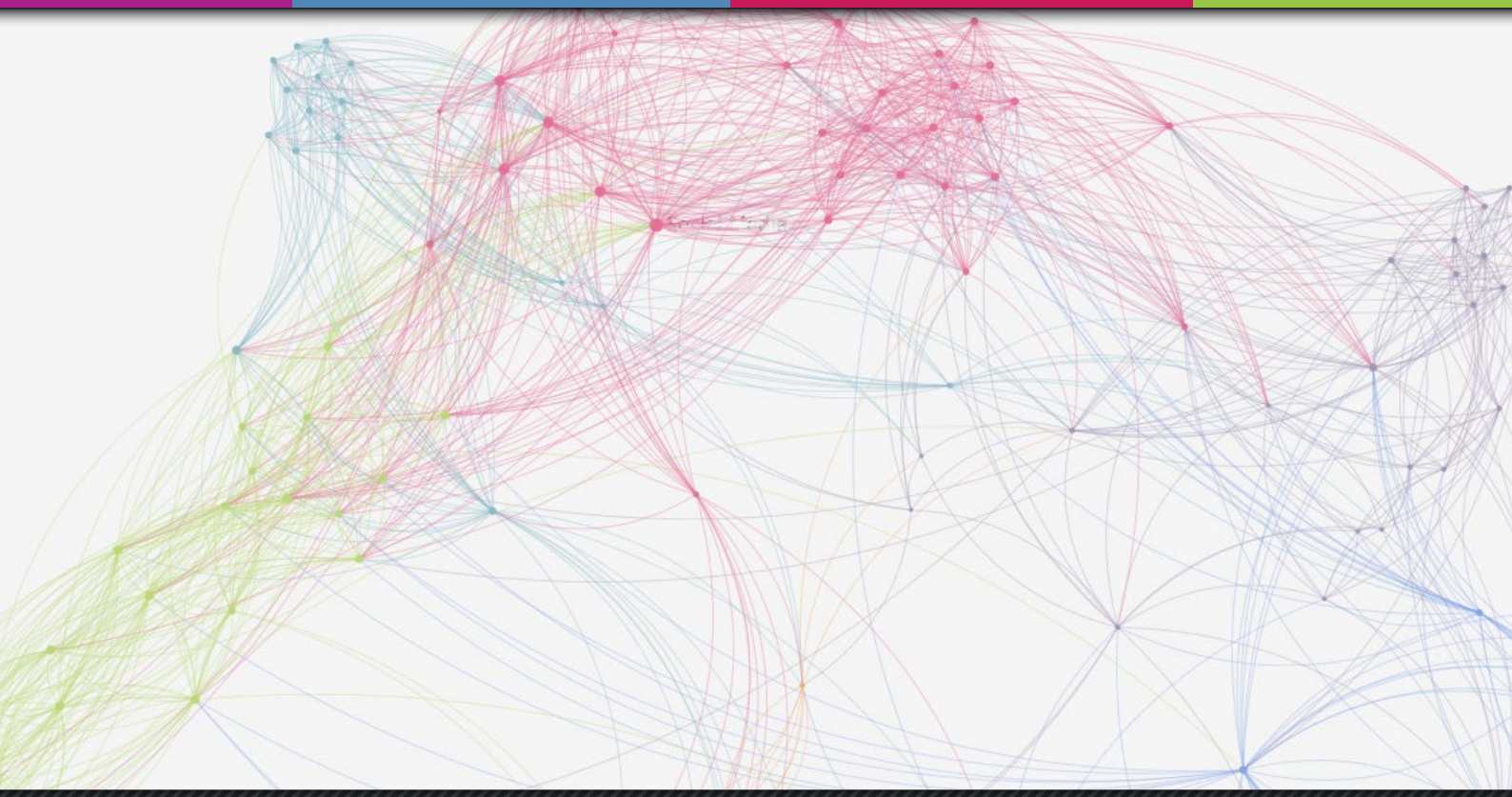
#DESINFORMATION

LAGE, PROGNOSE UND ABWEHR

Sicherheitsstudie zu
Desinformationsangriffen
auf Unternehmen



ASW Bundesverband

complexium UNTERNEHMENSBERATUNG

Deloitte.

Jan Wolter
Prof. Dr. Martin Grothe
Uwe Heim

Wir bedanken uns zuallererst bei den im Rahmen der Studie befragten Sicherheitsexperten für die umfangreichen und offenen Gespräche, die wir mit ihnen führen konnten.

Die so gewonnenen Erkenntnisse bilden das Rückgrat dieser Arbeit.

Ebenso bedanken wir uns bei allen Teilnehmern der Workshops und der Onlinebefragung zu dieser Studie. Nicht zuletzt gilt unser Dank den Teams von ASW Bundesverband, complexium und Deloitte.

Inhalt

Executive Summary

In der Politik werden inzwischen tagtäglich Falschinformationen in Umlauf gebracht: bewusste Desinformation, um einem Gegner zu schaden, um eigene Vorteile zu erringen – ganz offen oder aber subtil. Desinformation wird als Werkzeug eingesetzt, um offensiv von kritischen Themen abzulenken oder unterschwellig Meinung zu beeinflussen.

Desinformation ist die gezielte Verbreitung falscher oder irreführender Information. Motivation der Desinformation ist die Beeinflussung der Meinung der Öffentlichkeit, von Gruppen oder Einzelpersonen, um politische oder wirtschaftliche Ziele zu fördern.

Die öffentliche digitale Kommunikation im Internet bietet den zentralen Verbreitungsraum für Desinformationsmaßnahmen. Falsche Identitäten und Multiplikationsmechanismen bilden einen gefährlichen Werkzeugkasten. Wird dieses machtvolle Arsenal auf die Politik beschränkt bleiben? Keineswegs.

Die Digitalisierung macht solche Angriffsszenarien erschwinglich und damit auch für und gegen Unternehmen einsetzbar. Folglich ist die Verbreitung von Desinformation im aggressiven Unternehmenswettbewerb logische Konsequenz. **Im Rahmen dieser Studie wurde deutlich: Die ersten Desinformationsangriffe auf Unternehmen liegen bereits hinter uns.**

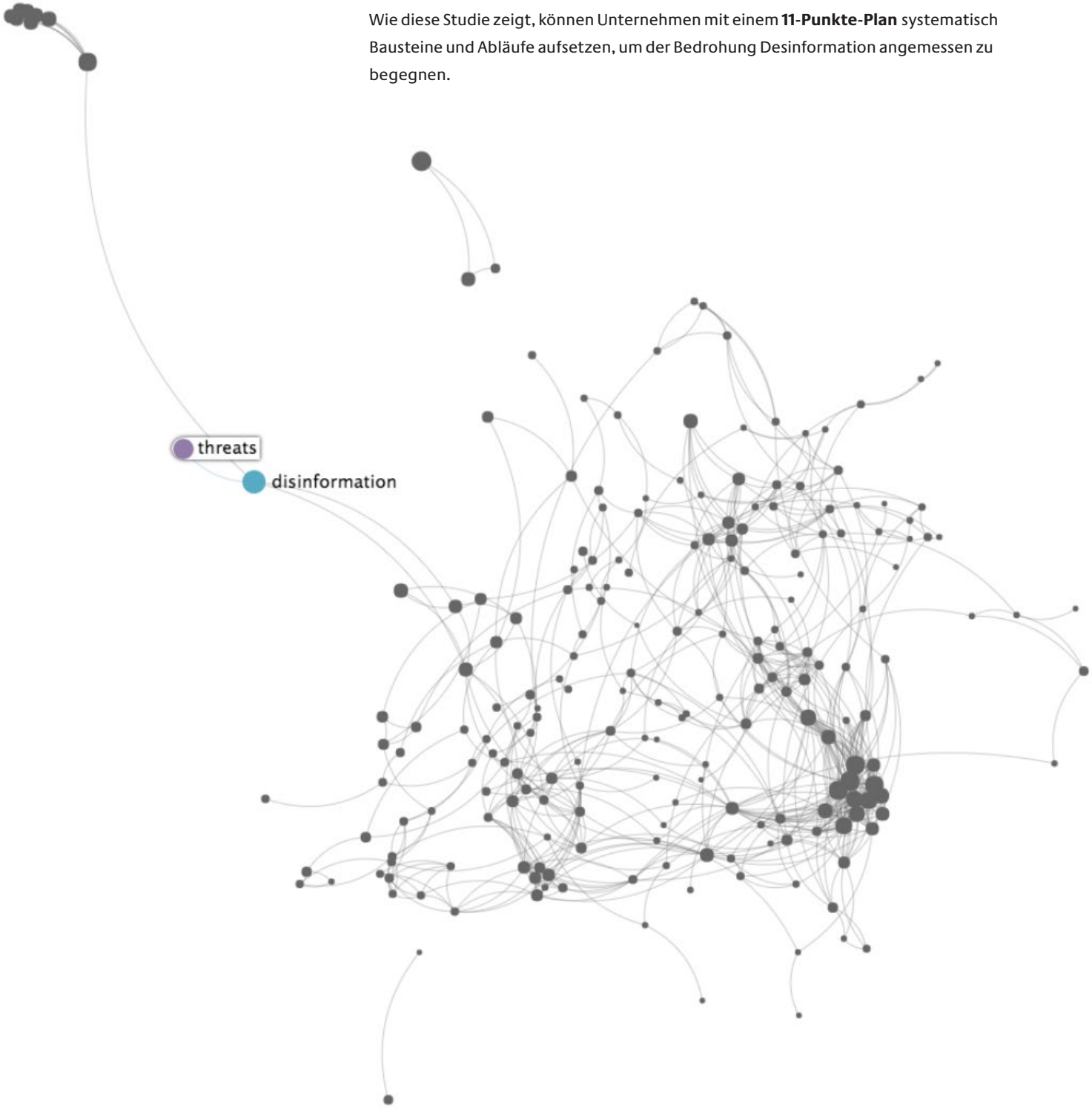
Umfang, Intensität und Steuerungsintelligenz der Angriffe werden dramatisch zunehmen. Dabei ist der technologische Fortschritt der entscheidende Treiber. Bots, Algorithmen und künstliche Intelligenz sind hier die Stichwörter.

Ziele von Desinformationsangriffen sind nicht wie im Bereich der Cyber Security Informationsbestände, Soft- oder Hardware innerhalb der eigenen Präsenz, sondern Meinungen, die sich auf externen Plattformen im Social Web bilden. Stehen Unternehmen im Visier, dann kann die Gesamtreputation des Unternehmens angegriffen werden, viel wirkungsvoller sind aber **gezielte Angriffe** auf einzelne Facetten und Stakeholder-Gruppen.

- So kann beispielsweise die **Reputation als Arbeitgeber** sehr wirkungsvoll auf den digitalen Hotspots einer Recruiting-Zielgruppe untergraben werden.
- Gleiches gilt für die Einschätzungen und Bewertungen zu den **Produkten und Leistungen eines Unternehmens**.
- Es können Gerüchte gestreut werden, die das Ansehen eines Unternehmens als verlässlicher und compliance-konformer **Geschäftspartner** beschädigen.
- Direkte Angriffe können auch auf **Schlüsselpersonen** eines Unternehmens oder deren Familienmitglieder zielen.
- Ein Unternehmen kann auch als **Mittel zum Zweck** für Desinformationsangriffe missbraucht werden.

Die Digitalisierung liefert aber auch den Verteidigern neue Werkzeuge in einer gleichwohl **asymmetrischen Auseinandersetzung. Von zentraler Bedeutung** sind dabei die Phasen **Prävention und Detektion**. So ist eine frühzeitige Erkennung von Desinformationsangriffen entscheidend für eine erfolgreiche Verteidigung. Die weiteren drei Phasen sind Bewertung, Eindämmung und Vorfall-Nachbehandlung.

Wie diese Studie zeigt, können Unternehmen mit einem **11-Punkte-Plan** systematisch Bausteine und Abläufe aufsetzen, um der Bedrohung Desinformation angemessen zu begegnen.



Studienziele und -aufbau

Die 9. Sicherheitstagung des ASW Bundesverbandes und des Bundesamtes für Verfassungsschutz stand 2016 unter dem Titel **„Neue Gefahren für Informationssicherheit und Informationshoheit“.** Die Diskussionen und Ergebnisse der Tagung haben gezeigt: Desinformation stellt eine ernst zu nehmende Bedrohung auch für Unternehmen dar. Daher hat der ASW Bundesverband gemeinsam mit der Wirtschaftsprüfungsgesellschaft Deloitte GmbH und der Unternehmensberatung complexium GmbH die Sicherheitsstudie zu Desinformationsangriffen auf Unternehmen initiiert. Ziel dieser Studie ist es, die aktuelle Bedrohungslage genauer zu analysieren.

Die vorliegende Studie zeigt auf, welchen Bedrohungen Unternehmen bereits heute im Bereich der Desinformation konkret gegenüberstehen. Es wird untersucht, ob und, wenn ja, welche Angriffe schon erfolgen. Zudem werden mögliche Szenarien vorgestellt, was an Gefahren noch bevorsteht. Die Studie formuliert aber auch Antworten, wie Unternehmen auf diese Herausforderungen reagieren können oder bereits reagieren. So macht diese Untersuchung vor allem eines deutlich: **Die Corporate Security muss auf die neue Herausforderung reagieren.**

Die Ergebnisse der Studie basieren auf systematischen Digital-Listening-Analysen, Expertendiskussionen, Interviews mit Vertretern aus Unternehmen und Behörden sowie einer Onlinebefragung.

- Im Rahmen der Studie fanden 30 qualifizierte Interviews mit Vertretern führender Unternehmen unterschiedlicher Branchen statt.
- Weitere Expertenmeinungen aus Gesprächen mit Unternehmens- und Behördenvertretern flossen in die spätere Bewertung ein.
- In Workshops mit Unternehmensvertretern und Studierenden wurden mögliche Angriffsszenarien durchgespielt.
- Mit einer systematischen Internetanalyse wurde ausgewertet, in welchen Kontexten Desinformation bislang in der öffentlichen digitalen Kommunikation diskutiert und bewertet wird.
- Eine Onlinebefragung, an der sich mehr als 100 Personen beteiligten, lieferte ergänzende Informationen.

In der Gesamtheit ergibt sich ein vielschichtiges und doch recht klares Bild der Lage in der deutschen Wirtschaft in Bezug auf die Bedrohung und Positionierung zum Thema Desinformation. Dabei ist hervorzuheben, dass die Befragungen im Rahmen der Studie mit Unternehmensvertretern durchgeführt wurden, die eine hohe **Expertise** besitzen und bei der Aufstellung ihrer Unternehmenssicherheiten zur Speerspitze der deutschen Wirtschaft zählen. Insofern sind deren Hinweise in Bezug auf Bedrohungslage und Abwehrmaßnahmen ohne Zweifel wegweisend. Gleichzeitig ergibt sich bei der Frage nach den bereits ergriffenen Maßnahmen jedoch ein Zerrbild. Ein Großteil der deutschen Unternehmen dürfte bei weitem nicht so gut aufgestellt sein.

Die Studie gibt zunächst eine Einschätzung der aktuellen **Bedrohungslage.** Dazu wurden die in den Interviews genannten Fälle ausgewertet, angereichert durch die Ergebnisse der Onlinebefragung. Darüber hinaus geben die Workshops und Expertengespräche aktuellen Aufschluss darüber, welche weiteren Gefahrenpotenziale Desinformation bildet. Ein zentraler Baustein dieses Kapitels ist die von complexium durchgeführte Digital-Listening-Analyse. Aufgezeigt werden zudem die technischen Möglichkeiten und Werkzeuge der Desinformation.

Es ist Anspruch dieser Studie, nicht nur die Bedrohungslage aufzuzeigen, sondern den Unternehmen auch erste Handlungsempfehlungen und Lösungsstrukturen an die Hand zu geben. Damit soll ein aktiver Beitrag zur Eindämmung dieser neuen Bedrohung geleistet werden.

Im zweiten Abschnitt werden **Angriffsziele** aufgeführt. Dabei wird zunächst erläutert, was heute schon technisch möglich ist, um dann an realen, anonymisierten und fiktiven Fallbeispielen die Bedrohung konkreter zu machen.

Nach den Angriffsszenarien folgt im dritten Abschnitt der **Verteidigungsprozess** – also Gegenmaßnahmen, angefangen von der Prävention bis zur Vorfall-Nachbehandlung.

Schließlich werden in einem **11-Punkte-Plan** die zentralen Handlungsempfehlungen für die Unternehmenssicherheit zusammengefasst.

1. Bedrohungslage

1.1 Diskussion zu „Desinformation“ bisher auf Politik fokussiert

Desinformation ist die gezielte Verbreitung falscher oder irreführender Information. Motivation der Desinformation ist die Beeinflussung der Meinung der Öffentlichkeit, von Gruppen oder Einzelpersonen, um politische oder wirtschaftliche Ziele zu fördern.

Durch diese Bedrohung und ihre technologischen Verstärker wird eine neue Detektionsfähigkeit notwendig, um

- mögliche Bedrohungen durch die Identifikation schwacher Signale frühzeitig zu erkennen und
- die thematischen Kontexte rasch erschließen und einordnen zu können.

Für diese Studie wurde eine entsprechende Lösung genutzt, um die thematischen Kontexte der digitalen Beiträge zum Themenfeld „Desinformation/Fake News/alternative Fakten“ zu erschließen. Das complexium-Entwicklerteam hat zur Erschließung thematisch relevanter Kontexte aus dem Social-Media-Universum das Analyse-Tool GALAXY aufgebaut. Es handelt sich dabei um ein Social-Big-Data-Informationstool, mit dem große Mengen digitaler Inhalte analysiert werden können. GALAXY ermöglicht die inhaltliche Erschließung und Verdichtung von Beiträgen aus Blogs, Foren, Nachrichtenportalen und weiteren Online-Quellen. Signifikante Themen und Diskussionen werden somit nahezu in Echtzeit aus dem digitalen Raum an die Oberfläche gespült.

»Die Digitalisierung macht solche Angriffsszenarien erschwinglich und damit auch für und gegen Unternehmen einsetzbar. Folglich ist ein Einsatz im aggressiven Unternehmenswettbewerb logische Konsequenz.«

Jan Wolter

Im Rahmen der Studie wurden im Sommer/Herbst 2017 über mehrere Wochen hinweg tagesgenau über 100.000 digitale Beiträge durch die Crawler des MATRIX-Systems von complexium aufgenommen und mit GALAXY inhaltlich erschlossen: Blog- und Forenbeiträge, Twitter-Tweets, News-Kommentare, Beiträge in Social Networks.

Zur Erschließung der Inhalte werden computerlinguistische Algorithmen eingesetzt, die die thematischen Schwerpunkte und Auffälligkeiten ohne Vorgabe errechnen. Durch diese innovative Technologie wird eine deutlich bessere Abbildung erreicht, als dies durch ein Abzählen nach vordefinierten Kategorien möglich ist.

Auf diese Weise wird transparent, wie das Thema Desinformation tatsächlich diskutiert wird: Hierbei bewirken die eingesetzten Algorithmen, dass nicht die häufigsten Bezüge herausgestellt, sondern besonders auffällige und neu hinzukommende Kontexte ermittelt werden. Solche Auffälligkeiten gelten als signifikant.

Für jeden Tag wird aus den auftauchenden Begrifflichkeiten mit den höchsten errechneten Signifikanzwerten ein Ranking gebildet, im folgenden Beispiel (Abbildung 1) das Tagesranking für den 10. September:

Abbildung 1:
Tagesgenaues Begriffsranking zu „Desinformation", erstellt mit dem Analyse-Tool GALAXY (Quelle: complexium)

Data for: **Sunday, 10 September 2017**

Emergent Terms | **Term Groups**

Rank Sun Sep 10 2017	Sat Sep 09 2017	Term	Change in rank
1	1	fake	— 0
2	2	cnn	— 0
3	3	fakenews	— 0
4	5	trump	↑ 1
5	4	isis	↓ -1
6	6	rt	— 0
7	7	america	— 0
8	9	people	↑ 1
9	8	hates	↓ -1
10	10	bbc	— 0
11	12	yahoo	↑ 1
12	14	media	↑ 2
13	13	propaganda	— 0
14	16	believe	↑ 2
15	17	myanmar	↑ 2
16	20	president	↑ 4
17	21	video	↑ 4
18	25	irma	↑ 7
19	23	real	↑ 4
20	37	hurricane	↑ 17
21	24	tornado	↑ 3
22	27	stop	↑ 5

Aus der Reihung dieser Tagesrankings ergibt sich das Themenspektrum im Zeitverlauf. Bereits ein schneller Blick zeigt den überwiegend politisch geprägten Kontext. In einigen Fällen zeigen zudem **frühe Signale** das Aufstreben neuer Aspekte im Vorlauf an.

	Sun Sep 17 2017	Mon Sep 18 2017	Tue Sep 19 2017	Wed Sep 20 2017	Thu Sep 21 2017	Fri Sep 22 2017	Sat Sep 23 2017	Sun Sep 24 2017
1	fake	fake	cnn	cnn	fake	fake	fake	fake
2	cnn	cnn	fake	fake	cnn	cnn	cnn	cnn
3	fakenews	fakenews	fakenews	fakenews	fakenews	fakenews	fakenews	trump
4	rt	rt	rt	rt	trump	trump	trump	fakenews
5	reporting	reporting	reporting	reporting	rt	rt	rt	rt
6	real	real	real	real	people	people	people	yahoo
7	realdonaldtrump	realdonaldtrump	realdonaldtrump	realdonaldtrump	isis	alternative	yahoo	people
8	country	sad	country	country	disinformation	isis	alternative	isis
9	sad	country	sad	trump	attack	yahoo	isis	alternative
10	dividing	dividing	dividing	sad	yahoo	president	president	president
11	narratives	narratives	narratives	dividing	network	facts	facts	facts
12	false	false	false	narratives	hybrid	disinformation	bbc	lies
13	gmoneyrainmaker	gmoneyrainmaker	gmoneyrainmaker	false	president	network	afd	bbc
14	trump	trump	trump	gmoneyrainmaker	under	bbc	media	**russia**
15	people	people	people	people	alternative	spreading	network	disinformation
16	story	isis	isis	isis	bbc	truth	disinformation	network
17	isis	network	network	disinformation	media	media	spreading	media
18	happened	facts	president	network	based	afd	truth	going
19	network	media	attack	attack	threats	lie	lies	afd
20	usa	change	disinformation	president	kremlin	lies	deutschland	real
21	seems	disinformation	alternative	hybrid	finland	believe	lie	believe
22	facts	story	change	under	centre	going	going	retweets
23	bag	climate	climate	media	disinforeview	verbreitet	verbreitet	propaganda
24	consequences	alternative	media	alternative	countering	real	**russia**	cukzrlg
25	change	president	lie	based	euvsdisinfo	**russia**	real	far

Abbildung 2:
Begriffsranking zu „Desinformation" im Zeitverlauf, erstellt mit dem Analyse-Tool GALAXY (Quelle: complexium)

Die ersten Plätze im Desinformations-Ranking scheinen von der amerikanischen Präsidentschaft gebucht zu sein. Es zeigt sich aber auch, dass in den letzten Tagen vor der Bundestagswahl die AfD massiv im Kontext Desinformation diskutiert wird. Nach der Wahl nimmt die Häufigkeit des Begriffs „AfD" im Ranking langsam ab.

Inhaltsrelevante Nennungen von Unternehmen, etwa aus dem DAX, kommen über den gesamtem Untersuchungszeitraum in der öffentlichen digitalen Diskussion im Zusammenhang mit Desinformation bis auf sehr vereinzelte Nennungen nicht vor.

Neben den Rankinglisten bietet das Analyse-Tool GALAXY die Möglichkeit einer visuellen Darstellung signifikanter Begriffe im Themenkontext. Algorithmen der Social Network Analysis (SNA) bilden aus den identifizierten Begriffen ein semantisches Netz: Diese Themenlandkarte macht deutlich, welche Aspekte häufig in einem Zusammenhang aufgeworfen werden.

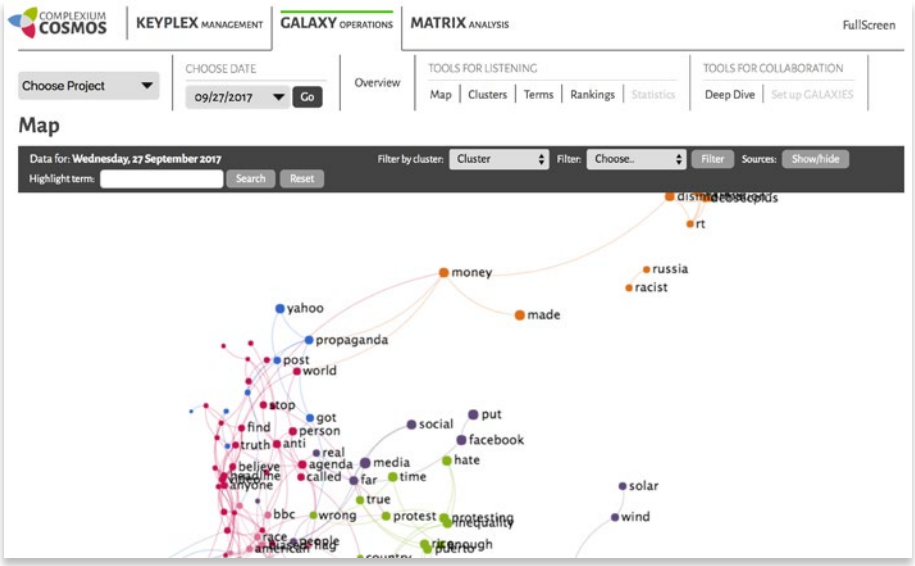


Abbildung 3:
Visuelle Darstellung signifikanter Begriffe aus der Nutzerdiskussion als semantisches Netz, erstellt mit dem Analyse-Tool GALAXY-Map (Quelle: complexium)

Hierbei markieren die Farben einzelne Inhaltscluster: Begrifflichkeiten, die untereinander stärker vernetzt sind als mit dem Rest der Inhalte aus dem aktuellen Diskussionsspektrum. In der Soziologie würde man von „Cliquen“ sprechen.

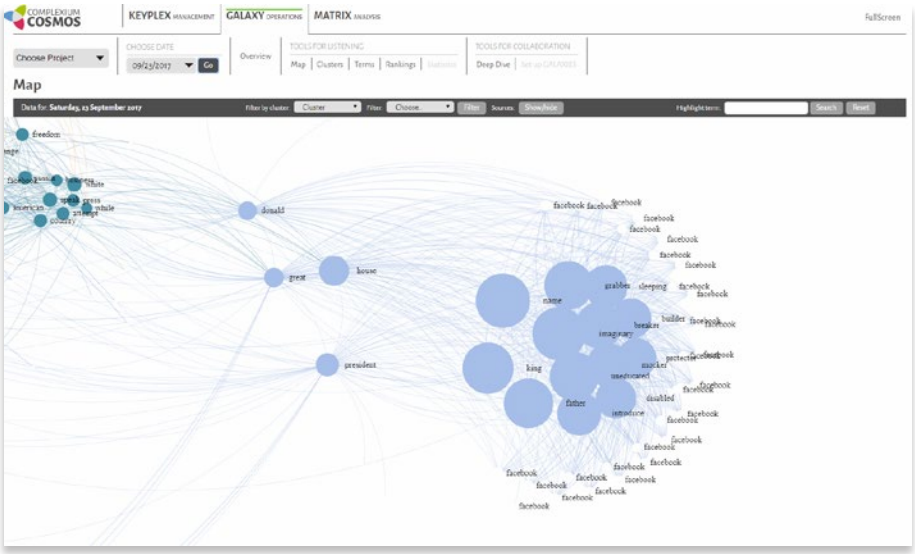


Abbildung 4:
Ausschnitt eines Inhaltsclusters zur visuellen Darstellung thematisch vernetzter Begriffe aus der Nutzerdiskussion, erstellt mit dem Analyse-Tool GALAXY-Map (Quelle: complexium)

Erwähnt werden soll an dieser Stelle noch, dass ein Klick auf einen farblichen Punkt zu den darunterliegenden Zitatstellen und Quellen (Links) führt. Die beiden folgenden Abbildungen zeigen beispielhaft Treffer zu „Macron“ und „AfD“ im Kontext Desinformation.

Abbildung 5:
Beispiel: Deep Dive zu „Macron“
(Quelle: complexium)

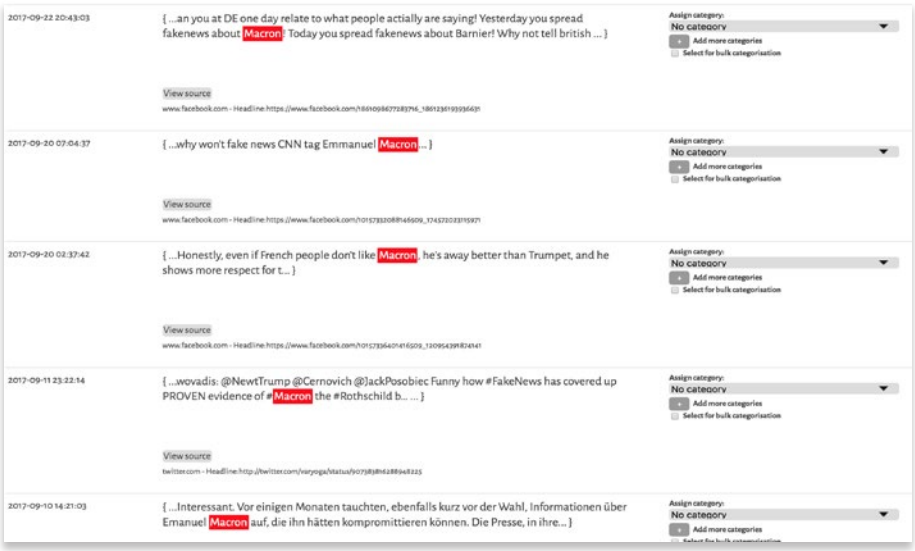
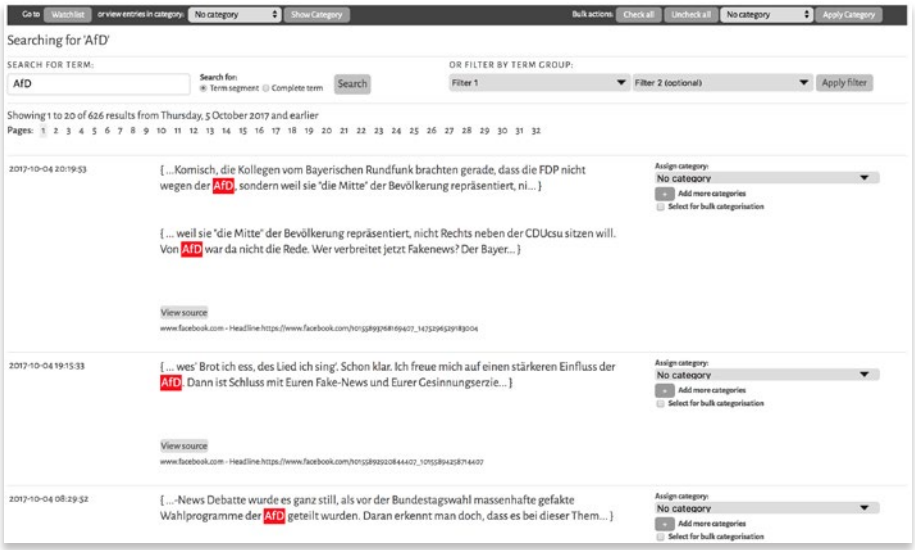
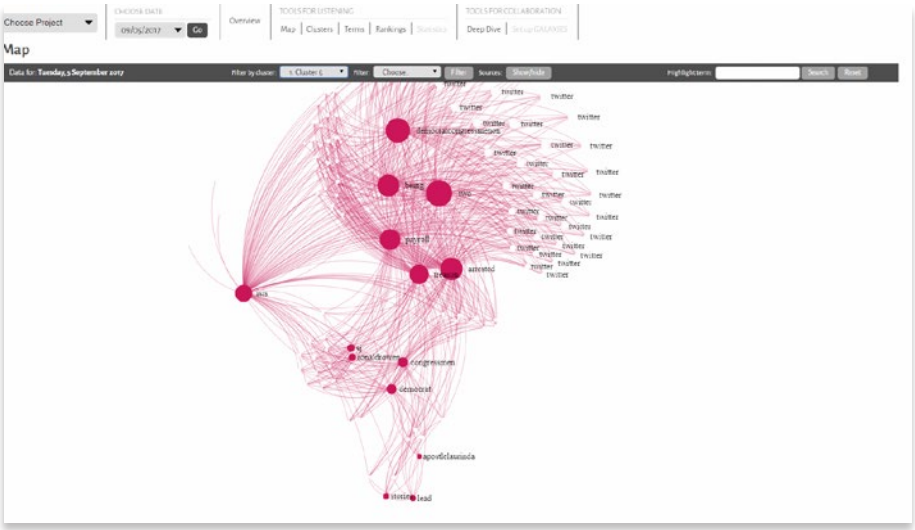


Abbildung 6:
Beispiel: Deep Dive zu „AfD“
(Quelle: complexium)



Werden auf einer zusätzlichen Ebene nun diese Quellen eingeblendet, dann tritt die große Verbreitungskraft insbesondere von Twitter zutage. Die folgende Abbildung illustriert die Themenverstärkung durch Twitter-Netzwerke.

Abbildung 7:
Themenverstärkung durch Twitter-Netzwerke – Detailansicht eines Inhaltsclusters, erstellt mit dem Analyse-Tool GALAXY-Map (Quelle: complexium)



Ein erstes Zwischenfazit ergibt sich.

- Zum einen zeigt sich, dass zumindest im breiten digitalen Diskurs das Thema Desinformation noch rein politisch verankert ist.
- Zum anderen soll hier bereits angedeutet werden, dass es technische Lösungen für unternehmensrelevante Sicherheitsbereiche gibt, die es ermöglichen, die öffentliche digitale Diskussion – etwa zum eigenen Unternehmen, seinen Liegenschafen und exponierten Persönlichkeiten – kontinuierlich im Blick zu behalten. Durch die hypothesenfreie Analyse der aktuellen digitalen Diskussion kann das Risiko von Überraschungen deutlich reduziert werden. Ein solches Digital Listening kann Desinformationskampagnen, aber auch andere Bedrohungen frühzeitig identifizieren – die Corporate Security kommt vor die Lage.

1.2 Fake News im Bundestagswahlkampf 2017

Gastbeitrag von Dr. Stefan Hennewig

CDU Bundesgeschäftsstelle

Im Vorfeld des Bundestagswahlkampfes nahm die Sorge um Fake News in der öffentlichen Debatte breiten Raum ein. In den Medien war das Thema sehr präsent. Im Spätsommer 2016 konnte man den Eindruck gewinnen, Fake News und Bots wären die entscheidende Gefahr für Demokratie und Gesellschaft in Deutschland. Die vorangegangenen Wahlkämpfe in Frankreich und insbesondere in den USA boten in der Tat einige Anhaltspunkte, um zu solch einer Einschätzung zu kommen.

Gleichwohl gab es aber auch zu diesem Zeitpunkt schon differenzierte Betrachtungen. Ein ganz wesentlicher Umstand: Die Welle von Fake News im Präsidentschaftswahlkampf der USA hatte häufig gar keinen politischen Hintergrund, sondern folgte allein monetären Interessen. Es ging nicht um die Verbreitung einer bestimmten politischen Botschaft. Fake News waren nur ein Vehikel für gewinnorientiertes Click-Farming. Durch möglichst reißerische Überschriften versuchten Seitenbetreiber, Besucher auf ihre Internetseiten zu locken, um so von Werbeeinnahmen aus den Netzwerken von Facebook und Google zu profitieren. In einer gut recherchierten Geschichte in der ZEIT (Quelle: ZEIT ONLINE: Ulrich Laduner, Fake News: Stadt der Lügner: http://www.zeit.de/2016/52/fake-news-hersteller-unternehmen-mazedonien) ist zum Beispiel von der mazedonischen Kleinstadt Veles zu lesen. Allein dort waren in der Hochphase 140 Internetseiten mit Falschnachrichten zum amerikanischen Wahlkampf registriert. Ein großer Teil der ansonsten arbeitslosen Einwohner finanzierte auf diesem Weg den eigenen Lebensunterhalt. Vor derartigen Entwicklungen schützt Deutschland zum Glück weitgehend die Sprachbarriere.

Daneben bleibt aber auch hier der Teil der politisch motivierten und gestreuten Fake News. Die Rolle Russlands in diesem Zusammenhang ist mit Bezug auf den US-Wahlkampf in den vergangenen Monaten ja bereits intensiv beleuchtet worden. Die Herkunft der im Bundestagswahlkampf verbreiteten Fake News ist teilweise unklar. Dies gilt auch für einen der weiter verbreiteten Fakes aus den letzten Wahlkampfwochen. Der Titel des CDU-Wahlprogramms, der auch als Kampagnen-Claim diente, war: „Für ein Deutschland, in dem wir gut und gerne leben." Der Claim wurde in einer Fotomontage verarbeitet, die beweisen sollte, dass der Spruch bereits für den 11. SED-Parteitag Verwendung gefunden habe. Die Fälschung wurde von politischen Mitbewerbern der CDU – verbunden mit viel Häme – verbreitet.

Die Fälschung wurde am 29. August 2017 gegen Mittag auf Facebook gepostet und fand sehr schnell Verbreitung. Neben dem softwaregestützten Social-Media-Monitoring verfügt die CDU über eine stabile Online-Community – alleine auf Facebook etwa 3.000 Menschen –, die in derartigen Fällen schnell für die Weiterleitung der Informationen an die zuständigen Stellen sorgt. Ersten Mitgliedern dieses Netzwerkes fiel das gefälschte Foto gut zwei Stunden nach der Veröffentlichung auf, sodass schnell reagiert werden konnte.

Das initiale Posting wurde gelöscht und auch die ersten beiden Verbreitungsseiten auf Facebook und Twitter korrigierten ihre Einträge schnell. Dieses rasche Vorgehen gegen die „Hubs der ersten Stunde“ ist die einzige Möglichkeit, Fake News einigermaßen in den Griff zu bekommen.

Abbildung 8:
Fake News im Bundestagswahlkampf 2017
(Quelle: CDU Bundesgeschäftsstelle)

Ergänzend muss auf allen eigenen Kanälen für die korrekte Darstellung des Sachverhaltes gesorgt werden. Sehr hilfreich im konkreten Fall war es auch, dass sowohl Buzzfeed.de wie auch Mimikama.at den Fake als solchen identifiziert und richtiggestellt haben.

Eine wichtige Rolle für die vom Fake betroffene Institution ist es dabei, das angesammelte Wissen über den Fake zu kuratieren und den Multiplikatoren zur Verfügung zu stellen. Primäres Ziel sollte es auch immer sein, möglichst viele der Fake-Einträge löschen zu lassen und nicht nur in den Kommentaren eine Klarstellung zu posten, da die Reichweiten dort um ein Vielfaches geringer sind. Auch hierfür sollten aber Ressourcen vorgehalten werden.

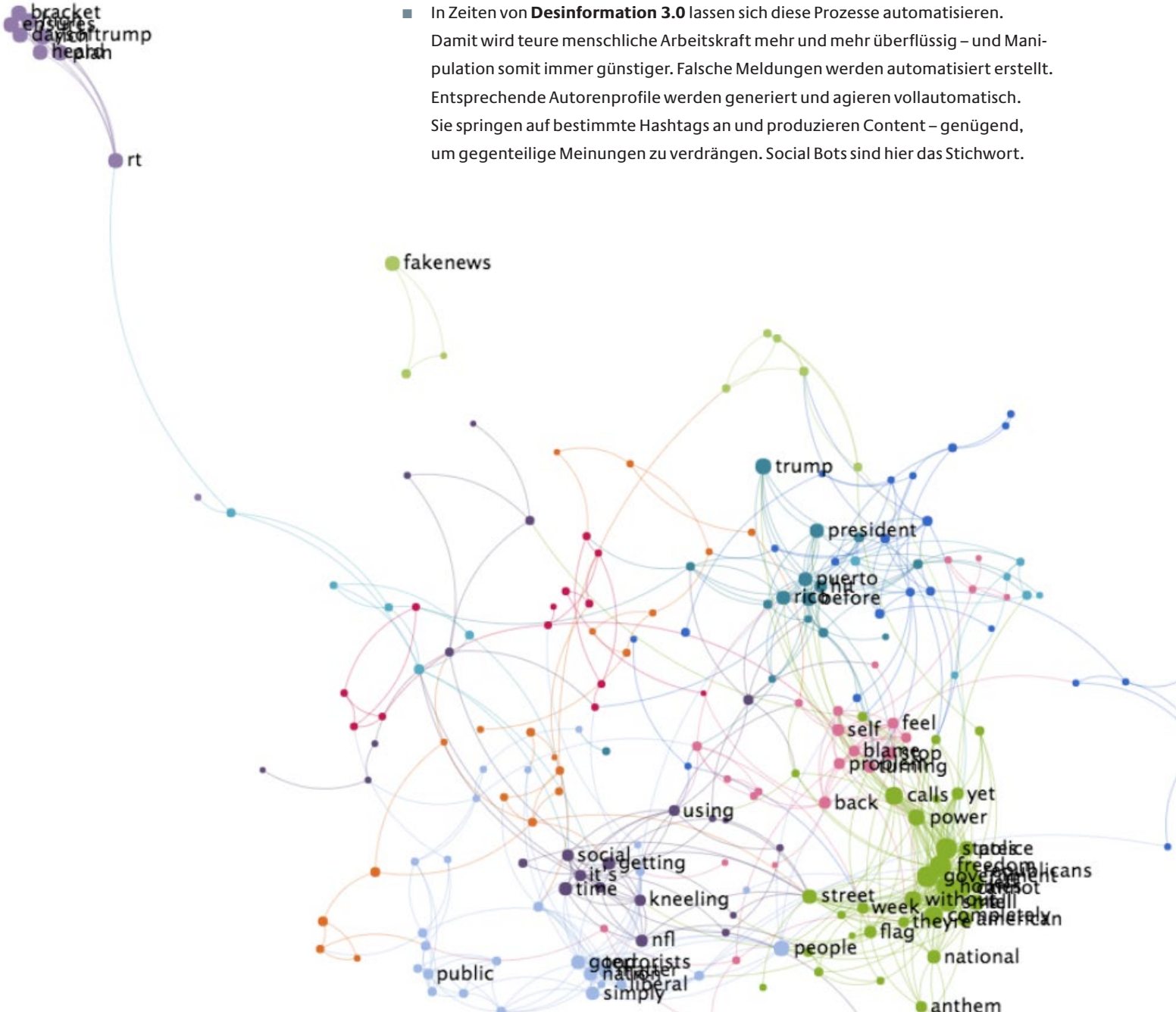
Und: Nicht zu früh mit der Richtigstellung nachlassen. Auch als Spiegel und Tagesschau-Online in den folgenden Tagen den Fake als solchen veröffentlicht haben, haben wir weiterhin in Social Media aktiv klargestellt, was Original und was Fälschung ist.

Abbildung 9:
Beitrag zu Fake News im Bundestagswahlkampf 2017
(Quelle: CDU Bundesgeschäftsstelle)

1.3 Technologie treibt die Entwicklung

Desinformation gab es in Form von übler Nachrede, dem Streuen von Gerüchten oder gezielter Propaganda schon immer. Doch mit dem zunehmenden Gewicht von Social Media ergeben sich hier ganz andere Möglichkeiten.

- Während in Zeiten von **Desinformation 2.0** Menschen dafür bezahlt wurden, im Internet böse Kommentare zu schreiben, um Gegner niederzumachen – die Trolle – , oder positive Bewertungen abzugeben, um Produkte oder Meinungen zu loben – die Influencer –, ist die Technik inzwischen deutlich weiter.
- In Zeiten von **Desinformation 3.0** lassen sich diese Prozesse automatisieren. Damit wird teure menschliche Arbeitskraft mehr und mehr überflüssig – und Manipulation somit immer günstiger. Falsche Meldungen werden automatisiert erstellt. Entsprechende Autorenprofile werden generiert und agieren vollautomatisch. Sie springen auf bestimmte Hashtags an und produzieren Content – genügend, um gegenteilige Meinungen zu verdrängen. Social Bots sind hier das Stichwort.



- Auf der nächsten Stufe **Desinformation 4.0** werden diese Angriffe noch ausgefeilter: Personalisierung und Machine Learning kommen hinzu. Über automatisierte Analysen von Profilen (Facebook, XING, Instagram etc.) mittels Algorithmen mit künstlicher Intelligenz können Persönlichkeitsprofile mit extrem hoher Genauigkeit erstellt werden. Heute sind Szenarien denkbar, in denen personalisierte Bot-Schwärme gezielt Menschen oder Menschengruppen beeinflussen. Bereits 300 Likes auf Facebook reichen aus, damit ein Algorithmus ein genaueres Bild von einem Menschen erhält, als es der Ehepartner oder beste Freund zeichnen könnte (Quelle: Computer-based personality judgments are more accurate than those made by humans; by W. Youyou, M. Kosinski, D. Stillwell, Proceedings of the National Academy of Sciences [PNAS], 2015).

Der Automatisierungsgrad ist inzwischen so hoch, dass Menschen nur noch für das Schreiben eines Gesamtkonzepts und Drehbuchs gebraucht werden – beispielsweise für besonders zugespitzte Dialogsequenzen, die der Algorithmus an einen Menschen zurückübergibt – sowie für bestimmte High-End-Lösungen, wie der Entwicklung ganzer Homepages mit komplett falschen Nachrichten. So werden etwa vermeintliche Nachrichtenmagazine aus der Taufe gehoben, die ihre frei erfundenen Meldungen in die sogenannten sozialen Medien streuen. **Mit Desinformation wird nicht nur manipuliert, sondern auch viel Geld verdient. Je zugespitzter ein gefälschter Artikel ist, desto eher wird er geklickt und damit wirtschaftlicher Gewinn über Werbung erzielt.**

Der wachsende Automatisierungsgrad macht Desinformationskampagnen künftig immer billiger. Der technische Fortschritt macht sie auch einfacher anwendbar. Desinformation wird mit vergleichsweise geringem technischem Sachverstand und geringem Mitteleinsatz möglich.

Wer Geld und Ressourcen zur Verfügung hat, kann mittelständische Unternehmen ohne ausgeprägte Corporate Security durch Desinformationskampagnen leicht in ernsthafte Schwierigkeiten bringen. Und auch große Konzerne können durch Desinformation in Bedrängnis gebracht werden.

Um Desinformation zu verbreiten, muss man keine Systeme hacken, benötigt kaum IT-Kenntnisse oder sonstiges Fachwissen. Man braucht nicht einzubrechen oder etwas zu stehlen. Es bedarf mitunter überhaupt keines Kontaktes mit dem Ziel. Die Hemmschwelle ist extrem gering, da viele sich nicht einmal einer Straftat bewusst sind und das Entdeckungsrisiko (noch) sehr niedrig ist.

1.4 Auch Unternehmen im Fokus von Desinformationsangriffen

Das Wort des Jahres 2016 bringt es auf den Punkt: **„postfaktisch“**. Wir befinden uns im postfaktischen Zeitalter. Doch das Thema Desinformation wurde bislang meist nur im Kontext von Politik und Wahlen als Herausforderung gesehen. Langsam wird deutlich, dass auch Unternehmen einer Bedrohung durch Desinformation gegenüberstehen: Dass es sich bei all dem nicht bloß um graue Theorie handelt, sondern Unternehmen sich mit Desinformation auseinandersetzen müssen, zeigen die im Rahmen dieser Studie durchgeführten Interviews wie auch die Onlinebefragung.

In den Interviews wurde außerdem deutlich, dass Unternehmen zwar Opfer von Desinformation(skampagnen) wurden, dabei mitunter aber gar nicht das eigentliche Ziel waren – sondern vielmehr Mittel zum Zweck.

Hier ist auch ein kritischer Blick auf die Medien und Nichtregierungsorganisationen (NGO) notwendig. So geraten Unternehmen schnell in den Fokus der Berichterstattung mit einer skandalisierenden oder zumindest dramatisierenden Note. Handfeste Fakten werden dabei schnell zur Nebensache. Auch Aktivistengruppen oder NGOs haben ein Interesse daran, Sachverhalte in ihrem Sinne darzustellen. Sie sind nicht objektiv und verfolgen oftmals selbst wirtschaftliche Interessen. Um Spendengelder zu generieren, helfen dramatisierte Zahlen oder Bilder mehr als die manchmal vielleicht recht nüchterne Wahrheit.

In diesem Kontext bietet jeder große, bekannte Konzern mehr Reibungsfläche und garantiert größere Aufmerksamkeit als ein kleinerer Zulieferer oder Abnehmer, der vielleicht der eigentliche Schuldige an einem Vorfall ist. So werden Geschichten geschrieben, die zwar sehr nah der Wahrheit sein mögen, aber am Kern der Sache dann doch vorbeigehen – zum Schaden schuldloser Unternehmen. Für eine höhere Auflage oder mehr Spendengelder werden Konzerne etwa zu Lieferanten des IS oder zu Verantwortlichen für Umweltverschmutzungen oder Unfälle, bei denen zwar ihre Produkte im Spiel waren, die Verantwortung jedoch bei jemand anderem lag.

Gerade große NGOs sind sehr medienaffin, bestens in den sozialen Medien vernetzt und genießen dort eine hohe Reputation. Die Auswirkungen solcher „scripted reality“ bekommen damit eine größere Dramatik als noch vor wenigen Jahren.

Mit der Vielzahl unterschiedlicher Meinungen und vermeintlicher Fakten entsteht auch eine gewisse „Faktenbeliebigkeit“. Gerade für Anbieter, die sich beispielsweise durch hohe Umwelt- oder Arbeitsstandards abheben möchten und dafür auch höhere Preise verlangen, entsteht eine besondere Gefahr. Werden entsprechende Zweifel gesät, kann beim Kunden schnell ein Gefühl entstehen, dass „die“ sowieso alle wahlweise „betrügen“, „ausbeuten“, „die Umwelt vergiften“ etc. – womit dann der Preis das einzige Kriterium bleibt, was für den Kunden real messbar und glaubhaft und damit auch die einzige Richtschnur ist.

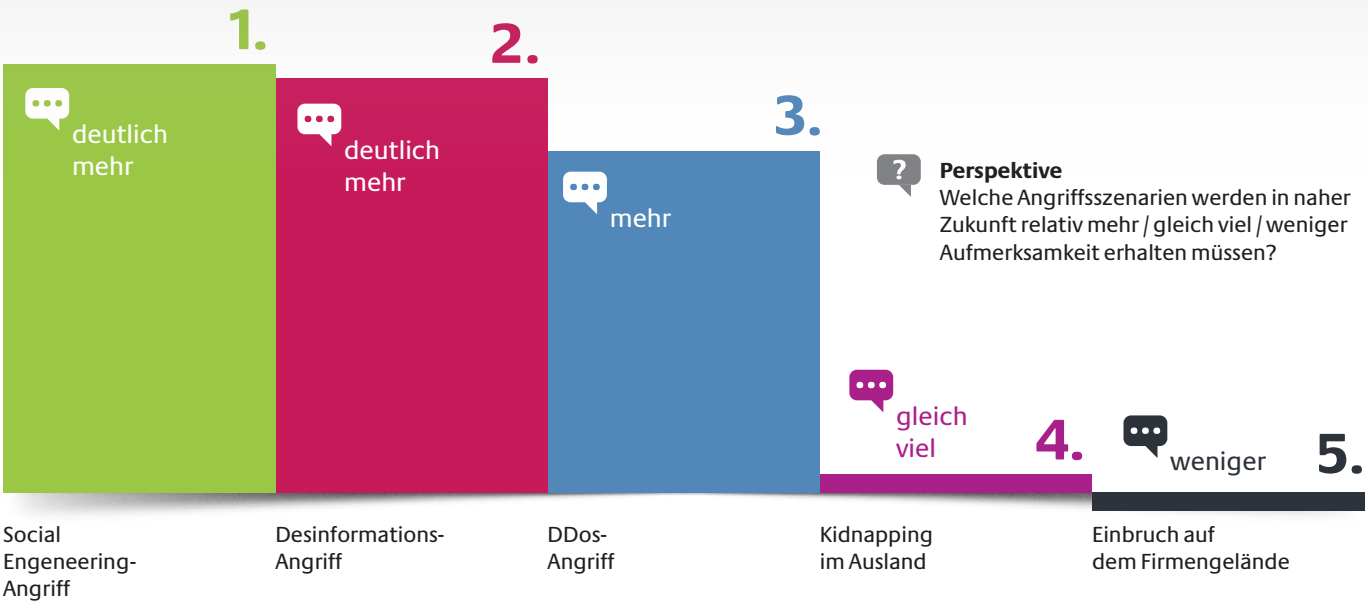


Abbildung 10:
Künftige Angriffsszenarien im Aufmerksamkeitsranking (Quelle: Onlinebefragung im Rahmen der Studie)

Aktivisten, NGOs oder Medien, deren eigentliches Ziel es sein mag, für eine „bessere Welt" zu kämpfen, befeuern dieses Misstrauen durch eine ungenaue Berichterstattung und erreichen damit das genaue Gegenteil. Verunsicherte oder desillusionierte Verbraucher wenden sich von denen ab, die eigentlich hohe Umwelt- oder Ethikstandards verfolgen.

Unternehmen können aber auch ganz gezielt mit einer auf sie ausgerichteten Desinformationskampagne angegriffen werden. Es existieren praktische Beispiele, die belegen, dass damit Unternehmensentscheidungen direkt beeinflussbar sind und sich Auswirkungen auf die Geschäftsentwicklung ergeben.

Größere Desinformationskampagnen sind im Rahmen der Studie von Unternehmensseite kaum genannt worden. Gleichwohl sind solche Szenarien auch in größerem Umfang denkbar. Nicht nur der US-Wahlkampf hat gezeigt, wie leistungsfähig die Waffe Desinformation sein kann. Es wäre töricht anzunehmen, sie würde nicht auch gegen Unternehmen in voller Stärke eingesetzt.

Ob von Konkurrenten, ehemaligen oder frustrierten Mitarbeitern, Kriminellen, die beispielsweise auf fallende Aktienkurse setzen, oder von fremden Mächten – die Zahl möglicher Angreifer ist groß. Und die Technik entwickelt sich weiter.

Die im Rahmen dieser Studie durchgeführten Interviews, Expertengespräche und die Onlinebefragung zur Studie zeigen, dass Unternehmen dem Schutz vor Desinformationsangriffen eine deutlich höhere Priorität als bislang beimessen wollen.

Fast 90 Prozent der befragten Unternehmen sind davon überzeugt, dass in naher Zukunft Desinformationsangriffen eine deutlich erhöhte Aufmerksamkeit zukommen muss.

Desinformation wird zu einer der zentralen Bedrohungen des 21. Jahrhunderts für deutsche Unternehmen.

1.5 Sicherheitsvisier mit (nun) vier Quadranten

Desinformation kann als Schattenseite der Digitalisierung der öffentlichen Kommunikation gesehen werden. So hat nicht nur, aber auch eine Beeinflussung unverbundener digitaler Räume Einfluss auf die Sicherheit.

Ein neuer Quadrant im Sicherheitsvisier gewinnt an Bedeutung. Unternehmen müssen entsprechende Prozesse in ihrer digitalen Transformation berücksichtigen. Früherkennung wird noch wichtiger:

Ein hoher Bedrohungslevel entsteht durch Identitätsdiebstahl/-design, Social Bots (und Botnets) und die Nutzung der Netzwerkdynamik: Angreifer streuen Fake News oder erstellen Bots (auch in Wartestellung), Bots initiieren oder verstärken Beiträge, normale Nutzer liken/sharen, Medien greifen Trending Topics auf – Wahrnehmungen und Entscheidungsprozesse werden verändert.

Die Unternehmenssicherheit kann jedoch durch Verbesserung der Früherkennung ebenso deutliche Mehrwerte aus der Digitalisierung ziehen: Digitale Signale zu bedrohlichen Entwicklungen sowie zu Vorlauf, Vorbereitung, Akutphase von sicherheitsrelevanten Aktivitäten können frühzeitig aufgenommen werden. Eine neue Art von Cyber-Lage entsteht.

Damit wird eine neue Detektionsfähigkeit gestützt, die den notwendigen Verteidigungsprozess auf eine valide Grundlage stellt: Digitale Früherkennung identifiziert direkte und indirekte Bedrohungen und verlängert die Vorwarnzeit.

Als Methode wird **Digital Listening** genutzt, um Einblicke in die Vorhaben und Vorgehensweisen auf Seiten von kritischer Öffentlichkeit, Aktivismus und Gegnerschaften zu gewinnen. Filter und Algorithmen machen die digitale Beitragsflut beherrschbar. Analysten können Relevantes identifizieren, in einen Kontext setzen und bewerten.

Digitale Früherkennung kann auch die Detektion von Desinformationsangriffen leisten – wichtig ist die Einbettung in durchgängige Prozessstrukturen.

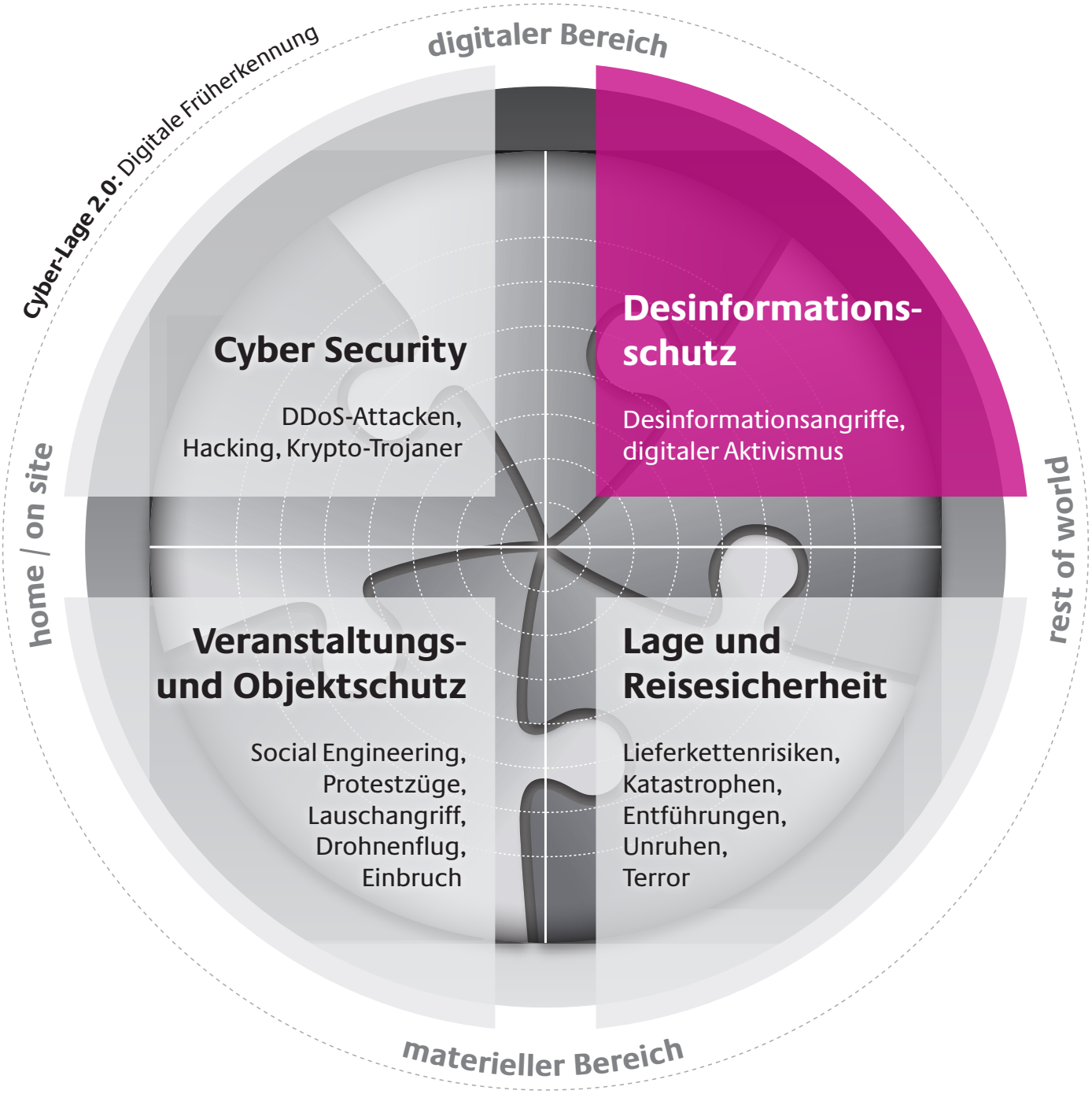


Abbildung 11:
Sicherheitsvisier mit vier Quadranten (Quelle: ASW Bundesverband und complexium)

2. Technologie der Angreifer und Verteidiger

In der Arena des wirtschaftlichen Geschehens müssen wir uns vom Denkmodell einer breiten Wählermanipulation durch Desinformation lösen. Unternehmen bieten sehr facettenreiche Angriffspunkte: Der Angreifer kann, muss aber nicht auf die Meinungsbeeinflussung der breiten Öffentlichkeit zielen.

Viel wirkungsvoller können einzelne Meinungsfelder angegriffen werden, etwa bezogen auf die Wahrnehmung bestimmter Produkte, auf das Arbeitgeberbild, die Integrität des Unternehmens oder die Nachhaltigkeit seiner Zulieferer.

Natürlich wird dabei kaum jemand bewusste Desinformation unter seinem realen Namen betreiben: Der digitale Raum ermöglicht es Akteuren aber, anonyme oder pseudonyme Beiträge zu verfassen. Ebenso ist es hinreichend einfach, sich eine falsche Identität zu entwerfen.

2.1 Desinformationsdreieck aus Identität, Umfang und Steuerung

Identität ist der erste Aspekt in der strukturierten Darstellung dieser neuen Bedrohungstechnologie. Desinformation wird durch unechte Benutzerkonten vorgetragen: Solche Profile werden Sockenpuppen genannt. Die wahre Absicht, das wahre Gesicht ist getarnt und unauffällig.

Digitale Akteure können sich fiktiver oder falscher (Fake) Identitäten bedienen:

- **Identitätsdesign** (z.B. der Fall der Kunstfigur „Robin Sage“) oder
- **Identitätsdiebstahl** (temporäre Übernahme von digitalen Profilen).

Jede vorschnelle Verlinkung bei einer digitalen Freundschaftsanfrage stärkt die Legende, verschafft der Sockenpuppe positive Netzeffekte. Schon einfache Checks können das Risiko reduzieren, sie unterbleiben jedoch zumeist.

Social Engineering bezeichnet das Vorgehensmuster, um mit solchen unechten Identitäten unter Erzeugung von Zeitdruck und Ausnutzung von Hilfsbereitschaft einen realen oder digitalen Zugang zu internen Informationen zu erhalten.

Wenn Ihr Gegner nur eine einzige Person mit Verständnis für soziale Netzwerke ist, dann ist die Informationssicherheit Ihres Unternehmens bereits bedroht.

Dieses Grundmuster lässt sich nun im **Umfang** multiplizieren:

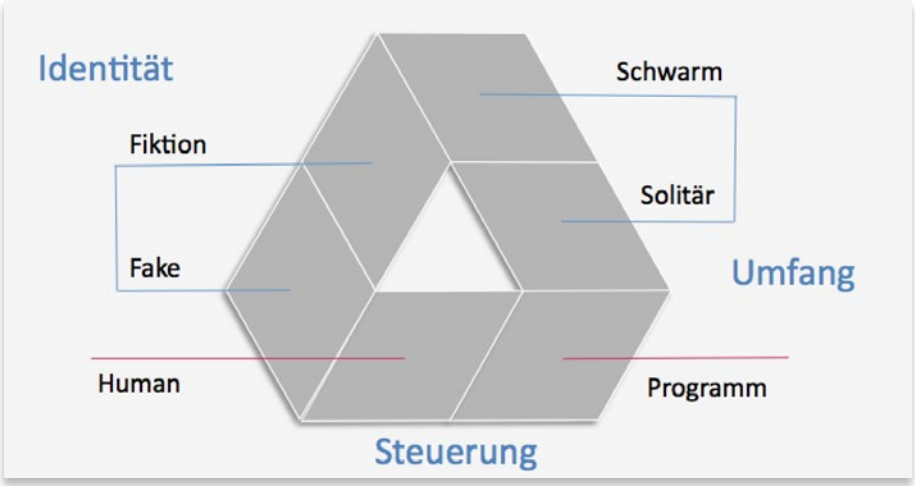
- **Solitäre** zielen auf einzelne oder wenige Zielpersonen.
- **Schwärme** zielen über Meinungs(trug)bilder auf die jeweilige Öffentlichkeit im Meinungsfeld.

Schwärme können in ganz unterschiedlichen Größenordnungen auftauchen: Vermögende Privatpersonen mögen einen „Small-Scale-Fanclub“ beschäftigen, staatliche Einrichtungen können eine „Large-Scale-Troll-Army“ unterhalten. Letztere stellt einen Aspekt des Information Warfare dar. In vielen Quellen, die russische Aktivitäten beschreiben, wird eine staatlich geführte **„digitale Infanterie“** umrissen. Es werden Ziele wie die öffentliche Meinung in Finnland oder der Ukraine genannt.

Wenn der Gegner eine Gruppe von Akteuren (Sockenpuppen) steuert, dann kann ein Meinungsbild/-umfeld wirksam beeinflusst werden.

Zielgerichtete Desinformation setzt **Steuerung** voraus. Aggressoren können diese Waffe effizient einsetzen, wenn sich sehr viele Sockenpuppen digital steuern lassen, sich reale Dialogpartner effektiv nicht daran stören und die Fake News sogar weiterverbreiten.

Abbildung 12:
Dreieck der Desinformation
(Quelle: complexium)



Vor 50 Jahren setzte Joseph Weizenbaum erstmals ein Softwareprogramm namens ELIZA auf den Turing-Test an: Können Menschen unterscheiden, ob sie mit Mensch oder Maschine kommunizieren? Der Turing-Test postulierte, dass Algorithmen erst dann als intelligent gelten sollten, wenn ein menschlicher Gesprächspartner nicht mehr unterscheiden könne, ob er sich mit seinesgleichen oder einem programmierten Regelwerk unterhält. Dieser Test blieb bisher weitestgehend erfolglos.

Am 12. April 2016 öffnete Facebook seinen Messenger für Chatbots. Menschliche Nutzer können nun ihre Fragen, etwa in Bezug auf einen Arbeitgeber oder seine offenen Stellen, direkt – in einer bestimmten Notation – im Messenger stellen. Künstliche Intelligenz verbunden mit automatisierter Internetsuche (Information Retrieval) liefert im Idealfall die Antworten. Siri und Amazon Echo sollten folgen. Der Turing-Test ist hinfällig geworden: Menschen stört es nicht mehr, mit Algorithmen zu parlieren.

2.2 Angriff durch digitale Infanterie

2.2.1 Digitalisierung der Meinungsmache – Bots, Bot-Netze, Algorithmen

Bots sind eine überaus wichtige Facette für die Bedrohung durch Desinformation. **Bots ...**

- **befördern die Digitalisierung der Desinformation, schaffen dadurch ein neuartiges Bedrohungslevel (über die klassische Rufschädigung und Propaganda hinaus) und**
- **erfordern als Konsequenz die Digitalisierung der eigenen Früherkennung.**

Durch die Digitalisierung steigen einerseits die Steuerbarkeit und damit der potenzielle Umfang von Desinformationsangriffen. Andererseits sinkt das dafür notwendige Budget: Folglich bedienen sich auch nichtstaatliche Akteure, etwa aggressive Unternehmen im Wettbewerb, zunehmend dieser Angriffsform.

Bots können nicht denken: Es handelt sich schlicht um Software-Automaten, die einfachen Wenn-Dann-Regeln gehorchen. Beispielsweise können sie beim Auftauchen vorher definierter Begriffe einen Twitter-Tweet weiterverbreiten oder einen Facebook-Beitrag liken. Bots können so programmiert werden, dass sie auf Beiträge von anderen Nutzern reagieren.

Wenn A, dann Aktion B. Social Bots simulieren menschliche Aktivitäten auf verschiedenen Social Media-Plattformen und sind Mittel zum Zweck. Mögliche Aufgaben von Social Bots sind:

- Liken (Favorisieren) und Sharen (Teilen) von Facebook-Beiträgen
- Retweeten (Weiterverbreiten) von Twitter-Nachrichten
- Standardisiertes Kommentieren von Beiträgen
- Folgen von anderen Nutzern, um deren Gewicht zu steigern
- Aufgreifen von populären Hashtags.

Bots werden von Menschen entworfen und geschrieben. Hierzu ist längst kein Informatikstudium mehr notwendig. Es gibt kostenlose und frei verfügbare Service-Plattformen im Internet, auf denen jeder Nutzer innerhalb von 15 Minuten einen Bot zusammenbauen kann. Dies ist inzwischen Allgemeingut, kein Spezialistentum mehr.

Ein einzelner Bot hat jedoch nur einen begrenzten Effekt. Erst das Zusammenspiel von sehr vielen solcher Regelwerke erzielt eine deutliche Wirkung und kann etwa das wahrnehmbare Meinungsbild für eine umrissene Zielgruppe beeinflussen oder gar gestalten.

Man spricht hier von Bot-Netzen, in denen mitunter tausende Bots zusammenwirken. Das sogenannte „Star Wars"-Botnet hatte über 350.000 einzelne Bots. Damit lassen sich die „Trending Topics" bei Twitter beeinflussen. Aber selbst mit einer dreistelligen Anzahl von Bots lassen sich Effekte etwa im Wahlkampf erzielen. Bei der Meinungsmache gegen Unternehmen sind die notwendigen Größenordnungen deutlich geringer.

Im Schwarm werden Bots damit zum Problem. Die Forschung im Bereich der Schwarmintelligenz zeigt, dass aus dem Zusammenwirken einfach strukturierter Akteure ein komplexes Gesamtverhalten entstehen kann: So lässt sich mit einem Set aus drei einfachen Regeln das Verhalten eines Vogelschwarms oder von Passanten in der Fußgängerzone simulieren. Komplexes Verhalten zeichnet sich dadurch aus, dass es adaptiv auf externe Einflüsse oder Änderungen reagieren kann.

Mit Fake-Accounts werden nicht-menschliche Profile angelegt, die programmiert sind, sich automatisiert an Diskussionen zu beteiligen oder Informationen zu verbreiten, um einen bestimmten Zweck zu erfüllen: zum Beispiel Meinungsbeeinflussung oder Diskreditierung.

Wenn Ihr Gegner Bots gegen Sie einsetzt, dann sollten Sie die Fähigkeiten zur Prävention und Detektion bereits breit in der Organisation verinnerlicht haben: Sie können massiv unter Stress gesetzt werden.

Bots haben massiven Einfluss darauf, wie Menschen nach Informationen suchen und kommunizieren. Durch ausgefeilte Steuerung „kennen" sie ihre menschlichen Dialogpartner und können profilkonform reagieren. Die Wirkung steigt auf eine weitere Stufe.

Algorithmen können anhand verfügbarer Profildaten (Likes, Bilder etc.) die Zielpersonen nach Persönlichkeitsmerkmalen und Präferenzen kategorisieren – wenngleich der aktuelle Nutzen dieser Möglichkeiten mitunter aus Vermarktungsgründen überhöht wird. Gleichwohl stehen wir hier in der Frühphase einer Entwicklung, die immer passgenauere und damit wirkungsvollere Ansprachen durch programmierte Bots hervorbringen wird.
Im Digitalraum und auf der Straße:

Es sind diese Algorithmen und Methoden, die auch digitale Werbedisplays in der Fußgängerzone in die Lage versetzen, für jeden stehenbleibenden Passanten abgestimmt auf seine aktuelle Emotion, seine Like-Historie und wahrscheinliche sexuelle Orientierung passende Angebote individuell zu selektieren und zu präsentieren.

2.2.2 Mechanik des Angriffs

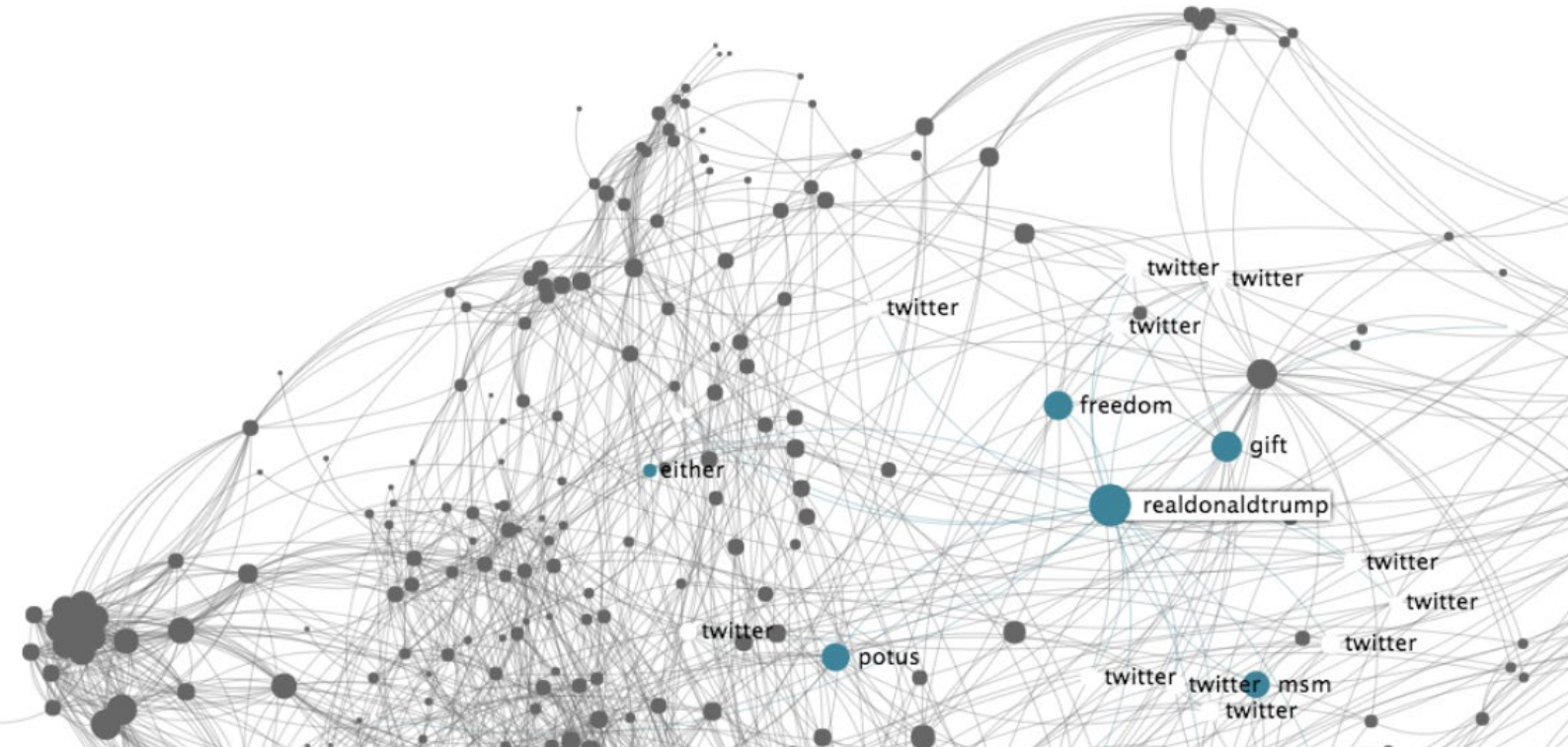
Fake News sind selten aus der Luft gegriffen. Sie müssen grundsätzlich glaubhaft sein und meist gibt es Hinweise oder Behauptungen, auf die referenziert werden kann. So kann unterstellt werden, dass Angreifer auf einen passenden Anlass – etwa einen Unfall mit einem Produkt des Zielunternehmens – warten, um dieses Thema dann aufzunehmen, für die eigenen Zwecke zu verzerren und in der Folge massiv zu multiplizieren.

Die erste Phase der Verbreitung kann durch Bots unterstützt werden. Auf diese Weise wird die Aufmerksamkeit anderer Nutzer erregt, die die Desinformation weiter teilen und sogar zum Überspringen in den Bereich der klassischen Medien tragen können.

Hinter Desinformationsangriffen stehen Menschen.

- Wenn diese die Möglichkeiten im Social Web für Desinformationsangriffe nutzen, dann haben sie einen mächtigen Hebel.
- Wenn sie zudem nicht nur auf das Lancieren einer einzigen Falschmeldung zielen, sondern einen mehrstufigen Angriff orchestriert haben, dann hat das Zielunternehmen ein großes Problem.
- Ein Angreifer kann die Wirkung der Desinformation weiter steigern, wenn er sich in seinem Drehbuch nicht auf deren Verbreitung im Social Web beschränkt, sondern zudem weitere Angriffsformen wie Cyber-Attacken oder Social Engineering einsetzt.

Folglich ist das frühe Erkennen solcher Angriffe die zentrale Herausforderung. Unternehmen müssen eine Früherkennung nutzen, denn die Kosten der Eindämmung steigen mit zunehmender Verbreitung der Desinformation stetig oder sogar exponentiell an.



2.3 Verteidigung durch Früherkennung

2.3.1 Asymmetrie und Herausforderung „unknown Unknowns“

Ein Desinformationsangriff zielt darauf, in spezifischen digitalen Meinungsforen Themen zu verstärken oder zu setzen. Der Angreifer kann hierzu aus einem großen Möglichkeitsraum konkrete Szenarien zusammenfügen, auch die thematischen Angriffspunkte sind a priori nicht begrenzt.

Der Verteidiger hingegen befindet sich in einer asymmetrischen und sehr ungünstigen Position: Denkbare Varianten können – in einem vorbeugenden Stresstest – durchgespielt werden, aber die Gefahr der Überraschung bleibt bestehen. Der Umgang mit unknown Unknowns bleibt erfolgskritische Herausforderung.

Für Früherkennungsfunktionen gilt, dass die Signal auslösende Information im Vorhinein nicht unbedingt beschrieben werden kann: Man weiß nicht, wonach gesucht werden soll, außer dem Umstand, dass es bedrohlich für das eigene Unternehmen, einen exponierten Unternehmensvertreter, einen Kunden oder Lieferanten sein könnte.

Damit scheiden für Sicherheitsanalysen solche Werkzeuge aus, die rein stichwortbasierte Suchmetriken einsetzen, etwa Monitoring-Dashboards. Werden im Entdeckungsprozess lediglich Beiträge nach vordefinierten Themenkarrieren erfasst, dann ist das Finden von Überraschungen per Definition ausgeblendet.

Wenn aber nun ein Angriff darauf zielt, in spezifischen digitalen Meinungsforen a priori unbekannte Themen zu verstärken, dann muss das Früherkennungswerkzeug darauf ausgerichtet sein, Änderungen linguistischer Strukturparameter zu identifizieren: Welche Themen werden (plötzlich) signifikanter?

Erkannten Begriffen wird ein Signifikanzgrad zugeordnet. Neben solchen Diskussionsthemen, die emergent aus den Beiträgen erschlossen werden, gibt es in der Praxis für jeden Beobachtungsbereich auch bereits definierte Suchkategorien. Erst das Zusammenspiel dieser beiden Sichtungsklassen, known Unknowns und unknown Unknowns, verhindert „Betriebsblindheit“ und lässt systematisch auch Neues erkennen.

2.3.2 Algorithmen zur hypothesenfreien Analyse

Auf Basis der Computerlinguistik und der sozialen Netzwerkanalyse lassen sich Algorithmen definieren, die hypothesenfrei aus großen Beitragsmengen die signifikanten Themen und Begrifflichkeiten destillieren: Nicht die absolute Häufigkeit eines Wortes zählt, sondern die relative Häufigkeit.

Wird ein Begriff häufiger als in der Normalverteilung verwendet, so steigt auch seine Signifikanz. Weitere Hinweise gibt etwa die Analyse der Frequenzverteilung von Begriffen in Beitragsmengen. Computerlinguistische Algorithmen erschließen durch Signifikanz- und Frequenzanalysen relevante Auffälligkeiten in einem umfangreichen Kontext ohne Vorgabe.

Gleichwohl erfordert eine – über das Banale hinausgehende – inhaltliche Bewertung menschlichen Verstand, also einen Analysten. Clustering-Algorithmen erkennen, welche Gruppen von Begriffen stärker untereinander als mit dem Rest der Begriffe verbunden sind. Mit dieser Metrik werden automatisch Begriffscluster abgegrenzt, der Analyst erkennt Zusammenhänge quellenübergreifend.

Diese inhaltlichen Strukturen können in semantischen Netzen abgebildet werden. Auf Basis der beschriebenen Metriken lassen sich solche Netzvisualisierungen generieren. Der Verteidiger erhält somit eine interaktive Echtzeitlandkarte, um die Kontexte unterschiedlicher Themen zu explorieren. Anhand dieser Landkarte kann er die jeweiligen Diskussionsräume „überfliegen". Das heißt, der Analyst kann anhand des visuellen Modells erschließen, wie die Textbeiträge im Diskussionsraum zu einer bestimmten Zeit verteilt sind.

Der Durchgriff auf die im Diskussionsraum verteilten Textbeiträge ist für die Qualifizierung eines möglichen frühen Signals oder auch nur eines interessanten Aspekts essenziell. Durch frühe Hinweise auf sich verstärkende Themenfelder erhalten Analysten den Vorlauf, um zu untersuchen, ob ein sicherheitsrelevantes Thema entsteht und ggf. wer Treiber des Geschehens ist. So wird sich eine gesteuerte Desinformationskampagne in steigender Signifikanz eines Themas niederschlagen. Das betroffene Unternehmen gewinnt somit Zeit zur Reaktion im Verteidigungsprozess.

Innovative Verfahren der Computerlinguistik und Netzwerkanalyse können im Aufgabenbereich Früherkennung die unstrukturierten Online-Diskussionen und Meldungen metrisch erfassen. So wird nach bereits bekannten Themen und Ereignissen automatisiert gesucht, aber auch Unerwartetes systematisch gefunden.

Auf diese Weise gelingt es, schwache Signale im digitalen Rauschen früher zu erkennen, Kontexte von Themen, Debitoren, Marken, Talentgruppen oder Personen besser zu verstehen und eigene Maßnahmen besser zu steuern. So kann die Früherkennung von Risiken (und Chancen) unternehmensspezifisch als wichtige Fähigkeit weiterentwickelt werden. Die Technologien hierzu sind verfügbar.

Die Aufnahme der Bereiche Früherkennung und Detektion von Desinformation bedeutet für die Corporate Security eine grundsätzliche Ausweitung ihres Abdeckungsfeldes: Ohne diesen Schritt wird es jedoch nicht gelingen, den aufkommenden hybriden Bedrohungen zu begegnen.

2.4 Zwischenfazit

Die technologische Entwicklung ist maßgeblich für die wachsende Bedrohungslage von Bedeutung. Die Angreifer profitieren von frei verfügbaren Werkzeugen, die ein hohes Maß an Automatisierung und zunehmend auch an Individualisierung ermöglichen. Bot-Schwärme, Algorithmen und künstliche Intelligenz sind hier die Schlagworte.

Dabei haben die Angreifer einen deutlichen Vorteil, da sie auf Technologien zurückgreifen können, die die Verteidiger nicht einsetzen dürfen. Die Auseinandersetzung wird asymmetrisch geführt.

Aber auch die Verteidiger profitieren vom technologischen Fortschritt. Gerade im Bereich der Detektion entstehen neue Werkzeuge und Möglichkeiten, sich gegen Desinformationsangriffe zielgenau zur Wehr zu setzen.

Letztlich müssen sich die Unternehmen diesem Wettlauf stellen, denn die Bedrohung ist kein Hype, der vorüberzieht.

3. Angriffsziele und -methoden

3.1 Gesamte Scorecard im Fokus

Die Angriffsmöglichkeiten durch Desinformation bezogen auf Unternehmen gehen deutlich über das aus der politischen Arena bekannte Spektrum hinaus. Potenzielle Angriffsziele sind insbesondere digitale Informationsbereiche, die eine relevante Stakeholder-Gruppe zur Entscheidungsfindung heranzieht. Hierbei kommt dem digitalen Raum und seiner Manipulierbarkeit eine entscheidende Bedeutung zu. Der erreichbare Einfluss kann auf direkte oder indirekte Weise gegen ein Unternehmen wirken.

Stellen Sie sich ein traditionsreiches, produzierendes Unternehmen vor, das in einen ausländischen Markt expandieren möchte. Der dortige Marktführer will diesen Plan verhindern, allerdings dabei dem direkten Wettbewerb eher ausweichen. Das Traditionshaus hat seine strategischen Erfolgsfaktoren für dieses Vorhaben etwa folgendermaßen auf Basis der Perspektiven einer Balanced Scorecard abgesteckt:

Markt und Kunden (Output): Platzierung von Marke und Produkten	**Finanzen:** Suche nach neuen Investoren und lokalen Partnern
Prozesse: Rekrutierung von lokalem Personal und Erweiterung der Lieferkette	**Potenzial (Input):** Lokale Anpassung von Produktsortiment und Kommunikation

»Stehen Unternehmen im Visier, kann deren Gesamtreputation angegriffen werden, viel wirkungsvoller sind aber gezielte Angriffe auf einzelne Facetten und Stakeholder-Gruppen.«

Uwe Heim

Der operativ unterlegene Platzhirsch hat nun vielfältige Ansatzpunkte für sämtliche Perspektiven, um seine Lage durch Desinformationsangriffe aufzuwerten. Beispielsweise:

- Angriffe auf die Reputation von Unternehmen und Mitarbeiterschaft: „Die Produkte werden auch beim Transport von Versuchstieren eingesetzt. Hier die Bilder! …“
- Diskreditierung der Qualität von Produkten und Leistungen: „Es haben sich schon Kinder beim Spielen mit den Produkten verletzt! Bitte weitersagen …“
- Platzierung von Compliance-Vorwürfen und Beschädigung der Kreditwürdigkeit: „Ohne Bestechung läuft da kaum etwas. Ich würde immer auf Vorkasse bestehen …“
- Verstärkung von Vorwürfen seitens der kritischen Öffentlichkeit. „Beutet ein Zulieferer beim Abbau von X in Südamerika nicht die Bergleute aus? Es gab sogar Todesfälle! Aber hier das Sauberimage. Das passt ja fein zusammen …“

- Angriffe auf den Ruf als Arbeitgeber bezogen auf Engpasszielgruppen: „Ich hatte mich auch dort beworben, aber der Befehlston war dann doch zu viel für mich. Nein Danke! …“
- Identifikation, Ausspähung und Ansprache von Schlüsselpersonal: „Sie suchen doch eine neue Herausforderung? …“
- und Schutzfamilien: „Wir wissen, wo Ihre Kinder zur Schule gehen. …“

Der Angreifer kann diese Botschaften unter falscher Identität verbreiten und verstärken: als Aktivist, Bewerber, Fan, Headhunter, Geschäftspartner, Mitarbeiter, Kunde, Student, Troll … aggressiv, besorgt, fröhlich, frech, liebreizend …

Desinformation beeinflusst die Meinungsbildung und Entscheidungsfindung von Akteuren: Analysten, Kunden, Talenten, Mitarbeitern und Geschäftspartnern. Mit koordinierten Desinformationsangriffen kann Unternehmen großer Schaden zugefügt werden.

Abbildung 13:
Angriffsvektoren Desinformation
(Quelle: ASW Bundesverband und complexium)

Desinformationsangriffe können die Aufmerksamkeit und Handlungsfähigkeit deutlich einschränken und dem Unternehmen in verschiedenen Dimensionen Einbußen zufügen. Folglich kann sich ein Wettbewerber durch solche Machenschaften Vorteile verschaffen, etwa den Markteintritt des angegriffenen Unternehmens verzögern oder beeinträchtigen.

Die Plausibilität dieser Szenarien konnte in den Interviews zu dieser Studie bestätigt werden. Aus den erhaltenen Darstellungen wurden Fallstudieneinblicke exzerpiert, die aufzeigen, dass tatsächlich jede Scorecard-Perspektive nicht nur in der Theorie das Ziel bewusster Desinformation sein kann. Alle Fallbeispiele, die für diese Studie herangezogen wurden (Kapitel 3.2 bis 3.6), wurden anonymisiert; die in den Fallbeispielen verwendeten Namen der genannten Unternehmen sind frei erfunden.

3.2 Angriffsvektor 1: Arbeitgeberbild

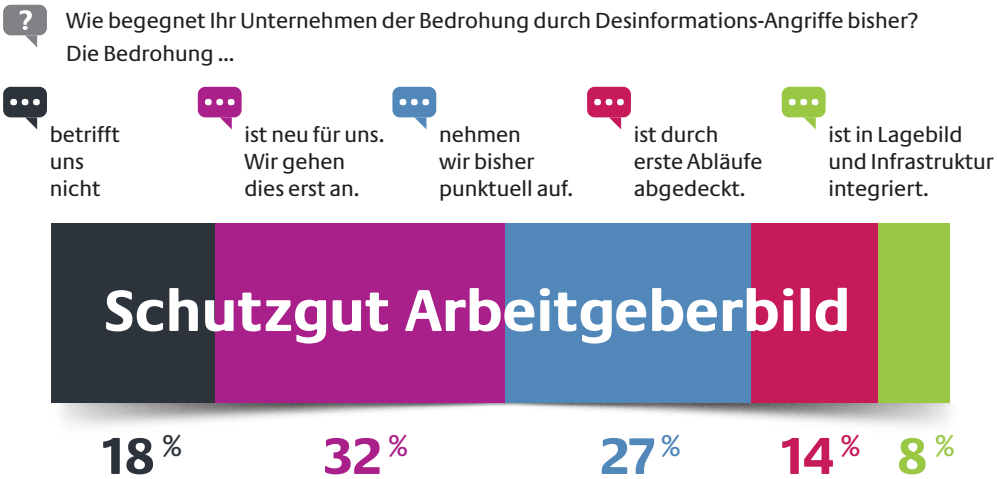
In der heutigen Zeit sind Talente online auf Informationssuche zu potenziellen Arbeitgebern. Die Karriereseite eines Arbeitgebers ist dabei nur eine Quelle unter vielen – nur bei sehr wenigen Unternehmen wird sie direkt angesteuert. Wichtigste digitale Tummelplätze für Talent-Zielgruppen sind Foren und Netzwerke. Auch Aussagen von anonymen Gleichgesinnten können auf diesen Plattformen hohes Gewicht erhalten. Jede authentische Teilnahme kann nachhaltige digitale Eindrücke zu einem Arbeitgeber hinterlassen. Die Vielzahl dieser Beiträge fließt ein in das Arbeitgeberbild.

Ein Angreifer kann damit die Recruiting-Pipeline eines Arbeitgebers gezielt treffen. Ein solcher Angriff kann auf Engpasszielgruppen abgestimmt werden.

Die im Rahmen der Studie geführten Interviews und die Onlinebefragung stützen dieses Bild: Über 80 Prozent der befragten Unternehmen haben realisiert, dass eine Bedrohungssituation existiert und Handlungsbedarf besteht.

Gleichwohl hat nur jedes vierte Unternehmen bisher konkrete Maßnahmen eingeleitet, um bei möglichen Desinformationsangriffen reaktionsfähig zu sein.

Abbildung 14:
Bedrohung durch Desinformation im Bereich Arbeitgeberbild (Quelle: Onlinebefragung im Rahmen der Studie; rundungsbedingte Differenzen)



3.2.1 Case: Softwarehersteller sucht Spezialisten

Der 30-Mitarbeiter-Betrieb „JP&M-Software-Solutions“ stellt Spezialsoftware her und benötigt dafür hochspezialisierte Entwickler. Nun entschließen sich vier zentrale Mitarbeiter, den Betrieb zu verlassen, da sie sich nicht angemessen am Gewinn beteiligt fühlen.

Den engen Markt betritt ein Konkurrent, der nicht nur Kunden streitig machen möchte, sondern auch mögliche Nachwuchskräfte. Schließlich hängen Qualität und Innovationskraft der Produkte maßgeblich von der Leistung der Entwickler ab. So entscheidet das Unternehmen den Wettbewerb um den Kunden für sich, das zuvor den Wettbewerb um die Talente gewinnen konnte. Das wissen auch die beiden Konkurrenten.

Über „JP&M-Software-Solutions“ wird in Tech-Foren, die gerne von Studierenden gelesen werden, berichtet, dass „Studis dort besonders ausgebeutet werden“ sollen – und dass dies wohl auch ein Grund sei, warum sich vier Mitarbeiter selbständig gemacht haben. Sie hätten das nicht unterstützen wollen. Hört man. Die Bewertung auf einschlägigen Arbeitgeberbewertungsportalen ist schon wenige Wochen vor dem Weggang der Mitarbeiter nach unten gegangen. Schließlich taucht ein interner E-Mail-Verkehr der Geschäftsführer von „JP&M-Software-Solutions“ auf, in dem sie über Bewerber herziehen und sich mit sexistischen Sprüchen über Bewerberinnen überbieten: „Die hatte zwar keine Ahnung, aber als Prämie für unsere besten Mitarbeiter wäre sie vielleicht etwas“.

Eine Frauenquote von Null, und ein oder zwei unzufriedene Mitarbeiter genügen, um den Gerüchten die nötige Glaubwürdigkeit zu verleihen. Es kommen zwar noch Bewerbungen rein, aber deutlich weniger als vorher. Das Unternehmen erleidet einen spürbaren Wettbewerbsnachteil.

3.2.2 Case: Größerer Mittelständler erschließt neue Märkte

Der Gang nach Kasachstan fällt dem mittelständischen Medizintechnikunternehmen „ModernMedTec“ nicht leicht. Doch der Markt ist interessant. Dem Unternehmen bieten sich mit seinen Produkten viele Chancen. Um den Vertrieb aufzubauen, sucht die Geschäftsleitung Mitarbeiter vor Ort. Die Konkurrenz ist seit wenigen Jahren bereits vor Ort und fürchtet den neuen Wettbewerber, der ihnen in anderen Ländern schon öfter das Wasser abgegraben hat. Qualifizierte Vertriebsleute sind hierzulande dünn gesät. Und so findet ein Ringen nicht nur um den Absatz statt, sondern auch um Mitarbeiter.

Als sich die Suche nach Mitarbeitern als noch schwieriger als erwartet herausstellt, möchte der Geschäftsführer der Ursache auf den Grund gehen. Dabei stößt er auf Arbeitnehmerforen in Kasachstan, in denen vor „ModernMedTec“ gewarnt wird. Das Unternehmen wäre bekannt dafür, in Schwellenländern seine Löhne nicht ordnungsgemäß zu bezahlen. Das wisse man aus Erfahrungen in Indien. In Thailand seien Mitarbeiter sogar geschlagen worden. Natürlich fände man nichts davon auf den internationalen Bewertungsportalen oder auf Facebook etc. Dort seien ja die Kollegen aus Europa tonangebend – so die Einträge in den lokalen Foren. Dass es nur vereinzelt solche Beiträge gibt, das sei eher ein Beweis für die Vermutung als ein Grund zum Zweifeln. Zudem würden auch die offiziellen lokalen Stellen die Gerüchte bestätigen, was tatsächlich stimmt.

Wer bereit ist, nicht nur online Desinformation zu betreiben, sondern auch ein, zwei Beamten zu schmieren, kann in bestimmten Ländern „wahre Wunder“ erreichen.

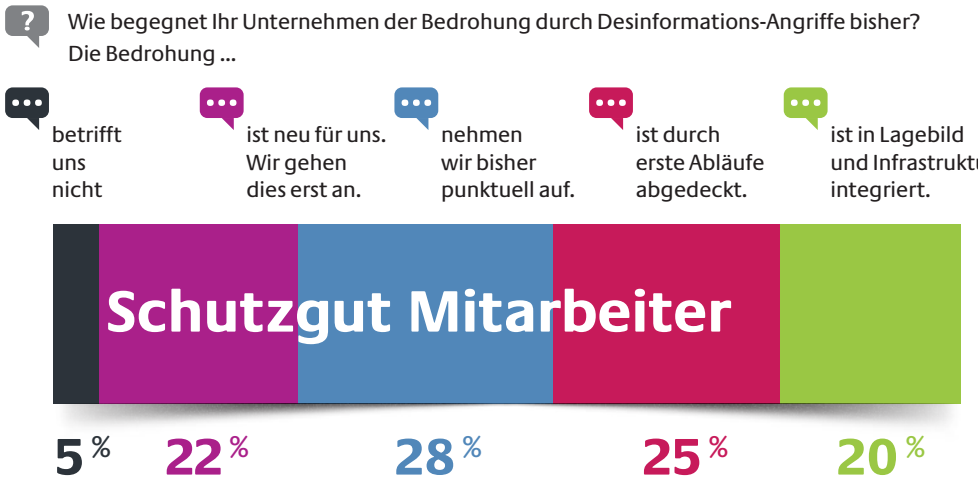
3.3 Angriffsvektor 2: Mitarbeiter/Mitarbeiterloyalität

Mitarbeiter, Meinungsführer, exponiertes Schlüssel- und Führungspersonal sowie Mandatsträger und Eigentümer hinterlassen durch eigenes Handeln oder Referenzierung durch Dritte Spuren im digitalen Raum.

Angreifer können daraus facettenreiche Profile rekonstruieren und für sicherheitsrelevante Zwecke nutzen: Desinformationsangriffe können auf eine größere Gruppe zielen oder gezielt einzelne Personen ins Visier nehmen. Eine mögliche Annäherung an Schutzpersonen oder die präzise Ausgestaltung von Social Engineering oder auch nur Ablenkung können Ausprägungen sein.

Auch die Interviews und die Onlinebefragung zeichnen dieses Bild. Fast alle befragten Unternehmen sind sich der Bedrohung bewusst. Trotz des hohen Problembewusstseins hat nur jedes fünfte befragte Unternehmen eine Infrastruktur zur Bewältigung von Desinformationsangriffen integriert.

Abbildung 15:
Bedrohung durch Desinformation im Bereich Mitarbeiter/ Mitarbeiterloyalität (Quelle: Onlinebefragung im Rahmen der Studie)



3.3.1 Case: Mobilisierung im Arbeitskampf

So richtig kommt der Streik nicht in Gang, dabei muss er wohl sogar noch länger durchgeführt werden als befürchtet. Da schlägt die Nachricht ein wie eine Bombe: Der Konzern soll aufgespalten und ein Teil der Belegschaft in eine Billiglohntochter verlagert werden. Jetzt schäumt die Belegschaft vor Wut. Kaum einer, der nicht auf die Straße gehen will.

Das Gerücht – keiner weiß, wo es hergekommen ist – wird von der Presse dankbar aufgegriffen. Wieder ein Großkonzern, der sich vor seiner sozialen Verantwortung drücken will. Das passt in die aktuelle Debatte um soziale Gerechtigkeit. Die Gewerkschaften freuen sich über eine hohe Mobilisierung, die Zeitungen über eine höhere Auflage, die Onlinemedien über stärkere Klickzahlen. Auch die Konkurrenz profitiert. Sie bekommt die Aufträge, die ihr Wettbewerber nun nicht mehr erledigen kann. Und das Unternehmen muss Arbeitsausfälle verkraften, die einen Millionenschaden verursachen.

3.3.2 Case: Projektgeschäft – alle Neune

Es ist ein wichtiges Projekt, wenn nicht das wichtigste Projekt überhaupt. Wenn sie das erfolgreich schaffen, spielen sie wieder ganz oben mit, wenn nicht, können sie vielleicht alles verlieren. Und so hängt die Zukunft des Unternehmens in erster Linie vom Kernteam ab. Diese zwanzig Leute müssen die nächsten Monate funktionieren wie ein Uhrwerk.

Wer das Unternehmen halbwegs kennt, weiß schnell, wer diese relevanten Personen sind. XING und Linkedin weisen die „Country Manager", „Project Leader", „Chief Developer" und wie sie alle heißen, fein säuberlich aus. Manch einer schreibt sogar Projektnamen und seine jeweilige Funktion in seinen öffentlichen Lebenslauf.

Da war es für den Konkurrenten nicht weiter schwer, einige Personen aus dem relevanten Kernteam etwas zu beschäftigen:

- Der eine, der auf XING im geschützten Karrierebereich angab, auf Stellensuche zu sein, wurde mit einem attraktiven Angebot abgelenkt.
- Ein anderer, der bereits gewisse Vorbehalte gegen das Projekt hatte, erfuhr „von einem Freund" Hintergrundinformationen zum Projekt, die es in ein ethisch fragwürdiges Licht rückten.
- Ein Dritter erhielt eine E-Mail, vermeintlich versehentlich vom Chef kommend, mit einer Übersicht der Gehälter – und er stand ganz unten auf der Liste.
- Ein Vierter bekam vom Fünften vermeintlich versehentlich eine E-Mail mit Links zu Kinderpornos.
- Und dann war da noch der Sechste, der endlich seine Traumfrau gefunden hatte – auf XING. Sie konnten sich so gut über ihre aktuellen Projekte austauschen.
- Der Siebte wiederum erlebte den Tiefpunkt seiner Beziehung, da er Fotos bekam, die seine Frau mit einem anderen Mann zeigten – und wenn sie auch nur redeten, so sah das doch nach mehr aus.
- Der Achte erhielt ebenfalls Fotos – von seinen Kindern auf dem Schulweg.
- Und der Neunte durfte sich mit Polizei und Staatsanwaltschaft rumschlagen, da er angeblich rechte Hetze im Netz verbreitete.

Die elf übrigen des Kernteams konnten den Leistungsabfall der neun nicht wettmachen.

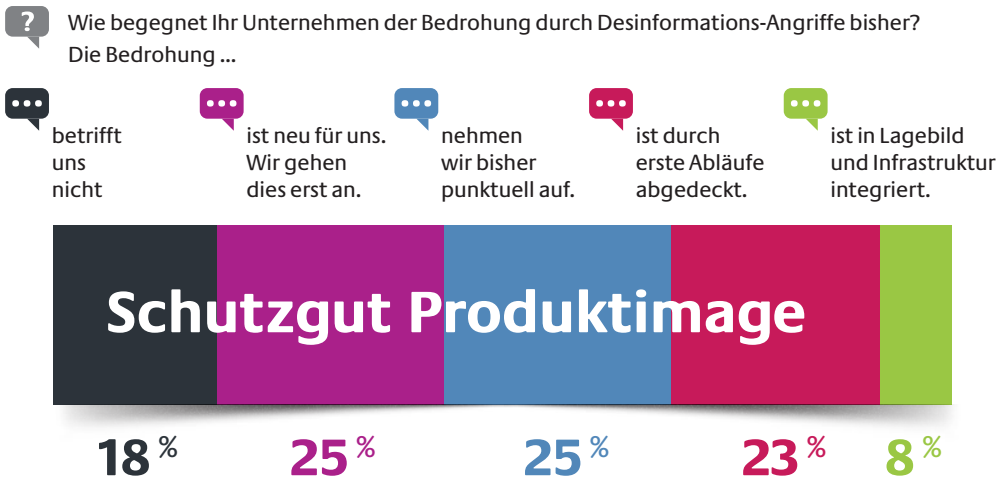
3.4 Angriffsvektor 3: Produktimage

Für einen großen Anteil der relevanten B2C-Kaufprozesse werden Online-Informationen – Nutzererfahrungen, Bewertungen, Empfehlungen – zu Rate gezogen. Zumeist unerreicht durch das klassische Marketing tauschen sich Interessierte und Nutzer aus. Diese Dialoge sind nachhaltig und beeinflussen Entscheidungen.

Ein Angreifer, etwa ein aggressiver Wettbewerber, kann durch Desinformation direkte Kaufentscheidungen potenzieller Kunden negativ beeinflussen. Durch etablierte (Fake-) Profile und automatische Verbreitung können negative Einschätzungen erstellt und verstärkt werden.

Über 80 Prozent der im Rahmen der Studie befragten Unternehmen sehen sich der Bedrohung ausgesetzt. Jedoch nur jedes zehnte der befragten Unternehmen hat über den Einzelfall hinausgehende Maßnahmen zur Abwendung dieser Bedrohungen eingeleitet.

Abbildung 16:
Bedrohung durch Desinformation im Bereich Produktimage (Quelle: Onlinebefragung im Rahmen der Studie; rundungsbedingte Differenzen)



3.4.1 Case: Angebliche Wettbewerbsverstöße – Produkt wird aus dem Verkehr gezogen

Vertriebsleiter und Regionalgeschäftsführer sind hochzufrieden. Das neue Produkt, das schon im Heimatmarkt ein voller Erfolg war, wird gleich nach seiner Einführung in Osteuropa auch dort zum Verkaufsschlager. Besonders zufrieden macht das die Geschäftsleitung, da aufgrund der scharfen Wettbewerbssituation mit einem deutlich schwierigeren Einstieg gerechnet wurde. Schließlich ist der Platzhirsch ortsansässig und seit Jahren etabliert. Doch offenkundig half das dem Konkurrenten nicht, denn die Verbraucher griffen zum Produkt aus Deutschland.

Nach kurzer Zeit jedoch kommen Gerüchte auf, der deutsche Anbieter verstoße gegen Wettbewerbsrecht. Angebliche Belege tauchen in den sozialen Netzwerken auf und schließlich auch in der Presse, die das Thema dankbar aufgreift und genüsslich ausweitet. Da sehen sich auch die lokalen Behörden in der Verantwortung und lassen das Produkt schließlich aus dem Verkehr ziehen.

3.4.2 Case: Böse Chemie

Der Spezialchemiehersteller InChDe produziert unterschiedlichste Chemieprodukte, die vor allem als Vorprodukte an große Konzerne geliefert werden. In den letzten Jahren ist das Unternehmen kontinuierlich gewachsen und hat dabei immer neue Kunden gewinnen und Marktsegmente bedienen können. Es produziert inzwischen in fast allen Teilen der Welt. Da es einen neuen Großauftrag für einen US-Chemiekonzern an Land ziehen – und dabei einen Konkurrenten ausstechen – konnte, plant das Unternehmen, ein neues Werk in den USA zu errichten.

Einige Wochen nach Vertragsunterzeichnung findet der Geschäftsführer im Pressespiegel einen Artikel, demzufolge sein Unternehmen im Verdacht stehe, die Terrororganisation IS zu beliefern, die Staatsanwaltschaft würde sich bereits damit befassen. Sein neuer Kunde hat diesen Artikel offenbar auch gelesen, denn er ruft wenige Minuten später an. Er droht den Auftrag zurückzuziehen, da in den USA bereits Boykottaufrufe gegen sein Unternehmen gestartet würden. Auf Twitter findet sich der Hashtag #InCheDe=Inshallah.

Wenige Tage später tauchen auch Beschwerden von Umweltschützern auf, InChDe würde in großem Stil Flüsse und Seen in Entwicklungsländern verseuchen. Menschenrechtsorganisationen und Arbeitnehmervertreter kritisieren die geringen Sicherheitsstandards an den Standorten in Schwellenländern. Der Geschäftsführer weiß, dass all das nicht stimmt, doch die Ereignisse prasseln jetzt immer schneller und heftiger auf das Unternehmen ein.

Bilder tauchen auf Facebook auf, die Menschen mit Verätzungen zeigen – angeblich Arbeiter in einem InCheDe-Werk in Indien. Ein Video dokumentiert, wie Chemie-Abwässer in einen Fluss geleitet werden – angeblich von InCheDe. Ein Foto, das einen Menschen im T-Shirt mit InCheDe-Aufschrift im Gespräch mit zwei vermummten Gestalten, die nach IS aussehen, zeigt, wird tausendfach auf Twitter geteilt. Derweil gibt es Proteste nicht nur vor der Zentrale von InCheDe, sondern auch der neue amerikanische Partner wird massiv mit Kritik überzogen. Schließlich sieht dieser keine andere Wahl, als seinen Vertrag rückabzuwickeln.

In der Bewältigung und Aufarbeitung des Falls durch externe Kommunikationsberater zeigt sich später, dass die Hetze gegen das Unternehmen bereits kurz vor Vertragsunterzeichnung mit dem US-Konzern begonnen hatte. Zu diesem Zeitpunkt entstanden hunderte neue Profile, die sich mit Islamismus, Umweltschutz und Menschenrechten befassten. Sie teilten und liketen gegenseitig ihre Kritik an InCheDe und konnten eine solche Wucht erzeugen, dass der Funke irgendwann aus ihrer Netzwerk-Blase übersprang, sich breit im Netz verteilte und dann auch von realen Personen, Organisationen und den Medien aufgegriffen wurde.

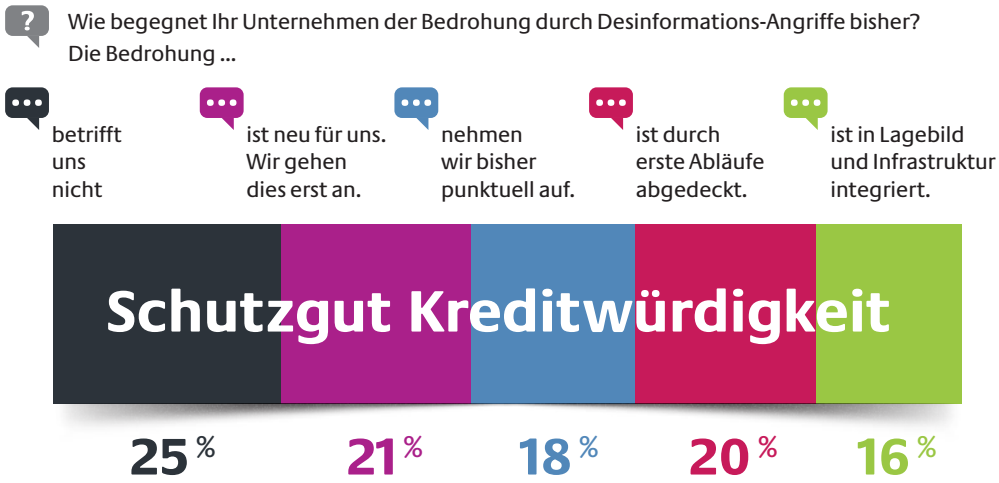
3.5 Angriffsvektor 4: Finanzielle Reputation/Kreditwürdigkeit

In den Bereichen M&A, Lieferantenauswahl sowie Kreditoren- und Debitorenmanagement spielt die Einschätzung der Unternehmensbonität und Zahlungsfähigkeit eine große Rolle. Zunehmend werden Daten aus dem Internet in diese Analysen aufgenommen. Hierbei werden auch unstrukturierte Informationen abseits der bekannten Datenauskünfte herangezogen.

Ein Angreifer kann hier das entsprechende Bild bewusst mit Falschinformationen anreichern.

Daher sehen auch drei Viertel aller befragten Unternehmen hier Handlungsbedarf. Aber nur etwa ein Drittel hat konkrete Maßnahmen zur Abwendung der Bedrohung eingeleitet.

Abbildung 17: Bedrohung durch Desinformation im Bereich Finanzielle Reputation/Kreditwürdigkeit (Quelle: Onlinebefragung im Rahmen der Studie)



3.5.1 Case: Kurssturz

Die Aktie entwickelte sich in den letzten Wochen schon ganz gut. Nachdem Gerüchte über ein neues Produkt die Runde machten, legte sie noch einmal kräftig zu. Jetzt, kurz vor der Weltleitmesse, waren alle gespannt, was das Unternehmen für eine Neuheit enthüllen würde.

Doch plötzlich tauchten Informationen in Technikforen auf, dass es Probleme mit dem neuen Produkt gäbe und noch andere Schwierigkeiten das Unternehmen heimsuchten. Der Entwicklungsleiter, heißt es weiter, soll kurz vor dem Abgang stehen. Waren dies zunächst vereinzelte Stimmen, vermehrte sich rapide die Zahl derer, die ähnliches gehört haben wollten. Immer weitere Spekulationen werden angestellt, auch über die Zuverlässigkeit und Zukunftsfähigkeit bestehender Produkte.

Schließlich büßt der Aktienkurs beträchtlich ein und fällt deutlich unter den Wert, den er noch vor wenigen Wochen hatte, als die positiven Nachrichten aufkamen. Der Aktienkurs erreicht auch dann noch nicht seinen alten Stand, als die Messe beginnt und tatsächlich eine neue Innovation vorgestellt wird. Da dominieren ganz andere Themen. Das Unternehmen wurde somit auch seiner Fähigkeit zum Agenda-Setting beraubt!

Und wer vorher wusste – oder ahnte –, dass der Aktienkurs fallen würde, konnte eine Menge Geld verdienen.

3.5.2 Case: Investorenschreck

Eigentlich war die Sache schon eingetütet. Der neue Investor war nicht nur von den Produkten und der Zukunftsfähigkeit der Firma überzeugt. Auch die Geschäftsführer wirkten überaus vertrauenserweckend und die Mitarbeiter motiviert. Schließlich liefen die Gespräche auch schon eine ganze Weile. Jetzt stand der Vertrag kurz vor dem Abschluss. Doch wenige Tage vor der Unterzeichnung tauchten Gerüchte über Bilanzfälschungen und Veruntreuung auf. Gelder sollen abgeflossen und rechten Gruppierungen zugutegekommen sein. Eine anonyme E-Mail eines „Insiders“ machte auf Unregelmäßigkeiten aufmerksam und riet dazu, sich einmal im Internet auf bestimmten Foren umzusehen; Links waren beigefügt.

Folgte man diesen, gelangte man zu Profilen der Geschäftsführer, die sich tatsächlich in geschlossenen Internetforen rechtsradikal äußerten – und dort für ihre großzügigen Spenden verehrt wurden. Auch leitende Angestellte waren hier vertreten. Das ganze Unternehmen ein Hort Rechtsradikaler? Es machte den Anschein. Wenn man sich genauer damit auseinandersetzte, wurde einiges klarer: Der Großvater von einem der Geschäftsführer in der Wehrmacht. Der stete Hinweis, man produziere nur in Deutschland. Die geringe Ausländerquote. All das hörte sich in diesem Lichte ganz anders an.

Man konfrontierte seinen Geschäftspartner mit den Anschuldigungen. Doch der reagierte sehr verärgert. Wie man dazu käme, so etwas zu glauben. Gut, dass es kürzlich noch ein zweites Angebot gab. Die zahlten zwar etwas weniger, doch glaubten sie solch Unfug nicht.

3.6 Angriffsvektor 5: „Mittel zum Zweck“/Mitverantwortung

Informationen über Unternehmen stehen in vielfältigsten Netzwerken, die nur unvollständig erfasst oder gar gesteuert werden können. Die erstellten Produkte werden von den Kunden zu eigenen Zwecken verwendet. In der Lieferkette befinden sich Unternehmen, deren Aktivitäten nicht vollständig überblickt werden. Die eigenen Mitarbeiter haben auch ein Leben abseits des Arbeitnehmertums.

„Störfälle“ in diesen Ausläufern des eigenen Eco-Systems können von Dritten aufgenommen, verstärkt und unmittelbar auf das Zielunternehmen projiziert werden. Die potenziell größere Öffentlichkeitswirkung wird für das originäre Vorhaben genutzt, das Unternehmen selbst ist nur das Mittel zum Zweck.

3.6.1 Case: Der Feind in meinem Projekt

Irgendwie stand das Projekt von Anfang an unter einem schlechten Stern. Dabei hatte man so große Erwartungen hineingesetzt. Der Markt ist immer noch mehr als vielversprechend und der lokale Partner „ZLQ-TEC“ schien genau der Richtige zu sein. Doch kaum war der Vertrag besiegelt, stellten sich Schwierigkeiten ein. Es kam immer wieder zu teuren Verzögerungen, weil ZLQ-TEC die zugesagten Leistungen nicht erbringen konnte. Da von der länderübergreifenden Partnerschaft eine gewisse Signalwirkung ausgehen sollte, stand das Vorhaben ärgerlicherweise auch noch unter recht hoher medialer Beobachtung.

Somit sah sich ZLQ-TEC zur Vorwärtsverteidigung animiert. Eigentlich hat man nichts gegen den deutschen Partner, aber die ganze Schuld auf sich laden, das will man dann doch nicht. Schließlich hat man einen Ruf zu verlieren. Lokal besser vernetzt als der deutsche Partner, streut ZLQ-TEC in Gesprächen mit den Behörden vor Ort Gerüchte, die an der Zuverlässigkeit der Deutschen zweifeln lassen. Auch die lokale Presse greift das Thema auf und ergreift dabei eine klare Position für den Landsmann: Die deutschen Invasoren, die wieder einmal in das Land einfallen und dann doch versagen. Begleitet wird das Ganze von eifrigen Diskussionen im Netz.

3.6.2 Case: Alles der Umwelt zuliebe – oder den Spenden und der Auflage?

Fast keine Branche kommt ohne Beanspruchung der Umwelt aus. Produktion, Transport, selbst Dienstleistungen haben immer auch negative Auswirkungen auf das Ökosystem. Vielen Unternehmen ist das sehr bewusst und sie bemühen sich, diese Belastungen zu reduzieren. Es ist Aufgabe auch der Medien und entsprechender Nichtregierungsorganisationen, ein wachsames Auge darauf zu haben, dass Konzerne ihren Verpflichtungen und Versprechungen auch nachkommen.

Ein Chemiekonzern lässt seine Ware von einem lokal ansässigen Logistikunternehmen „Müller-Maier-Schulz-Logistics (MMSL)“ transportieren. Dafür schult er deren Fahrer regelmäßig und verpflichtet das Unternehmen zu regelmäßigen Audits. Dennoch kommt es eines Tages zu einem Unfall. Dabei treten gefährliche Chemikalien aus und geraten in einen Fluss. In der Presse ist von einem Fahrzeug des Chemiekonzerns die Rede, NGOs prangern das Unternehmen für sein unverantwortliches Verhalten an. Schließlich kennt kein Mensch MMSL und ein Fehlverhalten eines unbekannten, kleinen Logistikdienstleisters bringt weder Aufmerksamkeit noch Auflage.

3.6.3 Case: Nicht vor meiner Haustür!

Das Geschäftsmodell der Firma WSG-DBB ist Herrn Krachmacher ein Dorn im Auge, erst recht, als eine Fabrik in der Nähe seines Wohnortes errichtet werden soll. Internetaffin und politisch gut vernetzt zieht er gegen das Unternehmen zu Felde. So werden Protestaktionen vor der Wohnung der Eigentümerfamilie organisiert und Politiker mit Informationen und Zahlen versorgt, die sich so biegen und darstellen lassen, dass WSG-DBB in einem äußerst schlechten Licht erscheint. Auch diverse NGOs springen auf das Thema an. Schließlich eignet sich das Unternehmen als Feindbild, gegen das man Stimmung machen kann. Und Stimmung braucht man, wenn man an Spendengelder kommen möchte.

Über Facebook und Twitter lassen sich Menschen mobilisieren und was man an echten Menschen nicht mobilisiert bekommt, füllt man mit Fake-Accounts auf. So zählt der Hashtag #NO-WSG-DBB an manchen Tagen zu den Trending Topics auf Twitter. Es dauert nicht lange, bis die lokalen Medien das Thema aufgreifen und schließlich auch überregional darüber berichtet wird. Den Eigentümern wird die Angelegenheit zu heiß, zumal sich der Protest zunehmend gegen sie persönlich richtet. Obwohl die Planungen für die neue Fabrik schon recht weit vorangeschritten waren, zieht man sich zurück und sucht nach einem neuen Standort. Das ist zwar teuer, aber vermutlich immer noch kostengünstiger als den Kampf gegen die Meinungsmacher auszufechten.

3.7 Zwischenfazit

Desinformationsangriffe gegen Unternehmen finden bereits statt und haben für die Angreifer auch schon zu Erfolgen geführt. Gleichzeitig spielen sie sich noch auf einem recht geringen Niveau ab. Das dürfte nicht lange so bleiben.

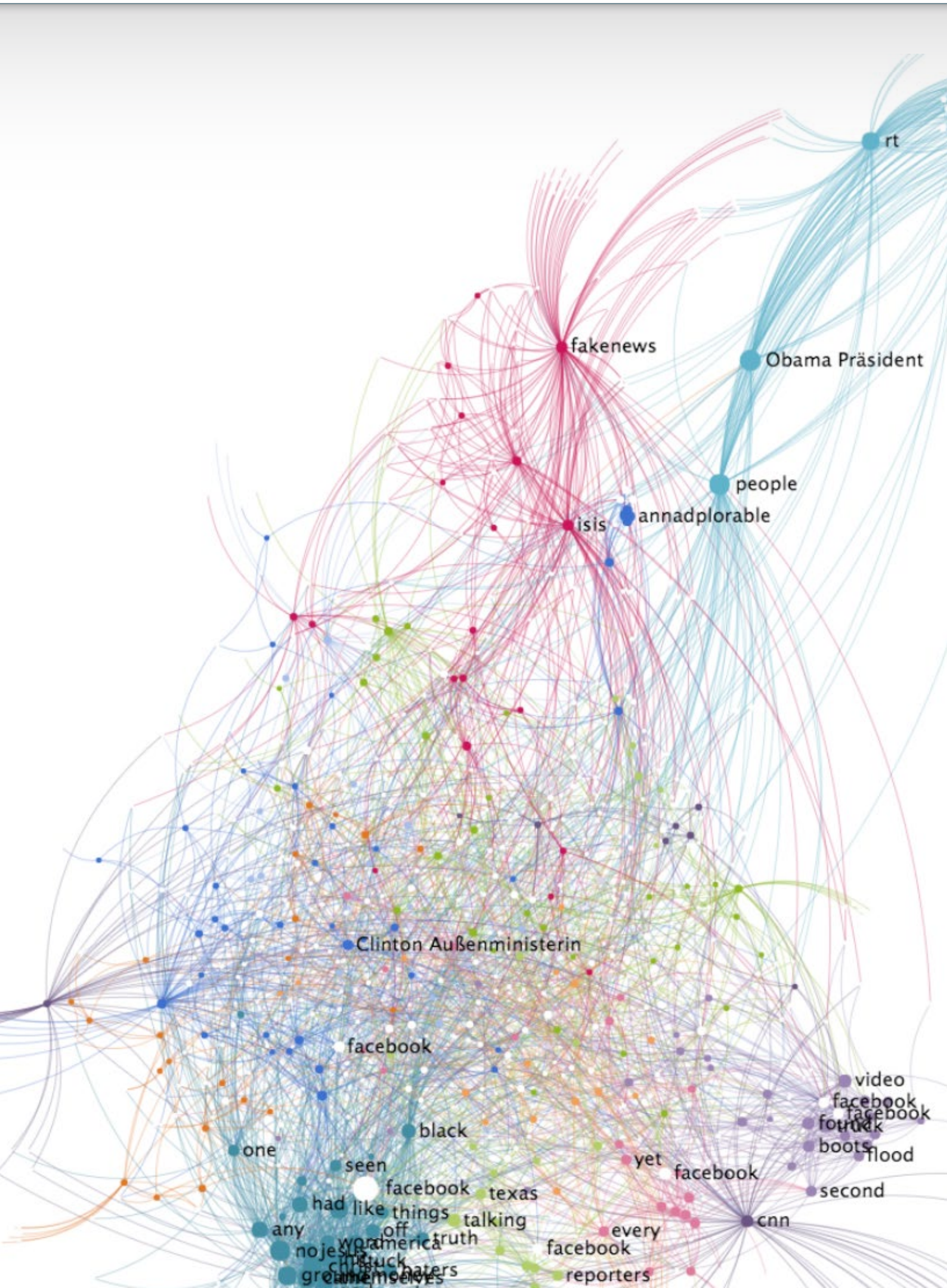
Szenarien sind denkbar und realistisch, in denen kombinierte Desinformationsangriffe gegen mehrere Ansatzpunkte im Unternehmen laufen und parallel dazu auch Hacks, Leaks und sonstige Angriffe zum Einsatz kommen. Werden die Angriffe über einen längeren Zeitraum geplant, vorbereitet und intelligent zeitlich gestaffelt, lassen sich auch große, gut aufgestellte Konzerne in Bedrängnis bringen.

So können Fake-Profile über Monate aufgebaut und gepflegt werden und damit ihr Netzwerk und ihre Reichweite massiv erhöhen. Über gute Beiträge bauen sie ihre Reputation im Netz auf und gelten schließlich als absolut glaubwürdig. Solche Sockenpuppen und Bots lassen sich auch in verschiedenen Sprachräumen und Gruppen über den Globus verteilt installieren. So kann ein Beitrag in einer kleinen regionalen Gruppe authentisch gestreut werden, der dann „zufällig" von einem Multiplikator aufgegriffen und in die Welt verteilt wird. Hier springen bereitstehende Bots auf das Thema an und es entsteht in Sekunden ein Lauffeuer, das alle Teile der Welt erreicht.

Auch Leaks helfen, Fake News authentischer zu machen. So kann eine geleakte Information aufgebauscht und um beliebige Gerüchte erweitert werden. Muss das Unternehmen den wahren Kern zugeben, wirkt der gesamte Rest authentisch. Durch Hackerangriffe erzeugte Störungen können Desinformationen ebenfalls Glaubwürdigkeit verleihen, ebenso wie die gezielte Diskreditierung von Managern oder leitenden Mitarbeitern.

Ein solch simultaner, länger anhaltender, kombinierter Angriff bindet massiv Ressourcen des Ziels und kann Unternehmen daran hindern, ihre Botschaften – über neue Produkte, Innovationen, einen Börsengang oder eine Ausgründung etc. – erfolgreich zu platzieren. Partner, Kunden und Investoren lassen sich abschrecken.

Für Unternehmen ist es daher besonders wichtig, sich präventiv mit den Bedrohungen durch kombinierte Desinformationsangriffe auseinanderzusetzen und entsprechende Abwehrprozesse zu entwickeln. Nur so können sie den Fall der Fälle erkennen und schnell und richtig reagieren.


rt
fakenews
Obama Präsident
people
isis
annadplorable
Clinton Außenministerin
facebook
video
facebook
boots
flood
black
one
seen
facebook
texas
had
like
things
talking
yet
facebook
second
any
off
truth
every
cnn
facebook
reporters

4. Verteidigungsphasen und -methoden

4.1 Verteidigungsprozess im Phasen-Radar

Unternehmen müssen auf Angriffe reagieren – auch und gerade bei neuartigen Angriffsvektoren. Dies setzt zunächst voraus, dass Unternehmen in der Lage sind, Angriffe zu bemerken (Detektion). Eine Reaktion auf einen Angriff ist geboten, wenn sie Aussicht auf Erfolg hat oder zumindest die Situation verbessert (Erfolgsgewissheit).

Angesichts der neuen Bedrohungslage durch Desinformationsangriffe sind hingegen mangelnde Detektion und Erfolgsungewissheit gewichtige Risikofaktoren. Sicherheitsbereiche von Unternehmen müssen daher bestrebt sein, diese beiden Risikofaktoren zu reduzieren. Die entsprechenden Präventionsmaßnahmen sollten dabei so weit wie möglich getroffen werden, bevor ein Störfall eintritt. Es gilt folglich, einen systematischen Verteidigungsprozess zu planen und zur Einsatzfähigkeit zu bringen.

Für den Bereich der Desinformation wird hier ein durchaus übliches, fünfstufiges Modell vorgeschlagen. In konzeptioneller Arbeit und befruchtet durch zahlreiche Tiefeninterviews im Rahmen dieser Studie haben sich dabei Schwerpunkte herauskristallisiert, die in den jeweiligen Phasen des Verteidigungsprozesses besonderer Aufmerksamkeit bedürfen.

Die nachfolgenden Ausführungen mögen als Blaupause für den neuen Quadranten im vorgestellten Sicherheitsvisier dienen. Die quantitative Erhebung hat die Einsichten bestätigt. Insbesondere wurde auch hier deutlich, dass die in den Unternehmen bisher erreichten Umsetzungsstände teilweise noch weit von den geplanten Realisierungen entfernt sind.

»Eine frühzeitige Erkennung von Desinformationsangriffen ist entscheidend für eine erfolgreiche Verteidigung – eine digitale Früherkennung kann dies leisten. Die Digitalisierung der Desinformation erfordert die Digitalisierung der Früherkennung.«

Prof. Dr. Martin Grothe

Die Hervorhebung besonders wichtiger Gestaltungsbereiche kann wohl in vielen Fällen als erste Leitplanke dienen. Herausstellen lässt sich die zentrale Bedeutung der Detektion und Bewertung der Angriffe im digitalen Raum. Nur wenn hier großer Zeitverlust vermieden werden kann, ist eine erfolgreiche Reaktion überhaupt noch möglich.

Da viele Sicherheitsbereiche jedoch keinen Zugriff auf geeignete Instrumente oder Services haben – darunter fallen auch die Standard-Tools der Kommunikationsbereiche – deutet sich hier bereits der größte Hebel zur Verbesserung der Reaktions- bzw. Schutzfähigkeit an.

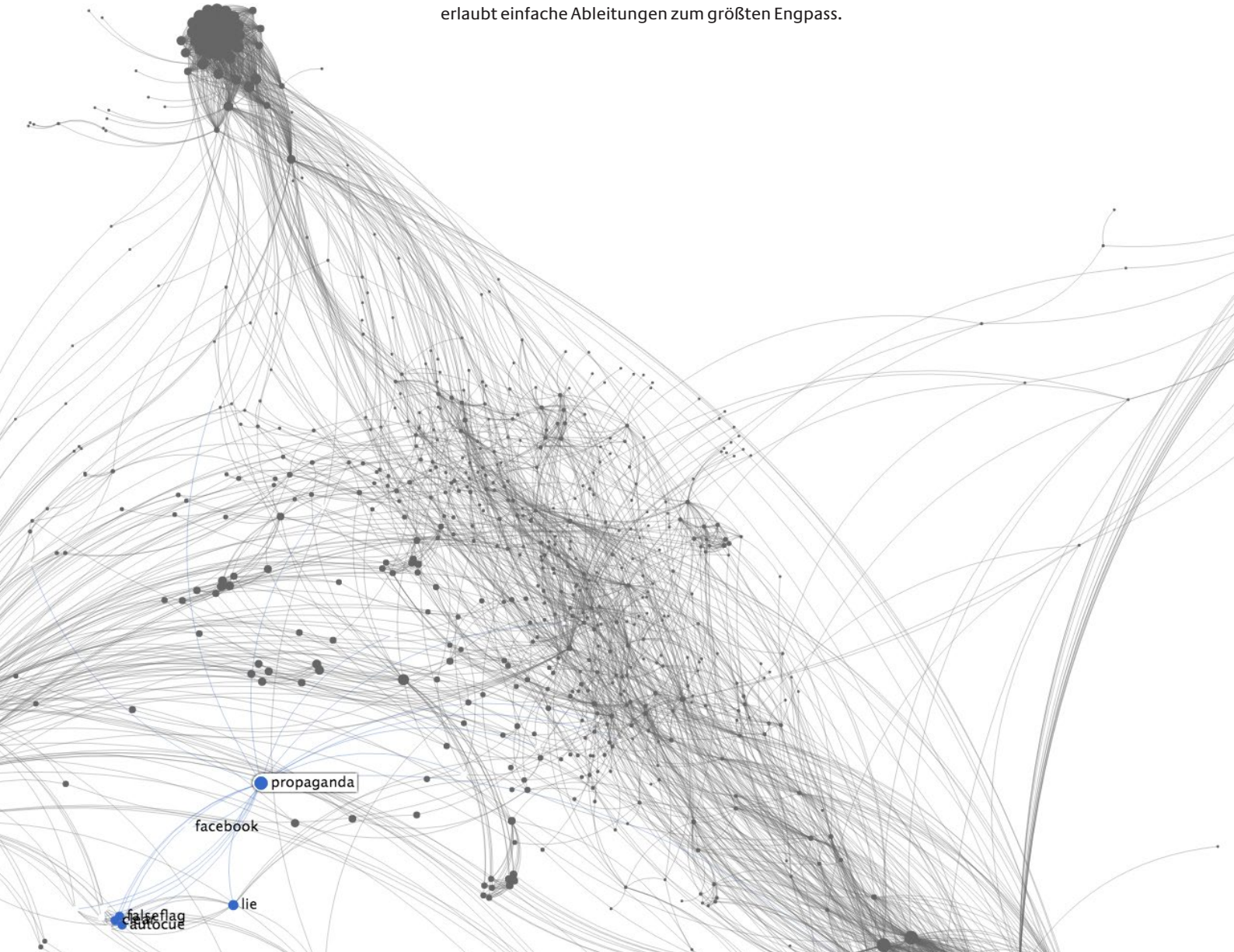
Insgesamt wird der Verteidigungsprozess hier in 5 Phasen gegliedert. Jede Phase trägt einen wichtigen Baustein zum erfolgreichen Umgang mit dieser neuen Bedrohung bei und orientiert sich an einer parametrisierbaren Leitfrage.

Abbildung 18:
Verteidigungsprozess Desinformation
(Quelle: ASW Bundesverband und complexium)

Dadurch lässt sich ein Phasen-Radar aufspannen:

1. Vorbereitung/Prävention: Wie weit sind Abläufe und Governance-Strukturen zum Umgang mit Desinformationsangriffen bereits konzipiert/implementiert?
2. Detektion: Mit welchem Nachlauf sollten Desinformationsangriffe identifiziert werden?
3. Bewertung: Wie schnell sollten entsprechende Signale qualifiziert und eskaliert werden?
4. Eindämmung/Lösung/Wiederherstellung: Wie weit sind direkte Gegenmaßnahmen bereits konzipiert/implementiert?
5. Vorfall-Nachbehandlung: Ist ein Konzept für weiterreichende Folgemaßnahmen bereits konzipiert/implementiert?

Dieses Phasen-Radar gibt Aufschluss über den jeweils bestehenden Soll-Ist-Gap und erlaubt einfache Ableitungen zum größten Engpass.



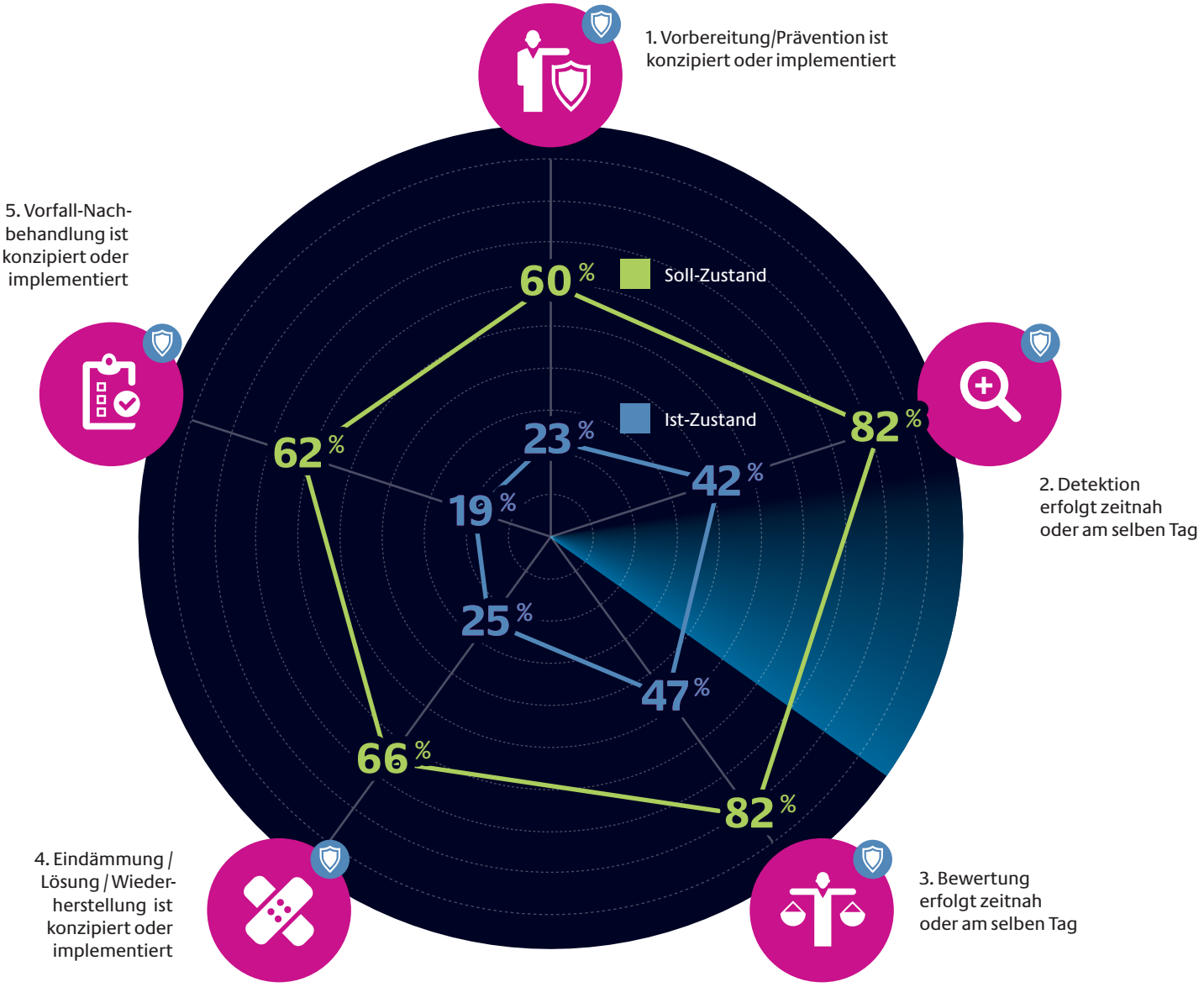


Abbildung 19:
Verteidigungsprozess im Phasen-Radar
(Quelle: Onlinebefragung
im Rahmen der Studie)

4.2 Phase 1: Vorbereitung/Prävention

Um der neuartigen Bedrohung professionell zu begegnen, sind definierte Abläufe und Governance-Strukturen unabdingbar. Mit fünf Punkten wird die Prävention wirkungsvoll aufgebaut:

1. Mit einem initialen **Stresstest** konfrontieren Sie die Organisation mit möglichen Desinformationsszenarien gegen Ihr Unternehmen. Gerade mehrschichtige Angriffe können Unternehmen vor große Herausforderungen stellen.
2. Die neue Bedrohung erfordert die Formulierung einer umfassenden **Security Policy** zur Vorbereitung auf entsprechende Angriffe. In der Policy werden Verantwortlichkeiten, Verhaltensleitlinien und insbesondere die notwendige Informationsintegration zwischen verschiedenen Fachbereichen strukturiert.
3. Die kontinuierliche **Sensibilisierung und Schulung** verschiedener Mitarbeitergruppen ist eine wesentliche Grundlage der Prävention. Wie auch im Bereich Social Engineering sind hier keineswegs nur obere Hierarchiestufen zu berücksichtigen. Ein geeignetes Format für Schulungen ist insbesondere E-Learning, um den Mitarbeitern die Komplexität der Bedrohung anschaulich und nachhaltig zu vermitteln.
4. In der Anpassung der Aufbau- und Ablaufstruktur des **Incident- und Krisenmanagements** sollte das spezifische Mengengerüst künftiger Angriffe seinen Niederschlag finden: Es sind deutlich weniger Störfälle als im Bereich der Cyber Security zu erwarten, aber es wird aller Voraussicht nach kontinuierlich Angriffe unterschiedlicher Intensität geben. Das Incident-Management muss in der Lage sein, laufend eine größere Anzahl von Detektionen zu evaluieren und zu verfolgen.
5. Der Umgang mit Desinformationsangriffen erfordert ein kontinuierliches Lernen. Hierbei kommt dem **regelmäßigen Austausch** mit Sicherheitsbehörden, Pressevertretern, Forschern und anderen Corporate Security-Professionals eine große Bedeutung zu.

Ergebnisse aus den Interviews

Eine der wichtigsten Verteidigungslinien im Kampf gegen Desinformation ist die Sensibilisierung der Mitarbeiter. Denn je mehr Informationen über ein Unternehmen nach außen gelangen, umso leichter fällt es Angreifern, Falschinformationen Authentizität zu verleihen. Von daher wünschen sich die Sicherheitsverantwortlichen von den Mitarbeitern vor allem eine gesunde Portion Skepsis: Welche Information kann ich wem weitergeben? Was kann ich im Netz posten? Was könnten mir oder dem Unternehmen feindlich gesinnte Menschen damit vielleicht anfangen?

Um Mitarbeiter zu sensibilisieren, setzen viele Unternehmen – aber längst nicht alle – auf Awareness-Maßnahmen. Dabei reicht die Palette von Unternehmens-Policies zum Verhalten im Internet über unternehmensweite Aufklärungskampagnen bis hin zu E-Learnings zu Social Engineering und anderen Themen. Bei manchen Unternehmen sind regelmäßige Schulungen obligatorisch, bei anderen freiwillig oder finden einmalig nach der Einstellung statt.

Notwendig wäre ein umfassendes und nachhaltiges Maßnahmenpaket. Eine Policy gibt einen guten Rahmen und Anlass für fortwährende Awareness-Kampagnen, verbunden mit verpflichtenden E-Learnings für die Mitarbeiter.

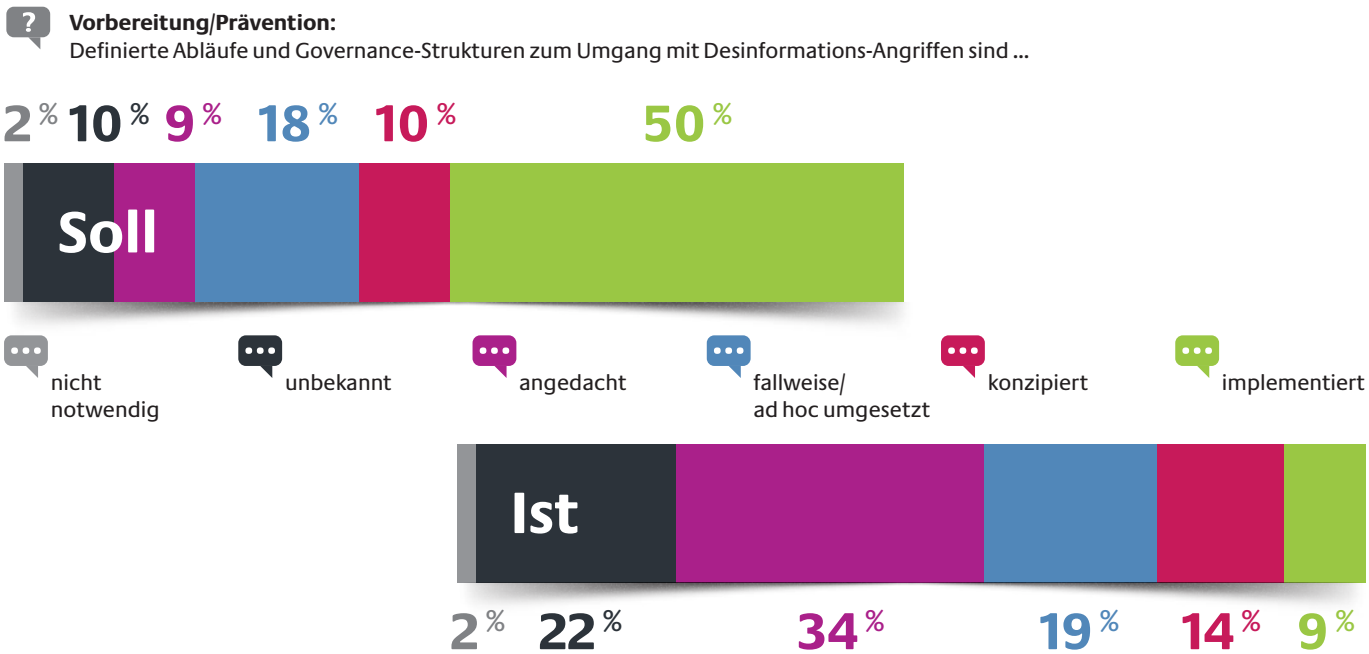
Sensibilisierte, internetaffine Mitarbeiter können zudem ein Frühindikator sein für auffällige Meldungen im Internet, die gegen das Unternehmen gerichtet sind.

Für den Ernstfall müssen die Strukturen stehen, um Incidents auch entsprechend handhaben zu können. So gibt es in den allermeisten Unternehmen Krisenpläne, die zumindest eine Struktur definieren: Wer sitzt im Krisenstab, wie sind die Meldewege etc.? Spezielle Pläne für eine Reputationskrise liegen längst nicht bei allen Unternehmen in der Schublade. Das zeigt auch die Onlinebefragung. Laut der Hälfte der befragten Unternehmen sollte dies jedoch Standard sein. Auch ein präventiver Austausch mit den Sicherheitsbehörden ist sinnvoll, zählt aber nicht bei allen Unternehmen zur Routine. Viele der Befragten wünschen sich einen intensiveren Austausch mit den Behörden, nicht nur allgemein zur Bedrohungslage, sondern auch speziell zum Thema Desinformation: Welche Erkenntnisse liegen hier vor und an wen kann man sich im Fall der Fälle wenden?

Darüber hinaus ist ein enger Draht und regelmäßiger Austausch mit der Presse hilfreich, um im Ernstfall die notwendige Glaubwürdigkeit zu besitzen und Desinformationen entgegentreten zu können, wenn sie bereits ihren Weg in die etablierten Medien gefunden haben. Zudem können solche Kontakte wertvolle Frühindikatoren sein, wenn gut vernetzte Journalisten das Unternehmen frühzeitig auf Gerüchte ansprechen, die gerade kursieren.

Es gibt einige wenige Unternehmen, die in der Präventionsarbeit sehr gut aufgestellt sind. Diese schulen ihre Mitarbeiter regelmäßig, sie haben definierte Krisenpläne – auch für eine Reputationskrise –, die Sicherheitsabteilung ist fest eingebunden. Darüber hinaus gibt es einen engen Austausch mit Behörden und der Presse.

Abbildung 20:
Phase Prävention im Ist-Soll-Vergleich (Quelle: Onlinebefragung im Rahmen der Studie; rundungsbedingte Differenzen)



4.3 Phase 2: Detektion

Jedes Unternehmen muss entscheiden, mit welchem Nachlauf Desinformationsangriffe identifiziert werden sollten und entsprechende Vorkehrungen treffen. Fünf Punkte sind für die Gewährleistung einer umfassenden Detektionsfähigkeit wichtig:

1. Es ist überaus förderlich, wenn Corporate Security über einen Zugriff auf eine **„artgerechte Systemunterstützung“** verfügt. Instrumente, die Daten für andere Zielsetzungen, etwa zur Ermittlung der Reichweite der eigenen Kommunikation, lediglich sammeln und zählen, sind nur im Zufallsfall hilfreich für Sicherheitsfragen.
2. Sicherheitsrelevant wertvolle Informationen sind zumeist a priori nicht exakt beschreib- oder geschlossen aufzählbar. Besonders relevant ist die Überraschung, der neue Angriffsmodus, der nicht in einem vordefinierten Suchmuster abgebildet sein kann. Security benötigt Ansätze, die **frühzeitig hypothesenfrei Ungewöhnliches** finden. Das Finden von solchen „unknown Unknowns“ ist zentraler Erfolgsfaktor dieser Anforderung.
3. Die Erfahrung zeigt weiterhin, dass Sicherheitsbereiche gut durch **qualifizierte Alerts und fundierte Lageberichte** unterstützt werden. Für die teilautomatisierte Durchsicht großer Treffermengen aus diversen Kanälen ist eine ressourcenseitige Ausstattung einzuplanen.
4. Es ist intern abzustimmen, welche **Indikatoren aus anderen Fachbereichen** in welchen Frequenzen zu einem integrativen Bild zugeliefert werden. Ein ganzheitliches Indikatorenmodell ist eine gute Zielvorstellung. Dies erfordert, dass die betroffenen Fachbereiche ein Digital Listening zu ihrem digitalen Relevanzbereich installiert haben: Wenn etwa der HR-Bereich die digitalen Hotspots seiner Engpasszielgruppen noch nicht im Blick hat, dann werden mögliche Desinformationsansätze (oder andere Bedrohungen) auch nicht erkannt. Über eine gemeinsame Perspektive ist funktionales Einvernehmen, in dem die Sicherheitsbelange nicht zu kurz kommen sollten, zu erzielen.
5. Weiterhin bietet der digitale Raum eine grundsätzlich einfache Möglichkeit, nicht nur den Status der eigenen Kontexte aufzunehmen und zu analysieren, sondern auch die Situation vergleichbarer oder besonders gefährdeter Unternehmen zu erschließen. Ein solcher **„Blick über den Tellerrand“** ist sehr geeignet, um die eigene Frühwarnfähigkeit weiter zu verbessern: potenziell „herüberschwappende“ Bedrohungen werden erkannt.

Ergebnisse aus den Interviews

Insgesamt ist die digitale Früherkennung bei den Unternehmen ausbaufähig. Die Zuständigkeit liegt fast immer und oftmals ausschließlich bei der Kommunikationsabteilung. Dort ist man zwar über die Erstellung klassischer Pressespiegel, die sich auf Printmedien fokussieren, hinausgegangen. So wird im Internet nach definierten Begriffen gesucht – wie Unternehmens- und Markennamen. Jedoch ist der Umfang der Internetbeobachtung oftmals noch begrenzt. Die Beschränkungen liegen zum einen in der Sprache – gesucht wird auf Deutsch und Englisch –, zum anderen sind sie bedingt durch die definierten Begriffe: Es fehlt die Suche nach den unknown Unknowns.

Gleichwohl ist die Bandbreite an Lösungen und Verfahren groß. Manche Unternehmen verfügen über eigene Tools zur Detektion, andere beauftragen professionelle Dienstleister, einige Unternehmen behelfen sich mit Google-Alerting oder anderen frei verfügbaren Werkzeugen.

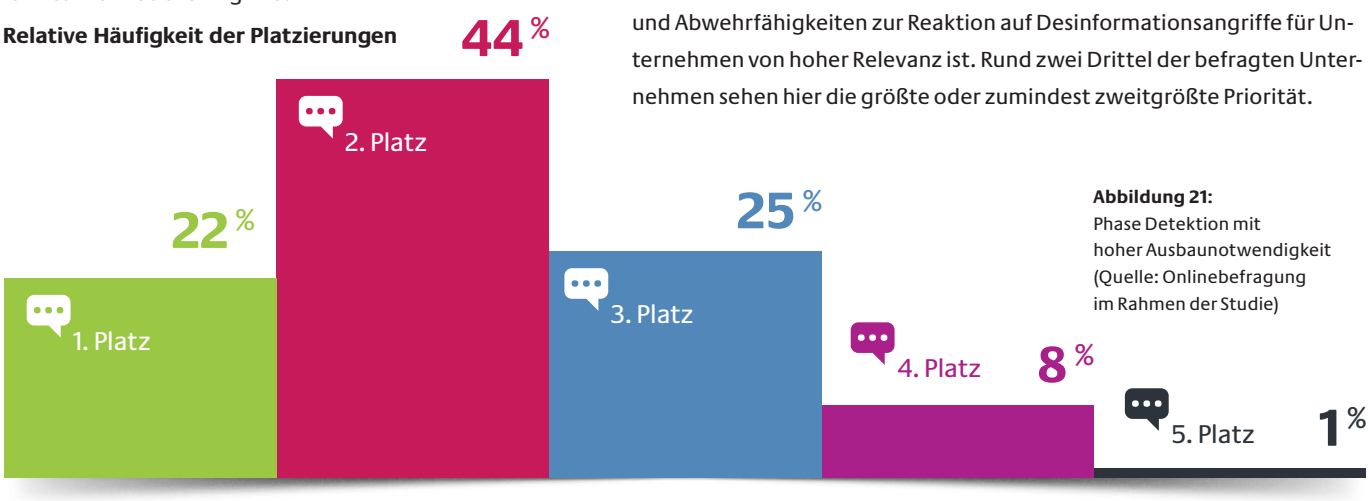
Professionell aufgestellte Unternehmen durchsuchen das Internet weltweit, in allen Ländern, wo sie präsent sind – und auch in allen relevanten Sprachen. Die regionalen Standorte informieren entsprechend über wesentliche Quellen und Suchbegriffe.

Auch die Sicherheitsabteilungen verfügen zum Teil über eigene Tools oder Dienstleister, die für sie das Internet nach relevanten Informationen zum Unternehmen durchsuchen – mit Bezug auf Sicherheitsrelevanz. Unternehmen, die das Thema „Netzbeobachtung“ ernst nehmen, können aber auch schnell in eine Kostenfalle laufen. So kommt es vor, dass neben der Kommunikations- und der Sicherheitsabteilung unter anderem auch die Bereiche Politik, Strategie, Marketing oder einzelne Länder das Netz durchforsten – und im schlimmsten Fall ihre Informationen nicht oder nur unstrukturiert und damit unzureichend miteinander teilen.

Eine hypothesenfreie Suche, ohne oder zumindest nicht nur nach vorgegebenen Suchbegriffen, findet im Rahmen der Netzbeobachtung von Unternehmen bislang noch kaum statt.

Bedarf
Wie notwendig ist der Ausbau der Detektions- und Abwehrfähigkeiten für Desinformations-Angriffe?

Relative Häufigkeit der Platzierungen



Auch die Onlinebefragung zeigt deutlich, dass der Ausbau der Detektions- und Abwehrfähigkeiten zur Reaktion auf Desinformationsangriffe für Unternehmen von hoher Relevanz ist. Rund zwei Drittel der befragten Unternehmen sehen hier die größte oder zumindest zweitgrößte Priorität.

Abbildung 21:
Phase Detektion mit hoher Ausbaunotwendigkeit (Quelle: Onlinebefragung im Rahmen der Studie)

4.4 Phase 3: Bewertung

Nach der Detektion schafft die Bewertung eines möglichen Desinformationsangriffs erste Klarheit: Wie schnell sollten entsprechende Signale qualifiziert und eskaliert werden? Der Sicherheitsbereich wird sich auch an diesem Key Performance Indicator messen lassen müssen. Die Bewertung dieser neuartigen Angriffsvektoren kann durch fünf Punkte abgesichert werden:

1. Die Erfassung und Bewertung von Bedrohungen und Angriffen muss ein **systematischer Prozess** sein. Nach der Detektion sind das Filtern und Kategorisieren wesentliche Herausforderungen.
2. In der Bewertung werden sowohl die jeweiligen **Inhalte** und ihr Kontext, als auch die jeweiligen **Quellen** und ihr Netzwerk berücksichtigt.
3. Es ist sinnvoll, ein entsprechendes **Daten-Verzeichnis** einzusetzen. Hier kann auch das Indikatorenmodell einfließen. Quantitative Maßstäbe und Vergleichswerte erleichtern die Lageeinschätzung.
4. Für die Bewertung etwa von auftauchenden Vorwürfen ist ein schneller und **eingespielter Austausch** mit verschiedenen Fachseiten und Unternehmensbereichen, auch aus der Lieferkette, essenziell. Nur so können potenzielle Desinformationen von korrekten Tatsachen getrennt werden.
5. Aus den Bewertungen wird ein **Lagebild** gespeist, das auch unabhängig von der Cyber-Lage bestehen sollte. Aus diesem Lagebild sind die Prioritäten der Eindämmung ersichtlich.

Ergebnisse aus den Interviews

Informationen über einen möglichen Desinformationsangriff laufen bei fast allen befragten Unternehmen in der Kommunikationsabteilung zusammen, die bei vielen Betrieben die Sicherheitsabteilung mit einbezieht. Eine organisatorisch festgeschriebene, formelle Einbindung fehlt jedoch bei einem guten Teil der Unternehmen.

Zudem würde es bei einigen Unternehmen nicht auffallen, wenn sich Desinformationsangriffe gleichzeitig gegen unterschiedliche Bereiche richten – beispielsweise Personal UND Vertrieb. Dies kann leicht dazu führen, dass eine Bedrohung eklatant unterschätzt wird. Ein Reputationslagebild, das eine genaue Übersicht zeichnet, in welchen Bereichen das Unternehmen wo und wie wahrgenommen wird, existiert in den wenigsten Fällen.

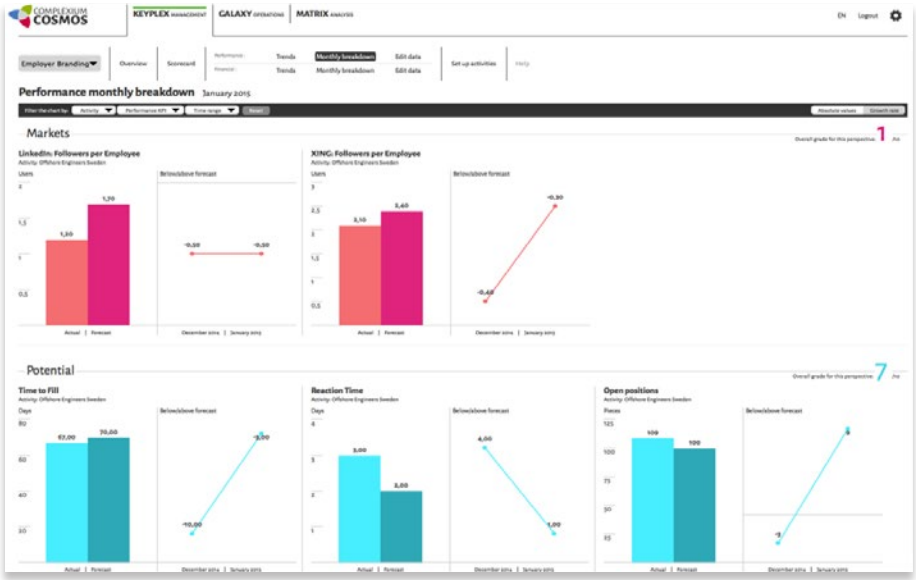
Würden in einem kombinierten Angriff zudem Hackerangriffe stattfinden, gäbe es bei vielen Unternehmen keine Stelle, die die Gleichzeitigkeit bemerken und einen Zusammenhang herstellen könnte.

Von zentraler Bedeutung ist es daher, Strukturen aufzubauen, die sicherstellen, dass Angriffe bzw. entsprechende Indikatoren hierfür, egal welcher Art und welchen Ausmaßes, an eine Stelle – hier kommt eigentlich nur die Sicherheitsabteilung infrage – kommuniziert werden. Denn eine Vielzahl kleiner Angriffe kann in der Summe einen großen Angriff ausmachen oder die Vorphase eines kombinierten Angriffs bedeuten.

Eine solche Bewertungslösung muss mehrere notwendige Anforderungen erfüllen:

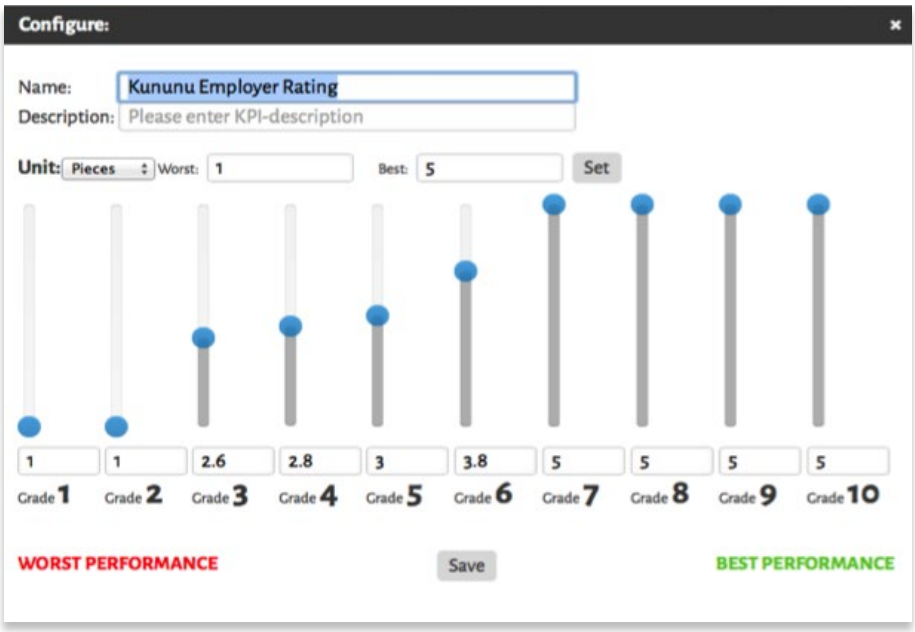
- So muss es möglich sein, relevante Daten, etwa Produktbewertungen, direkt aus dem Internet aufzunehmen. Andere Informationen stammen aus unternehmensinternen Quellen: Diese müssen entweder per Datenbank-Import oder aber manueller Eingabe aufgenommen werden.
- Idealerweise werden zudem nicht nur Ist-Daten festgehalten, sondern auch Plan-Daten bzw. Erwartungswerte integriert, um etwa Änderungen aufgrund bekannter Umfeldfaktoren zu berücksichtigen.

Abbildung 22:
Beispiel: Dateneingabe und Wertevergleich mit dem Kennzahlen-Tool KEYPLEX (Quelle: complexium)



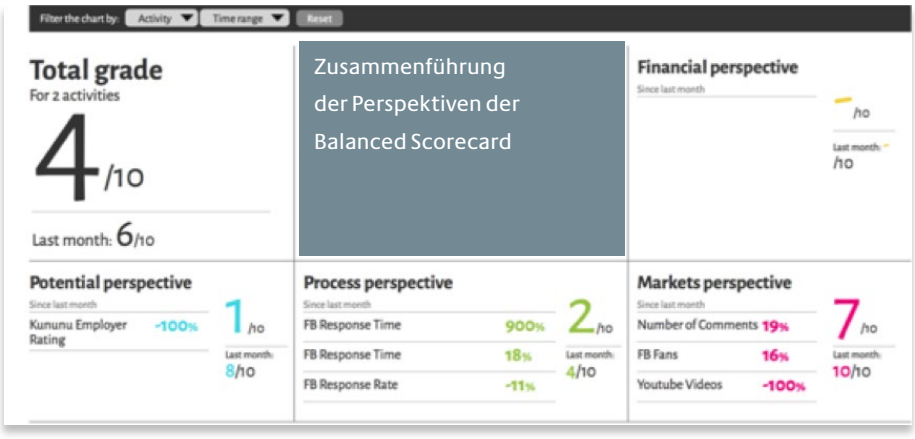
- Weiterhin ist es erforderlich, dass unterschiedliche Kenngrößen zu aggregierten Werten verdichtet werden, die etwa Auskunft über einzelne Scorecard-Perspektiven geben. Außerhalb der monetären Sphäre ist dies nur über Gewichtungsfunktionen möglich.

Abbildung 23:
Beispiel KEYPLEX Gewichtungsfunktion
(Quelle: complexium)



- Auf der Basis des Indikatorenmodells können auf einer Übersichtsebene verdichtete Lageparameter und individuelle Kenngrößen dargestellt werden.

Abbildung 24:
Beispiel KEYPLEX Übersicht
auf Basis des Indikatorenmodells
(Quelle: complexium)



Mit einer geeigneten Systemunterstützung (beispielsweise KEYPLEX) wird die Bewertung auftretender Unregelmäßigkeiten vereinfacht.

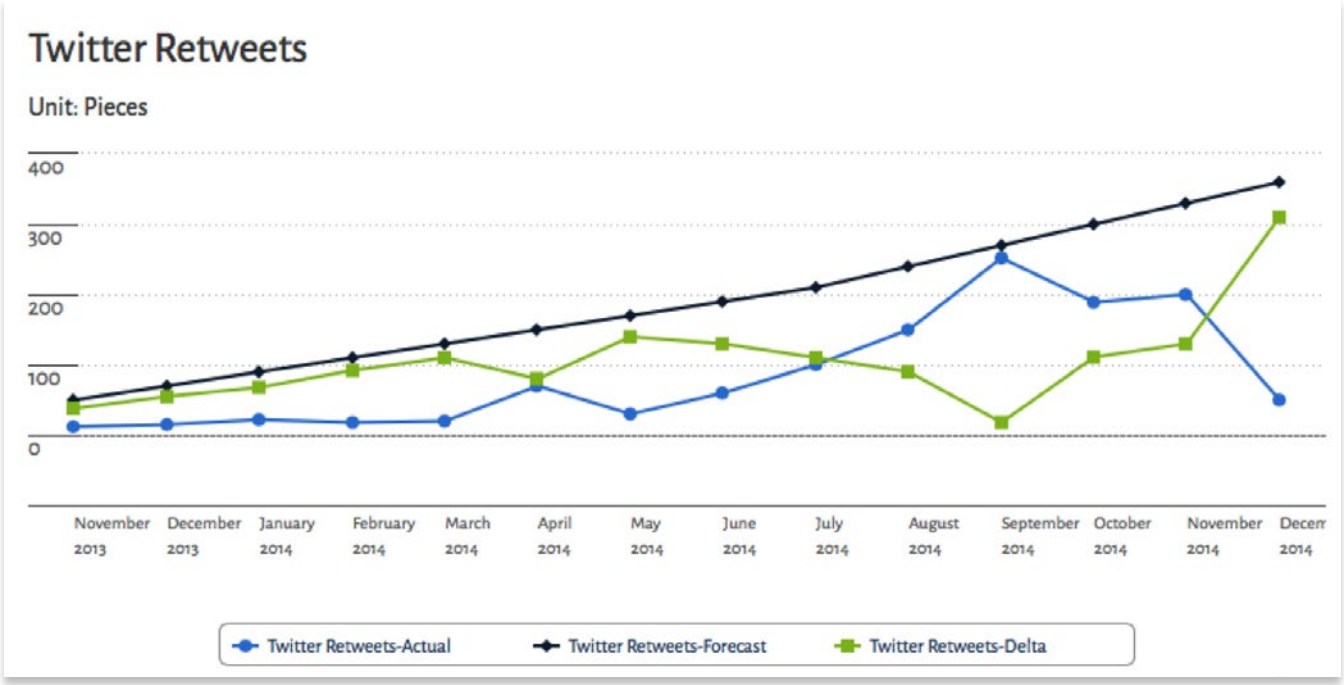


Abbildung 25:
Beispiel KEYPLEX Indikatorverlauf
(Quelle: complexium)

Die hier beispielhaft dargestellte Lösung KEYPLEX ist eine Co-Innovation von complexium und SAP.

4.5 Phase 4: Eindämmung/Lösung/Wiederherstellung

Die Eindämmung eines Desinformationsangriffs oder sogar direkte Gegenmaßnahmen können durch fünf Punkte abgesichert werden:

1. Grundlage der Eindämmung ist eine **strukturierte Fallbeschreibung** mit spezifischer Bewertung. Wesentlich ist die Identifikation des Ursprungs einer Desinformation.
2. Stets sollen **rechtliche Schritte** geprüft werden.
3. Für die Wirksamkeit einer Reaktion ist Geschwindigkeit ein wichtiger Faktor. Zudem sollte die Kommunikation dort ansetzen, wo der Angriff seinen Niederschlag gefunden hat. Entsprechend müssen Unternehmen grundsätzlich in den relevanten **Echokammern** präsent werden.
4. Fallbezogen kann es die Eindämmung deutlich unterstützen, **breite Medien** einzubeziehen, um Reichweite zu erzielen. Der Beziehungsaufbau zu diesen Medien sollte bereits in der Prävention angelegt sein.
5. Sämtliche Maßnahmen zur Eindämmung eines Desinformationsangriffs sollten im Einklang mit den betroffenen **internen Funktionsbereichen** konzipiert und umgesetzt werden.

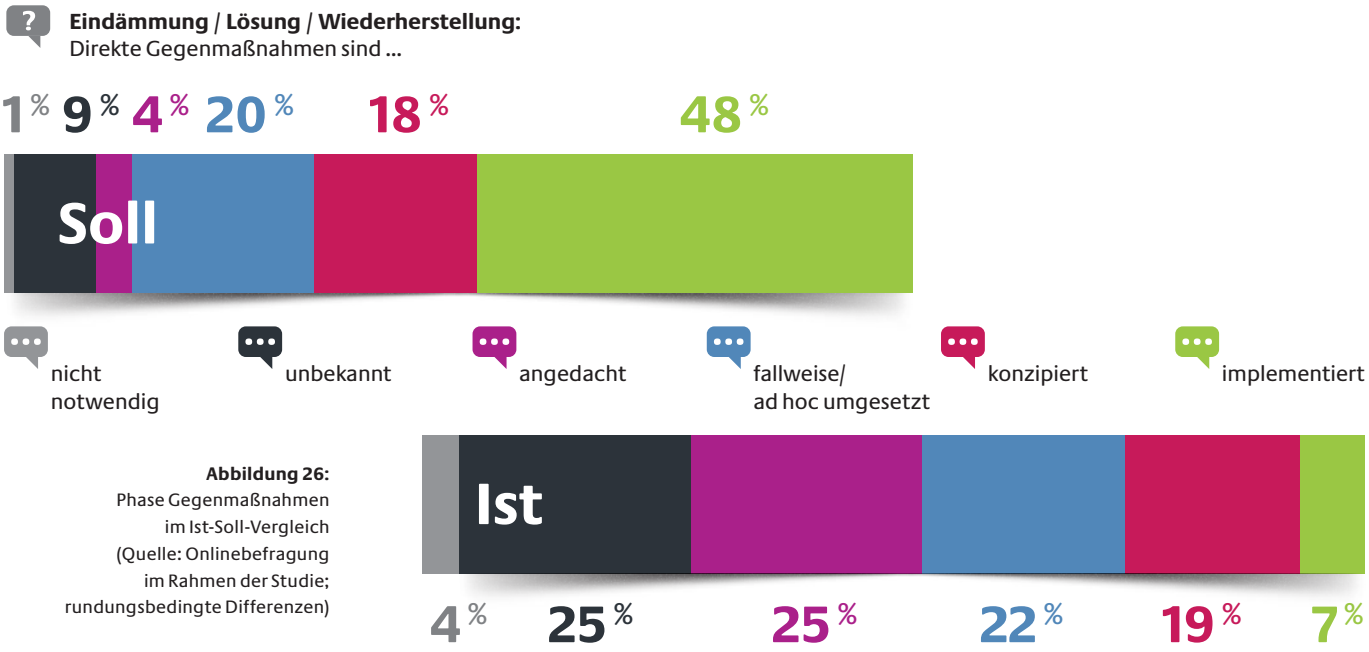


Abbildung 26:
Phase Gegenmaßnahmen im Ist-Soll-Vergleich (Quelle: Onlinebefragung im Rahmen der Studie; rundungsbedingte Differenzen)

Ergebnisse aus den Interviews

Eine der schwierigsten zu beantwortenden Fragen ist die, wie auf einen Desinformationsangriff reagiert werden kann und sollte. Die Frage lässt sich in dieser Allgemeinheit auch nicht zufriedenstellend beantworten. So können Desinformationsangriffe in Ausmaß und Art so unterschiedlich sein, dass auch die Antwort jeweils unterschiedlich ausfallen muss.

In einem Punkt sind sich jedoch alle Unternehmen einig, das zeigen zumindest die Interviews. Eigene Bot-Armeen einsetzen möchte keiner – so jedenfalls der jetzige Stand der Dinge. Die Gefahr wird als zu groß angesehen, dass ein Aufdecken solcher Maßnahmen einen beträchtlichen Reputationsverlust nach sich ziehen könnte und damit den Angreifern in die Hände spielen würde.

Dies zeigt bereits, dass eine Informations-/Desinformationsschlacht mit sehr ungleichen Mitteln geschlagen werden müsste. Es handelt sich um einen asymmetrischen Kampf, bei dem die Angreifer jede Waffe nutzen können, während den Verteidigern nur ein beschränktes Arsenal bleibt.

Gleichzeitig sieht etwa die Hälfte der befragten Unternehmen es als notwendig an, dass direkte Gegenmaßnahmen vorbereitet sein sollten. Dass diesen Stand nicht einmal jedes zehnte Unternehmen erreicht hat, dürfte ein realistisches Bild sein. Diese Einschätzung ergibt sich zumindest aus den im Rahmen dieser Studie geführten Interviews und Expertengesprächen. An dieser Stelle sei nochmals darauf verwiesen, dass für die Studie primär Vertreter von Unternehmen herangezogen wurden, die eine hohe Expertise besitzen und bereits überdurchschnittlich gut aufgestellt sind.

Somit überrascht es auch nicht, dass die Unternehmen, in den Interviews gefragt nach ihrer Reaktion auf einen Desinformationsangriff, überwiegend angaben, zunächst die Hintergründe (schnell) zu analysieren und dann fallbezogen angemessen zu reagieren. Angemessen bedeutet dabei meist, eher zurückhaltend zu agieren. Die wenigsten Unternehmen verfolgen eine offensive Kommunikationsstrategie.

Klassische Gegendarstellungen verfangen meist nicht, so die Erfahrungen der Unternehmen. Dennoch wird dieses Mittel weiterhin angewandt. Gegendarstellungen können jedoch auch ohne direkten Bezug zum Angriff erfolgen, um diesem nicht zusätzlichen Auftrieb zu verleihen. Im Zweifel greifen Unternehmen auch zum Mittel der Unterlassungsklage und ergreifen weitere rechtliche Schritte.

Die bisherigen Erfahrungen mit reputationsschädigenden Äußerungen beziehen sich jedoch meist auf bekannte Akteure, denen man auch in den klassischen Medien begegnen und mit denen man auch das Gespräch suchen kann. Das macht eine Reaktion vergleichsweise einfach.

Schwieriger dürfte es werden, wenn Desinformationsangriffe von unbekannter Seite im Internet auftauchen – und dann auch dort bekämpft werden müssen. Die hier angesprochene Zielgruppe wird nicht immer von den klassischen Medien erreicht, sodass eine Reaktion auf dieser Seite sicherlich unterstützend hilfreich sein kann, jedoch nicht den entscheidenden Ausschlag geben dürfte.

4.6 Phase 5: Vorfall-Nachbehandlung

Mit der Vorfall-Nachbehandlung beginnt die Prävention. Es gilt aus jedem Vorfall von Desinformation zu lernen. Ein Konzept für weiterreichende Folgemaßnahmen leitet dies ein. So kann diese wichtige Aufgabe durch fünf Punkte abgesichert werden:

1. Aufsetzpunkt für weiterführende Maßnahmen ist ein klares **Debriefing** des **Vorfall- bzw. Krisenmanagements.**
2. Mit dieser Reflektion lassen sich innengerichtet **Strukturen anpassen** und ggf. Suchparameter nachschärfen: Prävention, Detektion und Bewertung werden verbessert.
3. Das Unternehmen muss auch bestrebt sein, nicht nur einen eingetretenen Schaden zu begrenzen, sondern den Angreifer zu ermitteln und nachhaltig abzuwehren. Hierzu kann ein **Strategieprozess** notwendig sein.
4. Weiterhin gilt es zu analysieren, welche weiteren **Akteure** artverwandte Szenarien einsetzen könnten. Dies gilt es, proaktiv abzuwehren oder zumindest prohibitiv zu erschweren.
5. **Mit Information gegen Desinformation:** Das Unternehmen steht nicht alleine; es gilt, relevante Information mit dem Netzwerk zu teilen.

4.7 Zwischenfazit

Je später ein Vorfall von Desinformation erkannt wird, desto größer ist der mögliche Schaden und desto schwieriger wird es, den Vorfall zu beheben. Entscheidend sind daher vor allem Präventionsarbeit und eine gute, verlässliche Detektion.

Unternehmen müssen frühzeitig erkennen, welche Informationen über sie, aber auch über ihre Branche, ihre Mitbewerber und zu anderen Themen, die sie berühren könnten, kursieren. Wird bereits der erste Tweet, der erste Blockeintrag, der erste Facebook-Kommentar eingefangen, der Relevanz haben könnte, kann das Unternehmen gleich im Anfangsstadium die Quelle ausfindig machen und die Inhalte bewerten. Es kann sich dann sofort auf mögliche weitere Entwicklungen vorbereiten und gegebenenfalls entsprechend reagieren.

Vor allem aber kann das Unternehmen erkennen, ob ein komplexerer Angriff erfolgt, wenn alle Informationen (auch Indikatoren!) an einer zentralen Stelle gebündelt ankommen und bewertet werden. Eine solche Bewertung muss unmittelbar erfolgen – wenigstens innerhalb eines Tages. Für den Fall der Fälle muss ein ausgearbeiteter Krisenplan stehen, der Strukturen, Prozesse, Personen und Verantwortlichkeiten benennt – speziell für den Fall von Desinformation und Reputationskrisen.

Wer bei einer Reputationskrise externe Unterstützung hinzuziehen möchte, sollte nicht erst in der Krise die „Gelben Seiten“ zur Hand nehmen und mit der Suche beginnen, sondern sich bereits im Vorfeld für einen Partner entscheiden. Im Idealfall werden Verträge bereits vorab geschlossen und die Agentur, die das Unternehmen dann bereits kennt, ist gewissermaßen auf Standby. Mit diesem Dienstleister kann dann auch vorab ein Verteidigungsprozess aufgesetzt und eingeübt werden. Damit gewinnt man in der Krise wertvolle Zeit und ist sofort handlungsfähig.

5. Fazit: 11-Punkte-Plan für den Desinformationsschutz

Die Studie hat dargestellt, mit welchen Methoden und in welchen Kontexten Angriffe durch Desinformation ausgeführt werden können. Durch die Digitalisierung kann ein Bedrohungsniveau erreicht werden, auf das weder Unternehmen noch Staat bisher vorbereitet sind.

So fehlt es an vielen einzelnen Stellen an einer hinreichend leistungsfähigen Detektion, zumeist auch an einer Integration und Zusammenführung einzelner Erkenntnisse. Sicherlich fehlt es aber nicht an den grundlegenden Prozessen und Vorgehensweisen.

Im Folgenden wird ausgeführt, welche Bausteine und Abläufe Unternehmen aufsetzen und verbinden sollten, um diesen neuen Bedrohungen möglichst angemessen zu begegnen.

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!

Anhang

Erläuterung zur Onlinebefragung

Insgesamt nahmen 106 Personen an der Onlinebefragung teil. Erläuterungen zu einzelnen Abbildungen:

Abbildung 10:
Künftige Angriffsszenarien im Aufmerksamkeitsranking

Gefragt wurde:

- Welche Angriffsszenarien werden in naher Zukunft relativ mehr / gleich viel / weniger Aufmerksamkeit erhalten müssen?

Als mögliche Angriffsszenarien wurden aufgeführt:

- DDoS-Angriff
- Desinformationsangriff
- Einbruch auf dem Firmengelände
- Kidnapping im Ausland
- Social Engineering-Angriff

Hierzu gab es jeweils folgende Antwortmöglichkeiten:

- am meisten
- deutlich mehr
- mehr
- gleich viel
- weniger
- nicht relevant

Für die Auswertung wurde auf folgendes Verfahren zurückgegriffen:

1. Schritt: Scoring-Methode

Im ersten Schritt wird jeder ausgewählten Antwort eine Punktzahl (Score) zugeteilt. Das Scoring beläuft sich auf einer Skala von -100 (nicht relevant) bis 150 (am meisten). Die Scores zu den Antwortmöglichkeiten sind in Fünfziger-Blöcken unterteilt:

- am meisten 150
- deutlich mehr 100
- mehr 50
- gleich viel 0
- weniger -50
- nicht relevant -100

2. Schritt: Einstufung

Im zweiten Schritt wird die Summe der Scores pro genanntem Angriffsszenario durch die Anzahl der befragten Teilnehmer dividiert. Der sich daraus ergebende Durchschnitt wird mit dem folgenden Bewertungsrahmen gruppiert:

- am meisten > 120
- deutlich mehr 85 bis 119
- mehr 50 bis 84
- gleich viel 0 bis 49
- weniger -50 bis -1
- nicht relevant -100 bis -51

Abbildung 14:
Bedrohung durch Desinformation im Bereich Arbeitgeberbild
(Im Onlinefragebogen unter der Überschrift Recruiting)

Gefragt wurde:

- Wie begegnet Ihr Unternehmen der Bedrohung durch Desinformationsangriffe bisher?

Antwortmöglichkeiten waren:

- Die Bedrohung ist neu für uns – wir gehen dies erst an.
- Die Bedrohung nehmen wir bisher punktuell auf.
- Die Bedrohung ist durch erste Abläufe abgedeckt.
- Die Bedrohung ist in Lagebild und Infrastruktur integriert.
- Die Bedrohung betrifft uns nicht.

Abbildung 15:
Bedrohung durch Desinformation im Bereich Mitarbeiter/Mitarbeiterloyalität
(Im Onlinefragebogen unter der Überschrift Personal)

Gefragt wurde:

- Wie begegnet Ihr Unternehmen der Bedrohung durch Desinformationsangriffe bisher?

Antwortmöglichkeiten waren:

- Die Bedrohung ist neu für uns – wir gehen dies erst an.
- Die Bedrohung nehmen wir bisher punktuell auf.
- Die Bedrohung ist durch erste Abläufe abgedeckt.
- Die Bedrohung ist in Lagebild und Infrastruktur integriert.
- Die Bedrohung betrifft uns nicht.

Abbildung 16:
Bedrohung durch Desinformation im Bereich Produktimage
(Im Onlinefragebogen unter der Überschrift Vertrieb)

Gefragt wurde:

- Wie begegnet Ihr Unternehmen der Bedrohung durch Desinformationsangriffe bisher?

Antwortmöglichkeiten waren:

- Die Bedrohung ist neu für uns – wir gehen dies erst an.
- Die Bedrohung nehmen wir bisher punktuell auf.
- Die Bedrohung ist durch erste Abläufe abgedeckt.
- Die Bedrohung ist in Lagebild und Infrastruktur integriert.
- Die Bedrohung betrifft uns nicht.

Abbildung 17:
Bedrohung durch Desinformation im Bereich Finanzielle Reputation/Kreditwürdigkeit
(Im Onlinefragebogen unter der Überschrift Kreditwirtschaft)

Gefragt wurde:

- Wie begegnet Ihr Unternehmen der Bedrohung durch Desinformationsangriffe bisher?

Antwortmöglichkeiten waren:

- Die Bedrohung ist neu für uns – wir gehen dies erst an.
- Die Bedrohung nehmen wir bisher punktuell auf.
- Die Bedrohung ist durch erste Abläufe abgedeckt.
- Die Bedrohung ist in Lagebild und Infrastruktur integriert.
- Die Bedrohung betrifft uns nicht.

Abbildung 19:
Verteidigungsprozess im Phasen-Radar

Gefragt wurde:

- Mit einem fünfstufigen Prozess können Unternehmen einem potenziellen Angriff durch Desinformation begegnen. Wie ist der jeweilige Status der Prozesskonzeption und Implementierung?

Antwortmöglichkeiten waren:

Jeweils für den Ist- und Soll-Zustand ...

1. Vorbereitung/Prävention

- nicht notwendig
- angedacht
- konzipiert
- implementiert
- fallweise / ad hoc umsetzen
- unbekannt

2. Detektion

- zeitnah
- ein Tag
- eine Woche
- ein Monat
- mehrere Monate

3. Bewertung

- zeitnah
- am gleichen Tag
- in der gleichen Woche
- im gleichen Monat
- halbjährlich

4. Eindämmung / Lösung / Wiederherstellung

- nicht notwendig
- angedacht
- konzipiert
- implementiert
- fallweise / ad hoc umsetzen
- unbekannt

5. Vorfall-Nachbehandlung

- nicht notwendig
- angedacht
- konzipiert
- implementiert
- fallweise / ad hoc umsetzen
- unbekannt

Um eine Aussage zu der Konzeption und der Implementierung der einzelnen Prozessschritte treffen zu können (bzw. der zeitnahen Reaktion), werden die hervorgehobenen Antwortkategorien aggregiert.

Abbildung 20:
Phase Prävention im Ist-Soll-Vergleich

Gefragt wurde:

Definierte Abläufe und Governance-Strukturen zum Umgang mit Desinformationsangriffen sind ...

- nicht notwendig.
- angedacht.
- konzipiert.
- implementiert.
- fallweise / ad hoc umsetzbar.
- unbekannt.

Abbildung 21:
Phase Detektion mit hoher Ausbaunotwendigkeit

Gefragt wurde:

Wie notwendig ist der Ausbau der Detektions- und Abwehrfähigkeiten für Desinformationsangriffe? Bitte bringen Sie die genannten Angriffsszenarien in eine Rangfolge nach dem notwendigen Ausbau der Detektions- und Abwehrfähigkeiten:

- DDoS-Angriff
- Desinformationsangriff
- Einbruch auf dem Firmengelände
- Kidnapping im Ausland
- Social Engineering-Angriff

Abbildung 26:
Phase Gegenmaßnahmen im Ist-Soll-Vergleich

Gefragt wurde:

Direkte Gegenmaßnahmen sind ...

- nicht notwendig.
- angedacht.
- konzipiert.
- implementiert.
- fallweise / ad hoc umsetzbar.
- unbekannt.

Profile der Studienpartner

ASW Bundesverband

Der ASW Bundesverband vertritt die Interessen der deutschen Wirtschaft in Sicherheitsfragen gegenüber Politik und Medien. Er wird getragen von den deutschen regionalen Sicherheitsverbänden sowie diversen fachspezifischen Bundesverbänden und Fördermitgliedern. Er ist aktiver Partner in der Gesetzgebung, Kommunikationspartner der Medien und das Scharnier zwischen Sicherheitsbehörden und der Wirtschaft.

Der ASW Bundesverband arbeitet mit allen wichtigen nachrichtendienstlichen und polizeilichen Organen und Sicherheitsbehörden zusammen. Er stellt sicher, dass Informationen von den Behörden bei den Unternehmen und umgekehrt ankommen. Denn frühzeitiges Wissen bedeutet nachhaltige Sicherheit.

Themen, mit den wir uns befassen:

- Anti-Fraud-Management
- Aus- und Weiterbildung
- Cyber-Security
- Lage und Reisesicherheit
- Logistiksicherheit
- Personelle Sicherheit
- Wirtschaftsschutz und Spionageabwehr

Leistungen für unsere Mitglieder:

- Kompetenz-Center
- Workshops
- Informationen
- Netzwerk
- Politische Arbeit
- Medienarbeit

Leistungen auch für Nicht-Mitglieder:

- Veranstaltungen
- Leitfäden & Leitblätter
- Studien
- Politische Arbeit
- Medienarbeit

Die Gefährdungslage für Deutschlands Unternehmen ist dynamisch und komplex. Dem begegnet der Verband mit vorgreifender Präventionsarbeit, hoher Spezialisierung und der Kooperation mit Forschungseinrichtungen und weiteren Sicherheitsverbänden. So bildet der ASW Bundesverband Deutschlands Kompetenzzentrum für alle unternehmerischen Sicherheitsanliegen – qualifiziert, engagiert, neutral.

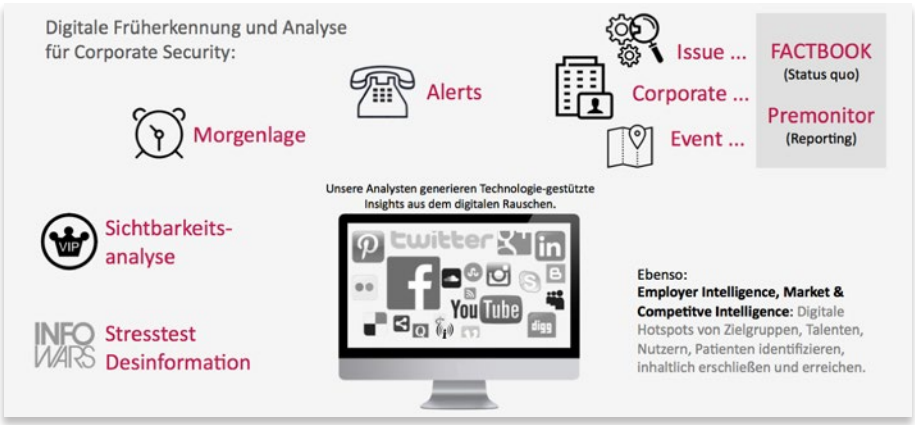
Der ASW Bundesverband unterhält sieben Kompetenz-Center, in denen seine Mitglieder zusammen mit Partnern und Sicherheitsexperten den jeweiligen Bedrohungen gezielt entgegenarbeiten.

complexium GmbH

complexium ist Vorreiter im Digital Listening und Partner des ASW Bundesverband – Allianz für Sicherheit in der Wirtschaft e.V.

Die Unternehmensberatung complexium GmbH unterstützt seit 2004 Klienten mit qualifizierten Alerts und passgenauen Reports. complexium hilft bei Bedrohungslagen und kritischen Öffentlichkeiten und reduziert Überraschungen.

complexium Lösungsraum
(Quelle: complexium)



Die Analysten und Entwickler von complexium arbeiten gemeinsam an und mit innovativen Werkzeugen zur Früherkennung und Inhaltserschließung. Bausteine der Analyse-Infrastruktur von complexium wurden im Programm „Forschung für die zivile Sicherheit“ vom Bundesministerium für Bildung und Forschung gefördert. Das von complexium entwickelte Analyse-Tool GALAXY beruht auf innovativen computerlinguistischen Algorithmen.
Die KEYPLEX-Lösung ist eine Co-Innovation mit SAP.

complexium arbeitet für Sicherheitsbereiche in den Feldern Automobil, Bank, Chemie, Defence, Energie, Family Office, Industrie, Pharma und Versicherung.

Mit diesen Erfahrungen unterstützt complexium Unternehmen beispielsweise bei folgenden Fragestellungen:

- Wie entwickeln sich kritische Vorwürfe und Bedrohungen spezifisch gegen unser Haus? Gibt es neue schwache Signale?
- Wie sieht die allgemeine Morgenlage für heute aus? Was haben Aktivisten auf der Agenda?
- Gibt es Tendenzen im Vorfeld unserer Hauptversammlung? Was passiert während des Verlaufs?
- Was passiert rund um unsere Lokation in Hamburg während des G20-Gipfels? Was müssen wir einplanen?
- Welche Risiken bringt der neue CEO mit? Wie transparent und wie sicherheitsaffin ist die Schutzfamilie?
- Können die Desinformationsangriffe der militanten Tierschützer gegen unsere Wettbewerber auf uns übergehen?
- Wie können mögliche Desinformationsszenarien gegen uns aussehen? Wie können wir uns vorbereiten?
- Welche Wellen schlägt der angekündigte Personalabbau? Kündigen sich Aktionen oder Blockaden an?

Deloitte GmbH

Deloitte.

Deloitte erbringt Dienstleistungen in den Bereichen Wirtschaftsprüfung, Risk Advisory, Steuerberatung, Financial Advisory und Consulting für Unternehmen und Institutionen aus allen Wirtschaftszweigen; Rechtsberatung wird in Deutschland von Deloitte Legal erbracht.

Mit einem weltweiten Netzwerk von Mitgliedsgesellschaften in mehr als 150 Ländern verbindet Deloitte herausragende Kompetenz mit erstklassigen Leistungen und unterstützt Kunden bei der Lösung ihrer komplexen unternehmerischen Herausforderungen.

„Making an impact that matters“ – für rund 263.900 Mitarbeiter von Deloitte ist dies gemeinsames Leitbild und individueller Anspruch zugleich.

Autoren

Jan Wolter

Jan Wolter war im Erstellungszeitraum dieser Studie Geschäftsführer des ASW Bundesverbandes sowie der ASW Projekt GmbH. Davor war er viele Jahre für einen Branchenverband in unterschiedlichen Leitungsfunktionen tätig.

Durch seinen Austausch mit Sicherheitsexperten unterschiedlicher Branchen und Unternehmensbereiche sowie Behördenvertretern, durch seine Tätigkeit in verschiedenen Gremien und Projekten sowie die Mitwirkung an Positionspapieren und anderen Publikationen des Verbandes hat sich Jan Wolter einen tiefen Einblick in die Bedrohungslage deutscher Unternehmen erarbeitet. Das Thema Desinformation setzte er bereits Ende 2015 auf die Agenda des Verbandes, als noch nicht von Fake News im Zuge des US-Wahlkampfes oder Brexit-Votums die Rede war.

Prof. Dr. Martin Grothe

Prof. Dr. Martin Grothe ist Gründer und geschäftsführender Gesellschafter der complexium GmbH sowie Honorarprofessor an der Universität der Künste (UdK) in Berlin.

Als Honorarprofessor an der UdK für das Fach „Digitale Kommunikation/Leadership, Social Media Management“ betreut er das berufsbegleitende Master-Programm „Leadership in digitaler Kommunikation“. Professor Grothe ist zudem Beirat des Queb Bundesverbandes für Employer Branding, Personalmarketing und Recruiting e.V. und Dozent am Institute for Competitive Intelligence (ICI).

Vorherige berufliche Stationen lagen parallel zur Promotion in der Controlling-Beratung, zur Zeit der Marktöffnung im Bereich der Telekommunikation sowie um die Jahrtausendwende in einer der größten Internet-Agenturen am Neuen Markt.

Sein Leitthema seit der Dissertation ist das Erkennen von Ordnung in hoher Komplexität: Hierzu fließen eigene Arbeiten aus den Feldern Business Intelligence, Swarm Intelligence und Social Network Analysis zusammen und führen zu neuartigen, praxiserprobten Digital Listening-Lösungen für den digitalen Raum.

Mit zahlreichen Vorträgen und Publikationen hat Professor Grothe in den letzten Jahren viele Beiträge geleistet, um für Unternehmen die notwendige digitale Transformation zu beschreiben.

Uwe Heim

Uwe Heim ist Service Line Leader und Partner von Deloitte Forensic. Vor seiner Tätigkeit bei Deloitte hat er mehrere Jahre bei einer anderen der ‚Big Four’ Wirtschaftsprüfungsgesellschaften in Deutschland sowie in einem Schwesterreferat der Financial Intelligence Unit im Bundeskriminalamt im Bereich Ermittlungen organisierter Kriminalität gearbeitet.

Uwe Heim ist spezialisiert in der Aufdeckung und Prävention von wirtschaftskriminellen Handlungen, zum Beispiel in Fällen von Korruption, Subventionsbetrug, Schmiergeld- und Kickback-Zahlungen, Unterschlagungshandlungen, sowie der Überprüfung von Vertragspartnern und der Einführung von Anti-Fraud Management Systemen.

Er besitzt umfangreiche und langjährige Erfahrung und Expertise in den unterschiedlichsten Branchen. Er ist Experte für Finanzermittlungen im Bereich Geldwäsche sowie zertifizierter Auditor für Managementsysteme durch die EOQ in London.

Abbildungen

Impressum

Herausgeber:

ASW Bundesverband

Allianz für Sicherheit
in der Wirtschaft e.V.

Bayerischer Platz 6
10779 Berlin

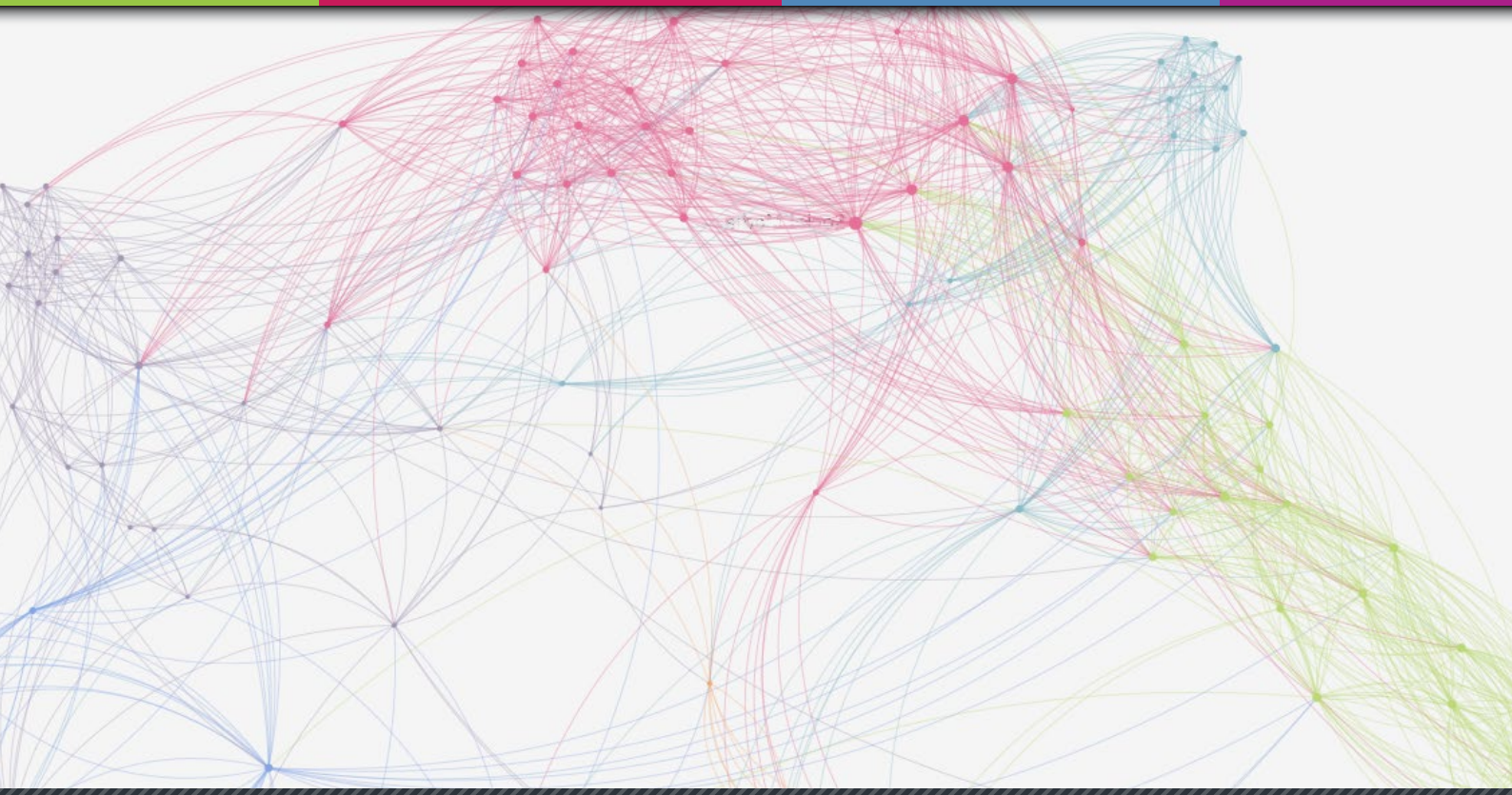
Telefon: +49 (0)30 246 37 175
Telefax: +49 (0)30 200 77 056

info@asw-bundesverband.de
www.asw-bundesverband.de

Stand:
Juli 2019

Gestaltung und Produktion:
GDE | Kommunikation gestalten.
www.gde.de

Redaktion:
Kurt Schlünkes



Bundesverband

complexium
UNTERNEHMENSBERATUNG

Deloitte.