und Deutschland weisen mit ca. 75% die höchsten Werte in der europäischen Union auf (der Schnitt liegt bei ca. 50%). Das ist insofern bemerkenswert, als dass gerade die NSA Affäre auch im österreichischen medialen Diskurs eine sehr hohe Aufmerksamkeit zukam (siehe Abb. 2).

¹ Damals wurden von dem ehemaligen Geheimdienstmitarbeiter Edward Snowden zahlreiche Dokumente der Öffentlichkeit zugänglich gemacht, die diverse Überwachungsprojekte der NSA belegten. Für Unternehmen bedeutete die Affäre, dass Wirtschafts- und Industriespionage nicht mehr nur aus Asien, sondern insbesondere aus den USA zur Bedrohung wurde (zu diesem Diskursstrang siehe auch Reichmann und Griesbacher 2018).

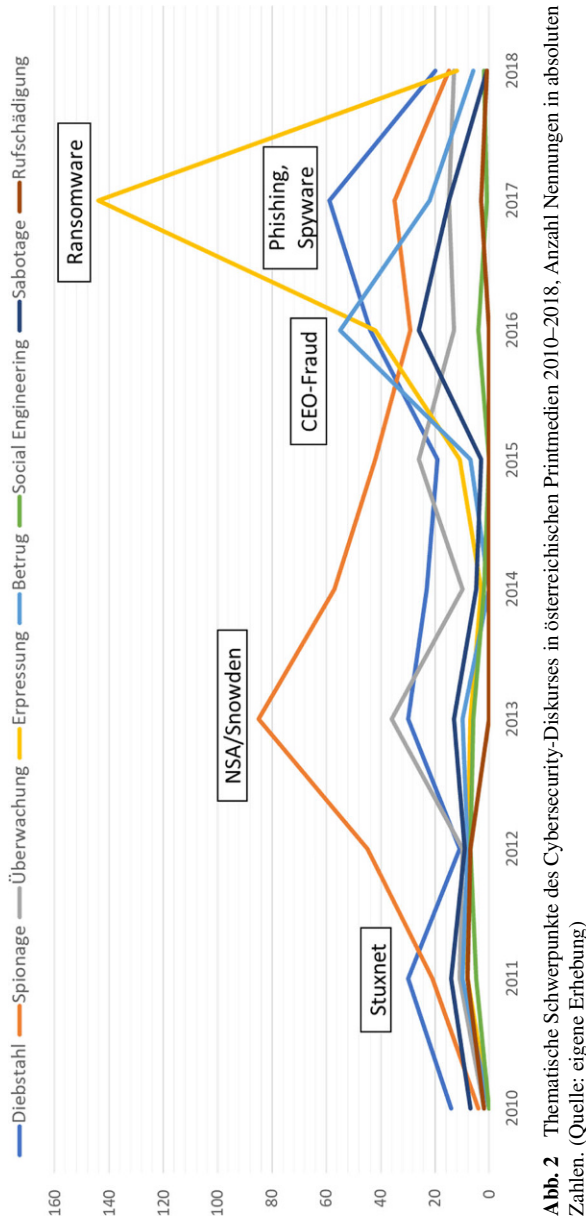


Abb. 2 Thematische Schwerpunkte des Cybersecurity-Diskurses in österreichischen Printmedien 2010–2018, Anzahl Nennungen in absoluten Zahlen. (Quelle: eigene Erhebung)

3 Zur Entwicklung der medialen Berichterstattung: Themen und Bedrohungen

Wie Schwankungen im Ausmaß der Berichterstattung bereits bemerkbar machen, haben sich die Medien der Logik der *Aufmerksamkeitsökonomie* folgend (siehe Franck 2010) weniger an langfristig bestehenden Bedrohungslagen orientiert,

sondern vielmehr an den spektakulärsten Zwischenfällen (STUXNET, NSA-Affäre, FACC CEO Fraud, Wannacry, Petya/Not-Petya) (siehe Abb. 2). Die Themen, die die österreichischen Medien in den letzten Jahren am meisten bewegt haben, waren einerseits *Snowden* und die *NSA-Affäre* im Jahr 2013. Die mediale Berichterstattung fokussierte sich dabei besonders stark auf den Spionagebegriff und sprach sowohl von staatlicher als auch von Wirtschaftsspionage. Ebenfalls, wenn auch wesentlich seltener wurde der seither konstant präsente Begriff der Überwachung in den Diskurs eingebracht sowie Sorge um Datendiebstahl ausgesprochen. Andererseits galt mit Petya und NotPetya besonders hohes mediales Interesse den *Ransomware*-Attacken des Jahres 2017, wo es zur Verschlüsselung von Daten und Erpressung zahlreicher Unternehmen kam. Weiters brachte der *CEO-Fraud*-Fall rund um den oberösterreichischen Luftfahrt-Zulieferer FACC 2016 überdurchschnittlich hohes Medieninteresse hervor. 2016 wurden verstärkt *DDoS*-Attacken und *Botnet*-Attacken thematisiert. Die Diskussion um Datendiebstahl verzeichnete zwischen 2013 und 2017 einen steten Zuwachs und scheint die meisten Cybersecurity-Zwischenfälle seither zu begleiten.

Um zu verstehen, inwiefern die Thematisierung von Zwischenfällen in den Medien die tatsächliche Gefahrenlage widerspiegelt, wurde ein Vergleich zu den von der Agentur der Europäischen Union für Cybersicherheit (ENISA) identifizierten Bedrohungslandschaft von 2012–2018 angestellt. Die seit 2012 jährlich erscheinenden *ENISA Threat Landscape Reports* enthalten Ranglisten mit den 15 wichtigsten Bedrohungsformen (ENISA 2012–2019). Um die Einschätzung der Top-Bedrohungen der ENISA mit unseren Daten vergleichbar zu machen, wurden die ermittelten Ränge in eine Zeittafel transferiert (siehe Abb. 3). Aus dem Vergleich mit Abb. 2 geht hervor, dass die mediale Aufmerksamkeit für das Thema Cybersecurity sich nicht an den (laut ENISA) tatsächlich höchsten Bedrohungen orientiert. Denn über die Jahre hinweg galten stets verschiedene Formen von Schadsoftware (Malware) und webbasierte Angriffe als die größten Bedrohungen aus dem Cyberraum, Spionage jedoch rangierte stets eher auf den untersten Rängen. Lediglich der Anstieg der Debatte um Ransomware in den Jahren 2016–2017 spiegelt sich auch in der Einschätzung der Bedrohungslage durch die ENISA wider.

Im Falle von Botnets scheint das mediale Interesse sogar gegenläufig zur durch die ENISA eingeschätzten Bedrohungslage zu sein. Während in den Medien in den Jahren 2010–2016 kaum von Botnets und *DDoS*-Attacken berichtet wurde, zählt die ENISA diese Formen von Attacken durchgängig zu den TOP-5-Bedrohungen aus dem Netz. Als das mediale Interesse an Botnets und *DDoS*-Attacken im Jahre 2017 plötzlich durch ein paar konkrete Zwischenfälle zunahm, fielen insbesondere Botnet-Attacken in den ENISA Rankings deutlich hinter Phishing und Spam zurück. EntscheidungsträgerInnen werden damit insgesamt durch den medialen Diskurs kaum bis gar nicht auf längerfristige bzw. kontinuierlich bestehende Bedrohungslagen sensibilisiert.

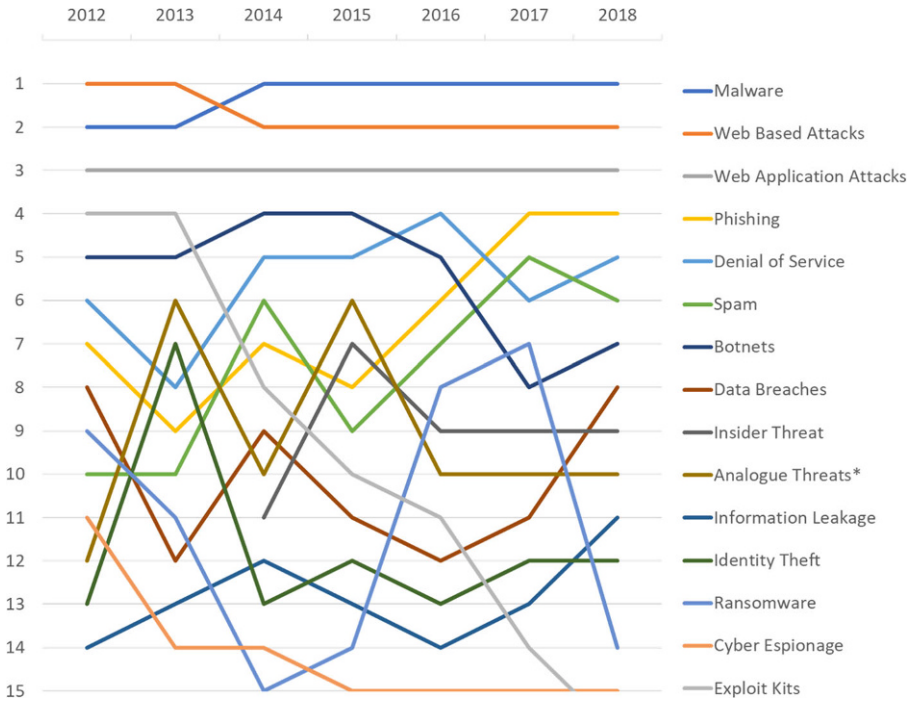


Abb. 3 Zeittafel der größten Cyber-Bedrohungen 2010–2018. Basis: ENISA Threat Landscapes 2012–2018 (y-Achse: Ränge: 1 = 1. (höchster) Rang unter den Bedrohungen, 15 = 15. Rang); *asterisk* Analogue Threats = „Physical Manipulation/damage/theft/loss“

4 Zentrale Akteure im Cybersecurity Diskurs

In ihren Berichten folgten die Medien in Bezug auf verschiedene Akteure im unternehmensnahen Cybersecurity-Diskurs dem klassischen Erzählschema der „Guten“ gegen die „Bösen“ (für die Anzahl der Nennungen siehe Tab. 1). Die Bösen waren dabei mit Abstand am häufigsten Hacker und Kriminelle. Aber auch MitarbeiterInnen wurden als Bedrohung für die Cybersecurity der Unternehmen dargestellt. Dementgegen wurden im medialen Diskurs IT-Sicherheitsdienstleistungs- und IT-Sicherheitsberatungsunternehmen sowie Cyber-Versicherungen in der Rolle der Guten, der Helfer in der Not betroffener oder sich in Gefahr befindlicher Unternehmen präsentiert. Die eigentlichen Aufklärungsinstanzen von Cyberkriminalität im Unternehmenskontext – Polizei, Bundeskriminalämter und deren auf Cybercrime spezialisierte Abteilungen wurden zwar auch durchwegs als helfende Hände bei Cybercrime-Zwischenfällen skizziert, jedoch deutlich seltener in den Diskurs eingebracht als IT-Sicherheitsberater und -Dienstleister.

Die mediale Aufmerksamkeit für unterschiedliche Akteursgruppen im Kontext von Cybersecurity hat sich über die Jahre 2010–2018 zudem stark verändert. Der Begriff des Hackers wurde im Laufe der Zeit durchaus ambivalent verwendet. So wurde von *Superhackern* und Hackerpreisträgern, *Whitehat* -Hackern und im Staatsdienst

Tab. 1 Akteure mit über 100 Nennungen (01.01.2010 bis 01.04.2019)

Akteur	Nennungen
Hacker	850
Internet-Konzerne (GAFAM)	548
MitarbeiterInnen	476
Geschäftsführung	430
IT-Sicherheitsdienstleister	397
Kunden	381
Kriminelle	304
IT-Sicherheitsberater	258
Cyber-Versicherungen	232
Staatliche Behörden	218
NSA	199
Polizei und Europol	179
Medien	137
Snowden	133
Täter	113
Bundesheer	102

beschäftigten professionellen Hackern mit einem außergewöhnlichen Wissensschatz und anerkannter Expertenstellung gesprochen, die sich für mehr IT-Sicherheit einsetzen. Die spezielle Deutung von *Whitehat*-Hackern als nach ethischen/moralischen Prinzipien handelnde Akteure ohne Profitinteressen wurde ebenfalls zitiert, jedoch auch instrumentell dazu eingesetzt, für diverse Ausbildungen und staatliche Karrierechancen (inkl. sehr guter Einkünfte) zu werben. Demgegenüber stehen Verweise auf *kriminelle* Hacker *Blackhat* -Hacker bzw. *Cracker*, die als kaufbar, profitorientiert, unberechenbar und ausgeklügelt bzw. zu *tausenden* aus Fremdstaaten (v. a. aus dem Iran, Osteuropa/Russland, China, Nordkorea, aber auch Türkei, Israel und der USA) kommand dargestellt wurden. Diese wurden einerseits als Hobbyhacker belächelt, aber andererseits auch mit organisierter Kriminalität und Terrorismus in Verbindung gebracht. In diese Akteursgruppe werden zum Teil auch jene inkludiert, die sich vordergründig nicht persönlich bereichern wollen, sondern sich für politische Ziele wie Internetfreiheit einsetzen. Der Begriff des *Kriminellen* scheint ab ca. 2016 den Begriff des bösen Hackers als Gefahr für Unternehmen zu verdrängen. Cyberkriminelle wurden dabei insbesondere in den Tatbereichen Erpressung und Betrug als immer professioneller und profitorientierter handelnd dargestellt.

Infolge der Verbreitung des Verschlüsselungs- und Erpressungstrojaners *WannaCry* gewannen 2017 auch diverse mit Cybersecurity befasste Polizeibehörden deutlich an Aufmerksamkeit. Sie ermahnten zu Sicherheitsmaßnahmen in Unternehmen, wiesen aber auch auf die teils mangelhafte personelle und technische Ausstattung der Polizei zur Verfolgung internationaler organisierter Cyberkriminalität hin.

Seit 2014 lässt sich ein starker Anstieg des medialen Interesses an den Personengruppen der bestehenden und ehemaligen MitarbeiterInnen sowie der Ebene der Geschäftsführung feststellen. Dabei hat sich über die Zeit die Rolle der Beschäftigten immer weiter weg vom Status der Betroffenen hin zu dem eines Risikofaktors im

Unternehmen gewendet. Hervorzuheben ist, dass in den letzten Jahren auch verstärkt MitarbeiterInnen von Unternehmen zunehmend als möglicherweise mit krimineller Energie ausgestattete Akteure dargestellt wurden. Vor allem, wenn sie sich ungerecht behandelt fühlten, würden sie unter Umständen durchaus aus *Rachegefühlen* oder *Geldgier* heraus *kriminelle Motive* auf digitalen Wegen verfolgen. Auch die Geschäftsführung wurde zunehmend als Risikofaktor für die Cybersecurity von Unternehmen thematisiert, insbesondere wenn es sich *nicht* um ein Unternehmen aus dem IT-Sektor handelte. Führungskräfte von *IT-Unternehmen (Dienstleistungen, Consulting und Entwicklung)* nahmen hingegen häufig eine zunehmend prominente SprecherInnenrolle im Diskurs ein.

In Bezug auf Kunden fokussierte sich das Interesse der Medien zuerst eher auf Privatkunden, deren Daten vor dem Zugriff von Kriminellen wie auch vor zumindest im rechtlichen Graubereich agierenden Unternehmen zu schützen sind. Zu den Unternehmen mit unlauteren Absichten in Bezug auf Kundendaten zählten dabei im Cybersecurity-Diskurs häufig die Internet-Giganten Google, Amazon, Facebook, Apple und Microsoft (GAFAM). Es wurde argumentiert, dass durch die gute Sicherung von Kundendaten Privatkunden gegenüber eine hohe Unternehmensreputation aufrechterhalten werden muss, um ihr Vertrauen in die Organisation und damit ihren Status als Kunden für das Unternehmen zu erhalten sowie Haftungsrisiken zu minimieren. Privatkunden wurden dabei häufig als nicht in der Lage beschrieben, selbst für Cybersecurity zu sorgen. Parallel dazu verlief zwischen 2010 und 2014 jedoch auch ein Diskursstrang, der sowohl Business- als auch Privatkunden in der Eigenverantwortung sah, Sicherheitsrisiken in Bezug auf ihre von diversen Unternehmen verarbeiteten Daten selbst zu erkennen und entsprechendes Sicherheitshandeln an den Tag zu legen. Dabei sollten sie nicht nur ihre eigenen Daten schützen, sondern auch die an sie digital angeschlossenen Unternehmen weder in ihrer Sicherheit gefährden noch ihrer Reputation schaden. Kunden seien insbesondere dann an der Entstehung von Sicherheitsmängeln in digitalen Produkten und Dienstleistungen mitschuldig, wenn sie erwarten, die entsprechenden Services zu immer günstigeren Preisen oder sogar gratis zu bekommen.

Im Rahmen des Diskursstranges um die potentiell desaströsen Auswirkungen von Industrie- und Wirtschaftsspionage auf den Innovationsstandort Österreich im Schatten der NSA-Affäre 2013 wurden „Geheimdienste“, Länder wie Russland, China und die USA als zentrale Akteure eingeführt. Insbesondere der US-Geheimdienst „NSA“ dominierte hier den Diskurs mit 199 Nennungen. US-nahe IT-Dienstleistungsunternehmen wurden dabei durch ihre Anbindung an die NSA als *Datenplünderer* bezeichnet. In diesem Kontext wurde der Wunsch vieler Akteure nach Datensicherheitslösungen/Cloudlösungen *made in Europe* ohne *Hintertüren für die NSA* medial zum Ausdruck gebracht, wobei gleichsam eine unabhängige Umsetzung solcher europäischen Lösungen als eher schwierig bis unmöglich dargestellt wurde.

5 Die Konstruktion von Sicherheit und Unsicherheit

Im Cybersecurity-Diskurs wurde mitunter auch verhandelt, inwiefern der Cyberspace für Unternehmen als unsicherer oder sicherer Raum gelten kann und was die

probaten Lösungsstrategien für etwaige problematische Cybersecurity-Situationen sind. Während einige, vor allem auch kleinere IT-Unternehmen mit der Betonung eines *überbordenden* Bedrohungspotentials für Unternehmen arbeiteten, konstruierten die Branchengiganten im IT-Sicherheitsbereich die digitale Welt als einen Raum *relativer* Unsicherheit mit *bewältigbaren* Risiken – soweit professionelle Hilfe hinzugezogen wird. Auf der einen Seite wurde also versucht, durch die Erzeugung von Unsicherheit und Angst Kunden zu gewinnen. Demgegenüber stand die Ansicht, dass das Zeichnen von so genannten *Cyberdoom*-Szenarien potenzielle Kunden eher von Investitionen in ihre IT-Sicherheit abhalten würde als diese zu fördern, da sie sich angesichts der überbordenden Bedrohungslage ohnehin machtlos fühlten. Medien beteiligten sich am diskursiven Prozess der Verunsicherung insofern, als dass sie der Logik der Aufmerksamkeitsökonomie entsprechend (also orientiert an einer Maximierung der Verkaufs- bzw. Klickzahlen) verstärkt über neue, besonders schwerwiegende oder bedrohliche Cybersecurity-Zwischenfälle berichteten. Um die polizeiliche Arbeit im Bereich Cybercrime zu erleichtern und um Unternehmen zu einer möglichst umfassenden Zusammenarbeit zu bewegen, betonten auch Akteure aus dem Bereich der Kriminalitätsbekämpfung (Polizei, Bundeskriminalamt, EUROPOL) das hohe Ausmaß des Gefährdungspotentials von Unternehmen durch Cyberkriminalität. Letztlich kamen zu diesem Diskursstrang auch noch Berichte hinzu, die den *Cyberwar* als etwas reales, versteckt vor den Augen aller in der digitalen Welt Ablaufendes konstruierten, indem entsprechende Akteure aus dem Bereich der österreichischen Landesverteidigung zitiert wurden. Von diesem postulierten Cyberwar seien Unternehmen auch betroffen (z. B. direkt als Angriffsziele oder indirekt als Unterstützter der Landesverteidigung, indem sie Softwarelösungen für das Heer entwickeln). Insgesamt ergibt sich aus dem Zusammenspiel der interessensgebundenen Aussagen dieser wortführenden Akteursgruppen (IT-Unternehmen, Polizei und Bundesheer) eine starke Dominanz von Aussagen im medialen Diskurs, welche die digitale Welt als übermäßig unsicheren Raum für Unternehmen darstellen.

Infolge der zunehmenden Darstellung der digitalen Welt als unsicher kämpften verschiedene, teilweise gegenläufige, Vorschläge zur Verbesserung der Sicherheit um Aufmerksamkeit. Hier hatten in der medialen Öffentlichkeit wiederum IT-Sicherheitsexperten die Wortführerschaft, wenn sie auch aufgrund ihrer unterschiedlichen Interessenslagen für unterschiedliche Strategien für Unternehmen plädierten. So hoben Anbieter von IT-Sicherheits-Dienstleistungen die fehlenden finanziellen Ressourcen und Kompetenzen von KMUs zur selbstständigen Problembewältigung hervor und setzten sich häufig für das Outsourcing der IT-Sicherheit ein. Beratungsunternehmen hingegen fokussierten im medialen Diskurs eher darauf, wie sich Betriebe selbst schützen können. Dabei betonten sie die Wichtigkeit der Aktualität der betrieblichen IT-Infrastruktur, aber auch die Wichtigkeit der Absicherung menschlichen Verhaltens für die IT-Sicherheit im Betrieb. Um diese zu verbessern, müsse der *Faktor Mensch* durch Awareness-Trainings, IT-Sicherheitsschulungen und Kontrolle bewältigt werden. Beide Sicherheitsstrategien stürzten sich damit implizit oder explizit auf MitarbeiterInnen als größten unter Kontrolle zu bringenden Risikofaktor für die IT-Sicherheit von Unternehmen.

Sicherheit sollte hauptsächlich über Technik, Kontrolle und verordnetes Lernen hergestellt werden, wobei den MitarbeiterInnen das Vertrauen in ihre Loyalität dem

Unternehmen gegenüber sowie in ihre selbstständigen Lern- und Entwicklungsfähigkeiten entzogen wurde. Um finanzielle Risiken zu vermeiden, wurden sogar ethisch bedenkliche Mittel wie die versteckte Kontrolle von MitarbeiterInnen über die IT-Sicherheitsinfrastruktur diskursiv legitimiert. Der mediale Diskurs um Cybersecurity in Unternehmen ließ neben Argumenten hinsichtlich der Leistbarkeit von Maßnahmen und der potenziell hohen Kosten infolge von Cyberattacken kaum Raum für ethische bzw. grundrechtsorientierte Überlegungen.

Der starke Fokus auf technische Aspekte und Expertenlösungen im Cybersecurity-Diskurs und die übermäßige Betonung von Sicherheit (Hypersecuritization) angesichts der zunehmenden Unsicherheit in der digitalen Welt deckt sich mit den Ergebnissen früherer Diskursanalysen in anderen Sprachräumen (Barnard-Wills und Ashenden 2012, S. 121; Dunn Caveltly 2008; Mieg 2008; Cruz Lobato und Kenkel 2015, S. 31). Neu ist die zunehmende Kriminalisierung von MitarbeiterInnen in der medialen Diskussion.

6 Resümee: Implikationen für die Praxis

Der vorliegende Beitrag zeigt, wie die mediale Aufmerksamkeit je nach Interessenskonstellation auf unterschiedliche Gefahrenmomente hinweist (z. B. Cyberkriminalität, staatliche Überwachung oder intensiviert Anschaffungen im Bereich Sicherheits-IT). Für IT-Unternehmen, Polizeibehörden und die Forschung, welche sich für eine umfassende Verbesserung von Cybersecurity in Unternehmen einsetzen, bedeutet der Nachvollzug des medialen Cybersecurity-Diskurses eine verbesserte Einsicht in die selektive und situative Behandlung von Bedrohungslagen durch Medien und die damit verbundenen Verzerrungen unternehmerischer Risikoeinschätzungen. Aus der vorliegenden Studie lassen sich Praxisimplikationen in drei zentralen Bereichen ableiten:

1. **Risikoeinschätzung:** Risiken für die digitale Infrastruktur von Unternehmen sollten nicht nur auf Basis von Medienberichten eingeschätzt werden. Während Medien aufgrund ihrer hohen Reichweite für akute Gefahrenmeldungen (z. B. neuartige Malware-Varianten) hinreichend Aufmerksamkeit (Awareness) erzeugen können, bleiben konstante Bedrohungen im täglichen Auf und Ab medialer Berichterstattung nicht ausreichend präsent. Eine gewisse kritische Distanzierung zur Tagespresse ist aber auch insofern nötig, als dass hinter berichteten Gefahren und zugehörigen Statistiken konkrete Interessenslagen von Medien und Unternehmen stecken können und das Ausmaß einer Bedrohung entsprechend verzerrt dargestellt werden kann. Wichtig ist, hinreichend Sensibilität für kontinuierlich bestehende Risiken aufzubringen, zu denen es ggf. keine Berichterstattung in der Tagespresse gibt (siehe z. B. das Thema Wirtschafts- und Industriespionage).
2. **Stärkung des Faktor Mensch:** Worauf der mediale Diskurs einerseits durchaus treffend sensibilisiert, ist die Notwendigkeit, im Cybersecurity-Bereich nicht nur technische Maßnahmen vorzunehmen, sondern insbesondere den Faktor Mensch verstärkt im Auge zu behalten. Andererseits ist der medialen Einteilung zwischen „guten“ und „bösen“ Akteuren mit Vorsicht zu begegnen. Gerade die tendenzielle

Kriminalisierung von MitarbeiterInnen kann für Unternehmen negative Konsequenzen haben – gilt es doch im Regelfall Vertrauen und Motivation im alltäglichen Betrieb aufrecht zu erhalten. So müssen nicht als Zeichen des Misstrauens zwingend Kontrollen der MitarbeiterInnen erhöht werden, sondern es können diese auch gleichermaßen positiv in Form von Kompetenzförderung im Bereich Cybersecurity Awareness adressiert werden (s. a. Weber et al. 2019).

- 3. Sicherheitskooperation:** KMU sind aufgrund im Regelfall geringer personeller und technischer IT-Ressourcen auf Informationen und Dienstleistungen von außen angewiesen, um den jeweils aktuellen Risiken der digitalen Welt begegnen zu können. Sie brauchen Unterstützung jener Institutionen, die Cybersecurity als gesamtgesellschaftliche Aufgabe verstehen. Beispiele hierfür sind die Polizei, die sich mit verstärktem Fokus auf Prävention und Awareness bemerkbar macht, nationale „computer emergency response teams“ (CERTs), die aktuelle Risikomeldungen kommunizieren und in Österreich die Wirtschaftskammer, die eine eigene Cybersecurity-Hotline für Unternehmen eingerichtet hat. In diesem kooperativen Bereich ist auch die Sicherheitsforschung gefragt, zentrale Aspekte für robusteres Cybersecurity-Verhalten und Awareness zu identifizieren und darauf ausgerichtete Trainings zu entwickeln (siehe z. B. Oltramari et al. 2014; Li et al. 2019; Aldawood und Skinner 2019). Die Bemühungen dieser Institutionen sollten gestärkt und besser vernetzt werden, um eine zentrale Quelle für akkurate Risikoeinschätzungen zu schaffen.

Funding Open access funding provided by University of Graz.

Open Access Dieser Artikel wird unter der Creative Commons Namensnennung 4.0 International Lizenz veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Artikel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.

Weitere Details zur Lizenz entnehmen Sie bitte der Lizenzinformation auf <http://creativecommons.org/licenses/by/4.0/deed.de>.

Literatur

- Aldawood H, Skinner G (2019) Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet* 11:73. <https://doi.org/10.3390/fi11030073>
- Barnard-Wills D, Ashenden D (2012) Securing virtual space: cyber war, cyber terror, and risk. *Space Cult* 15(2):110–123
- Cruz Lobato L, Kenkel KM (2015) Discourses of cyberspace securitization in Brazil and in the United States. *Rev Bras Polit Int* 58(2):23–43
- Dunn Cavelty M (2008) Cyber-terror—Looming threat or phantom menace? The framing of the US cyber-threat debate. *J Inf Technol Polit* 4(1):19–36
- ENISA (2019) Enisa threat landscapes. www.enisa.europa.eu. Zugegriffen: 29. Sept. 2019
- Eurobarometer (2015) Special Eurobarometer 431 „Data protection“ <https://doi.org/10.2838/552336>

- Evans M, Maglaras LA, He Y, Janicke H (2016) Human behaviour as an aspect of cybersecurity assurance. *Secur Commun Netw* 9:4667–4679. <https://doi.org/10.1002/sec.1657>
- Franck G (2010) Kapitalismus Zweipunktnull: Über die Kommerzialisierung der Ökonomie der Aufmerksamkeit. In: Neckel S (Hrsg) *Kapitalistischer Realismus*. Campus, Frankfurt a.M.
- Hillebrand A, Niederprüm A, Schäfer S, Thile S, Henseler-Unger I (2017) Aktuelle Lage der IT-Sicherheit in KMU, Bad Honnef: Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste. <https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Redaktion/DE/PDF-Anlagen/Studien/aktuelle-lage-der-it-sicherheit-in-kmu-langfassung.pdf>. Zugegriffen: 14. Juni 2019
- IFES Institut für empirische Sozialforschung (2018) LAE 3.0 – Leseranalyse Entscheidungsträger 2018. Prorecon, Wien
- Li L, He W, Xu L, Ash I, Anwar M, Yuan X (2019) Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *Int J Inf Manage* 45:13–24. <https://doi.org/10.1016/j.ijinfomgt.2018.10.017>
- Mieg HA (2008) Expertisierung vs. Professionalisierung: relative und andere Experten aus Sicht der psychologischen Expertiseforschung. In: Rehberg KS (Hrsg) *Die Natur der Gesellschaft*. Verhandlungen des 33. Kongresses der Deutschen Gesellschaft für Soziologie in Kassel 2006. Campus, Frankfurt a.M.
- Oltamari A, Cranor LF, Walls JR, McDaniel P (2014) Building an ontology of cyber security. In: CEUR Workshop Proceedings, 9th Conference on Semantic Technology for Intelligence, Defense, and Security Fairfax, United States, S 54–61
- Reichmann S, Griesbacher M (2017) Data report: Assurance and certification of privacy and security of ICT products and services as a question of trust, acceptance and perceived risks across Europe (Deliverable 3.1). TRUESSEC.eu, EC H2020 Project Nr 731711. <https://cordis.europa.eu/project/id/731711/results>. Zugegriffen: 1. Dez. 2019
- Reichmann S, Griesbacher M (2018) Current exemplary discourse dynamics in the field of privacy and security assurance (Deliverable 3.2). TRUESSEC.eu, EC H2020 Project nr 731711. <https://cordis.europa.eu/project/id/731711/results>. Zugegriffen: 1. Dez. 2019
- Weber K, Schütz AE, Fertig T (2019) Grundlagen und Anwendungen von Information Security Awareness. Mitarbeiter zielgerichtet für Informationssicherheit sensibilisieren. Springer, Wiesbaden