08. VSW-BB vor Ort

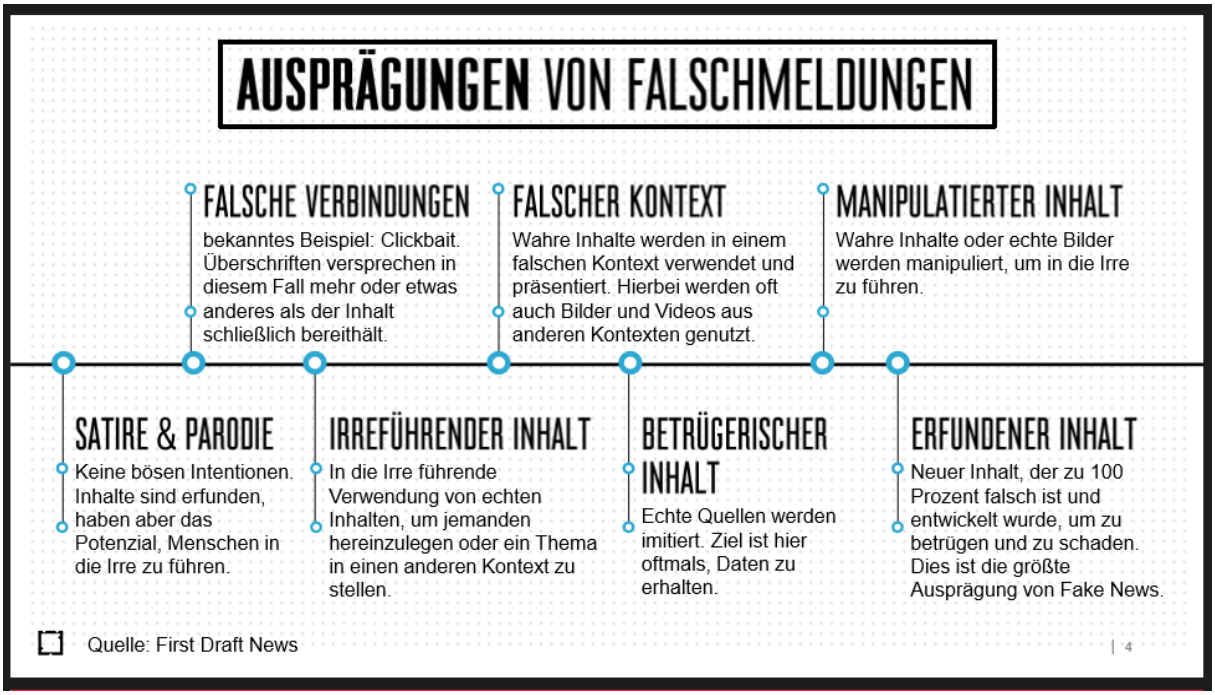
Die achte Ausgabe des VSW-BB vor Ort fand am 27.06.2018 statt und hatte das Thema Fake News – WIE und WARUM Sie Ihr Unternehmen schützen sollten, zum Gegenstand. Die Begrüßung der Teilnehmer übernahmen die Compliance-Bereichsleiterin der Berliner Sparkasse Agnes-Maria Wildner und der VSW-BB-Vizepräsident Carsten Baeck. Beide wiesen darauf hin, dass die eigene Reputation ein wichtiges Gut für Unternehmen darstellt, welches durch Fake News gefährdet wird.

Als erste Referentin konnte die CEO der international agierenden PR-Agentur "Weber Shandwick" und Präsidentin der "Gesellschaft der führenden PR- und Kommunikationsagenturen in Deutschland (GPRA)", Christiane Schulz, gewonnen werden. In dieser Doppelfunktion ist für Frau Schulz das Thema Fake News von zentraler Bedeutung, welches Unternehmen aktiv angehen müssen, da es sonst zu massiven Reputationsschäden kommen kann. Die effektivste Art der Gegenmaßnahme ist zum einen die Aufklärung, wenn Fake News ein Unternehmen bereits attackiert haben. Zum anderen empfiehlt sich eine präventive Bildung der Stakeholder, damit diese in die Lage versetzt werden, einen Angriff als Falschmeldung identifizieren können, wodurch eine Verleumdungskampagne gegen das Unternehmen an Wirkungskraft einbüßt. Bei beiden Maßnahmen steht die Sensibilisierung der Zielgruppen im Fokus, mit dem Ziel, dass diese Dinge hinterfragen und Nachrichten über das Unternehmen nicht einfach so hinnehmen.

Frau Schulz wies darauf hin, dass Fake News kein neuartiges Phänomen ist, sich aber das Setting verändert hat. Demzufolge haben der technische Fortschritt im Allgemeinen und die sozialen Medien im Besonderen dafür gesorgt, dass Leute in ihrer eigenen Informationsblase leben und dadurch anderen Informationen keine oder kaum Beachtung schenken. Dieses Phänomen zeichnete die Referentin an Hand des Beispiels Facebook nach. Demnach lesen viele Leute nur die Links ihrer Facebook-Freunde, welche nicht selten die eigene Meinung wiederspiegeln. Auf diese Weise manifestiert sich das eigene Weltbild und der Glaube, dass die eigene Meinung, die der breiten Masse entspricht. Dieser Prozess wird verstärkt durch das sinkende Vertrauen in die sogenannten "Mainstream-Medien", welches in Deutschland aber noch vergleichsweise hoch ist, und der politischen Ungewissheit, wodurch Themen emotionalisiert werden und reale Fakten in den Hintergrund rücken.

Frau Schulz betonte ausdrücklich, dass der Begriff Fake News sehr inflationär benutzt wird. Sie verwies auf "First Draft News", die eine strukturierte Darstellung der Ausprägungsformen von Falschmeldungen konzipierten (Siehe Abbildung 1)

Abbildung 1 – Ausprägungen von Falschmeldungen



Die Abbildung zeigt wie vielfältig Fake News sein können. Demnach können bereits falsche Verbindungen/Überschriften oder die Imitation von echten Quellen (betrügerischer Inhalt), die zur Generierung von Clicks bzw. Daten initiiert werden, als Falschnachrichten bezeichnet werden. Gleiches gilt für Satire und Parodien, die, wenn sie nicht eindeutig als frei erfunden erkennbar sind, Leute in die Irre führen können. Die weiteren erwähnten Ausprägungen sind geläufige Varianten von Falschmeldungen, wobei der erfundene Inhalt die originäre Form darstellt. Hierbei ist neben dem falschen Inhalt der Absender unbekannt, was eine strafrechtliche Verfolgung erschwert.

In diesem Zusammenhang war für Frau Schulz die Internetunterteilung von Bedeutung, welche man sich als Eisberg vorstellen kann. Demzufolge sind die Mainstream-Medien die Spitze des Eisbergs, die über die Wasseroberfläche hinausragt, wodurch Nachrichten – unabhängig davon, ob sie echt oder falsch sind – sichtbar sind. Für diese Ebene des Internets können Suchmaschinen wie Google und Co. benutzt werden. Eine Ebene darunter befindet sich das Deep Web, welches sich somit unterhalb der Wasseroberfläche befindet. Das Deep Web kann durchaus mit normalen Browsern erreicht werden, allerdings sind die Foren und Datenbanken nicht durch Suchmaschinen indexiert, wodurch man auf dieser Ebene etwas anonymer agieren kann. Noch anonymer ist die dritte Ebene, das sogenannte Dark Web, wodurch man sich, bleibt man bei der Eisbergmetapher, auf dem Meeresgrund befindet. Das Dark Web ist nur durch eine verschlüsselte Technologie erreichbar, wodurch der Zugang nur einem bestimmten Personenkreis gewährt wird. Dementsprechend ist es auf dieser Webebene umso schwieriger gegen Fake News vorzugehen, weil ein Unternehmen erstmal einen Zugang erhalten muss.

Im Anschluss an die theoretischen Grundlagen nannte Frau Schulz Beispiele für Fake News, die Wirtschaftsunternehmer in Misskredit ziehen sollten. Demnach muss sich beispielsweise

Red Bull immer wieder mit der falschen Behauptung auseinandersetzen, wonach der künstlich hergestellte Wirkstofftransporteur Taurin aus Stiersperma gewonnen wird. Durch das Beispiel "Pizzagate" wurde offensichtlich, dass Fake News nicht nur wirtschaftliche Schäden anrichten, sondern durchaus auch Lebensgefährlich sein können. Während des US-Präsidentschaftswahlkampfs wurde behauptet, dass in einer Washingtoner Pizzeria, welche angeblich von Hillary Clinton, Barack Obama und Lady Gaga betrieben wird, ein Kinderpornoring agiere. Diese Verschwörungstheorie verbreitete sich unter anderem über Twitter (auch mit Hilfe von sogenannten Social Bots) millionenfach und führte dazu, dass ein mit einem Sturmgewehr bewaffneter Mann in die Pizzeria eindrang, um die missbrauchten Kinder zu befreien. Erst als man ihn davon überzeugen konnte, dass diese Nachricht jeglicher Wahrheit wiederspricht, ließ er sich widerstandslos festnehmen – verletzt wurde niemand. Der oder die Urheber wurden im Wahlkampflager von Donald Trump vermutet, was sich allerdings nicht beweisen ließ.

Laut Frau Schulz muss jedes Unternehmen drei Schritte durchlaufen, um zu prüfen, ob man bei der Bekämpfung von Fake News richtig aufgestellt ist. Beim ersten Schritt – Assessment und Planung – sollte jedes Unternehmen überprüfen und evaluieren, wie gut das eigene Issue- und Krisenmanagement auf Fake News ausgerichtet ist. Dabei gilt es fünf Fragen zu beantworten:

1. Kann man Trends in Echtzeit identifizieren?
2. Wo informieren sich die eigenen Stakeholder und wie kann man diese dort erreichen?
3. Wie wird in der Medienlandschaft über das Unternehmen berichten bzw. diskutiert?
4. Ist der eigene Krisenplan auf Neuerungen (Trends) ausgerichtet?
5. Ist das Risk-Management-Team richtig autorisiert, um im Ernstfall zu handeln und stimmen die internen Abwehrprozesse noch?

Durch das Beantworten dieses Fragen werden Handlungsbedarfe identifiziert, welche man im zweiten Schritt – Optimieren und engagen – umsetzen sollte. Hierbei sollte regelmäßig trainiert werden, was in einem Krisenfall zu tun ist (z.B. durch eine jährliche Krisensimulation). Dadurch wird ein schnelles und sicheres Agieren, wenn Fall X eintritt, gewährleistet. Zu diesem Zweck ist es unabdingbar, dass das Krisenteam mit der Thematik der Fake News vertraut ist und jeder weiß, was er oder sie im Krisenfall zu tun hat. Aus diesem Grund empfiehlt es sich, dass die beteiligten Mitarbeiter in den Krisenplan mit eingebunden werden. Auf diese Weise partizipiert das Unternehmen zum einen am Wissen der eigenen Fachkräfte. Zum anderen legitimiert sich somit der Krisenplan, weil die Mitarbeiter sich mit diesem identifizieren. Darüber hinaus sollten alle Mitarbeiter über das Phänomen Fake News aufgeklärt werden und darüber, worauf zu achten ist. Als Nebeneffekt können die Mitarbeiter ihr persönliches Umfeld bezüglich Falschmeldungen sensibilisieren, wodurch sie als Multiplikator im Kampf gegen diffamierende Unterstellungen fungieren.

Als dritten Schritt sollte die eigenen Unternehmenswerte überprüft und als Erfolgsgarant verstanden werden, da diese für die Reputation eines Unternehmen von elementarer Bedeutung sind. Frau Schulz wies allerdings auch darauf hin, dass ethische Maßstäbe wie Transparenz, Integrität, Fairness, Wahrhaftigkeit, Loyalität und Professionalität, nicht nur in Bezug auf die Kommunikation beachtet werden sollten, sondern grundsätzlich für Unternehmen einen hohen Stellenwert haben sollten.

In der anschließenden Diskussion wurde als Gegenmaßnahme das Mittel der Gegendarstellung diskutiert. Hierbei wurde von einer Teilnehmerin angemerkt, dass eine Gegendarstellung immer von Vorteil ist, da sich auf diese Weise die Verbreitung eindämmen lässt und sich die Falschmeldung nicht als wahr manifestiert – so ihre Berufserfahrung. Frau Schulz stand dieser Behauptung skeptisch gegenüber, weil sie aus ihrer Erfahrung weiß, dass sich Fake News bis zu sechsmal schneller verbreiten als echte Nachrichten. Sie gab allerdings den Tipp, dass bei einer Gegendarstellung nicht der Link zur Falschmeldung mit veröffentlichen werden sollte, weil man auf diese Art Teil der Fake-News-Attacke wird, die gegen einen selbst gerichtet ist. Des Weiteren sollten Fake News so schnell wie möglich begegnet werden, was wiederum Kompetenzen und thematisches Wissen auf allen Unternehmensebenen voraussetzt – sind die Fake News in den Mainstreammedien angekommen, dann ist es meist zu spät.

Der zweite Fachvortrag wurde von Prof. Dr. Martin Grothe gehalten – CEO der complexium GmbH. Prof. Grothe verwendete den Begriff Desinformationen für die Thematik Fake News, weil der Terminus Desinformationen aus seiner Sicht greifbarer ist. Dass es sich dabei um denselben Sachverhalt handelt, verdeutlicht ein Blick auf die Definition von Desinformationen, welche ebenfalls in der Studie "#DESINFORMATION LAGE, PROGNOSE UND ABWEHR - Sicherheitsstudie zu Desinformationsangriffen auf Unternehmen" publiziert wurde. Demnach sind Desinformationen "die gezielte Verbreitung falscher oder irreführender Information[en]. Motivation der Desinformation ist die Beeinflussung der Meinung der Öffentlichkeit, von Gruppen oder Einzelpersonen, um politische oder wirtschaftliche Ziele zu fördern."

Wie wirtschaftliche Ziele durch Desinformationen gefördert werden, zeigte ein von Prof. Grothe vorgestelltes Beispiel, bei dem die Firma Viceroy Research auf einen sinkenden Aktienkurs der MiMedx Group wettete und dieses Ziel durch die Verbreitung von Fake News erreichte. Gleiches gelang Viceroy Research in Deutschland mit der ProSieben-Sat.1-Gruppe. Hierbei wurde behauptet, dass die Aktie überbewertet sei, wodurch die ProSieben-Sat.1-Aktie innerhalb von Minuten an Wert verlor. Um diesem Problem Herr zu werden empfiehlt Prof. Grothe, dass Unternehmen in Foren nicht nur als Gastgeber, sondern ebenso als Gast aktiv sind, um somit zum einen Desinformationen schneller identifizieren zu können und zum anderen, um auf diese Weise zeitnahe Gegenmaßnahmen einzuleiten. Als Nebeneffekt lernen die Unternehmen ihre Kunden besser verstehen.

Dass sich Desinformationsangriffe nicht nur auf das operative Geschäft beschränken müssen, was sich beispielsweise durch eine schädliche Darstellung der Produkte äußern kann, zeigte Prof. Grothe, indem er weitere Angriffsfelder nannte. Demzufolge können Konkurrenten

ebenso die Kreditwürdigkeit oder das Arbeitgeberimage des Unternehmens diffamieren. Bei letzteren können zum Beispiel in Arbeitnehmerforen potenzielle neue Mitarbeiter abgeschreckt werden, indem die Unternehmenskultur als stark hierarchisch oder ausbeuterisch beschrieben wird. Des Weiteren können, durch im Darknet gekaufte bzw. gehackte Datenprofile, falsche Nachrichten im Namen der Geschäftsführung initiiert werden (Identitätendiebstahl), wodurch im schlimmsten Fall finanzielle Transaktionen veranlasst werden, welche nicht im Interesse des Unternehmens sind. Darüber hinaus besteht hierbei die Möglichkeit einzelne Mitarbeiter zu erpressen, damit diese im Sinne der Angreifer handeln ("Wir wissen wo deine Kinder zur Schule gehen").

In der anschließenden Teilnehmeraktivierung durften alle Anwesenden in Teams einen Desinformationsangriff konstruieren. Dabei wurde ein fiktives Beispiel vorgegeben, bei dem der Markteintritt eines neuen Wettbewerbers mit Hilfe von Fake News verhindert werden sollte. Es zeigte sich, dass die Initiierung von Desinformationen/Fake News kein großes Problem darstellt, wenn ein gewisses thematisches Wissen vorhanden ist, welches mit ein bisschen kreativen Denken angereichert wird. Darüber hinaus wurde durch den aktiven Part umso deutlicher, dass die Digitalisierung Unternehmen hinsichtlich Desinformationen vor neue Herausforderungen stellt und neue Wege der Reputationssicherheit gefunden werden müssen. Prof. Grothe sprach sich in diesem Zusammenhang dafür aus, dass Unternehmen auf digitale Aufklärer setzen sollten, die, analog zu Personenschützern, den digitalen Raum ausspähen. Weitere Empfehlungen lassen sich in der erwähnten Studie zu Desinformationen finden. Diese ähneln zwar den Tipps von Frau Schulz, fassen diese allerdings nochmal zusammen und wirken ergänzend.

1. Seien Sie sich der Bedrohung durch Desinformation bewusst!

2. Schulen Sie Ihre Mitarbeiter im Umgang mit Social Media und mit Blick auf Social Engineering!

3. Setzen Sie ein umfassendes Krisenmanagement für Desinformations-/Reputationskrisen auf!

4. Binden Sie möglichst erfahrene Dienstleister im Bereich der Krisenkommunikation schon in der Vorbereitungsphase ein!

5. Machen Sie einen Desinformations-Stresstest!

6. Setzen Sie eine umfassende Früherkennung auf! Diese muss alle für Sie relevanten Länder/Märkte abdecken!

7. Suchen Sie bei der Früherkennung nicht nur nach festen Begrifflichkeiten!

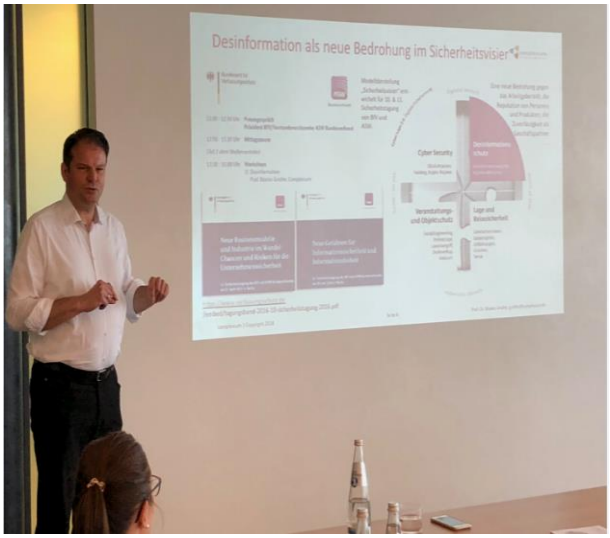
8. Bauen Sie Strukturen auf, die sicherstellen, dass alle Informationen über (mögliche) Desinformation an einer Stelle zusammenlaufen!

9. Reagieren Sie auf (mögliche) Fälle von Desinformation schnell, umfassend und zielgerichtet!

10. Überprüfen Sie bei allen Fällen von Desinformation die Herkunft und auch mögliche rechtliche Schritte! Setzen Sie dort an, wo der Ursprung liegt, ohne dabei die breiten Medien zu vernachlässigen!

11. Kommen Sie wieder vor die Lage und lernen Sie aus Erfahrungen.

Christiane Schulz



Prof. Dr. Martin Grothe

Bilder: Jonathan Strelow (VSW-BB)