Bundeskriminalamt

HACKTIVISTEN

Ergebnisbericht Online-Befragung

- Projektteil Dunkelfeld -

Bundeskriminalamt
Kriminalistisches Institut
Forschungs- und Beratungsstelle Cybercrime KI 16

BKA

Wendy Füllgraf
KI 16 Forschungs- und Beratungsstelle Cybercrime
Bundeskriminalamt
65173 Wiesbaden
ki16@bka.bund.de

Inhalt

Abbildungsverzeichnis

1. Das Projekt

Das Projekt Hacktivisten wurde im Januar 2013 begonnen und gliedert sich in zwei Projektteile: die Hellfeld- und die Dunkelfeld-Studie. Die Ergebnisse beider Projektteile werden in einem Abschlussbericht voraussichtlich Ende des Jahres 2015 veröffentlicht werden. Ziel des Projekts ist es, vor dem Hintergrund der zunehmenden medialen Präsenz von hacktivistischen Aktivitäten und Taten und einem uneinheitlichen Verständnis der Bedrohungslage sowie des Gefährdungspotenzials dieses Phänomens, die Materie grundlegend aufzuschließen und darzulegen. Neben einer empirisch fundierten kriminalistisch-kriminologischen Erkenntnisbasis zum Phänomen des Hacktivismus soll auch eine klare begriffliche Abgrenzung des Phänomens zu verwandten und ähnlichen phänomenologischen Strömungen hergestellt werden.

Die Menge an (wissenschaftlicher) Literatur zum Phänomen Hacktivismus im deutschsprachigen und angelsächsischen Raum ist bislang überschaubar. Wenn das Phänomen behandelt wird, dann häufig peripher im Rahmen der Auseinandersetzung mit anderen Phänomenen aus dem Bereich „Cyber", wie z. B. Cybercrime-Delikte in Form von Phishing, Online-Betrug und Hacking, Cyberterrorismus und Cyberwar. (Publizierte) Wissenschaftliche Untersuchungen von Hacktivismus und Hacktivisten sind rar, es liegen wenig Ergebnisse quantitativer Untersuchungen wie z. B. Nutzerbefragungen sowie qualitativer Untersuchungen wie z. B. Auswertungen von Pressemitteilungen vor.
Damit stellt die Hacktivisten-Studie mit der Umsetzung der angestrebten Ziele eine Erweiterung der bisherigen Wissens- und Erkenntnisbasis über das Phänomen Hacktivismus – und damit auch des Untersuchungsfeldes Cybercrime insgesamt – dar.

Aufgrund der Erkenntnisse des ersten Projektteils ist zu vermuten, dass nicht alle bekannt gewordenen strafrechtlich relevanten Vorfälle von Hacktivismus auch zur Anzeige gebracht werden. Diese Taten – sowie jene, die von den Opfern erst gar nicht bemerkt wurden – bestimmen das Dunkelfeld. In einem zweiten Projektteil wurde daher der Versuch unternommen, einen Überblick über das Dunkelfeld im Bereich Hacktivismus zu gewinnen. Zur Ergründung der Fragen, ob bestimmte Branchen und Einrichtungsgrößen stärker von Hacktivismus betroffen sind als andere, welche Schäden dabei entstehen und welche Gründe Einrichtungen davon abhalten, Anzeige zu erstatten bot sich eine Befragung deutscher Unternehmen und öffentlicher Einrichtungen an. Es wurde eine repräsentative Stichprobe von ca. 5.000 Institutionen gezogen und diese befragt.
Daneben sollten Zusammenhänge durch folgende Fragen erfasst und überprüft werden: Sind von Hacktivismus betroffene Einrichtungen auch von analogen aktivistischen Maßnahmen betroffen? Haben diese Einrichtungen auch schon digitale Shitstorms erlebt? Wie groß ist der Zusammenhang zwischen dem Auftreten von Shitstorms und der Nutzung sozialer Medien? Und tritt auch Hacktivismus häufiger auf, wenn die Einrichtungen soziale Medien nutzen? Existiert eine generelle Vulnerabilität gegenüber Formen von Cyberangriffen, d. h. wenn Einrichtungen von digitalen Angriffen betroffen sind, sind diese auch wahrscheinlicher von Hacktivismus betroffen?

2. Online-Befragung

2.1 Methodisches

2.1.1 Stichprobe und Rücklauf

Die Ziehung der Stichprobe erfolgte aus einer Datenbank, in welcher über 300.000 Unternehmen und öffentliche Einrichtungen in Deutschland verzeichnet sind. Ein Konzept zur Durchführung der Ziehung einer Zufallsstichprobe stellte die Repräsentativität[1] der gezogenen Stichprobe sicher.
Anhand der Konzeption wurden – unter Berücksichtigung einer erwartbaren Rücklaufquote von 10 % für eine Online-Befragung – 5.008 Unternehmen und öffentliche Einrichtungen gezogen. Die bereinigte Stichprobe[2] umfasste letztlich 4.543 Einrichtungen.

971 Einrichtungen haben nach Abschluss der Erhebungsphase an der Online-Befragung teilgenommen. Das entspricht einer Rücklaufquote von 21 % und übertrifft damit die erwarteten 10 % deutlich. Die vorliegenden Ergebnisse sind somit als repräsentativ zu bewerten.

2.1.2 Fragebogen-Hosting und Ablauf der Befragung

Vor Beginn der Befragung erhielten die gezogenen Einrichtungen ein postalisches Anschreiben, welches die Adressaten über die Befragung und die randomisierte Stichprobenziehung informierte sowie um die Teilnahme an der nachfolgenden Online-Befragung bat. Das folgende elektronische Einladungsschreiben mit dem Link zu der Befragung wurde angekündigt, den Adressaten die E-Mail-Absenderadresse der kommenden elektronischen Einladung, das Grundmuster des Links zur Online-Befragung sowie die jeweils anzuschreibende E-Mail-Adresse zur Authentifizierungs- und Verifizierungszwecken von Absender und Maßnahme mitgeteilt.
Die Befragungsphase dauerte fünfeinhalb Wochen, innerhalb derer zwei Reminder verschickt wurden, um Einrichtungen, die bis dahin noch nicht an der Befragung teilgenommen hatten, doch noch zu einer Beteiligung zu animieren. Der versendete Link zum Online-Fragebogen war nach Ablauf der Befragungsphasen nicht mehr aktivierbar.

Der Dienstleister Bitkom Research GmbH hostete den Online-Fragebogen auf BSI-zertifizierten Servern. Die Daten[3] aus der Befragung wurden dem Projektteam des BKA für die Auswertung als SPSS-Datensatz zur Verfügung gestellt.

---

[1] Die Stichprobe ist dann repräsentativ, wenn die Zusammensetzung der gezogenen Unternehmen und öffentlichen Einrichtungen möglichst stark der Zusammensetzung aller Unternehmen und öffentlichen Einrichtungen in Deutschland ähnelt. Das der Befragung zugrundeliegende Konzept zur Ziehung einer geschichteten disproportionalen Zufallsstichprobe, stellt sicher, dass aus jeder Branche jede Unternehmensgröße (klein, mittel, groß) zufällig gezogen wurde und zwar entsprechend der Gesamtverteilung aller Branchen und Größen in Deutschland.

[2] Ausgeschieden sind hierbei Doppelungen (d. h. Einrichtungen mit denselben Kontaktdaten), Einrichtungen ohne E-Mail-Adresse sowie Einrichtungen, die postalisch nicht angeschrieben werden konnten (unzustellbare Rückläufer).

[3] Hierbei handelte es sich ausschließlich um die Ergebnisse der gewählten Antwortvorgaben aus dem Fragebogen. Daten zu den Teilnehmern wurden nicht erfasst bzw. übermittelt. Von Interesse für die Erhebung war nicht, wer die Teilnehmer sind, sondern lediglich die Größe der Einrichtung (Mitarbeiterzahl) und die Branche.

2.2 Ergebnisse

Von 971 antwortenden Einrichtungen gaben **35** an, in der Vergangenheit bereits **mehrmals** Opfer von Hacktivismus geworden zu sein und **45** gaben an, **einmal** von Hacktivismus betroffen gewesen zu sein. D. h. insgesamt wurden 80 Einrichtungen in den letzten Jahren ein- oder mehrmals Opfer hacktivistischer Aktivitäten[4], wobei größere Einrichtungen eher und auch häufiger von Hacktivismus betroffen waren als kleinere. 818 Einrichtungen konnten keine hacktivistischen Angriffe ausmachen (ggf. könnten diese stattgefunden haben, wurden aber nicht bemerkt bzw. als sonstiger Systemausfall/-fehler gewertet).

Von digitalen Angriffen waren bereits 251 Einrichtungen mehrmals betroffen und 113 einmal. 505 Einrichtungen gaben an, noch nie Opfer digitaler Angriffe geworden zu sein.[5]

Unternehmen, die bereits Opfer von Shitstorms[6] waren, waren auch eher von einem oder mehreren hacktivistischen Angriffen betroffen. Die Nutzung sozialer Medien begünstigt die Betroffenheit von Shitstorms. Diese auf der Hand liegende Verknüpfung konnte hier auch empirisch belegt.

Insgesamt lässt sich festhalten, dass Aktivismus, Shitstorms, Hacktivismus und digitale Angriffe untereinander und miteinander korrelieren, d. h. Einrichtungen, die von dem einen Phänomen betroffen waren auch viel eher von einer oder mehrerer der anderen Varianten betroffen waren.

[4] Zum Vergleich: In der Erhebung deutscher polizeilich registrierter Fälle konnten 78 Fälle von Hacktivismus identifiziert werden. Siehe Abschlussbericht zum Projektteil der Hellfeldbeforschung: https://www.bka.de/nn_196810/sid_D1EB3F0446945828570AA6B8AA1CA1D0/DE/ThemenABisZ/Forschung/Hacktivismus/hacktivismus.html?__nnn=true

[5] Auch hier muss beachtet werden, dass ggf. Angriffe stattgefunden haben, diese jedoch nicht bemerkt oder nicht als solche erkannt wurden, sondern als interne Systemausfälle behandelt wurden.

[6] Shitstorm, ein Begriff, der sich am ehesten mit „Sturm der Entrüstung“ übersetzen lässt. Unter einem Shitstorm wird ein Internetphänomen verstanden, bei dem in kurzer Zeit sehr viele beleidigende oder empörte Beiträge auf Internetplattformen wie Sozialen Netzwerken, Internetforen oder Blogs gegen Unternehmen, Personen des öffentlichen Lebens, Verbände oder Einzelpersonen geäußert werden.

2.2.1 Teil 1: Allgemeine Fragen zum Unternehmen

Wie gestaltet sich die Verteilung der Größe der Unternehmen, die an der Befragung teilgenommen haben? Ca. 50 % der Einrichtungen (497), die an der Befragung teilgenommen haben, haben bis zu 50 Beschäftigte.

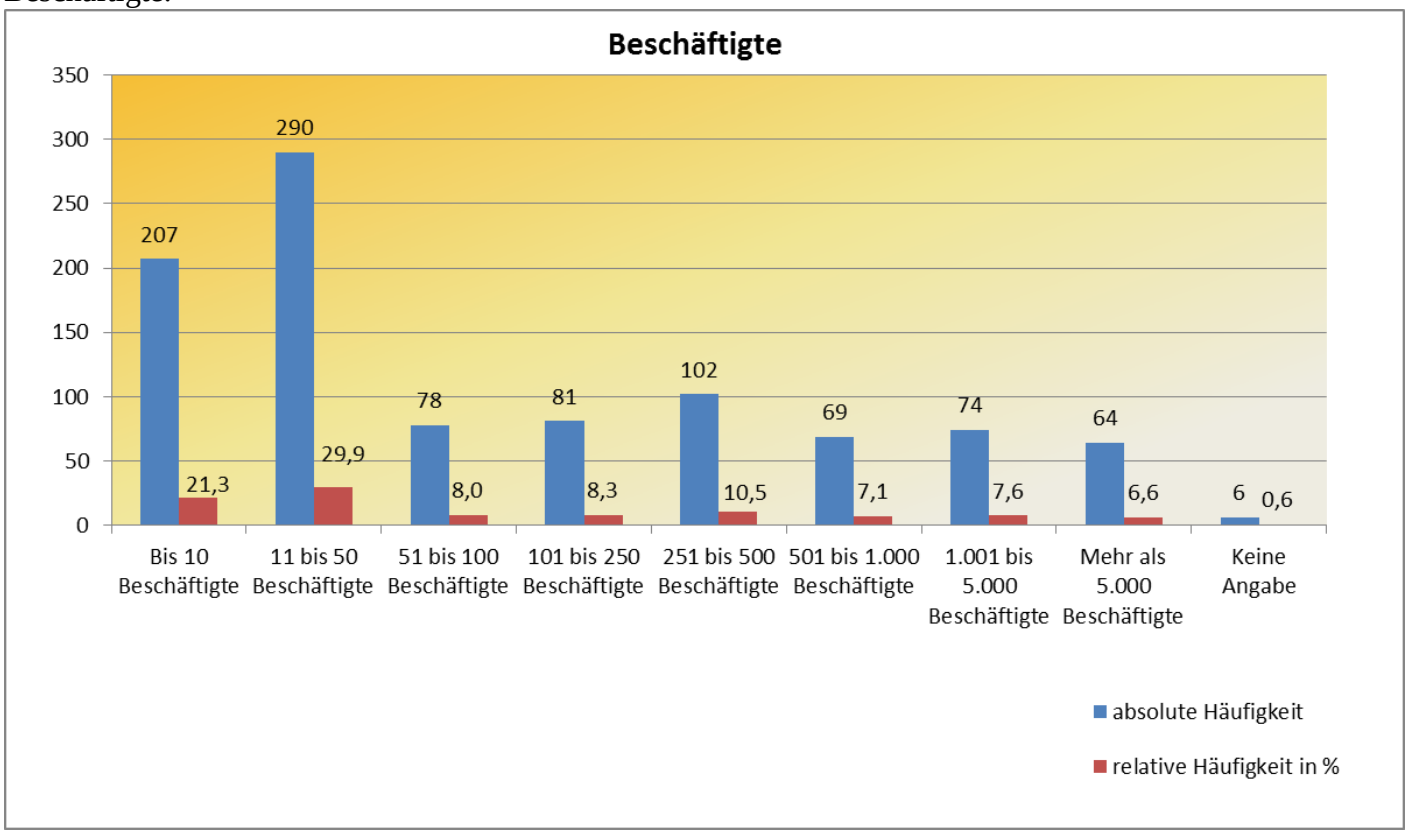


Abbildung 1: Beschäftigte

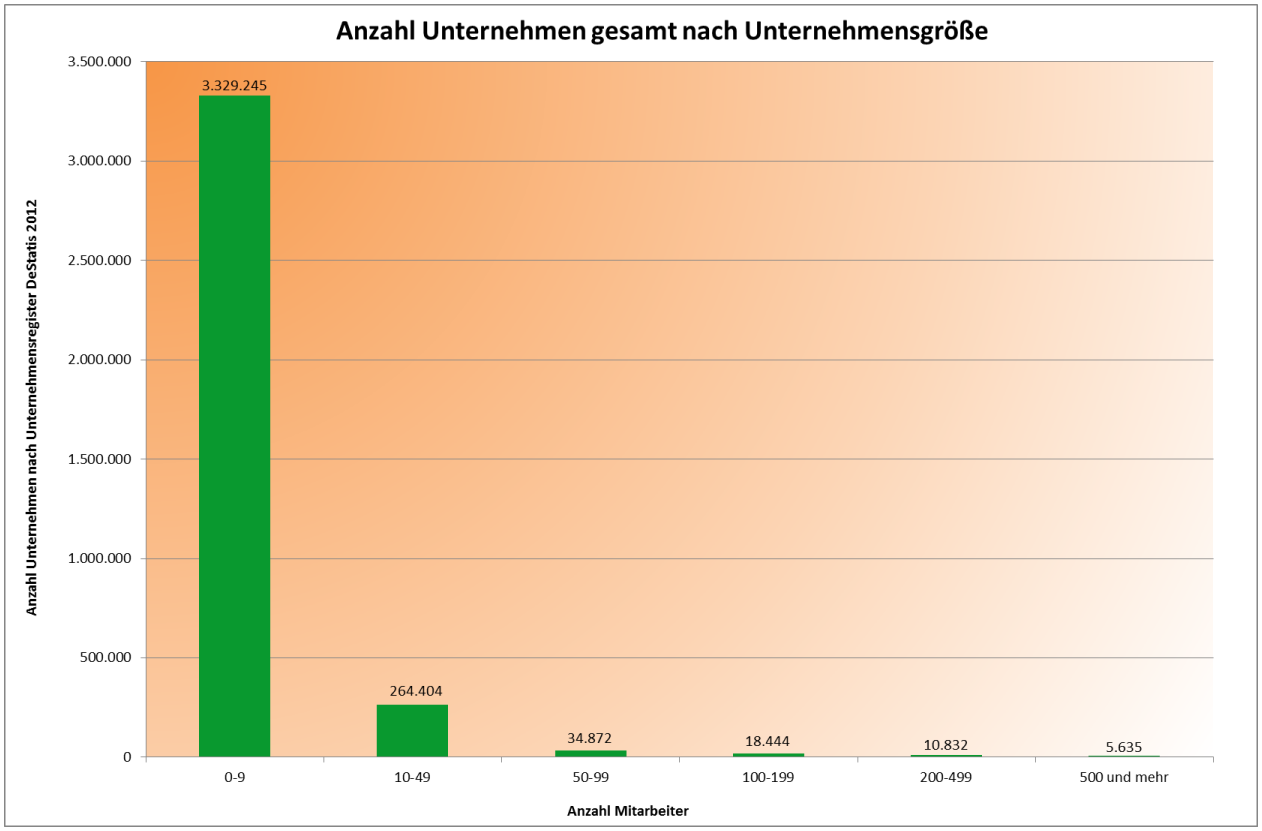


Abbildung 2: Anzahl Unternehmen nach Unternehmensgröße

Mit 14,6 % war das *verarbeitende Gewerbe* die Branche, in der die meisten Teilnehmer[7] verortet sind. Gefolgt von der Branche *Handel; Instandhaltung und Reparatur von Kraftfahrzeugen und Gebrauchsgütern* mit 9,5 %, dem *Baugewerbe* mit 8,7 % sowie der Branche *Erbringung von sonstigen wirtschaftlichen Dienstleistungen* mit 8,3 %.

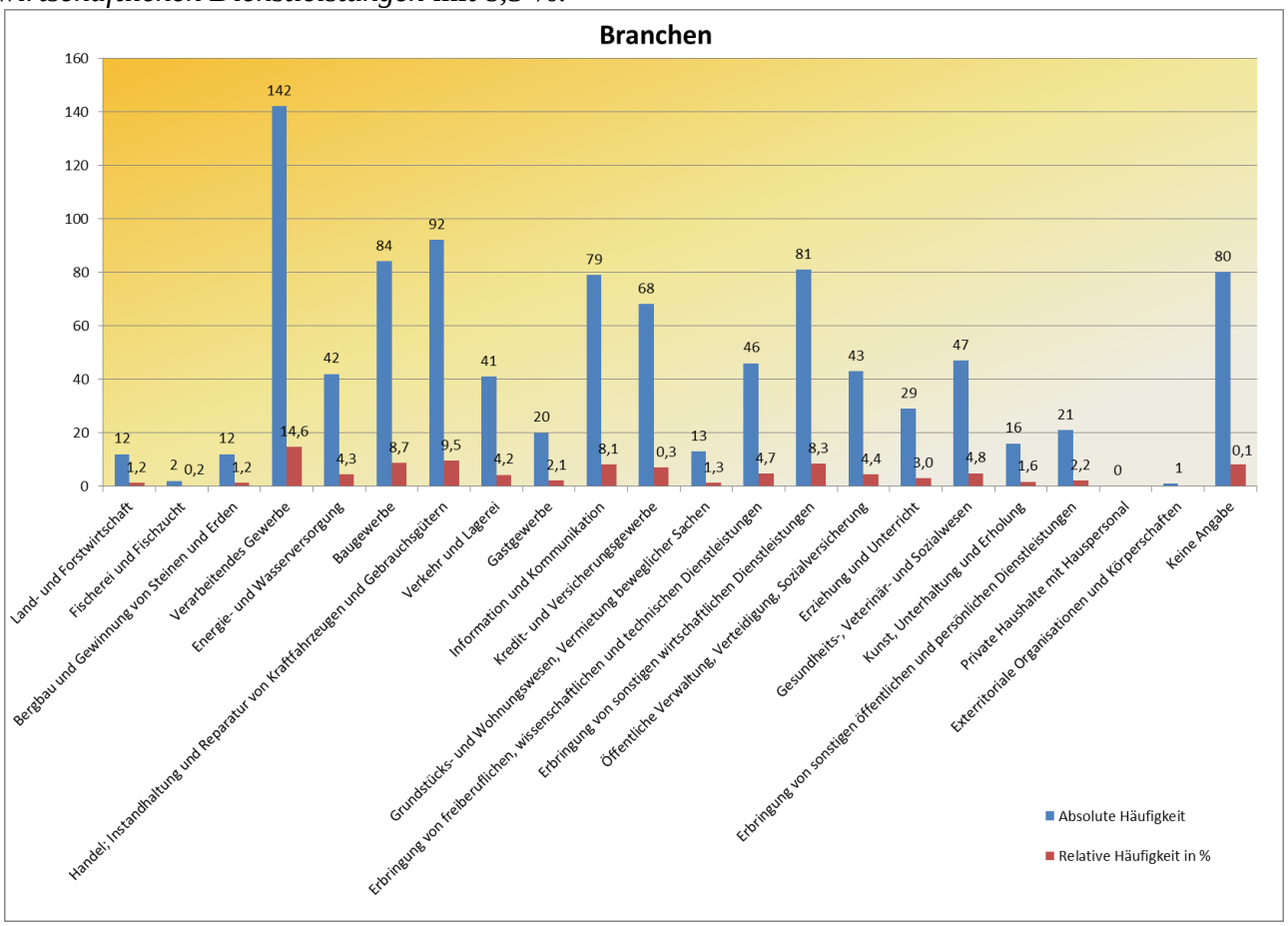


Abbildung 3: Branchen

7 Aus Gründen der Lesbarkeit wird im Folgenden lediglich die männliche Form verwandt.

Die Verteilung der Branchenzugehörigkeit unter den befragten Unternehmen entspricht bis auf die nachstehend genannten Abweichungen somit nahezu der Gesamtverteilung der Unternehmen nach Branchen in Deutschland. Unternehmen aus der Land- und Forstwirtschaft sind in den Befragungsergebnissen aufgrund der geringen Rückläufe aus diesem Bereich deutlich unterrepräsentiert. Unternehmen aus der Informations- und Kommunikationsbranche sind dafür in den Rückläufen stärker vertreten, als in der Gesamtverteilung. Die Anzahl der Unternehmen aus dem Gastgewerbe, die an der Befragung teilgenommen haben, ist geringer als in der Gesamtverteilung. Unternehmen aus dem verarbeitenden Gewerbe stellen die Mehrheit der Befragungsteilnehmer und weichen damit deutlich von der Gesamtverteilung ab.

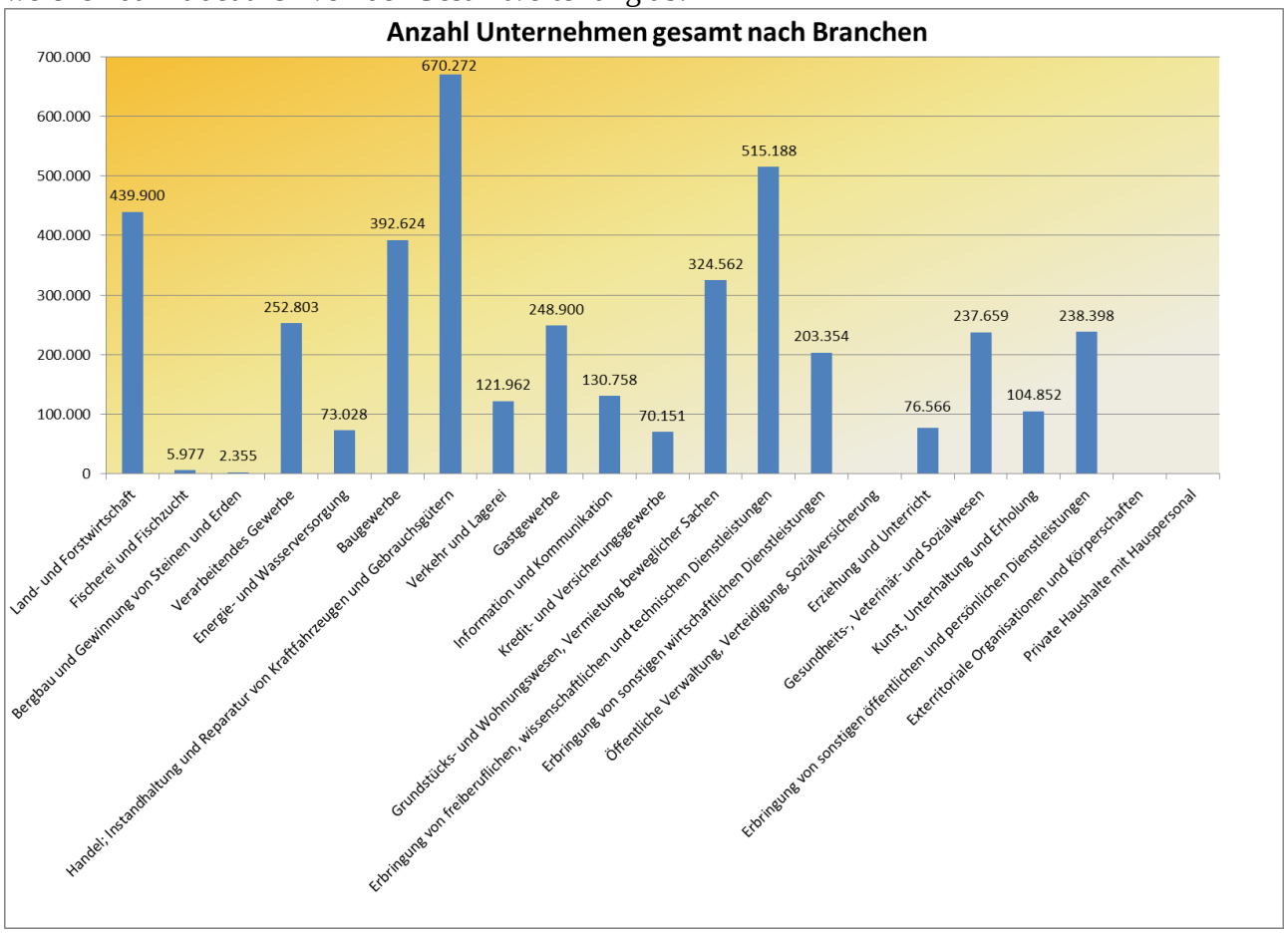


Abbildung 4: Anzahl Unternehmen gesamt nach Branchen

2.2.2 Teil 2: Social Media

Soziale Netzwerke bzw. Social Media sind Plattformen im Internet, auf denen sich Personen ein eigenes Nutzerprofil anlegen und mit anderen Nutzern austauschen können wie zum Beispiel Facebook, LinkedIn oder Instagram.

413 Einrichtungen gaben an, für eigene Zwecke soziale Medien zu nutzen. 550 Einrichtungen verneinten dies. Je größer das Unternehmen, desto eher werden soziale Medien genutzt.

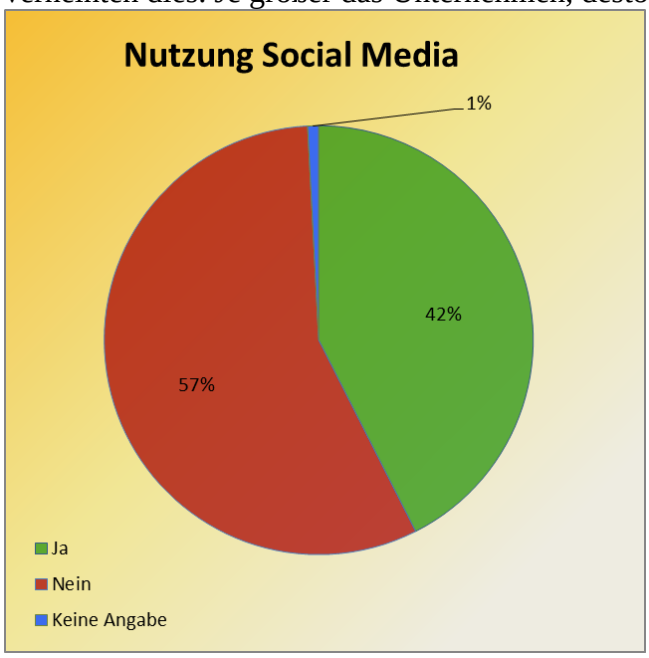


Abbildung 5: Nutzung Social Media

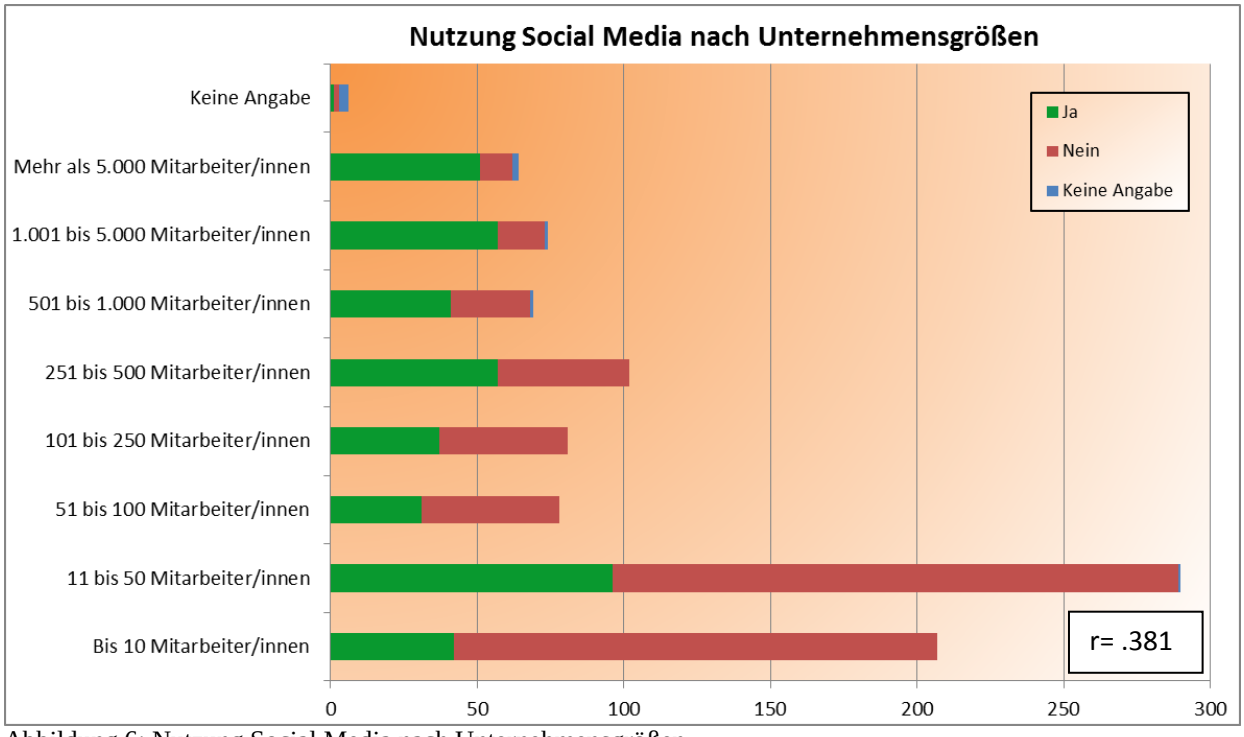


Abbildung 6: Nutzung Social Media nach Unternehmensgrößen

Die Mehrheit nutzt Facebook, gefolgt von Xing, Youtube und Twitter:

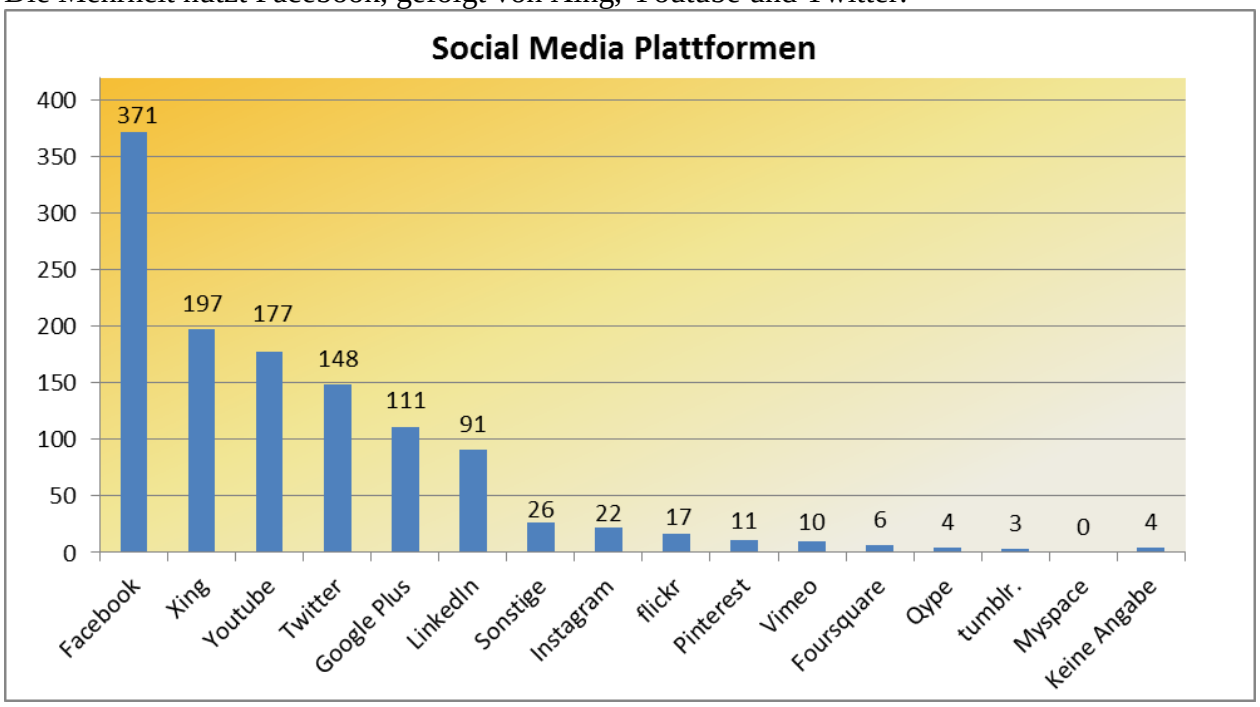


Abbildung 7: Social Media Plattformen

Die Mehrheit der befragten Einrichtungen gab an, soziale Medien in erster Linie für die Kommunikation aktueller Entwicklungen und Ereignisse zu nutzen und/oder für Werbezwecke. Daneben werden soziale Medien auch für Kundenzwecke wie z. B. Feedback und Betreuung genutzt. Gewinnspiele und technischer Support sowie sonstige Zwecke machen einen kleinen Teil der Nutzungszwecke aus.

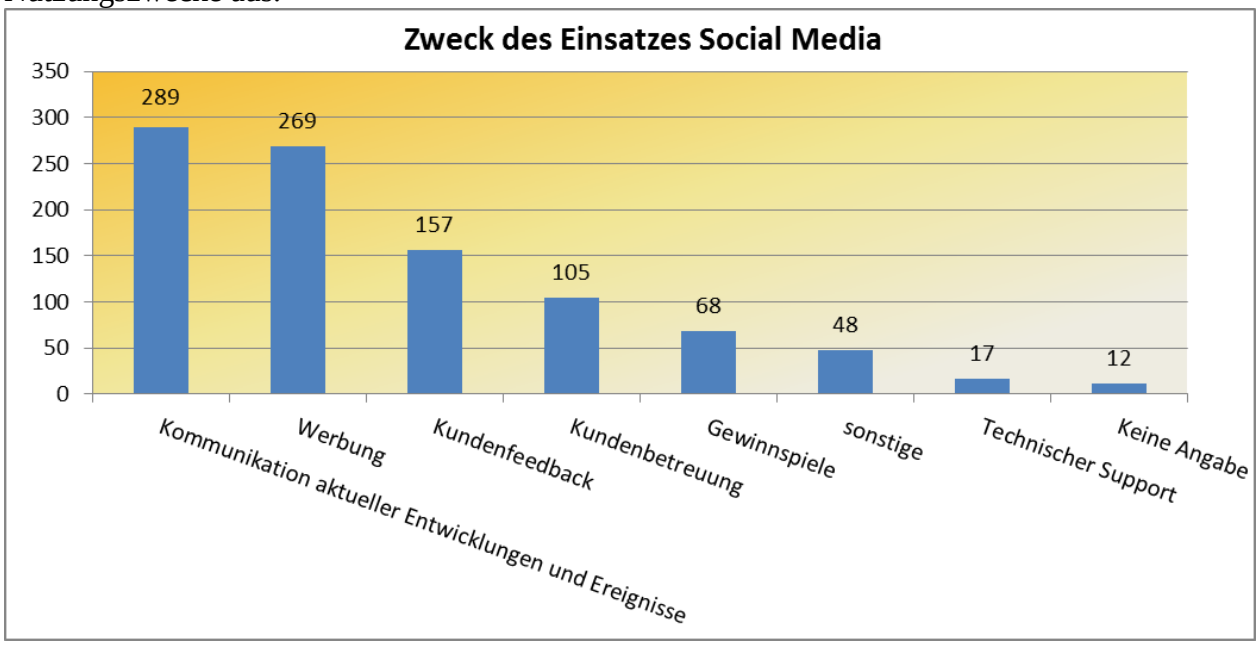


Abbildung 8: Zweck des Einsatzes Social Media

Es ließ sich ein leichter positiver Zusammenhang zwischen der Nutzung für Gewinnspiele und der Unternehmensgröße feststellen, d. h. je größer das Unternehmen, desto eher werden soziale Medien für Gewinnspiele genutzt.[8] Daneben besteht ein negativer Zusammenhang zwischen Werbezwecken und Größe, d. h. je kleiner das Unternehmen desto eher werden soziale Medien für Werbezwecke eingesetzt.[9]

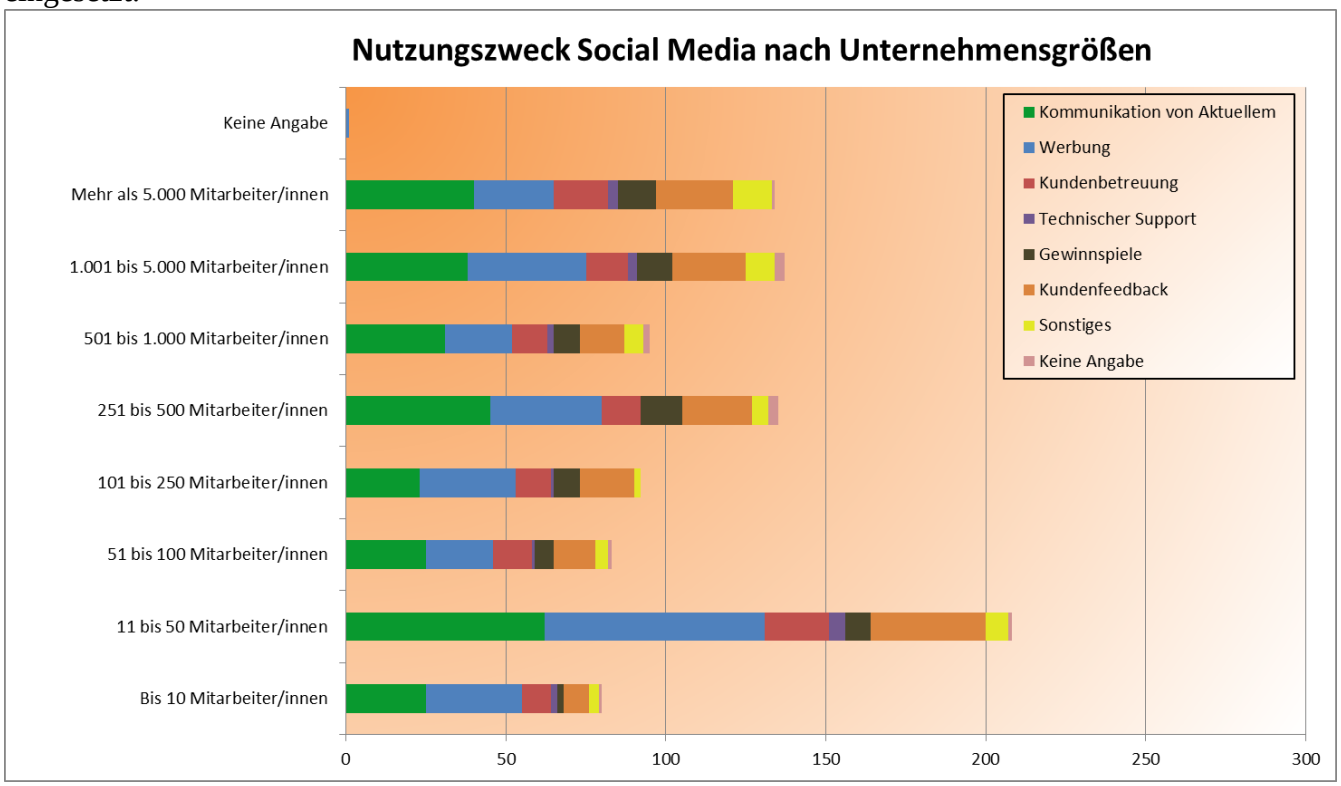


Abbildung 9: Nutzungszweck Social Media nach Unternehmensgrößen

[8] r= .149

[9] r= -.144

Die sonstigen Zwecke der sozialen Mediennutzung bestehen überwiegend aus der Personalgewinnung:

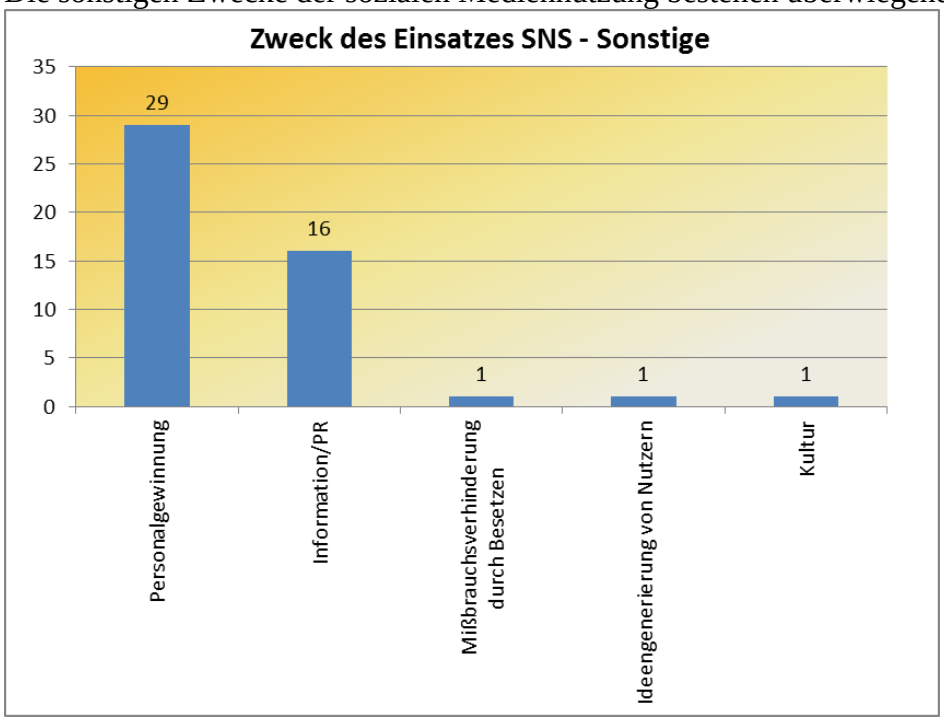


Abbildung 10: Zweck des Einsatzes SNS – sonstige

Zu der Frage nach der Betroffenheit von beleidigenden Kommentaren im Internet (sog. Shitstorms) gab die Mehrheit mit 81 % an, noch nie davon betroffen gewesen zu sein. 3 % gaben an, bereits einmal von Shitstorms betroffen gewesen zu sein und 3 % waren schon mehrmals davon betroffen. 13 % konnten hierzu keine Angabe machen.

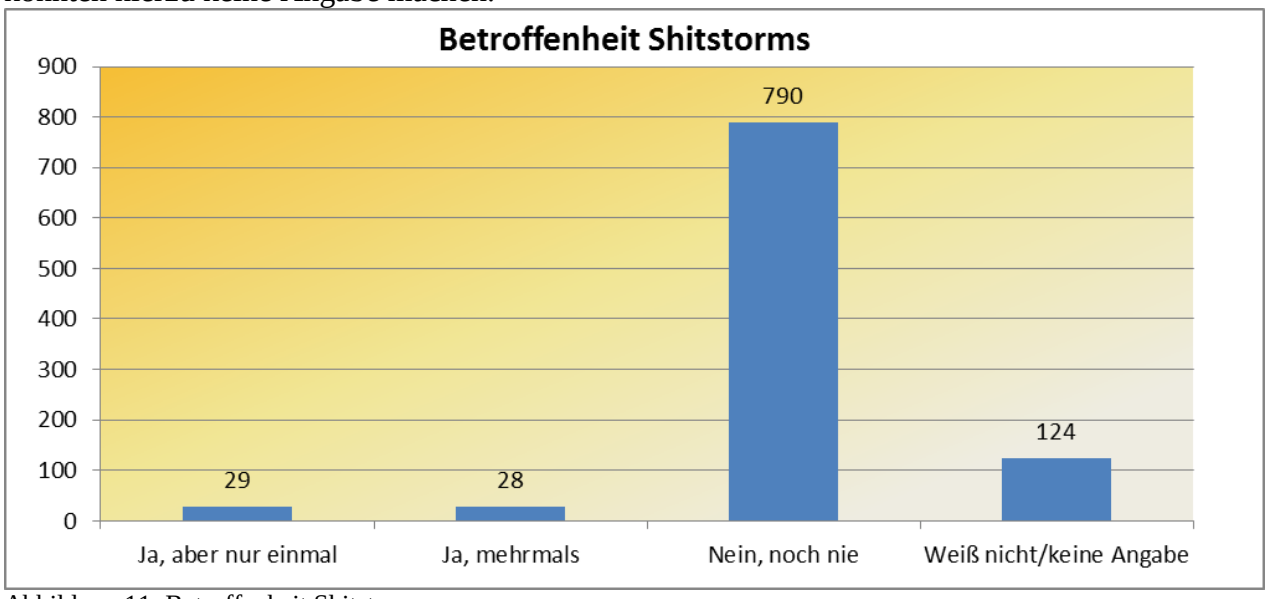


Abbildung 11: Betroffenheit Shitstorms

Bei der Betroffenheit von Shitstorms ließ sich kein Zusammenhang zur Unternehmensgröße ausmachen. Kleine wie große Unternehmen waren gleichermaßen Opfer von Shitstorms.

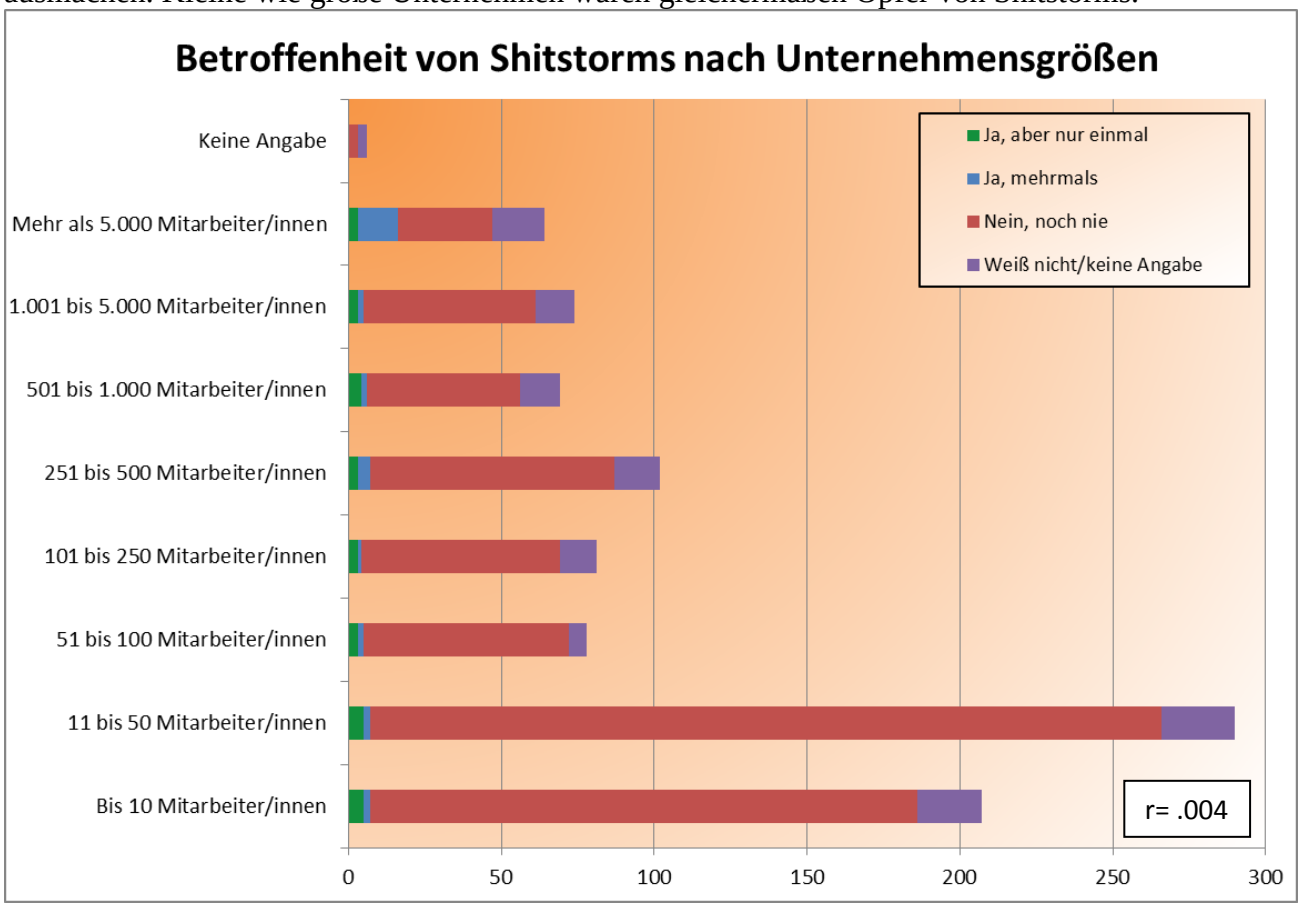


Abbildung 12: Betroffenheit von Shitstorms nach Unternehmensgrößen

Die Shitstorms fanden überwiegend sowohl auf den eigenen Social Media-Auftritten als auch in einrichtungsfremden sozialen Medien sowie in Internetforen statt:

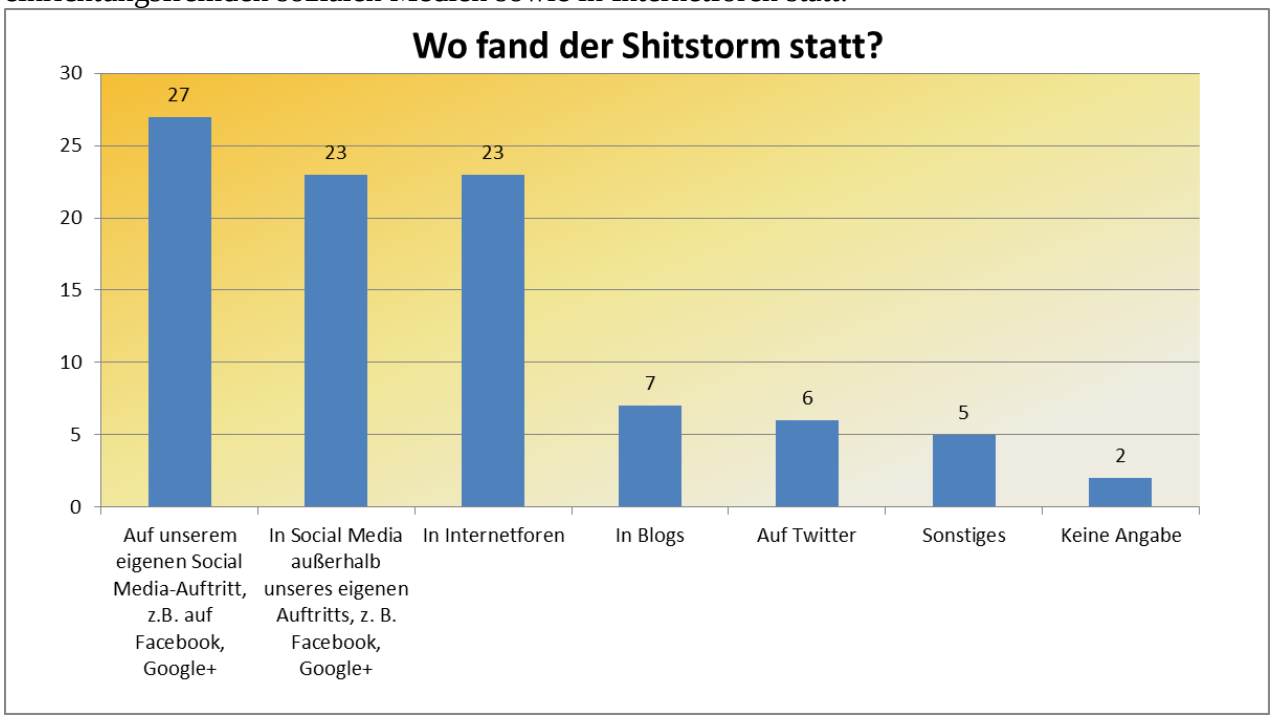


Abbildung 13: Wo fand der Shitstorm statt?

Aus welchen Branchen die Einrichtungen stammen, die ein- oder mehrmals von Shitstorms betroffen waren, lässt sich folgender Grafik entnehmen. Die Branche *Information und Kommunikation* sticht hierbei besonders hervor.

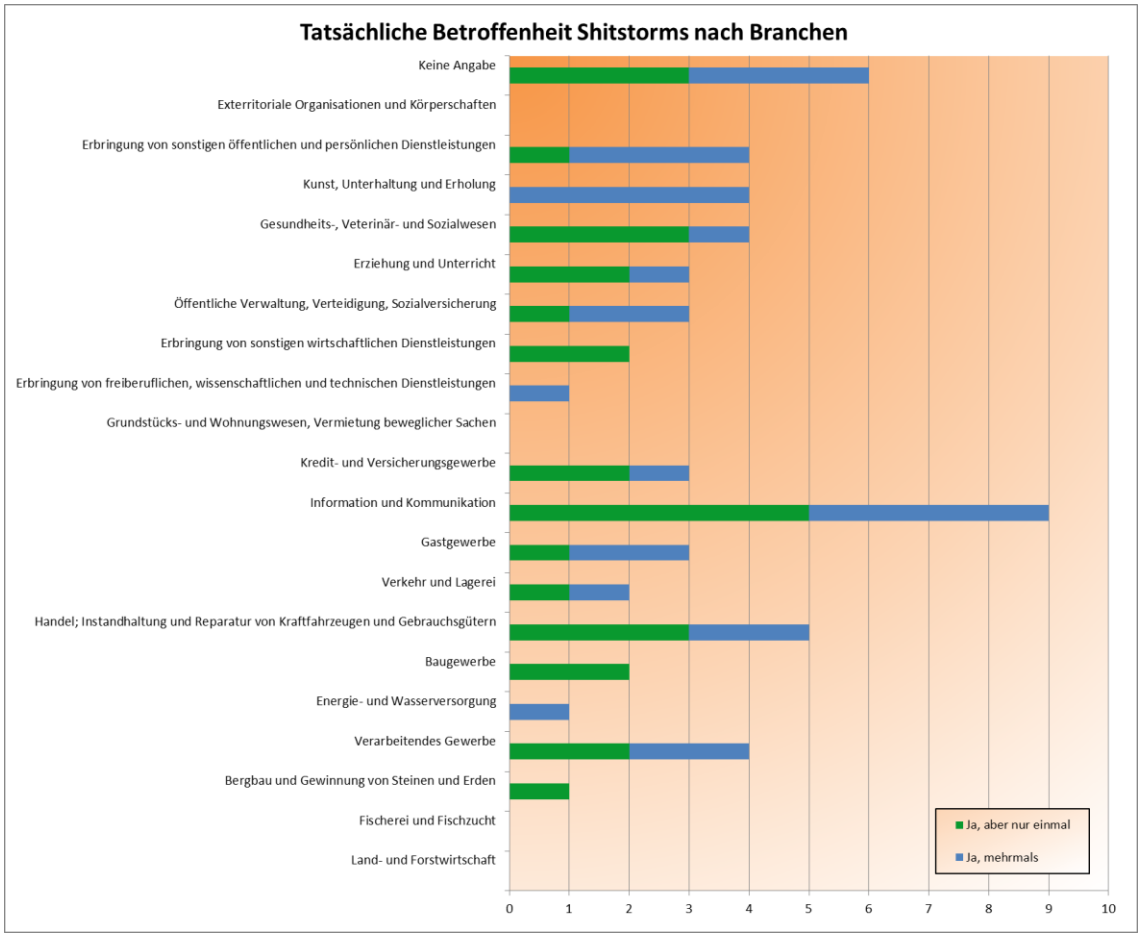


Abbildung 14: Tatsächliche Betroffenheit Shitstorms nach Branchen

Einrichtungen, die von Shitstorms betroffen sind, nutzen auch eher soziale Medien:

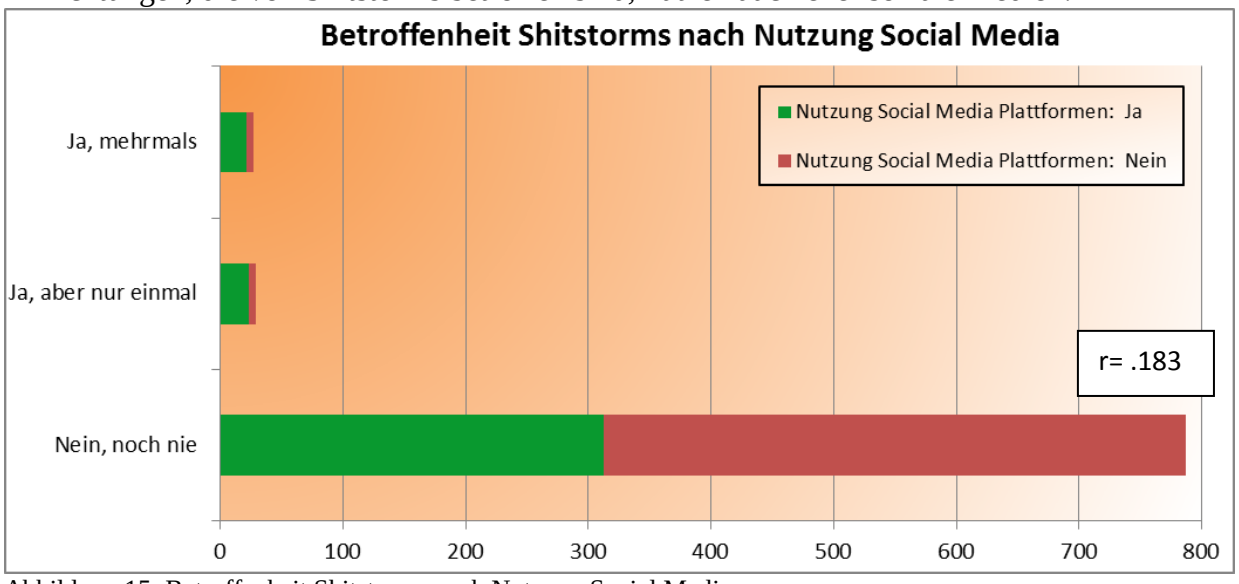


Abbildung 15: Betroffenheit Shitstorms nach Nutzung Social Media

Auf den Plattformen Facebook, Youtube, Twitter, Xing, Google Plus und LinkedIn waren die Unternehmen am häufigsten – auch mehr als einmal – von Shitstorms betroffen. Dies steht im Verhältnis zur Nutzungshäufigkeit der entsprechenden Plattformen (s. o.).

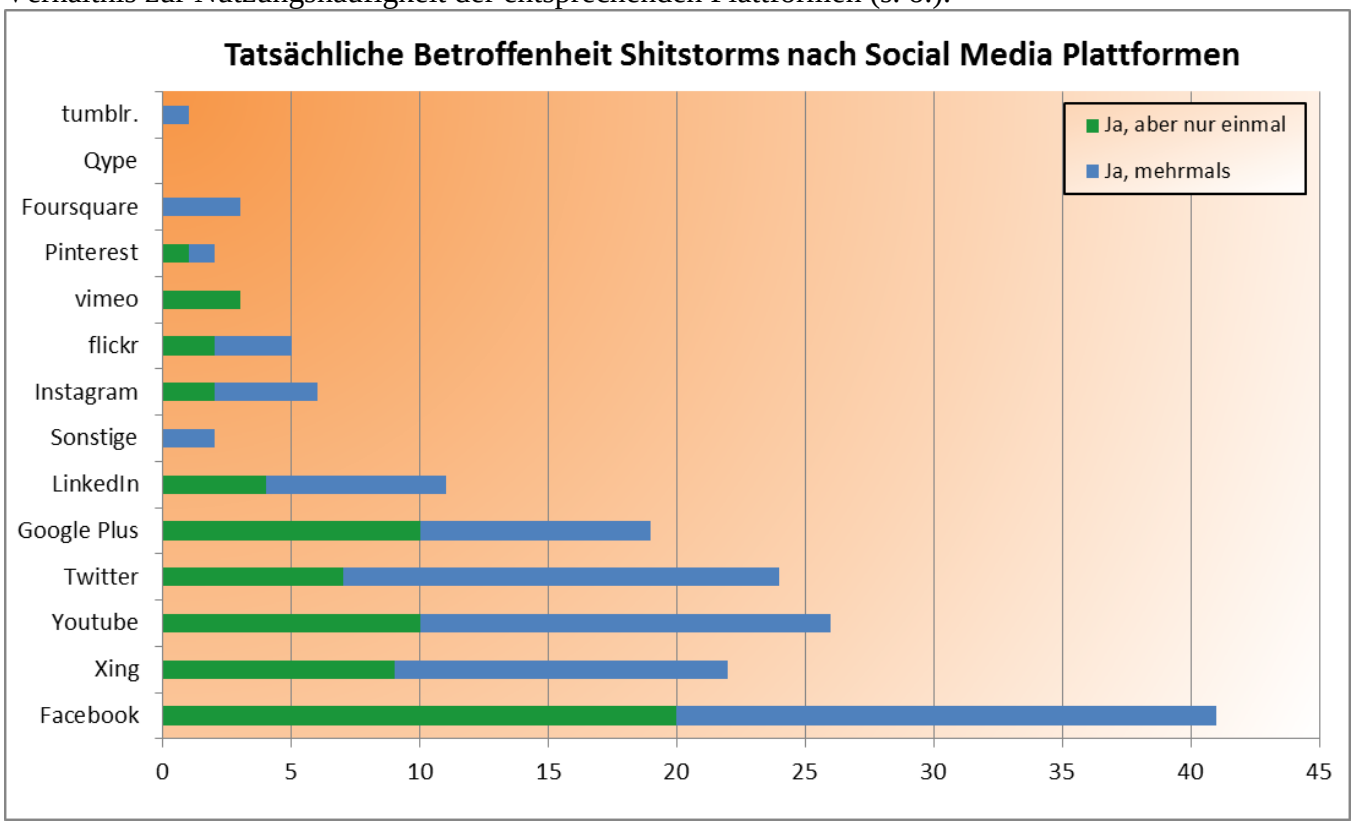


Abbildung 16: Tatsächliche Betroffenheit Shitstorms nach Social Media Plattformen

Es fällt auf, dass Einrichtungen, die einen Mitarbeiter-Zugriff auf das Netzwerk von außerhalb erlauben (siehe auch Teil 3: IT- und Informationssicherheit), besonders von Shitstorms betroffen waren.

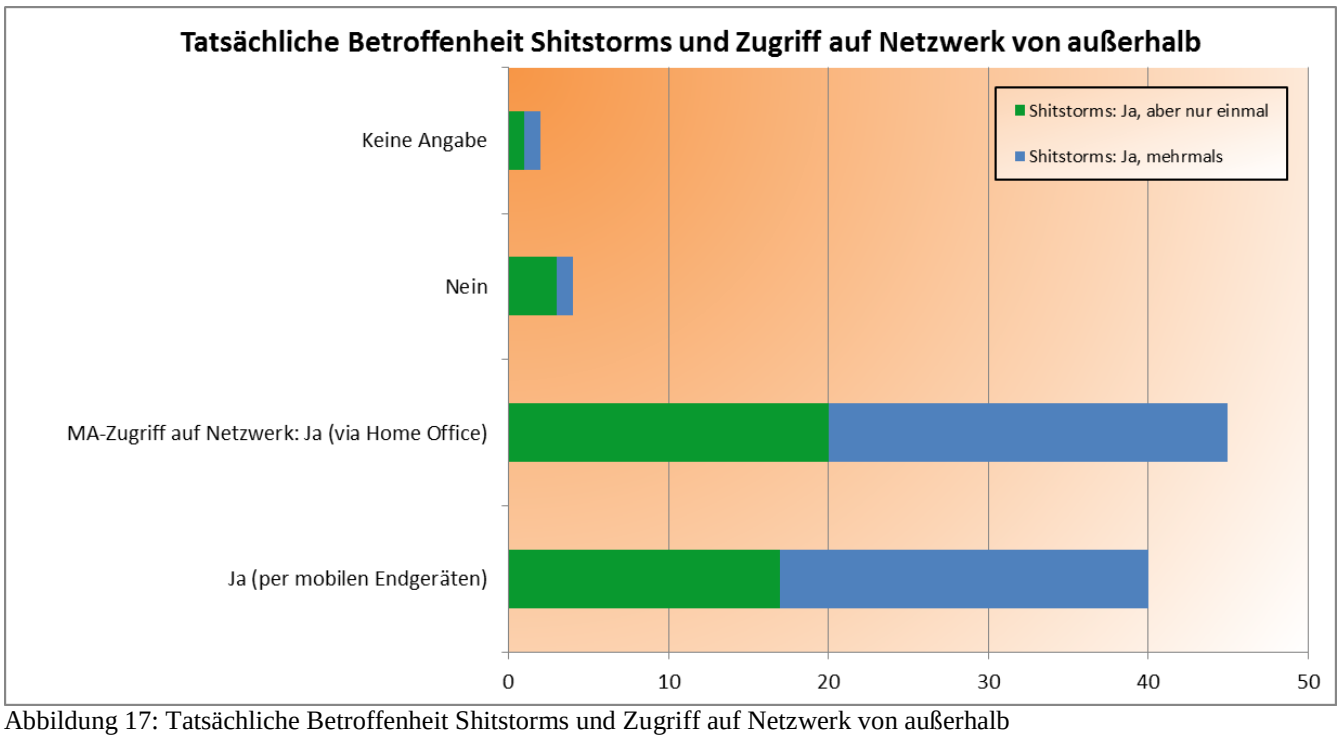


Abbildung 17: Tatsächliche Betroffenheit Shitstorms und Zugriff auf Netzwerk von außerhalb

2.2.3 Teil 3: IT- und Informationssicherheit

Im Gegensatz zu Shitstorms ist zu vermuten, dass digitale Angriffe über das Internet auf IT-Systeme häufig kaum als solche identifiziert werden, sondern eher ein nicht von außen beeinflusstes Systemversagen in Betracht gezogen wird. 52 % der befragten Einrichtungen gaben immerhin an, noch nie von digitalen Angriffen betroffen gewesen zu ein. 12 % wurden bereits einmal zum Opfer eines digitalen Angriffs und 26 % sogar schon mehrmals.

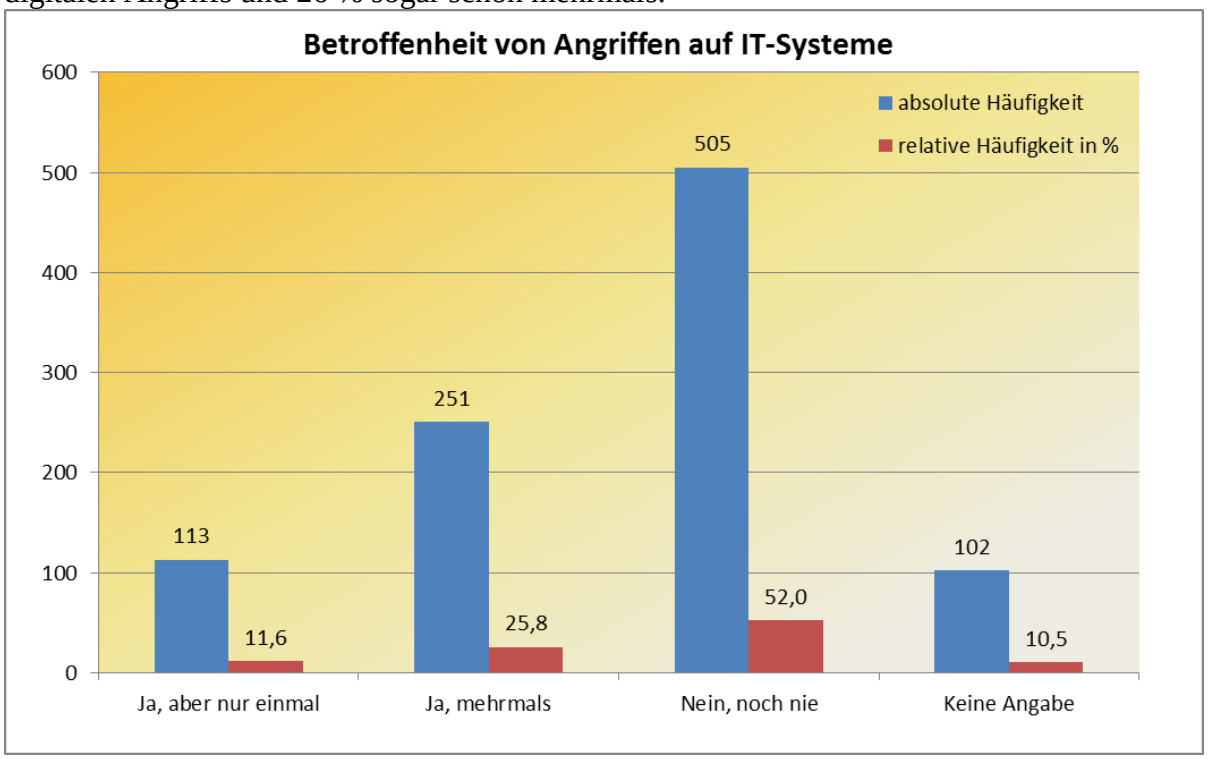


Abbildung 18: Betroffenheit von Angriffen auf IT-Systeme

Je größer das Unternehmen, desto eher war es von mehr als einem digitalen Angriff betroffen

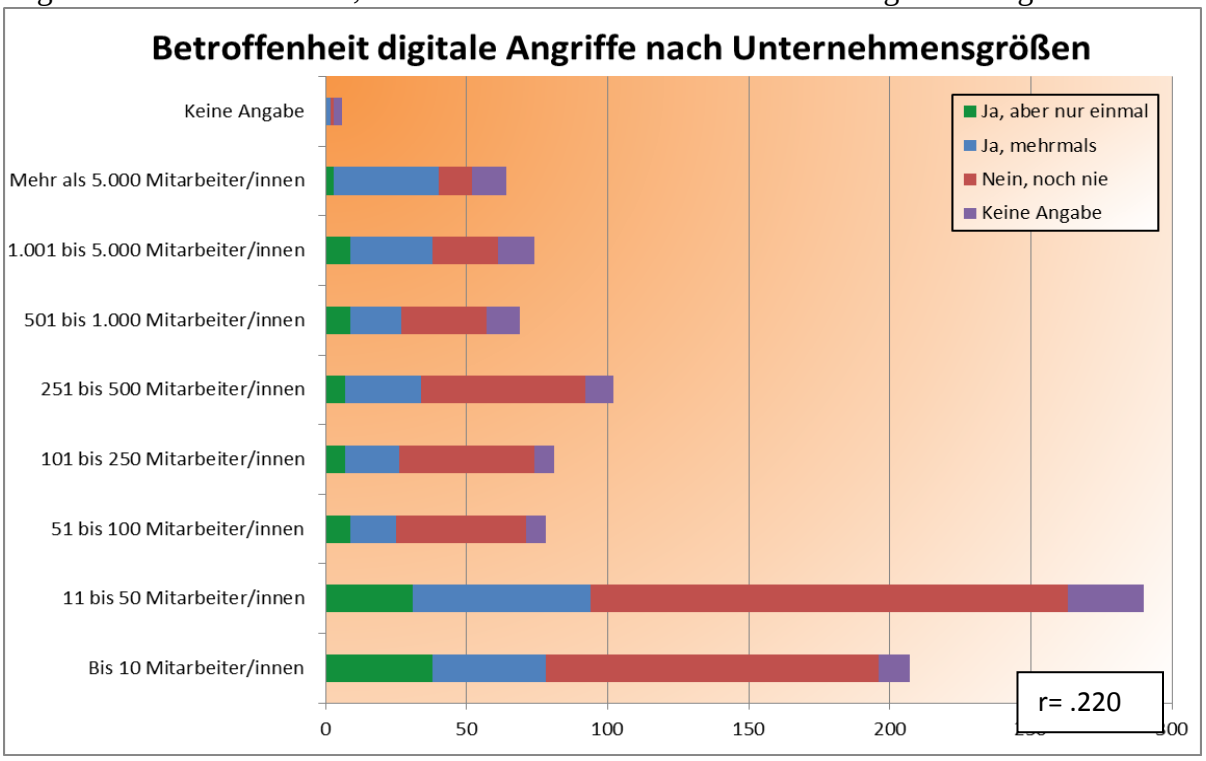


Abbildung 19: Betroffenheit digitale Angriffe nach Unternehmensgrößen

Differenzierung der digitalen Angriffe nach Branche:

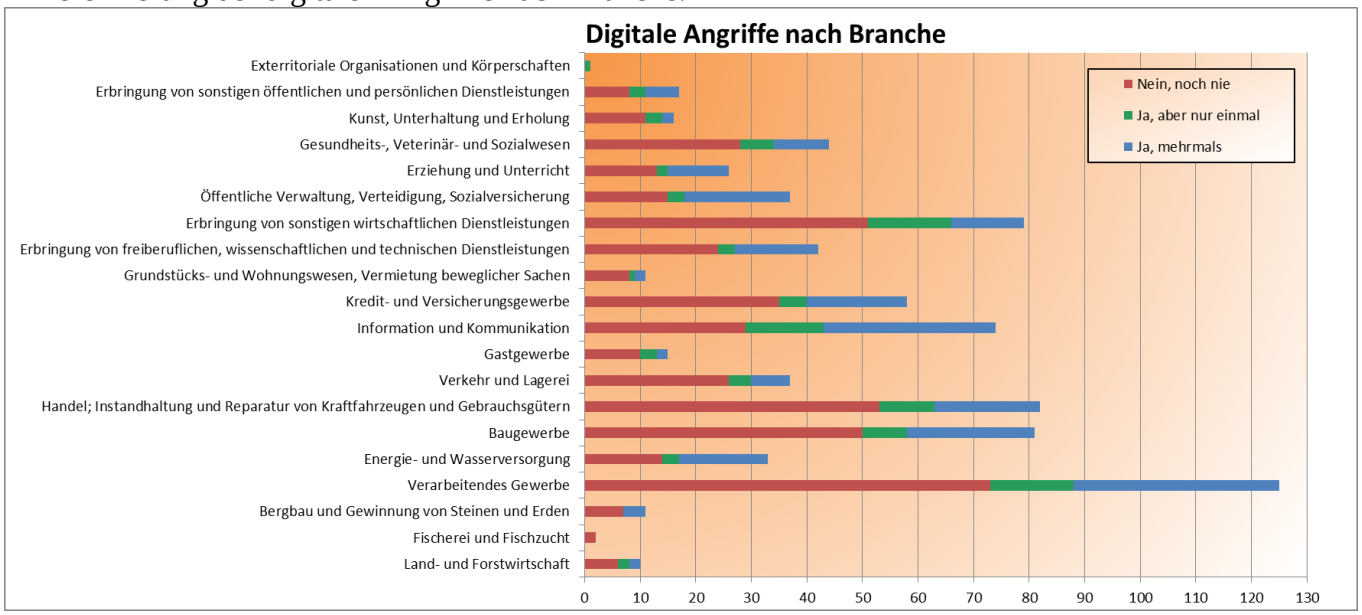


Abbildung 20: Digitale Angriffe nach Branche

Einrichtungen, die Ziele digitaler Angriffe geworden sind, waren auch von Shitstorms betroffen; die Anzahl der erfahrenen Shitstorms korreliert hier positiv mit der Anzahl der digitalen Angriffe.

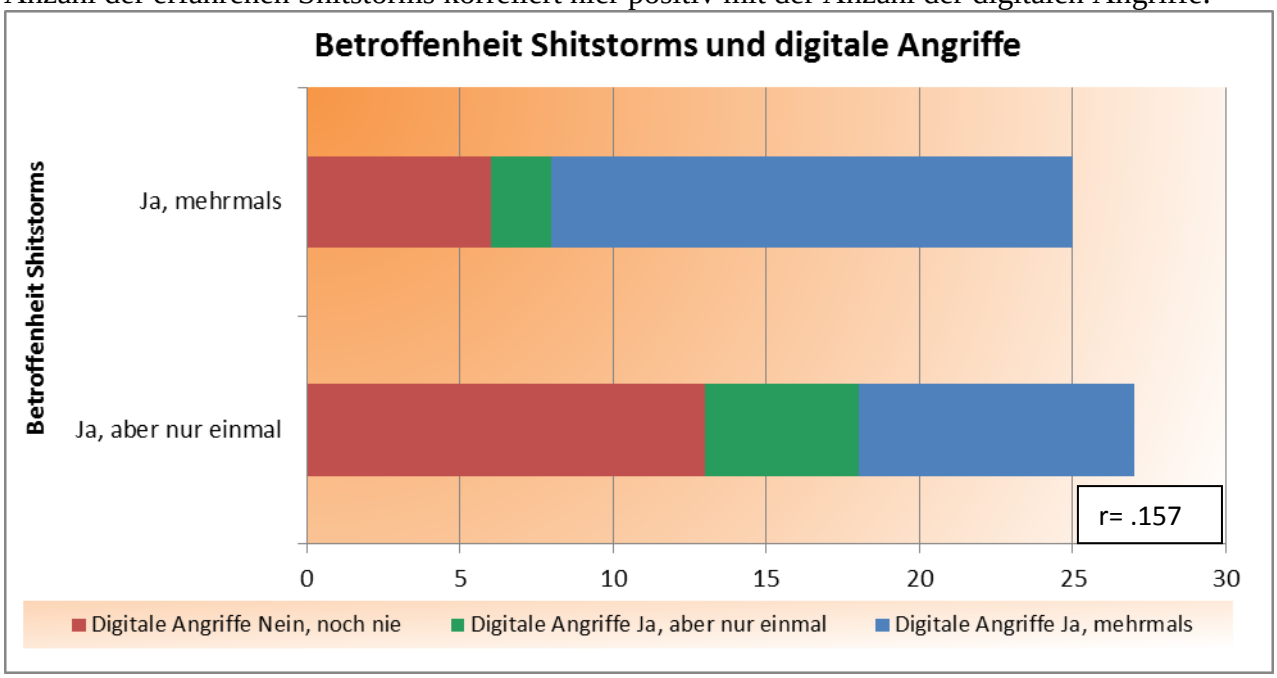


Abbildung 21: Betroffenheit Shitstorms und digitale Angriffe

615 der befragten Einrichtungen gaben an, dass ihre Beschäftigten via Home Office auf das Unternehmensnetzwerk zugreifen können und 557 Einrichtungen gaben an, dass die Beschäftigten dies mit einem mobilem Endgerät tun können. 223 der Einrichtungen verneinten den Zugriff der Beschäftigten von außerhalb auf das Unternehmensnetzwerk.

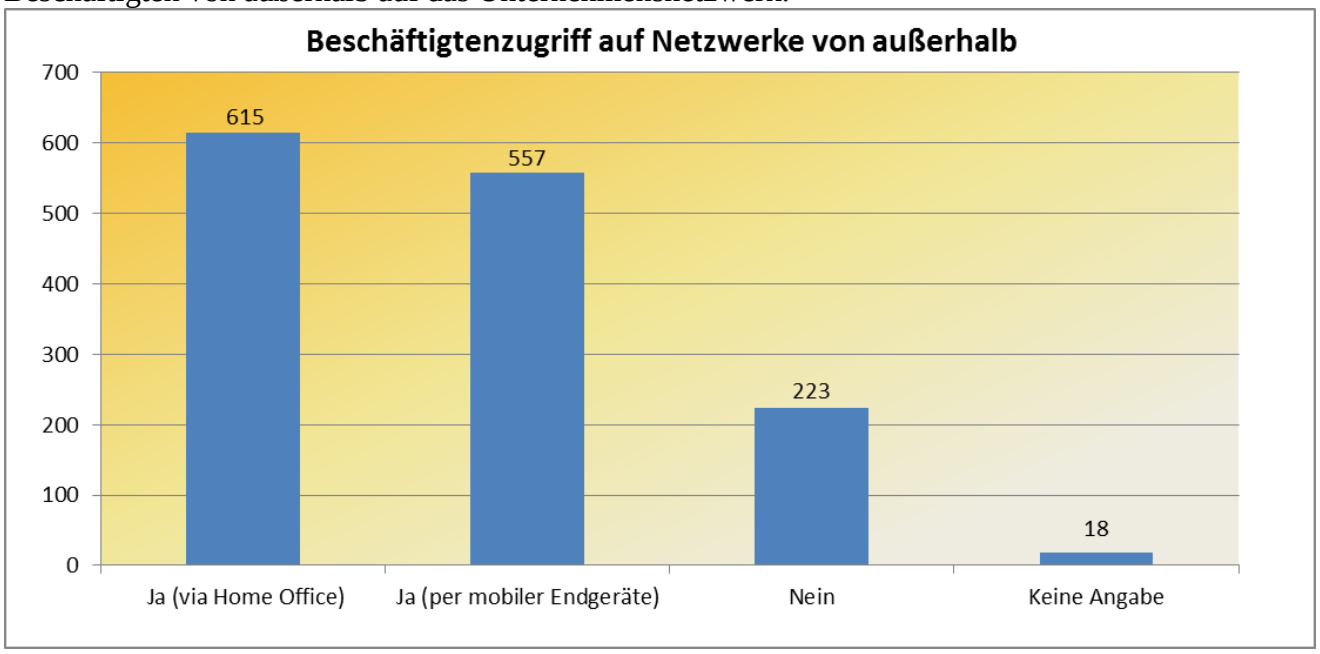


Abbildung 22: Beschäftigtenzugriff auf Netzwerke von außerhalb

Ähnlich wie zuvor bei der Betroffenheit von Shitstorms fällt auch bei den digitalen Angriffen auf, dass Einrichtungen, die ihren Beschäftigten den Zugriff auf das eigene Netzwerk von außerhalb ermöglichen, häufiger angeben, von digitalen Angriffen betroffen gewesen zu sein. Die aufgezeigte Korrelation begründet jedoch keine ursächliche Beziehung zwischen der externen Zugriffsmöglichkeit und digitalen Angriffen.

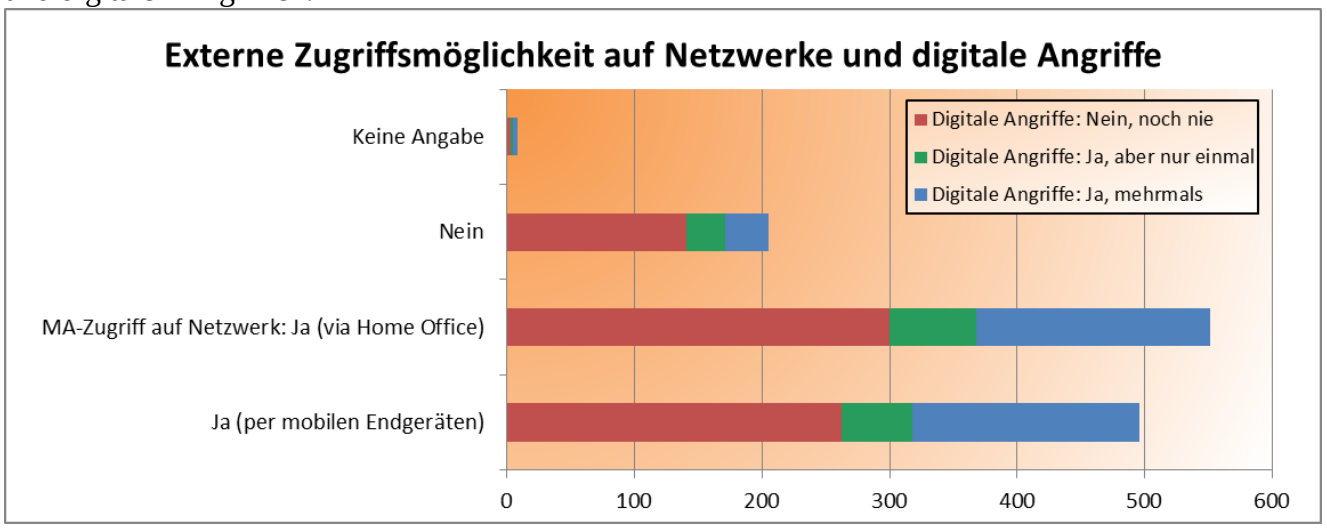


Abbildung 23: Externe Zugriffsmöglichkeit auf Netzwerke und digitale Angriffe

Zur Gewährleistung der Sicherheit eigener IT-Infrastrukturen ergreifen die befragten Einrichtungen in erster Linie folgende technische Maßnahmen: Schutzsoftware (Antivirenprogramme), Firewall, regelmäßige Software-Updates, Spam-Filter, Erstellung von Sicherungskopien und Passwortschutz auf allen Geräten. Daneben werden auch Verschlüsselungstechniken, Beschränkung des Zugriffs auf Unternehmensdaten vom Home-Office, Monitoring von Log-Dateien auf Unternehmens-IT, Intrusion Detection Systeme (Einsatz von Sensoren in der Unternehmens-IT zur Früherkennung von digitalen Einbrüchen) und die erweiterte IT-Zugangsbeschränkungen durch Benutzeridentifikation (z.B. Biometrie) genutzt.
Keine einzige Einrichtung gab an, keine technischen Sicherheitsmaßnahmen zu nutzen.

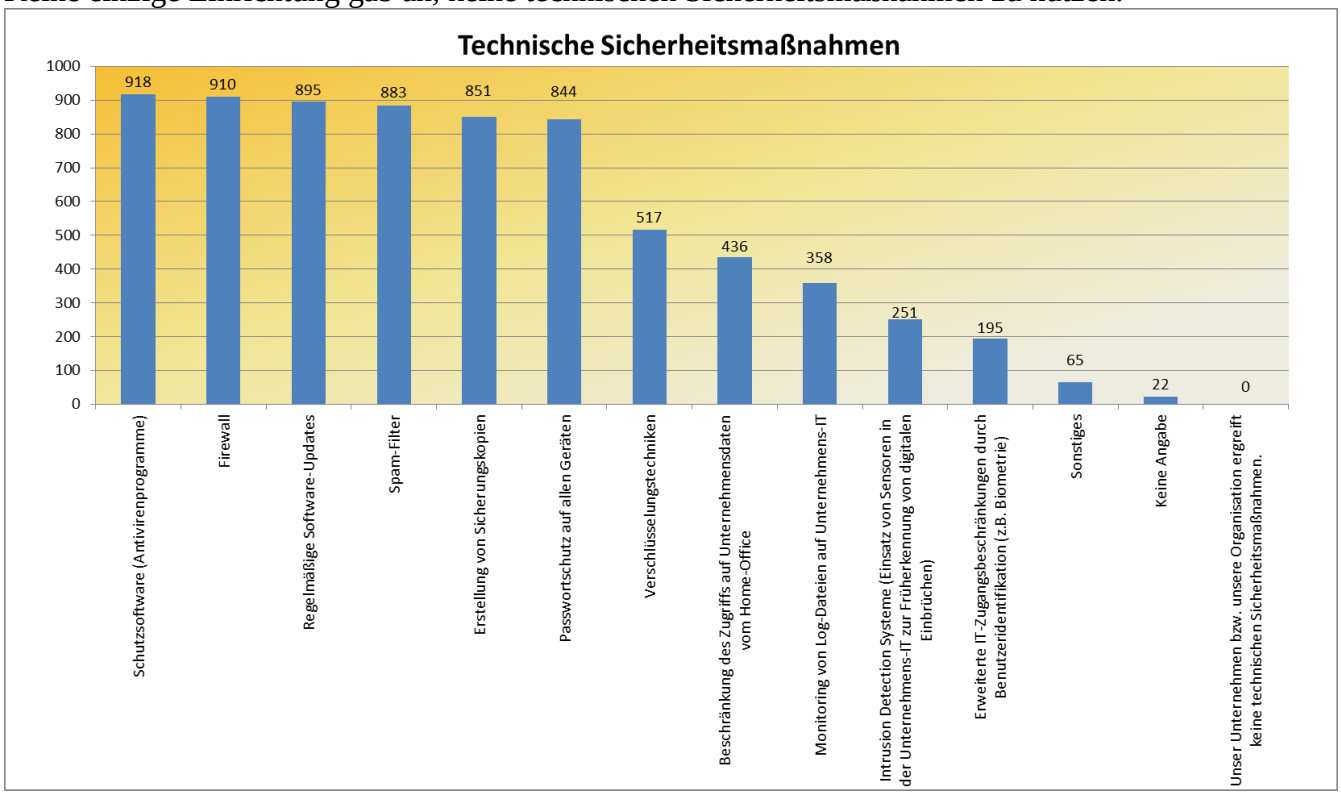


Abbildung 24: Technische Sicherheitsmaßnahmen

Bei den nicht-technischen Sicherheitsmaßnahmen (d. h. den verhaltensorientierten Maßnahmen) nutzt die Mehrheit der Einrichtungen Passwort Richtlinien und Richtlinien zum Umgang mit IT. Daneben werden Beschäftigte geschult und regelmäßige Sicherheitsaudits durch externe Beauftragte durchgeführt. 120 Einrichtungen gaben an, keine nicht-technischen Sicherheitsmaßnahmen zu nutzen.

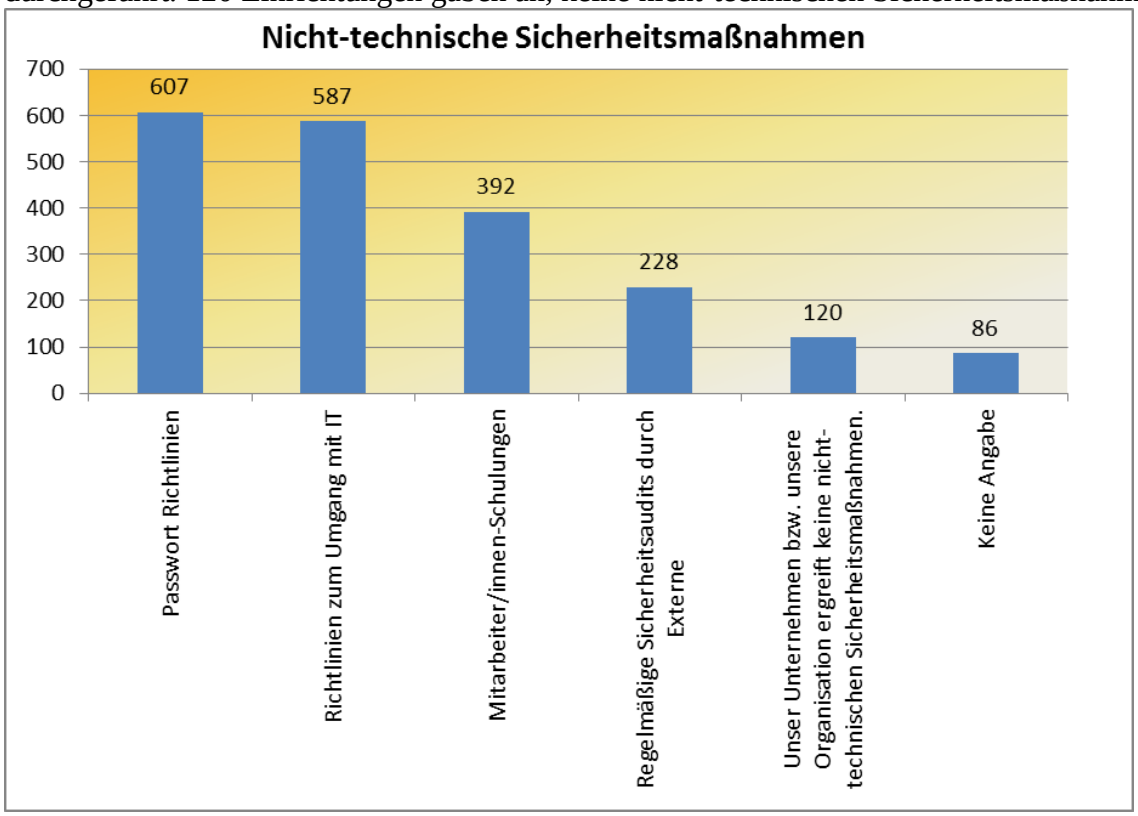


Abbildung 25: Nicht-technische Sicherheitsmaßnahmen

Zu der Höhe des Anteils von Ausgaben für IT-Sicherheitsmaßnahmen am Gesamtbudget der Einrichtung für das Jahr 2014 machten 734 Einrichtungen keine Angabe. Die Verteilung der durch die restlichen 237 Einrichtungen angegebenen Anteile ist heterogen. 47 Einrichtungen gaben an, dass der Anteil für IT-Sicherheitsmaßnahmen am Gesamtbudget für 2014 0 % betrug. In 103 Einrichtungen lag der Anteil zwischen 1 % und 2 %. 5 % betrug er in 35 Einrichtungen und Anteile zwischen 10 % und 25 % wurden von 28 befragten Einrichtungen angegeben.

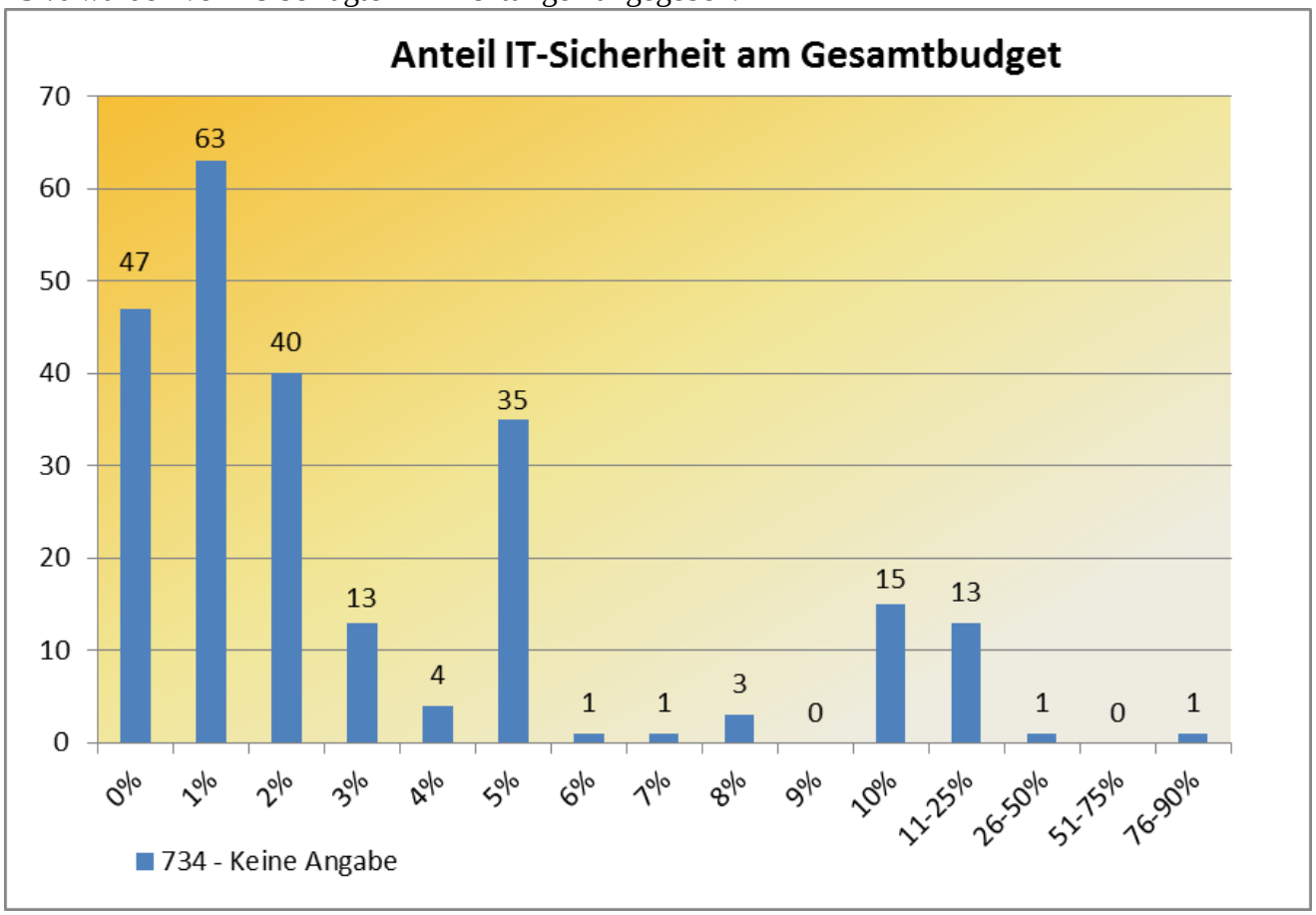


Abbildung 26: Anteil IT-Sicherheit am Gesamtbudget

2.2.4 Teil 4: Aktivismus

870 der befragten Einrichtungen (90 %) schätzen die Gefährdung, Ziel von politisch oder ideologisch motivierten Aktivitäten, wie z. B. Demonstrationen, Informationskampagnen und mutwilligen Sachbeschädigungen zur Erreichung ideologischer Ziele zu werden, gering bis sehr gering ein. Bei 63 Einrichtungen (6,5 %) fiel die Gefährdungseinschätzung hoch bis sehr hoch aus.

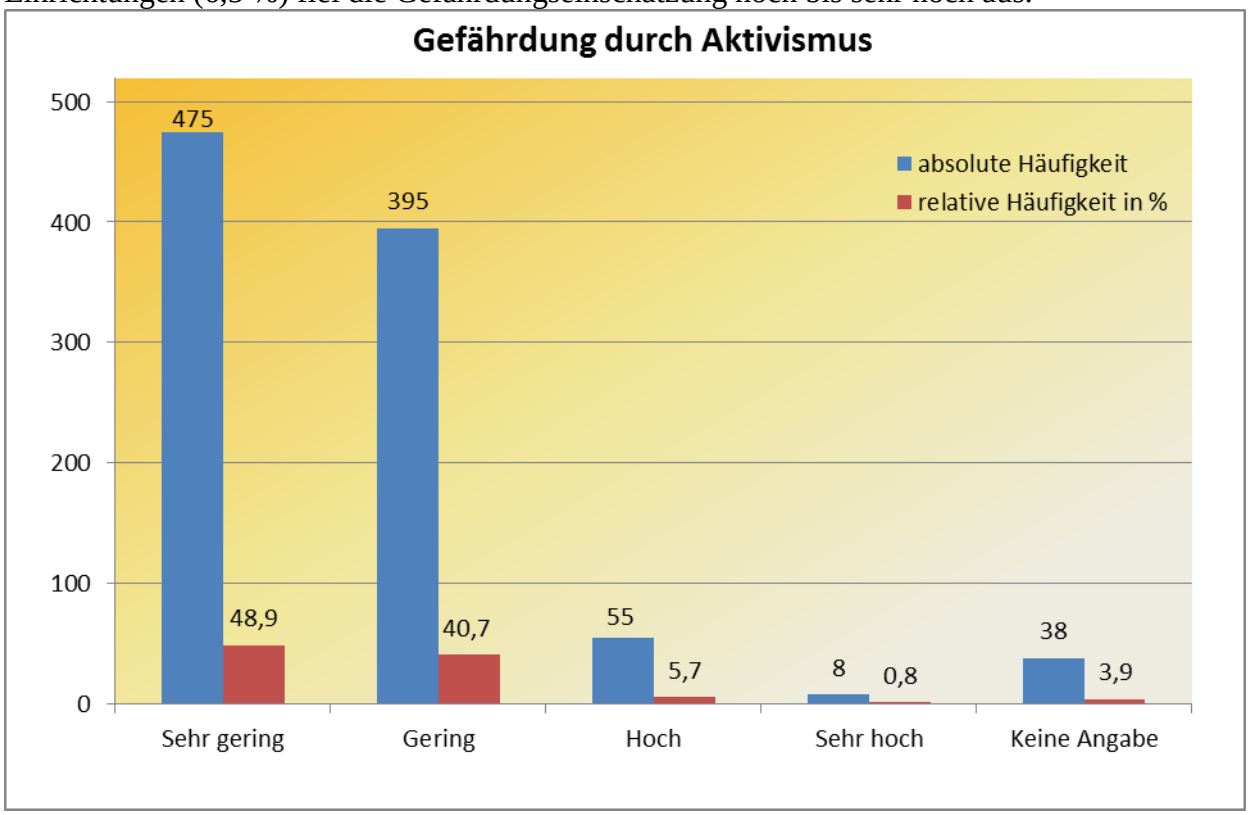


Abbildung 27: Gefährdungseinschätzung Aktivismus

Die Gefährdungseinschätzung steigt mit der Mitarbeiterzahl der Einrichtung. Größere Unternehmen schätzen die Gefahr Opfer von Aktivismus zu werden höher ein.

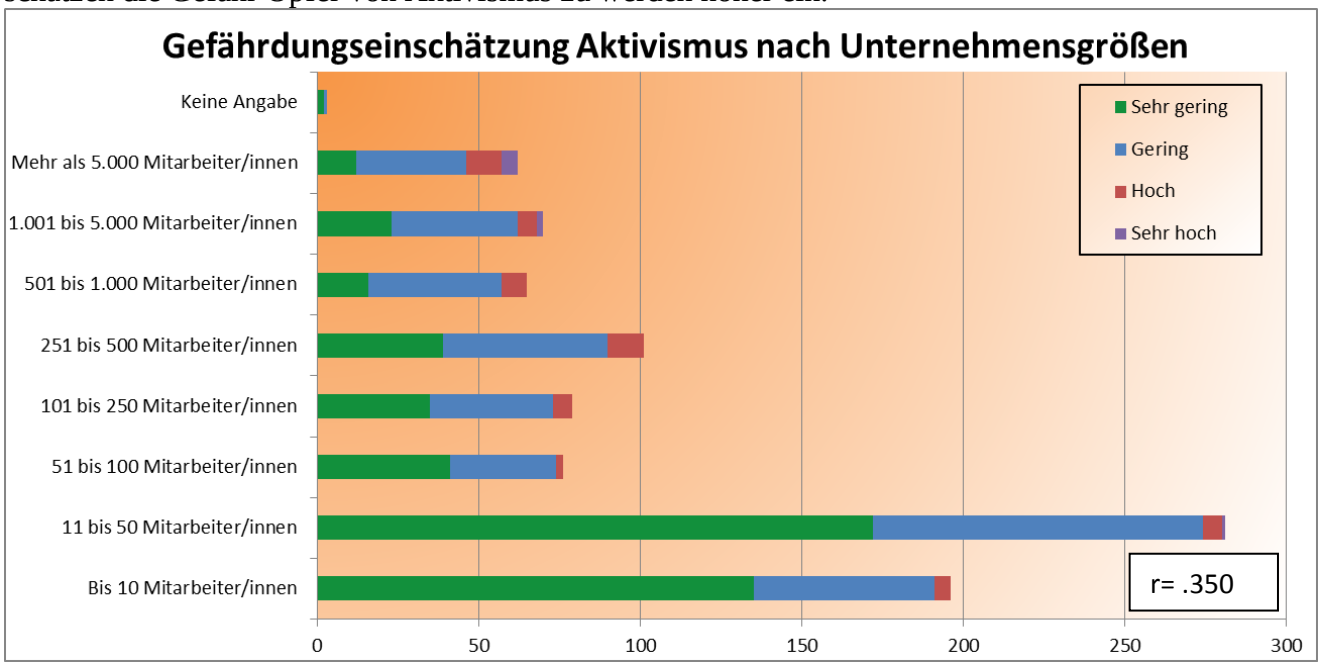


Abbildung 28: Gefährdungseinschätzung Aktivismus nach Unternehmensgrößen

87 % der Befragten wurden bisher auch noch nicht Ziel von politischen oder ideologisch motivierten Aktivitäten:

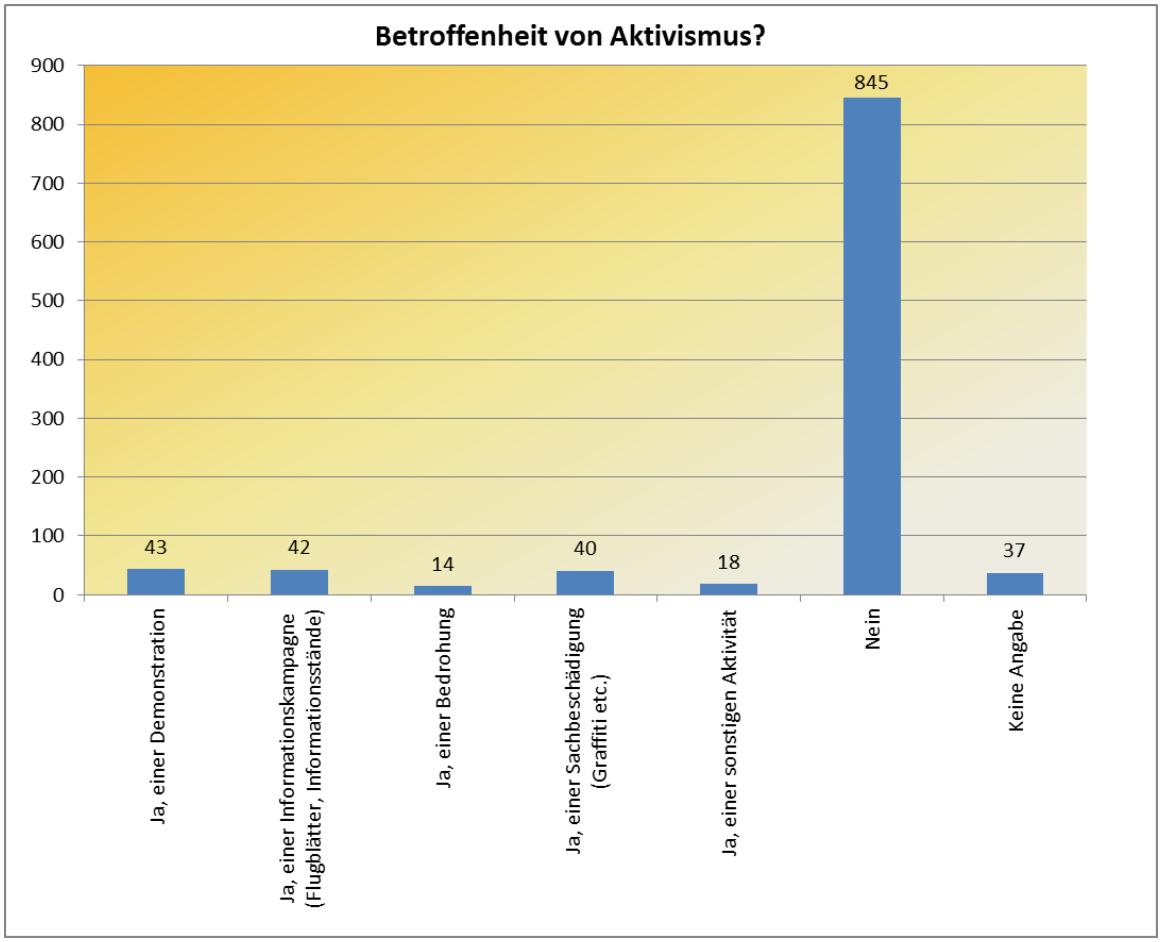


Abbildung 29: Betroffenheit von Aktivismus?

Erlittene aktivistische Aktivitäten verteilen sich auf die Branchen wie folgt:

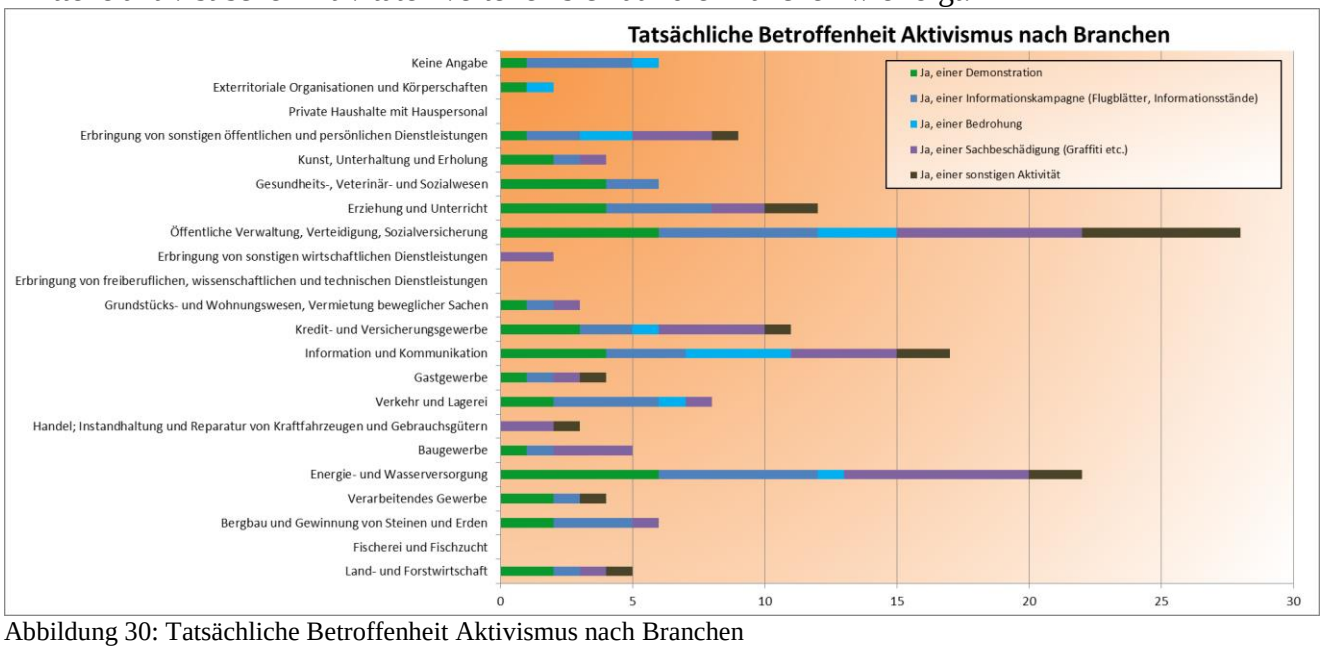


Abbildung 30: Tatsächliche Betroffenheit Aktivismus nach Branchen

Auch wenn die Angabe von 1 bis 10 Standorten die Mehrheit der befragten Einrichtungen stellt, so fällt auf, dass Einrichtungen mit einer geringen Standortzahl einen verhältnismäßig höheren Anteil an Sachbeschädigungen erlitten haben.

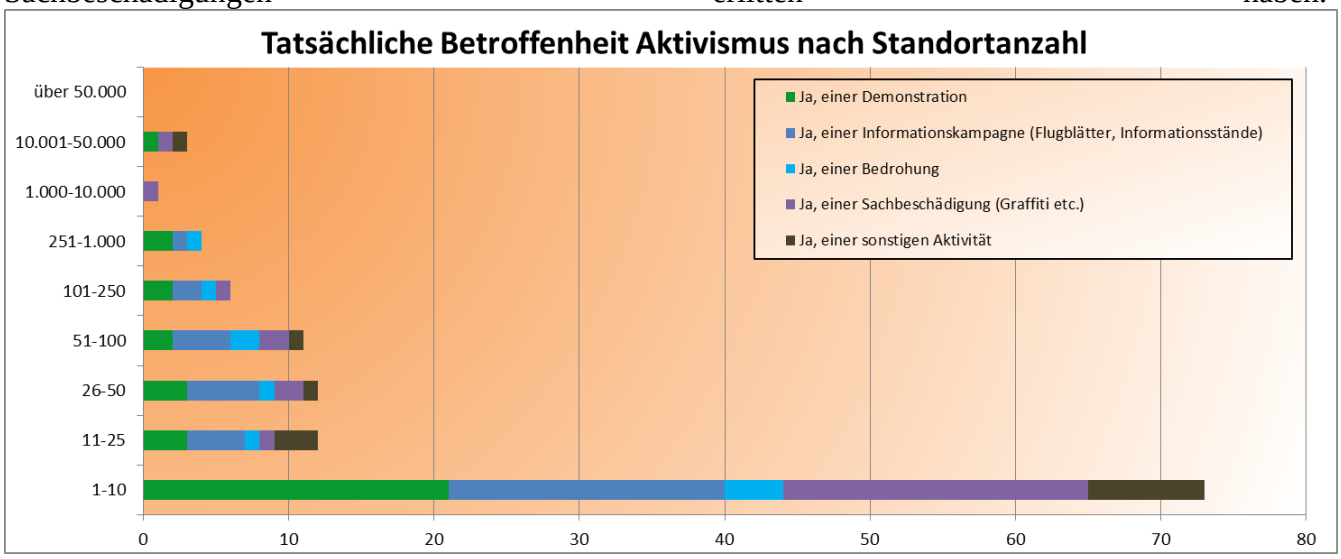


Abbildung 31: Tatsächliche Betroffenheit Aktivismus nach Standortanzahl

Einrichtungen, die bereits analogen Aktivismus erfahren haben, waren auch schon von mehreren Shitstorms betroffen.

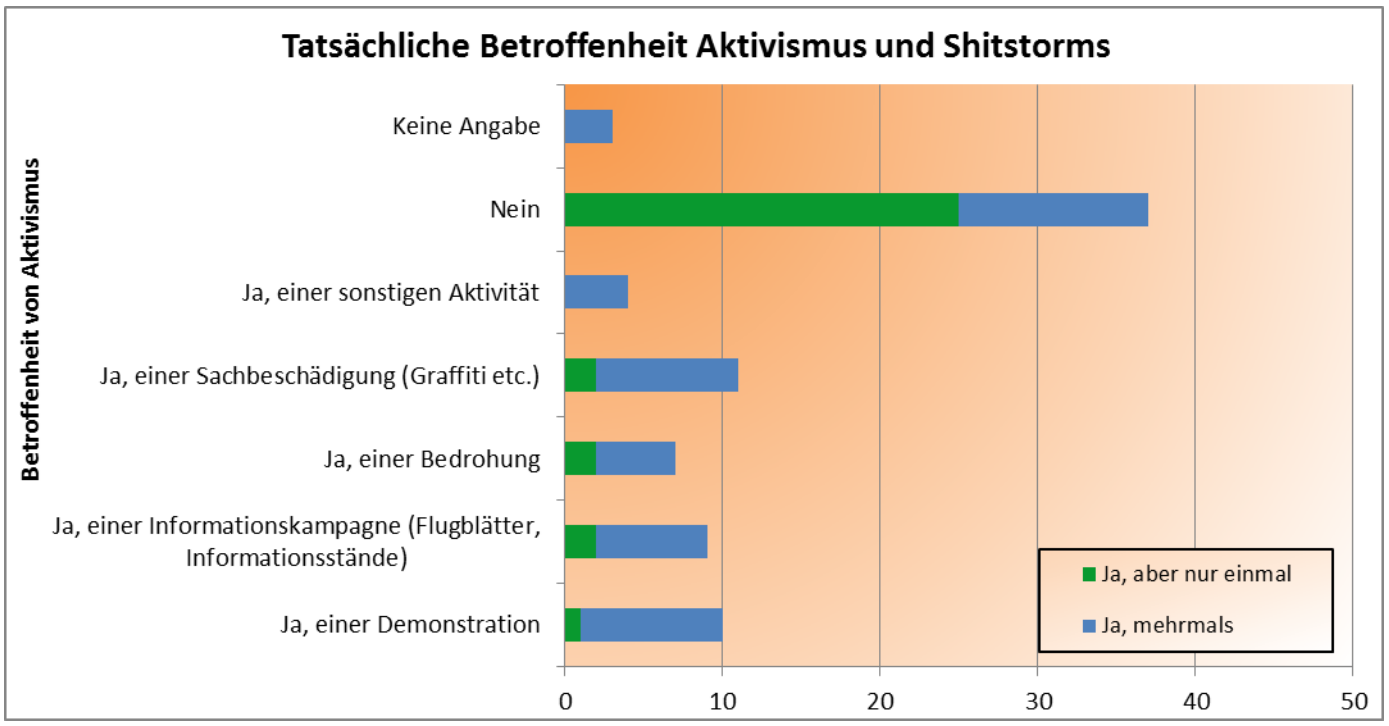


Abbildung 32: Tatsächliche Betroffenheit Aktivismus und Shitstorms

2.2.5 Teil 5: Hacktivismus

Der Begriff Hacktivismus beinhaltet die Konzepte Hacking und Aktivismus: Das Nutzen von Hacking- bzw. IuK-Tools zur Verdeutlichung und Durchsetzung politischer wie sozialer Ziele (Ideologien) bildet die Schnittmenge beider Konzepte. Die Hacking-Tools werden u. a. für Protest- und/oder Propagandazwecke eingesetzt und sind nicht profitorientiert, d. h. hacktivistische Taten zielen nicht darauf ab, illegal materielle und finanzielle Gewinne zu erzielen (wie z. B. das Phishing).
Anders als finanziell motivierte Hacker veröffentlichen Hacktivisten aus ideologischen Gründen bspw. gestohlene Daten wie Zugangspasswörter, persönliche und vertrauliche Informationen, E-Mail-Adressen usw. im Internet. Hacktivistische Aktivitäten müssen nicht in jedem Fall strafrechtlich relevant sein. Da bei dem zum Hacktivismus unabdingbaren Einsatz von Online-Tools jedoch häufig Systeme manipuliert und/oder Daten ausgespäht werden, werden in solchen Fällen verschiedene Straftatbestände erfüllt (§ 303 a StGB (Datenveränderung), § 303 b StGB (Computersabotage), § 202 a StGB (Ausspähen von Daten), § 202 b StGB (Abfangen von Daten.

87 % der befragten Einrichtungen schätzen die Gefährdung, Ziel von hacktivistischen Angriffen zu werden, als gering bis sehr gering ein. Als hoch bis sehr hoch schätzen dies 9 % der Einrichtungen ein.

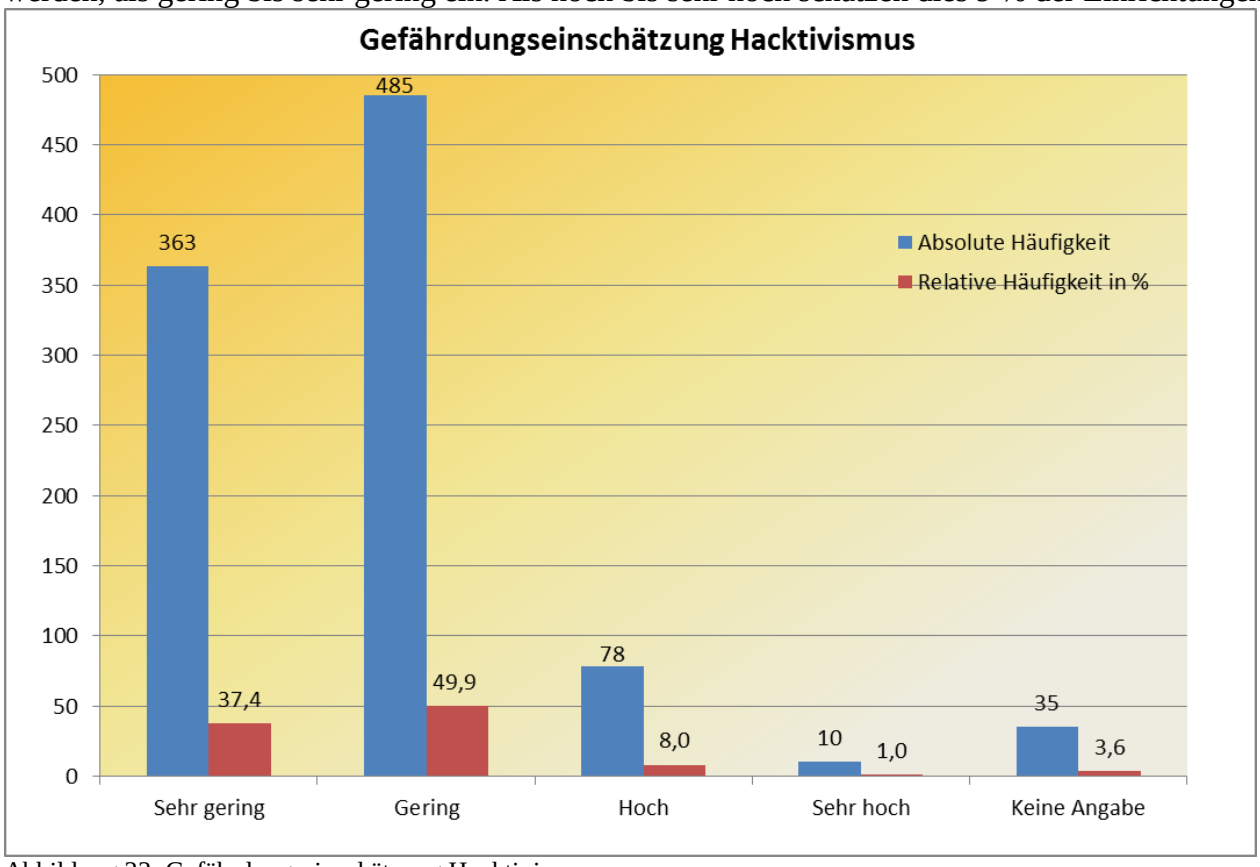


Abbildung 33: Gefährdungseinschätzung Hacktivismus

Ähnlich wie bei der Gefährdungseinschätzung für Aktivismus, schätzen größere Einrichtungen die Gefahr, Ziel von hacktivistischen Angriffen zu werden höher ein.

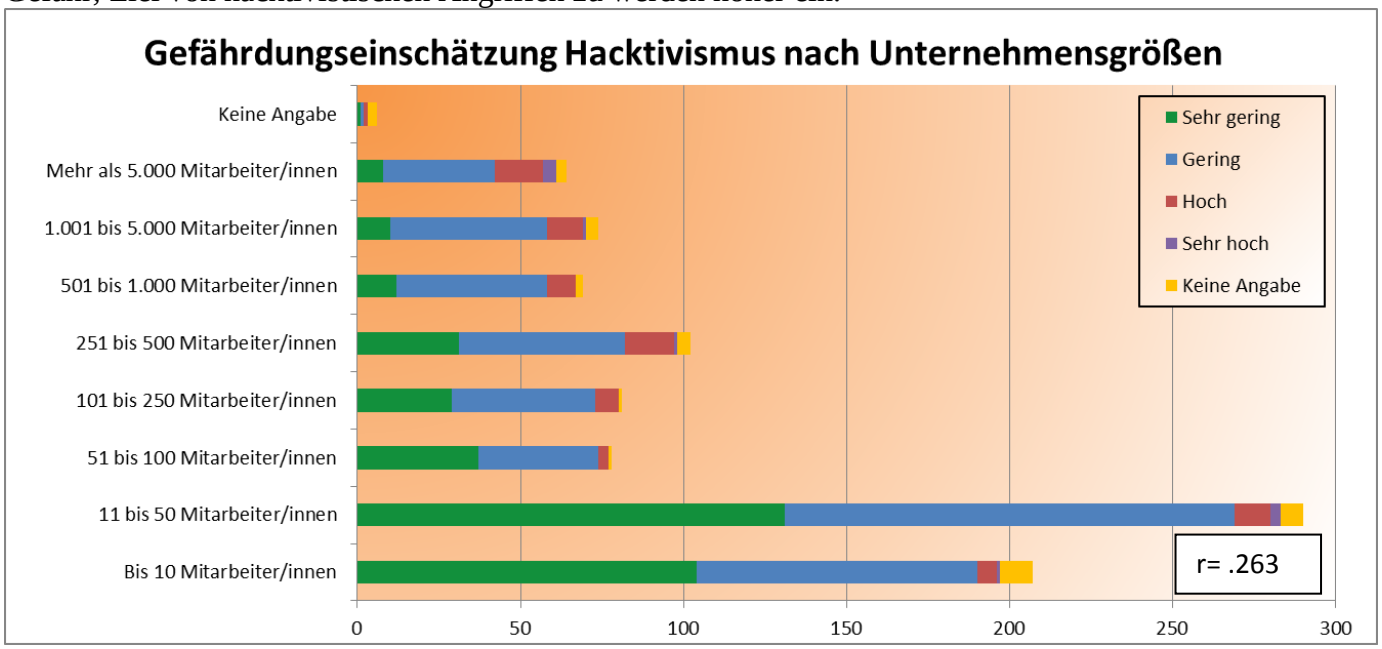


Abbildung 34: Gefährdungseinschätzung Hacktivismus nach Unternehmensgrößen

Einrichtungen, die bereits von mehreren Shitstorms betroffen waren, schätzen auch die Gefahr, Opfer von Hacktivismus zu werden, höher ein.

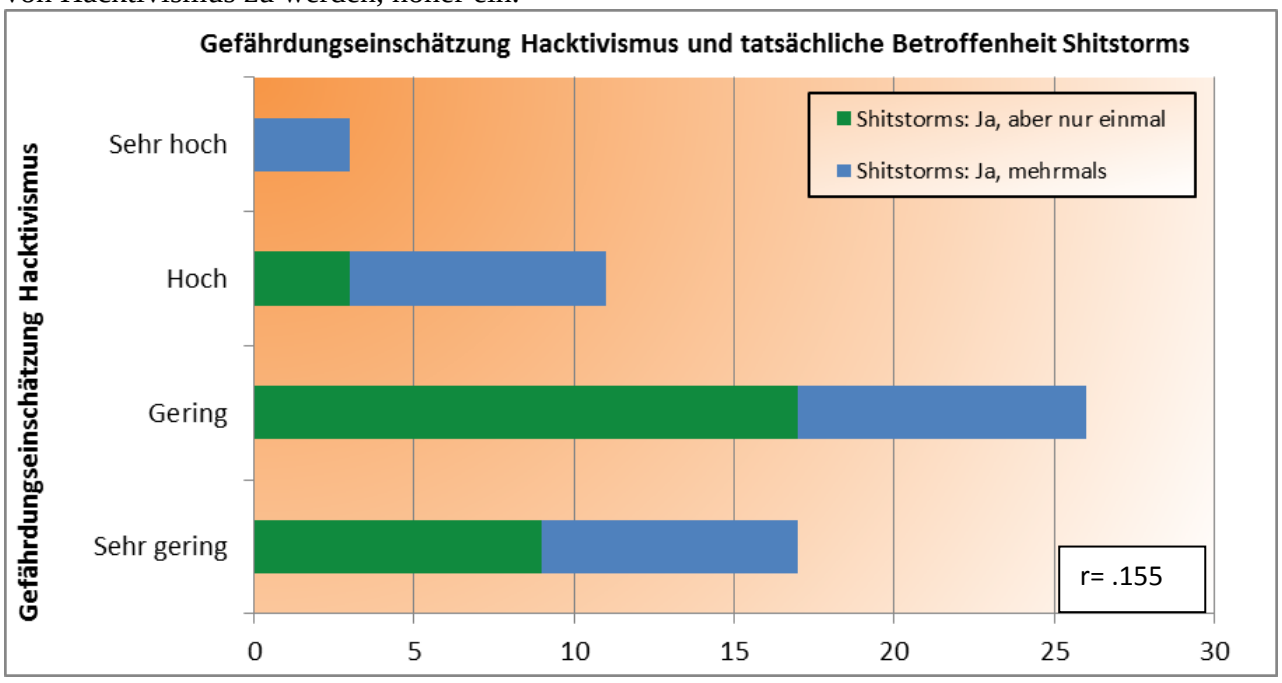
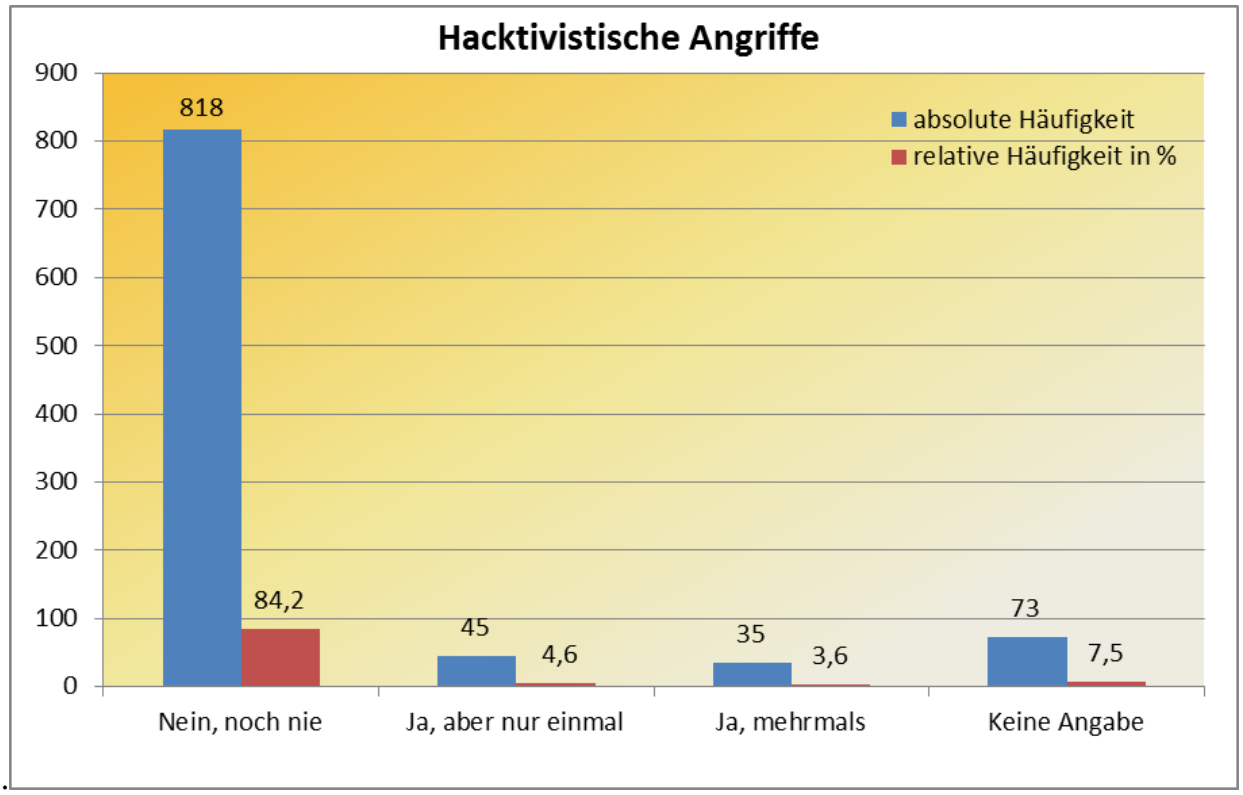


Abbildung 35: Gefährdungseinschätzung Hacktivismus und tatsächliche Betroffenheit Shitstorms

Von hacktivistischen Angriffen waren 45 Einrichtungen bisher einmal und 35 Einrichtungen mehrmals betroffen. 818 Einrichtungen gaben an, noch nie hacktivistischen Angriffen unterlegen gewesen zu sein.



.

Abbildung 36: Hacktivistische Angriffe

Es ließ sich ein leichter positiver Zusammenhang zwischen der Größe des angegriffenen Unternehmens und der Angriffszahl ausmachen. Je größer ein Unternehmen ist, desto eher war es bereits mehrmals von hacktivistischen Angriffen betroffen.

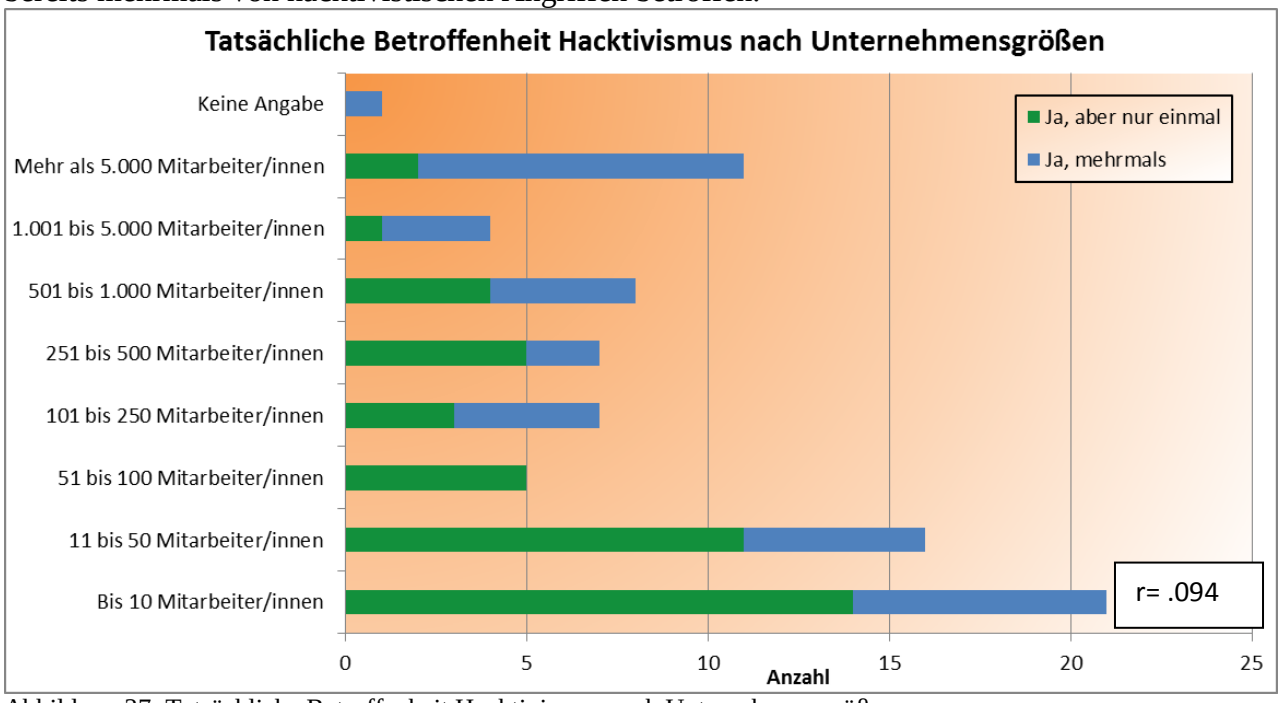


Abbildung 37: Tatsächliche Betroffenheit Hacktivismus nach Unternehmensgrößen

Die Differenzierung der Angriffe nach Branchen zeigt, dass die Branche *Information und Kommunikation* die meisten Fälle von Hacktivismus erfahren hat. Zu beachten ist, dass diese Branche mit 7,8 % nicht die Mehrheit der in der Befragung verorteten Branchen stellt. Mit 14,6 % war das *verarbeitende Gewerbe* die Branche, in der sich die meisten Teilnehmer verorten. Gefolgt von der Branche *Handel; Instandhaltung und Reparatur von Kraftfahrzeugen und Gebrauchsgütern* mit 9,5 %, dem *Baugewerbe* mit 8,7 % sowie der Branche *Erbringung von sonstigen wirtschaftlichen Dienstleistungen* mit 8,3 %.

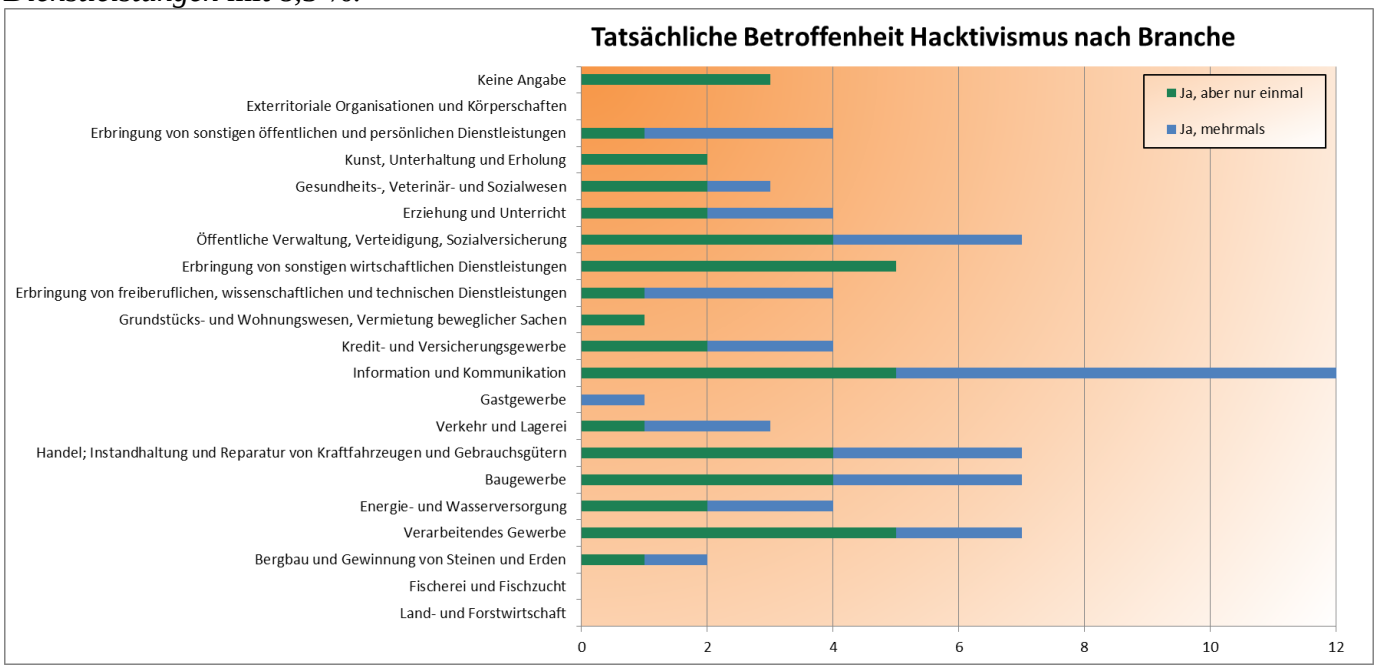


Abbildung 38: Tatsächliche Betroffenheit Hacktivismus nach Branche

Auffällig ist, dass Unternehmen und Einrichtungen ab 100 Standorten keine hacktivistischen Angriffe erlebt bzw. angegeben haben:

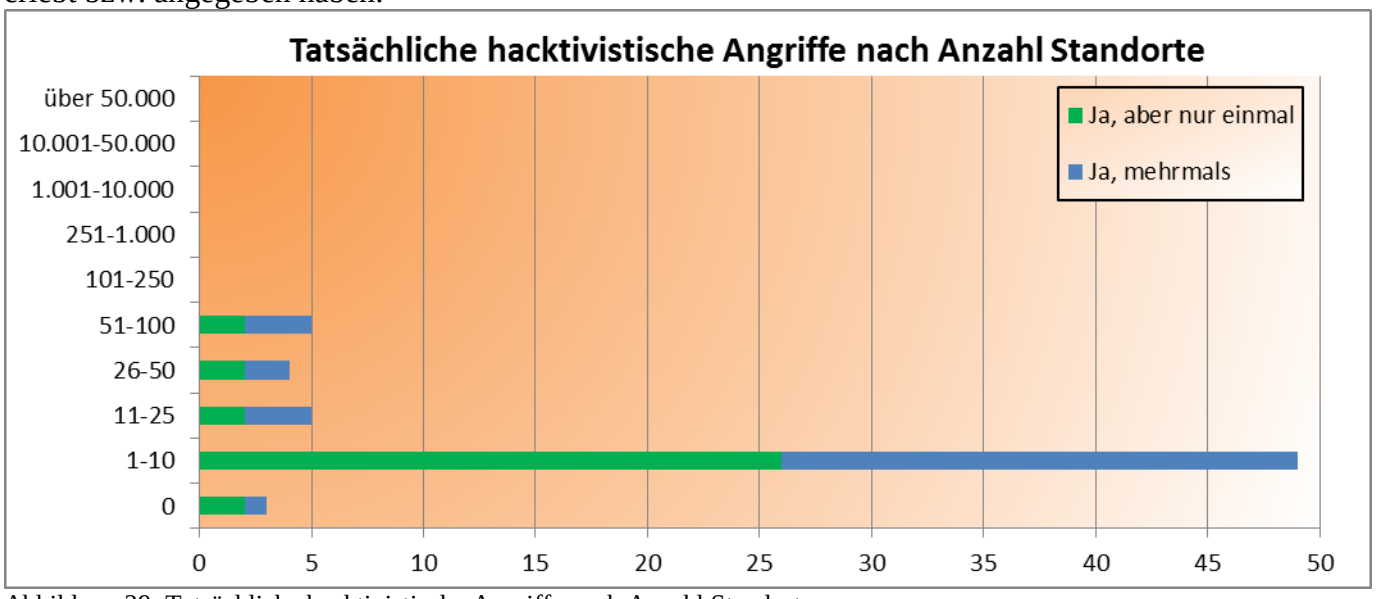


Abbildung 39: Tatsächliche hacktivistische Angriffe nach Anzahl Standorte

Betrachtet man das Auftreten hacktivistischer Angriffe in Beziehung zur Nutzung sozialer Medien, so fällt auf, dass Einrichtungen, die bereits mehrere hacktivistische Angriffe erfahren haben, auch mehrheitlich soziale Medien nutzen. Einrichtungen, die nicht von Hacktivismus betroffen waren, nutzen überwiegend keine sozialen Medien.

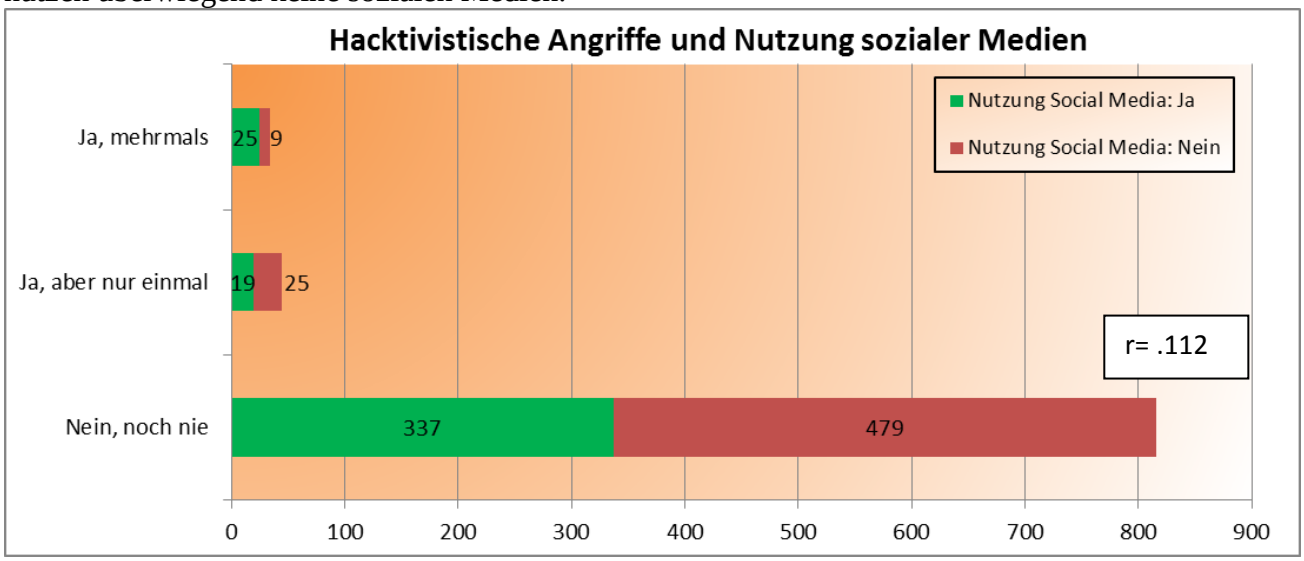


Abbildung 40: Hacktivistische Angriffe und Nutzung sozialer Medien

Einrichtungen, die von Shitstorms oder auch digitalen Angriffen betroffen waren, waren auch eher von hacktivistischen Angriffen betroffen.

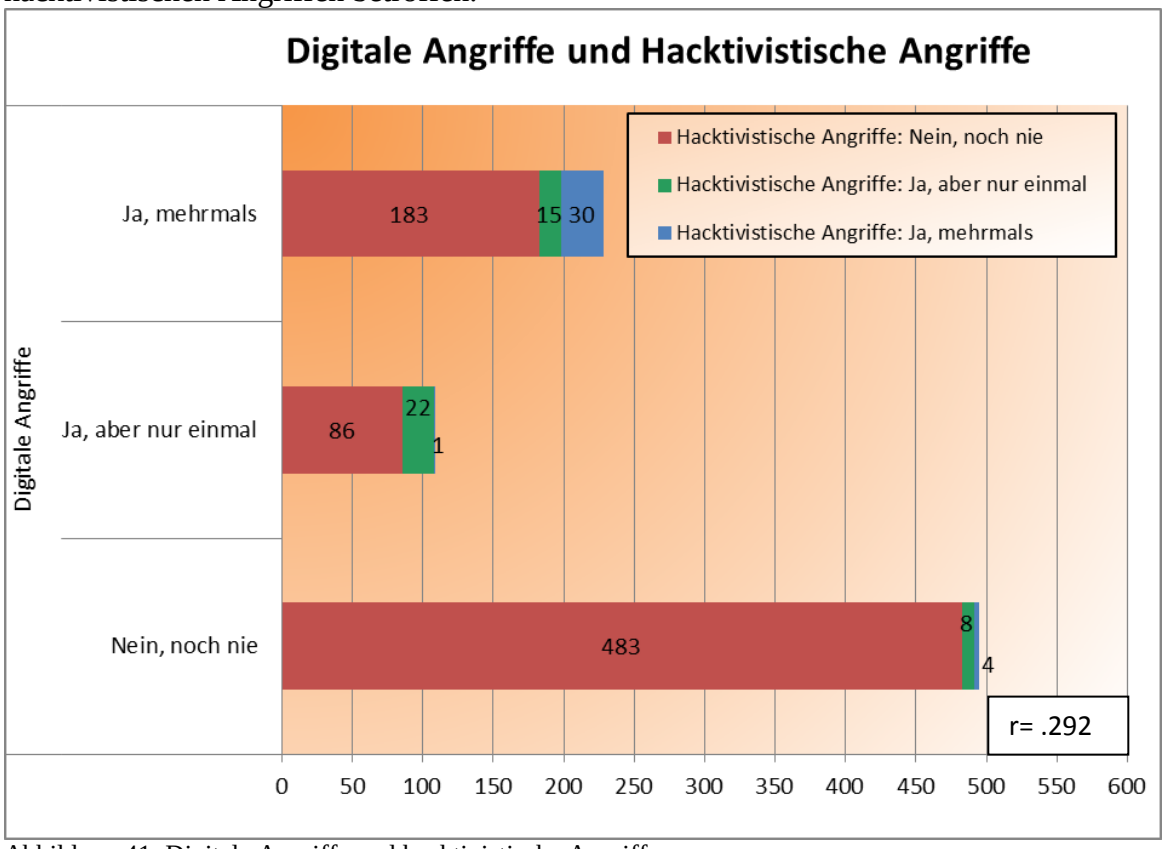


Abbildung 41: Digitale Angriffe und hacktivistische Angriffe

Die von den Einrichtungen erfahrenen hacktivistischen Aktivitäten bestanden überwiegend aus E-Mail-Spams, gefolgt von DDoS-Angriffen und Webdefacements.

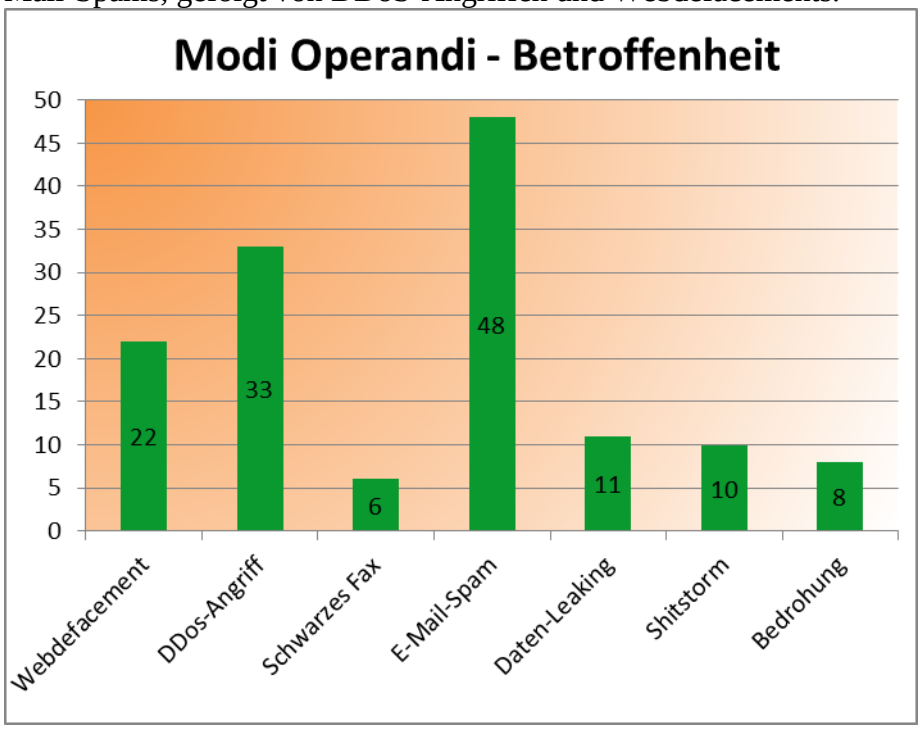


Abbildung 42: Modi Operandi – Betroffenheit

Die Einrichtungen gaben an, dass die hacktivistischen Angriffe überwiegend eine Infektion des eigenen Systems mit Schadsoftware sowie Serverausfälle zur Folge hatten. Daneben bewirkten die hacktivistischen Angriffe auch Sachschäden, Systemabstürze, Daten- und Reputationsverluste, Umsatzeinbußen und unerwünschte Presseberichterstattungen. 15 Einrichtungen gaben an, dass die Angriffe keine Folgen hatten.

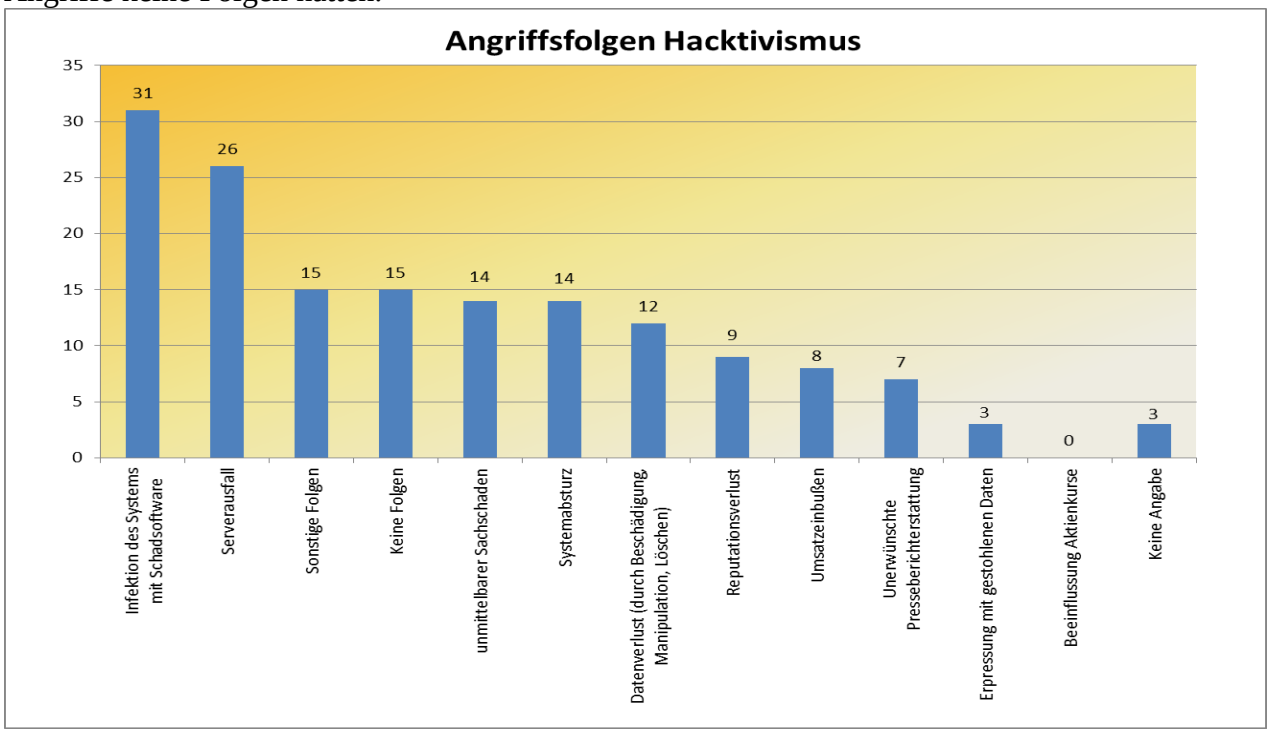


Abbildung 43: Angriffsfolgen Hacktivismus

43 Einrichtungen gaben an, dass ihnen durch die hacktivistischen Angriffe finanzielle Schäden entstanden sind, wozu auch Systemausfälle, Mehraufwand für Informationstechnik, Wiederherstellungskosten und zusätzliche Arbeitsbelastung zählen.

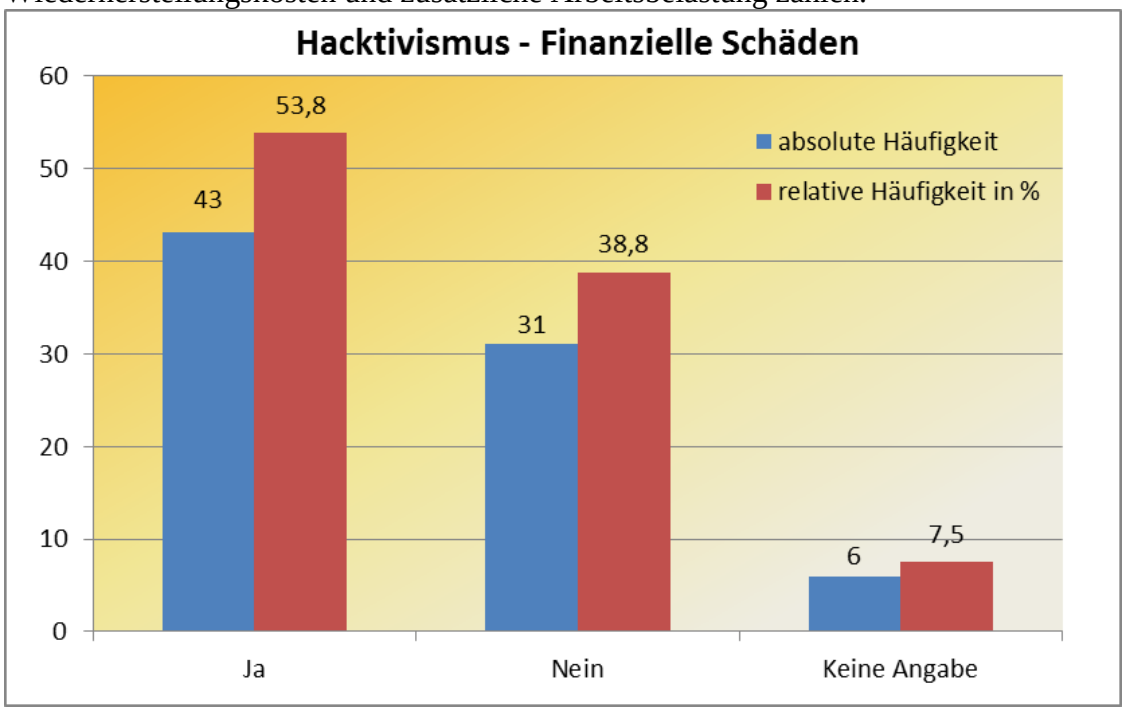


Abbildung 44: Hacktivismus – finanzielle Schäden

Betrachtet man die Art dieser finanziellen Schäden genauer, so handelte es sich in erster Linie um Kosten für die Behebung der Störung sowie um zusätzlichen Arbeitsaufwand. Auch zusätzliche Investitionen in Informationstechniken wurden als finanzielle Schäden angegeben. Der Verlust von Profiten sowie der Ausfall der Produktion spielte in wenigen Fällen eine Rolle.

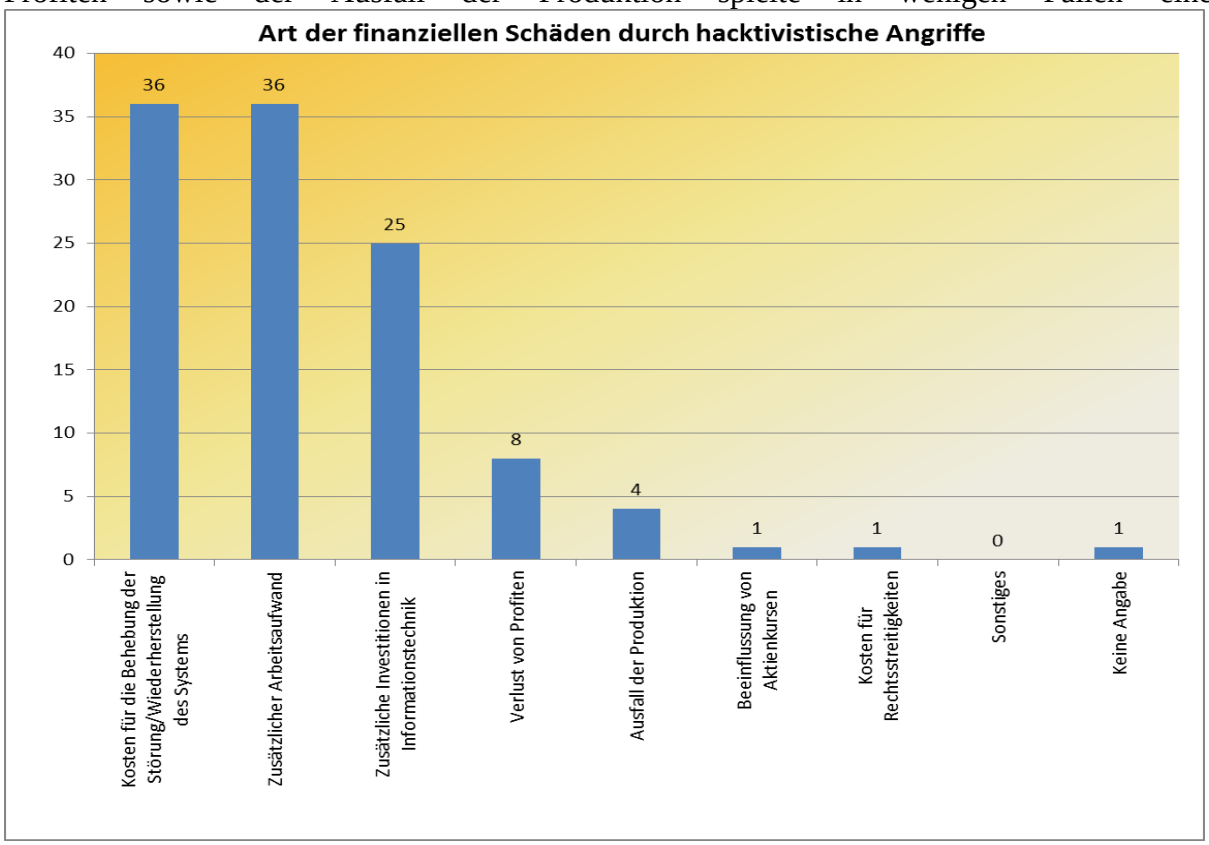


Abbildung 45: Art der finanziellen Schäden durch hacktivistische Angriffe

Die entstandenen Schäden (finanzieller und nicht-finanzieller Art) wurden in erster Linie intern behoben und Sicherheitsmaßnahmen intensiviert. Externe Auftragnehmer behoben die Schäden in 27 Fällen. Eine Anzeigenerstattung erfolgte in nur 15 % der Fälle.

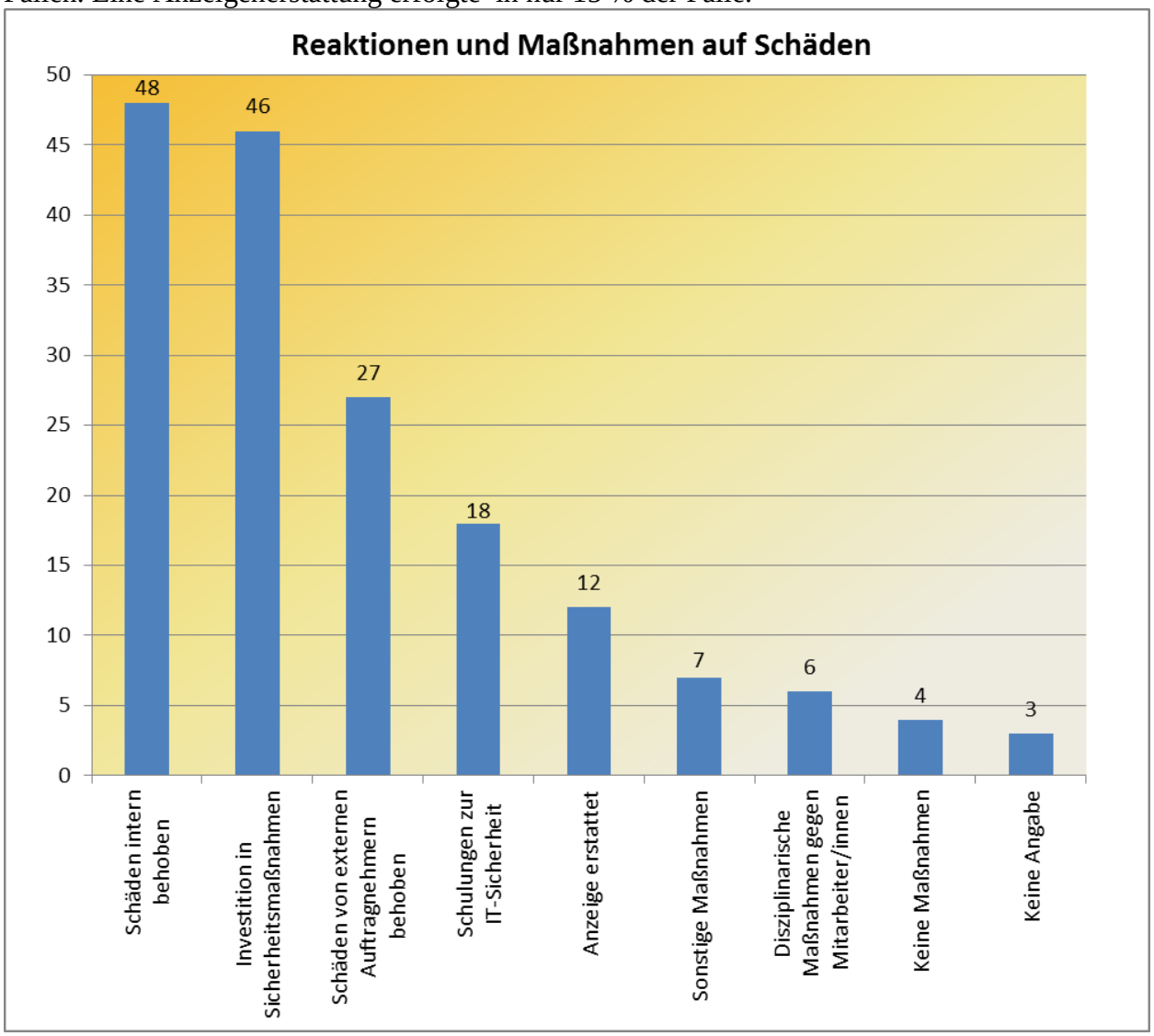


Abbildung 46: Reaktionen und Maßnahmen auf Schäden

Wenn die betroffene Einrichtung keine Anzeige erstattet hat, so lag das vor allem am Zweifel am Erfolg einer Anzeige, an dem zu großen Aufwand oder daran, dass ein zuständiger Ansprechpartner nicht bekannt war. In 26 Fällen wurde keine Anzeige erstattet, da keine Angriffsfolgen vorlagen.

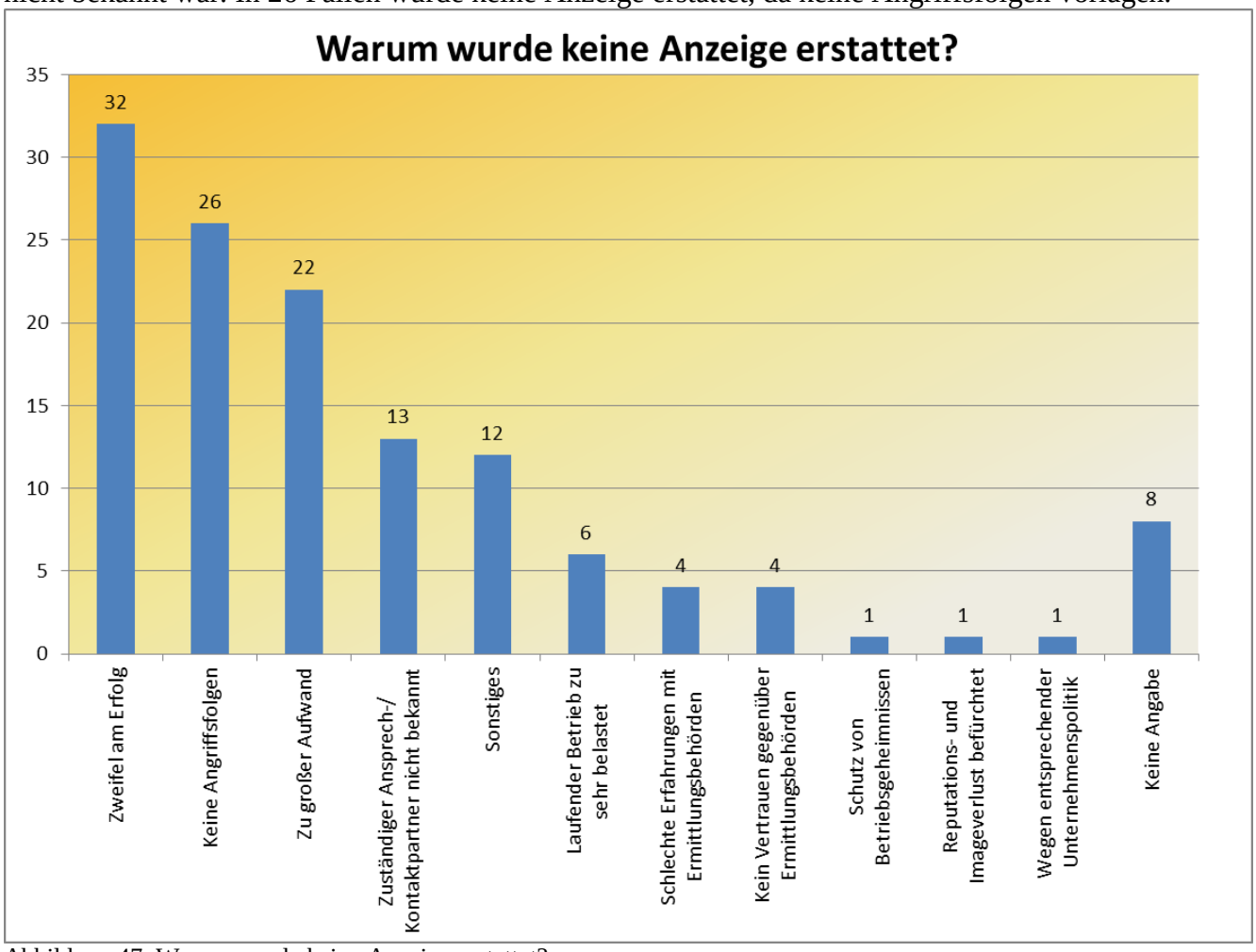


Abbildung 47: Warum wurde keine Anzeige erstattet?

Von den von hacktivistischen Angriffen betroffenen Einrichtungen gaben 70 % an, dass nach dem Angriff weder polizeilich noch außeramtlich (d .h. z. B. durch einen Privatdetektiv) ermittelt wurde. In 17,5 % der Fälle führten die Ermittlungen nicht zum Täter und lediglich in drei Fällen konnte der Täter ermittelt werden.

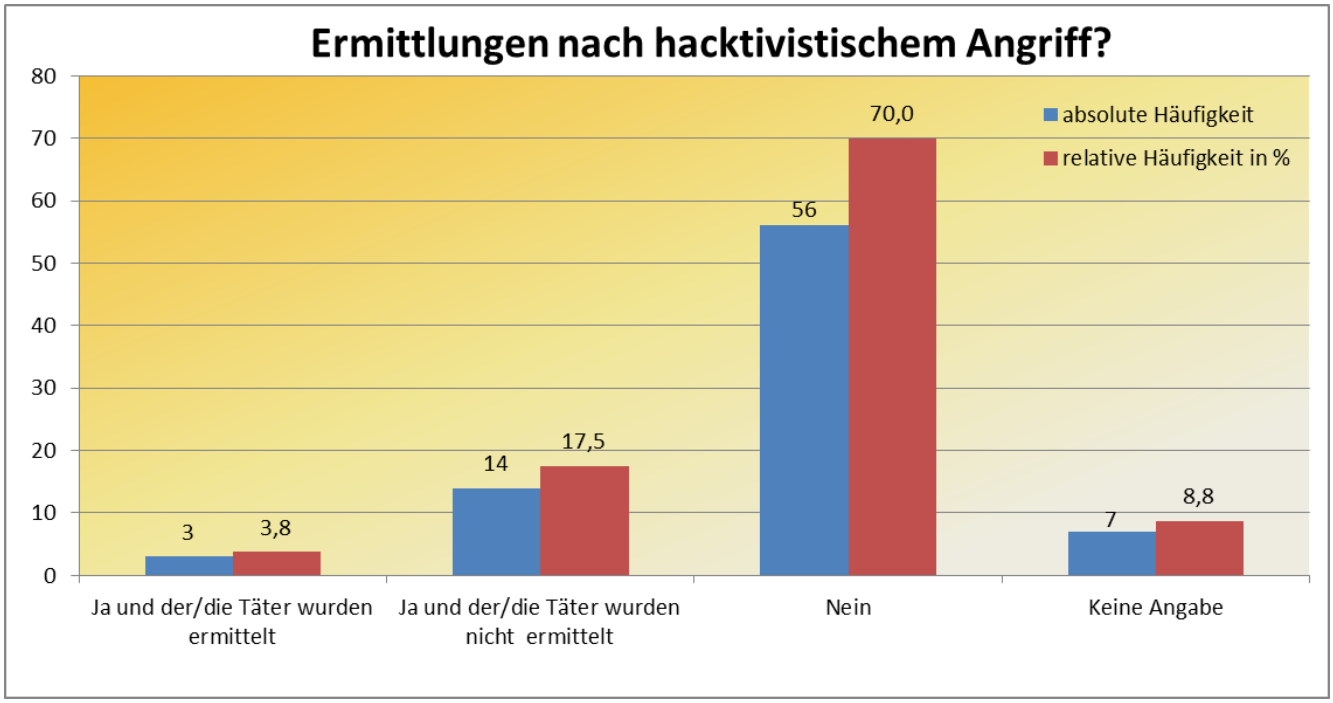


Abbildung 48: Ermittlungen nach hacktivistischem Angriff?

Bezüglich der hacktivistischen Angriffe wurde in fünf Fällen das BSI kontaktiert, in vier Fällen das Bundes-/Landesamt für Verfassungschutz und in sieben Fällen sonstige (Polizeien, Computer Emergency Response Team). In 69 % der Fälle wurde kein Kontakt aufgenommen.

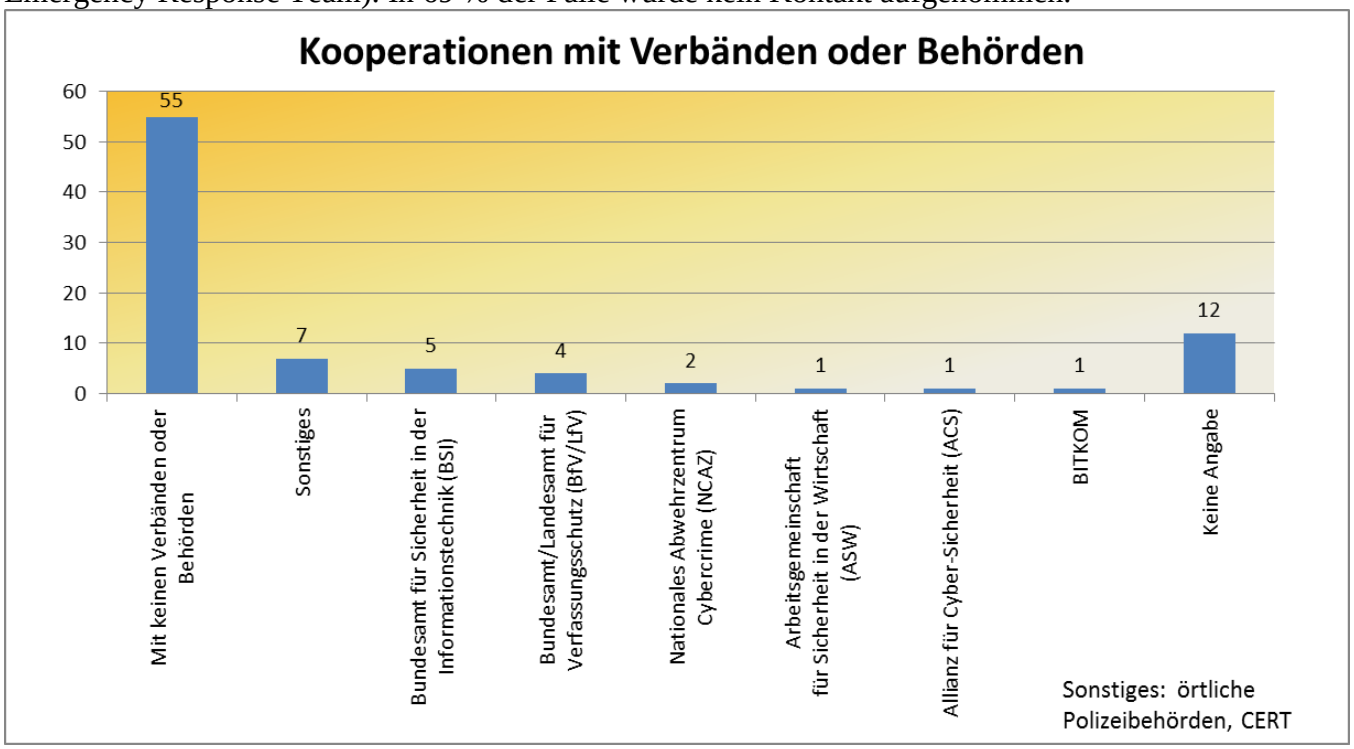


Abbildung 49: Kooperationen mit Verbänden oder Behörden

Insbesondere große Unternehmen haben Kontakt zu verschiedenen Verbänden und Behörden aufgenommen:

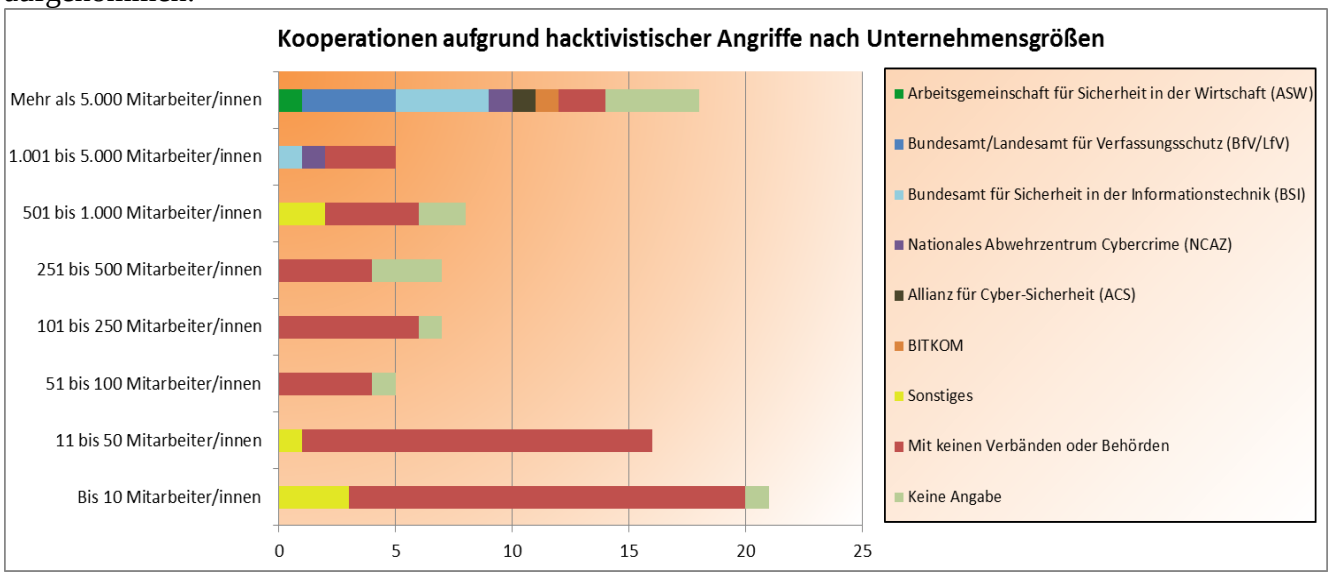


Abbildung 50: Kooperationen aufgrund hacktivistischer Angriffe nach Unternehmensgrößen

3. Fazit

Aus einer Stichprobe von 4.543 Einrichtungen und mit einer Rücklaufquote von 21 % liegen die Befragungsergebnisse von 971 Unternehmen und öffentlichen Einrichtungen vor. Die gewonnenen Aussagen sind damit hinreichend belastbar. Die Verteilung der Größen und Branchenzugehörigkeit der Unternehmen, die an der Online-Befragung teilgenommen haben, entspricht zudem – bis auf wenige Ausreißer, die vermutlich dem unterschiedlichen digitalen Vernetzungsgrad der jeweiligen Branchen geschuldet sind – der Gesamtverteilung aller Unternehmen in Deutschland.

Von 971 Unternehmen, die an der Befragung teilnahmen, gaben 80 Unternehmen an, bereits ein- oder mehrmals von Hacktivismus betroffen gewesen zu sein. Damit liegt die Häufigkeit für Unternehmen und öffentliche Einrichtungen in Deutschland Ziel von Hacktivismus zu werden bei 8 %. Hier sind es insbesondere Unternehmen aus der **Branche** Information und Kommunikation, die überdurchschnittlich häufig mit hacktivistischen Angriffen belastet sind. Die **Unternehmensgröße** spielt hinsichtlich der Angriffshäufigkeit eine Rolle: Je größer das Unternehmen ist, desto eher war es bereits mehrmals von hacktivistischen Angriffen betroffen.

Die hacktivistischen Angriffe verursachten in den meisten Fällen Infektionen mit Schadsoftware und Serverausfälle. 43 Einrichtungen gaben an, dass ihnen finanzielle **Schäden** entstanden sind, zu denen Kosten für die Behebung der Störung, zusätzlicher Arbeitsaufwand und zusätzliche Investitionen in die Informationstechnik zählten. In 15 Fällen verursachten die hacktivistischen Aktivitäten keinen Schaden. 60 % der betroffenen Einrichtungen behoben die Schäden intern, 15 % erstatteten Anzeige. Als Gründe, von einer **Anzeigenerstattung** abzusehen, gaben 33 % der Unternehmen an, dass es keine Angriffsfolgen gab, auch wenn ein folgenloser Angriff strafbar sein kann. 40 % sahen in einer Anzeigenerstattung keine Aussicht auf Erfolg. Insbesondere große Unternehmen gaben an, nach hacktivistischen Angriffen mit einer Bandbreite an Institutionen wie der ASW, dem Verfassungsschutz, dem NCAZ, BSI, der ACS und der Bitkom zu kooperieren.

Für das **Dunkelfeld** von Hacktivismus bedeuten diese Ergebnisse, dass die Anzeigequote für hacktivistische Aktivitäten bei 15 % liegt und damit 85 % der Aktivitäten im relativen Dunkelfeld liegen (68 Fälle). Dem Dunkelfeld hinzuzurechnen sind die Fälle, welche vom Opfern nicht bemerkt werden (absolutes Dunkelfeld).

Mit 845 Unternehmen war die Mehrheit bislang noch nicht von **Aktivismus** betroffen. Auffällig oft waren Einrichtungen der öffentlichen Verwaltung, Verteidigung und Sozialversicherung von aktivistischen Aktionen wie Demonstrationen, Bedrohungen und Sachbeschädigung betroffen, gefolgt von Einrichtungen der Energie- und Wasserversorgung. Einrichtungen mit einer kleinen Standortzahl erlitten überdurchschnittlich viele Sachbeschädigungen im Vergleich zu Einrichtungen mit einer größeren Standortzahl (hier dominieren Informationskampagnen die erfahrene aktivistische Bandbreite). Einrichtungen, die von Aktivismus betroffen waren, erlebten auch schon mehrere Shitstorms.

Insgesamt wird die eigene **Gefährdung** durch Aktivismus und Hacktivismus durch die befragten Einrichtungen als eher gering bis sehr gering eingeschätzt. Mit zunehmender Größe der Firmen steigt auch das eingeschätzte Gefährdungspotenzial. Es besteht ein positiver Zusammenhang zwischen der Betroffenheit von Aktivismus und der Betroffenheit von Hacktivismus, d. h. dass Einrichtungen die im Fokus von Aktivismus standen mit großer Wahrscheinlichkeit auch durch hacktivistische Angriffe betroffen sind und umgekehrt.

Eine knappe Mehrheit der befragten Unternehmen (550) gab an, keine **sozialen Medien** zu nutzen. Nutzen Unternehmen soziale Medien, so sind diese auch eher von **Shitstorms** betroffen: 57 Unternehmen gaben an, bereits einen oder mehrere Shitstorms erfahren zu haben (überwiegend auf den eigenen Social Media-Auftritten), hierbei ließen sich keine Zusammenhänge zur Unternehmensgröße feststellen. Die Einrichtungen, die bereits mehrere hacktivistische Angriffe erfahren haben, nutzen überwiegend soziale Medien. Unter den Einrichtungen, die keinen Hacktivismus erlebt haben, nutzt die Mehrheit keine sozialen Medien. Zwischen der Betroffenheit durch Shitstorms und der Betroffenheit durch Hacktivismus konnte ebenfalls ein Zusammenhang entdeckt werden: Von Shitstorms betroffene Unternehmen sind auch eher von Hacktivismus betroffen.

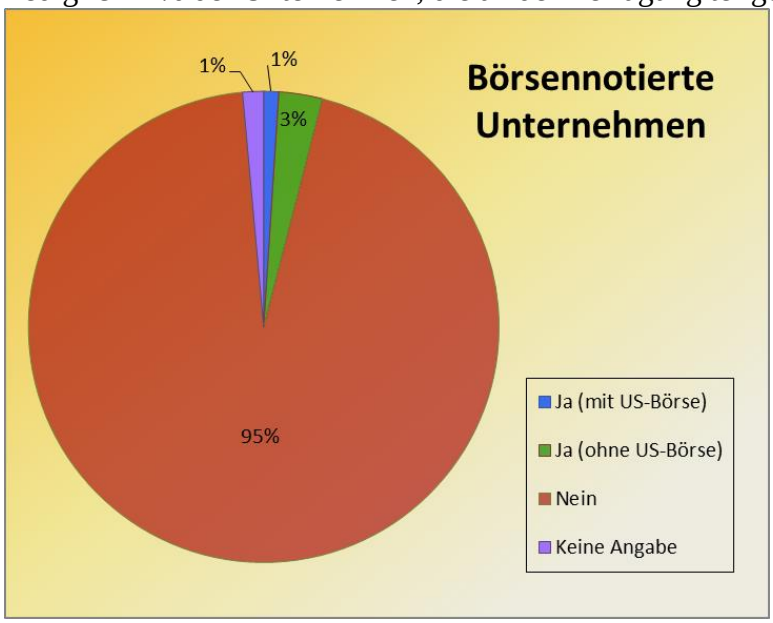
364 befragte Unternehmen waren bereits Opfer von einem oder mehreren **digitalen Angriffen**, hier erlebten insbesondere größere Unternehmen mehrere Angriffe. Einrichtungen, die schon öfters Ziele digitaler Angriffe waren, wurden auch schon mehrmals Opfer von Hacktivismus. Es lässt sich festhalten, dass alle Angriffsformen (aktivistische, Shitstorms, digitale Angriffe) sowohl mit Hacktivismus als auch untereinander korrelieren.

Die Ergebnisse der Hellfeldbeforschung, d. h. der Sekundär- und der Fallanalyse, sowie der Dunkelfeldbeforschung werden in einem abschließenden Projektbericht zusammengeführt werden. Schon jetzt lässt sich feststellen, dass die Ergebnisse darauf hinweisen, dass es sich bei Hacktivismus weder im Hellfeld noch im Dunkelfeld um eine signifikante Bedrohung mit ausgeprägtem Schadenspotenzial handelt.

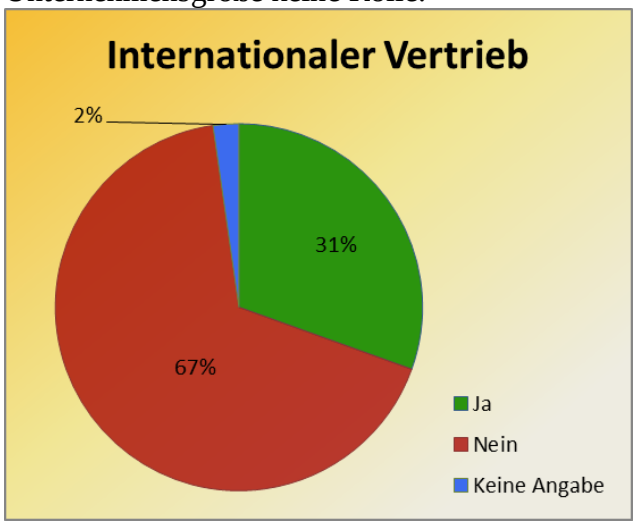
4. Anhang
4.1 Restliche Ergebnisse

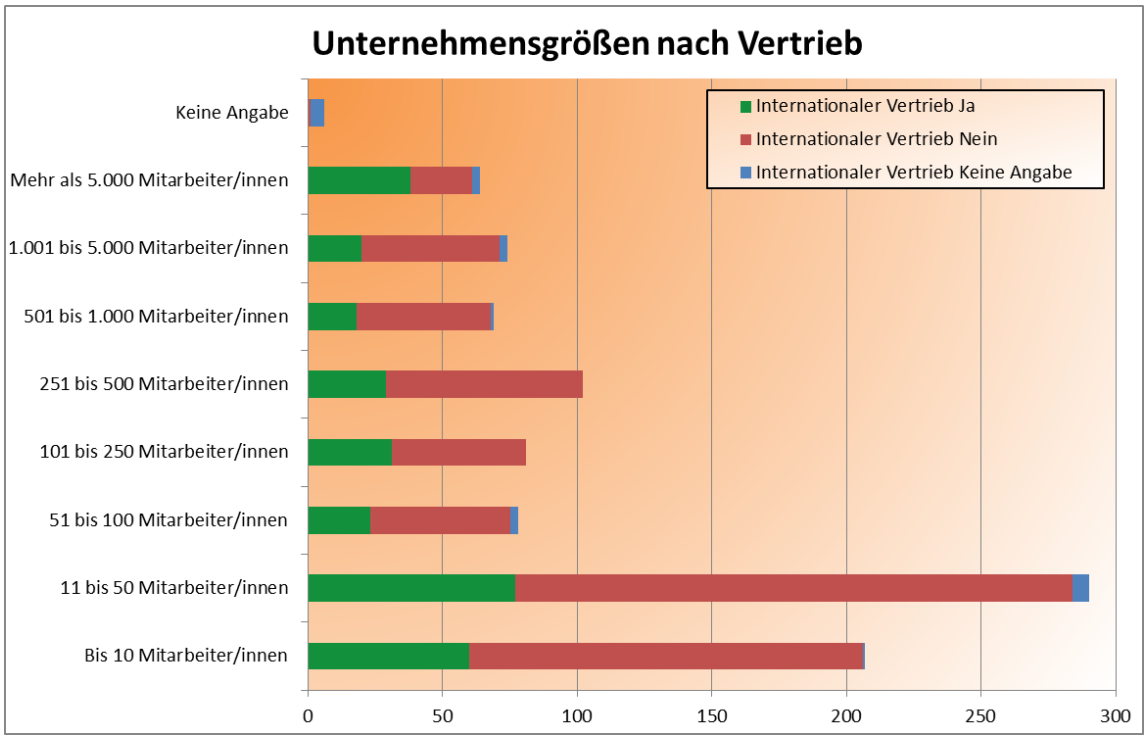
Teil 1: Allgemeine Fragen zum Unternehmen

Frage 3: Ist Ihr Unternehmen börsennotiert?
Lediglich 4 % der Unternehmen, die an der Befragung teilgenommen haben, sind börsennotiert.

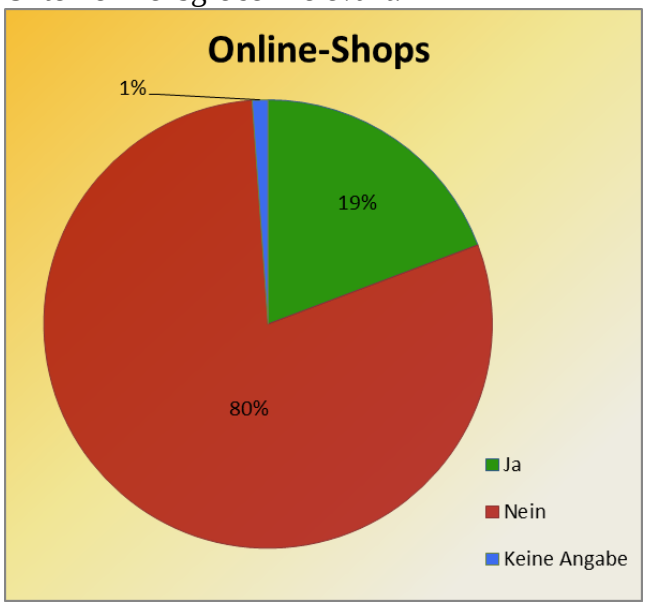


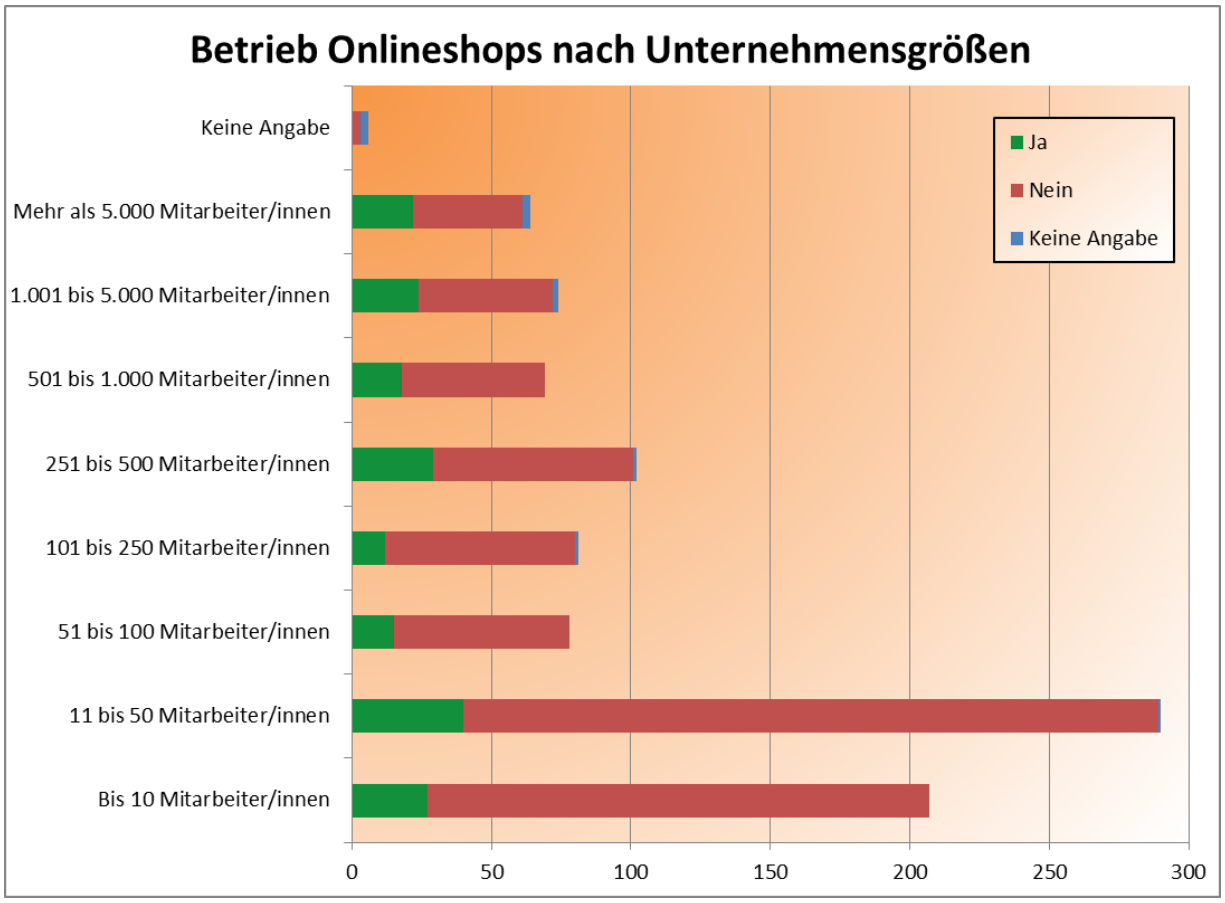
Frage 4: Hat Ihr Unternehmen einen internationalen Vertrieb?
296 der befragten Unternehmen verfügen über einen internationalen Vertrieb. Hierbei spielt die Unternehmensgröße keine Rolle.





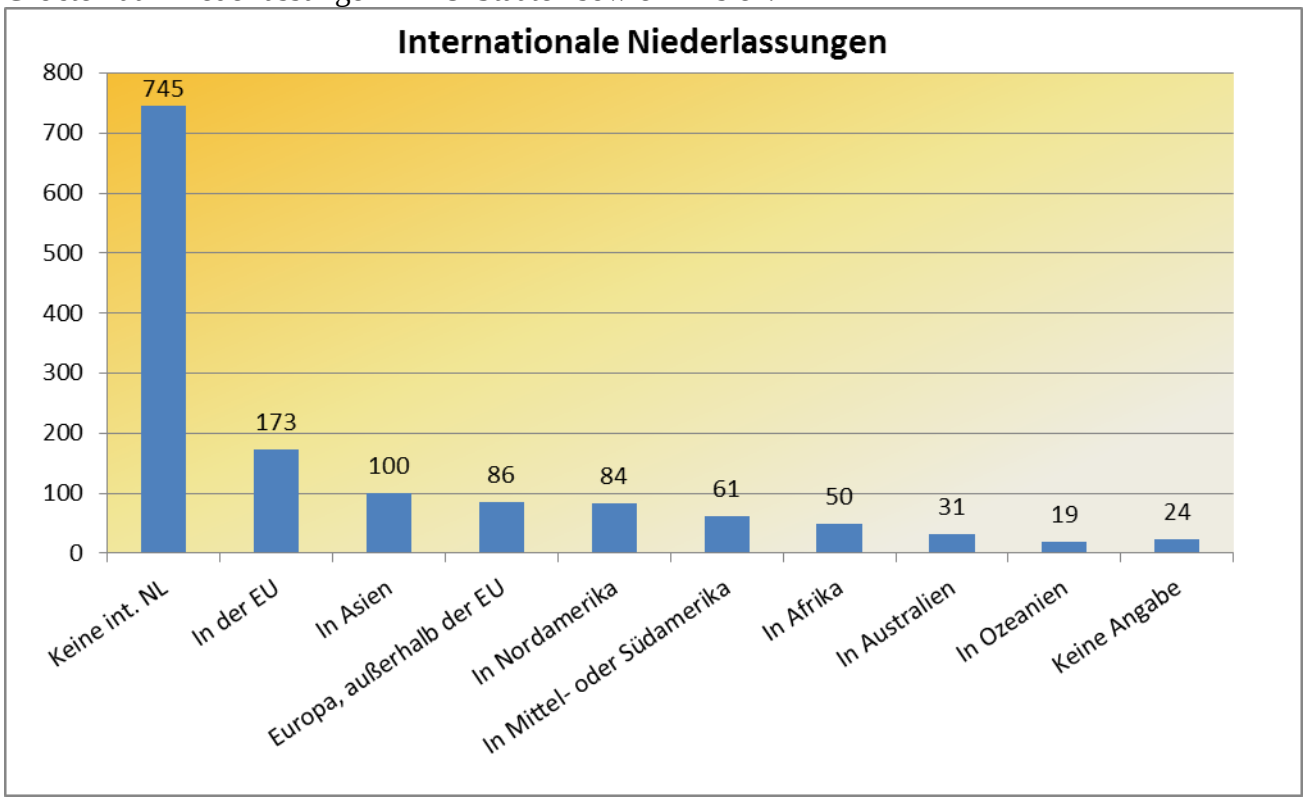
Frage 5: Betreibt Ihr Unternehmen einen oder mehrere Onlineshops?
Zur Frage nach dem Betrieb von Online-Shops gaben 187 Einrichtungen an, einen solchen zu betreiben. 773 nutzen keine Online-Shops. Auch für den Betrieb eines Online-Shops, ist die Unternehmensgröße irrelevant.





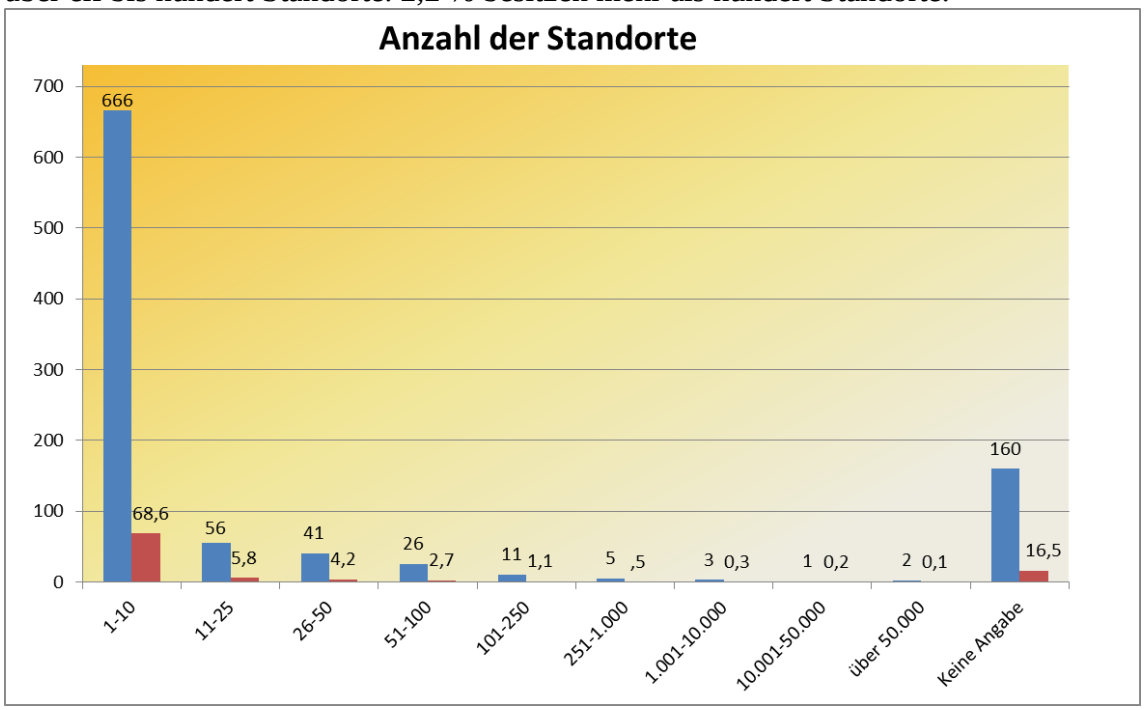
Frage 6: Ist Ihr Unternehmen durch Niederlassungen im Ausland international vertreten? (Mehrfachnennung möglich)

202 Unternehmen gaben an, Niederlassungen (auch mehrere) im Ausland zu führen. Davon entfällt ein Großteil auf Niederlassungen in EU-Staaten sowie in Asien.



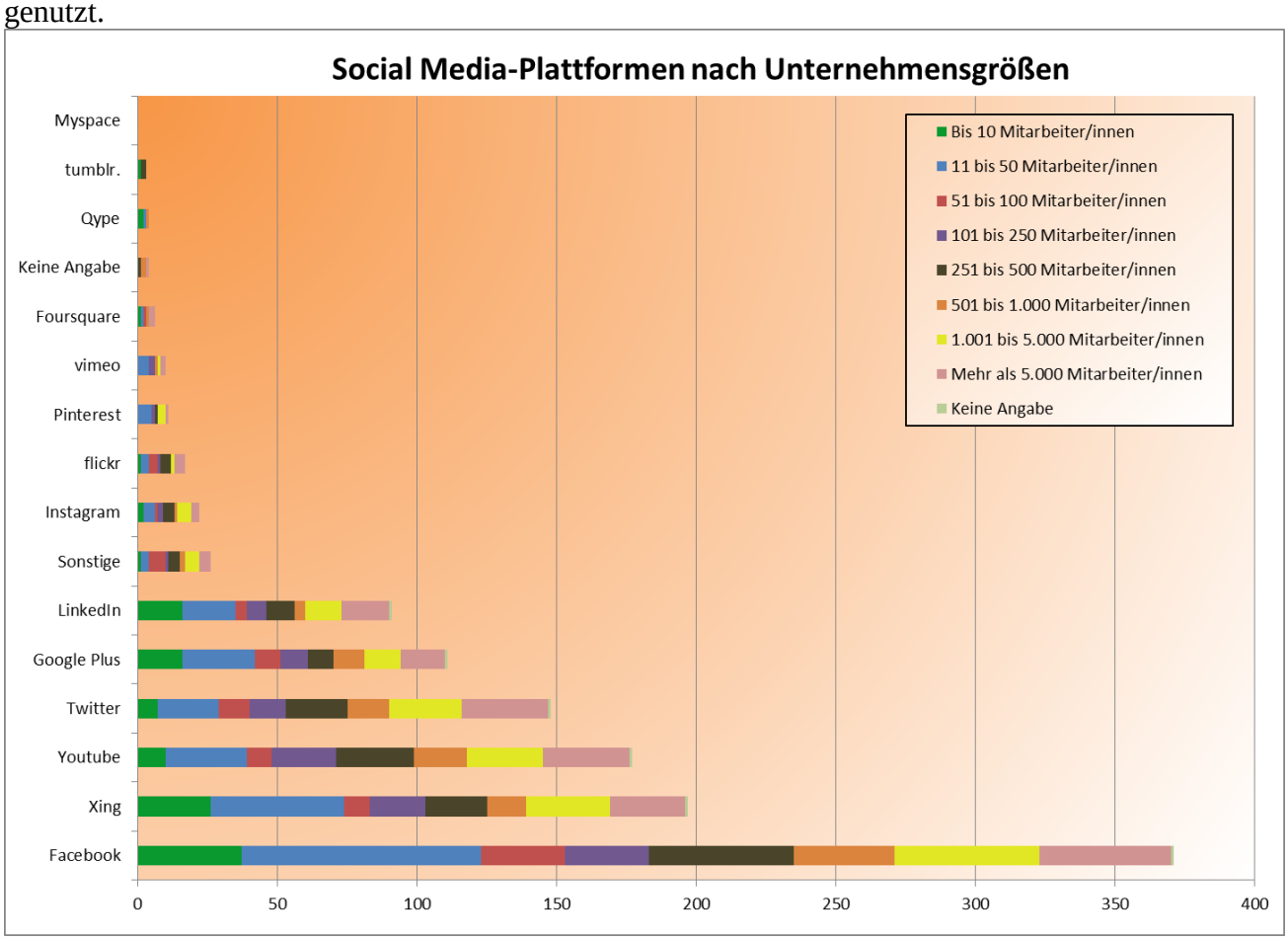
Frage 7: Wie viele Standorte hat Ihr Unternehmen weltweit?

68,6 % der befragten Einrichtungen besitzen zwischen einem und zehn Standorte. 12,7 % verfügen über elf bis hundert Standorte. 2,2 % besitzen mehr als hundert Standorte.



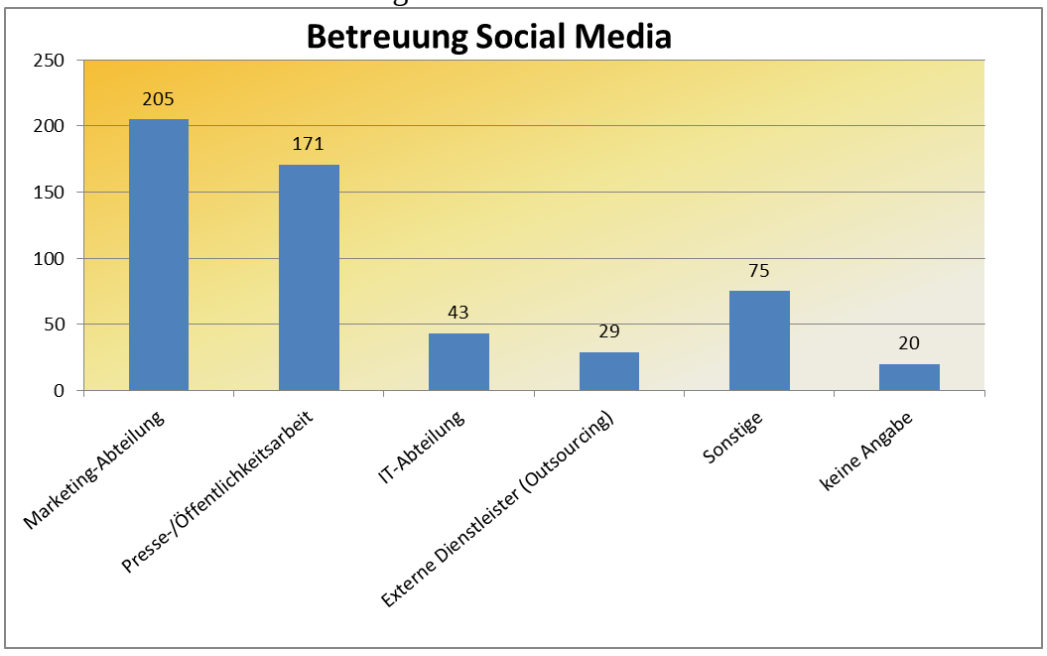
Teil 2: Social Media

Die Social Media-Plattformen werden relativ betrachtet von allen Unternehmensgrößen gleichermaßen genutzt.

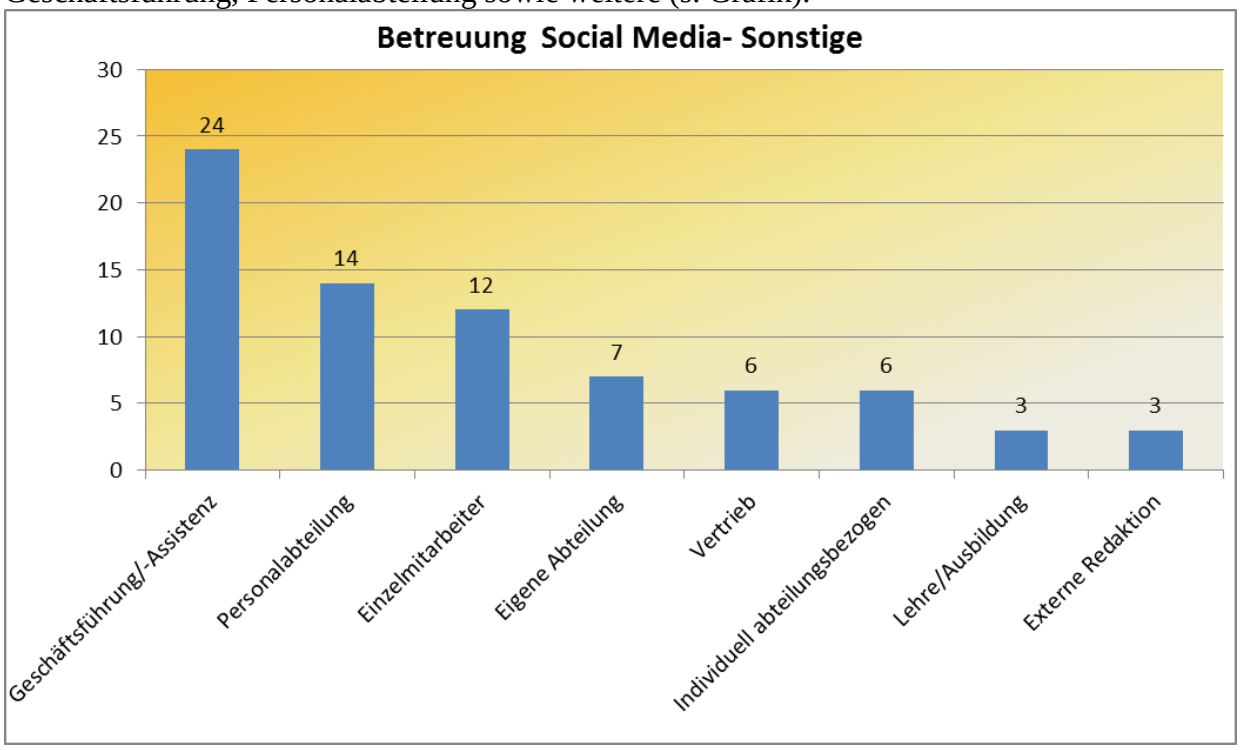


Frage 10: Wer ist in Ihrem Unternehmen für die Social Media-Auftritte zuständig? (Mehrfachnennung möglich)

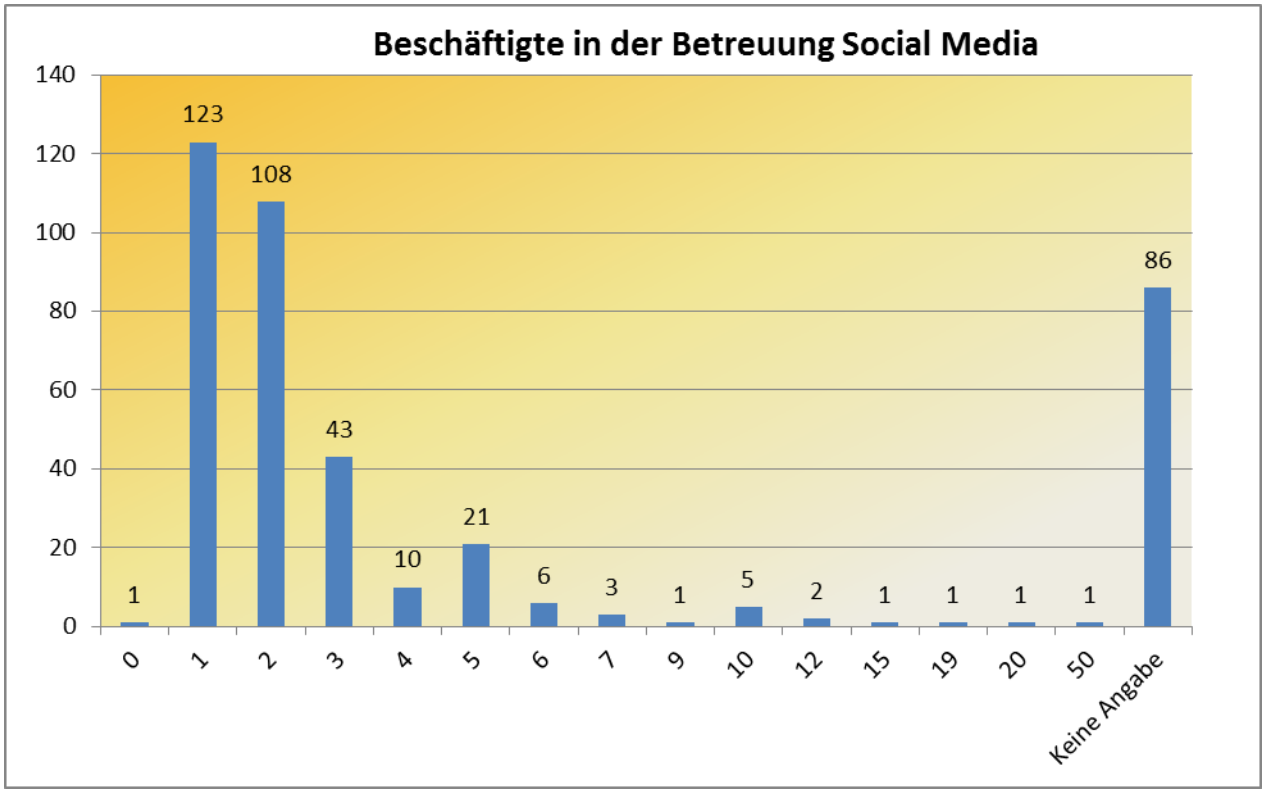
Für die Auftritte in sozialen Medien sind mehrheitlich Marketing-Abteilung und/oder Presse-/Öffentlichkeitsarbeit zuständig.



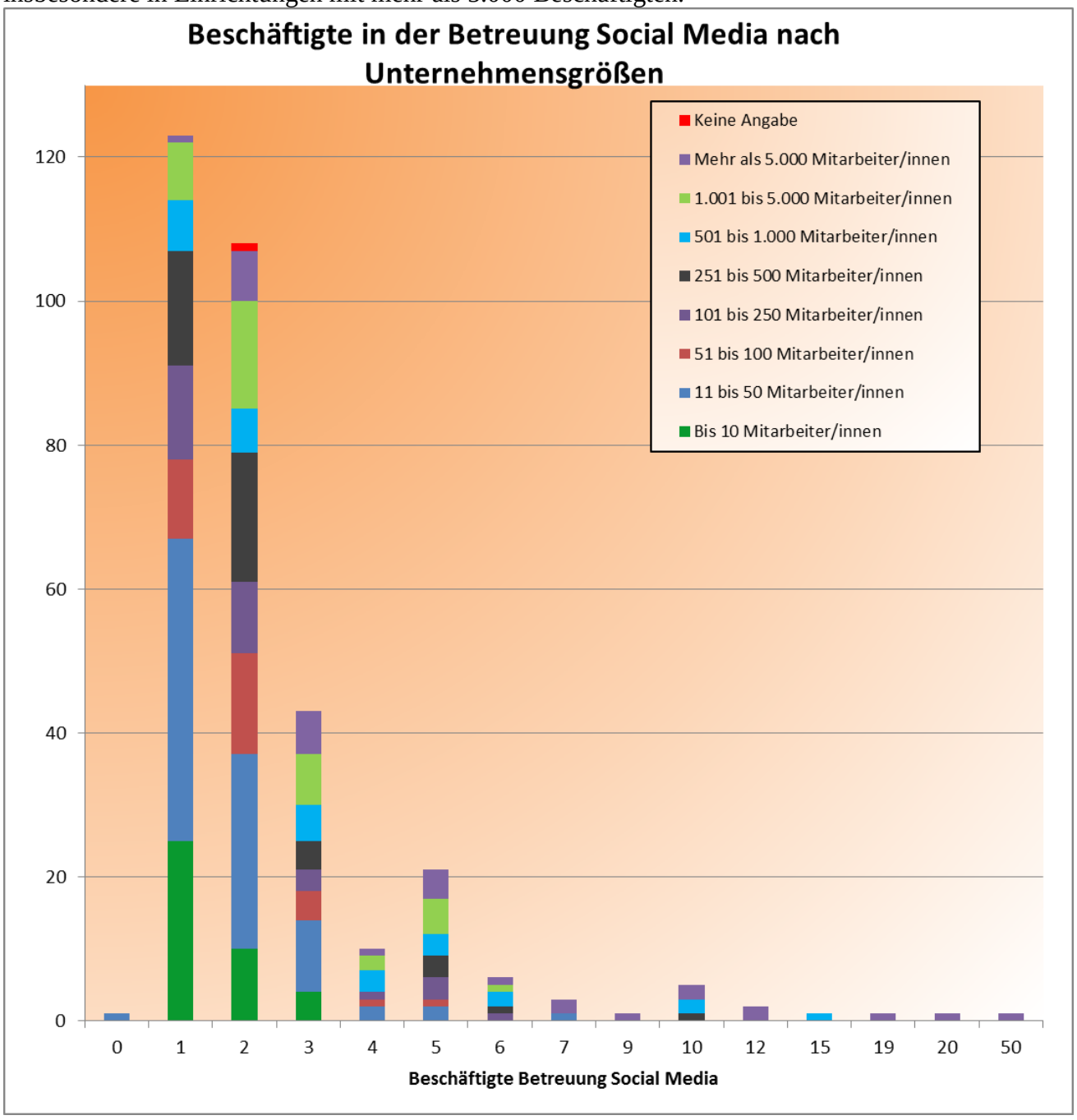
Daneben wurden weitere Zuständige für die Medienbetreuung angegeben, wie z. B. die Geschäftsführung, Personalabteilung sowie weitere (s. Grafik).



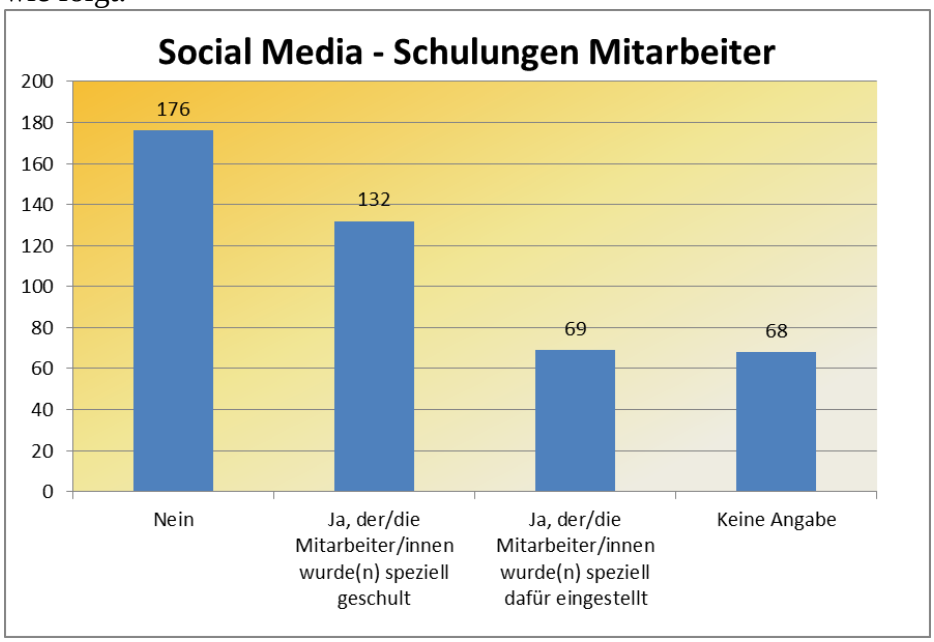
Frage 11: Wie viele Mitarbeiter betreuen und pflegen die Social Media-Auftritte Ihres Unternehmens?
327 befragte Einrichtungen machten Angaben zur Mitarbeiteranzahl in der Betreuung der sozialen Medien. 70 % gaben an, dass ein oder zwei Beschäftigte mit der Pflege und Betreuung der sozialen Medien betraut sind. 27 % haben zwischen drei bis zehn Beschäftigte, die die Social Media Auftritte betreuen.



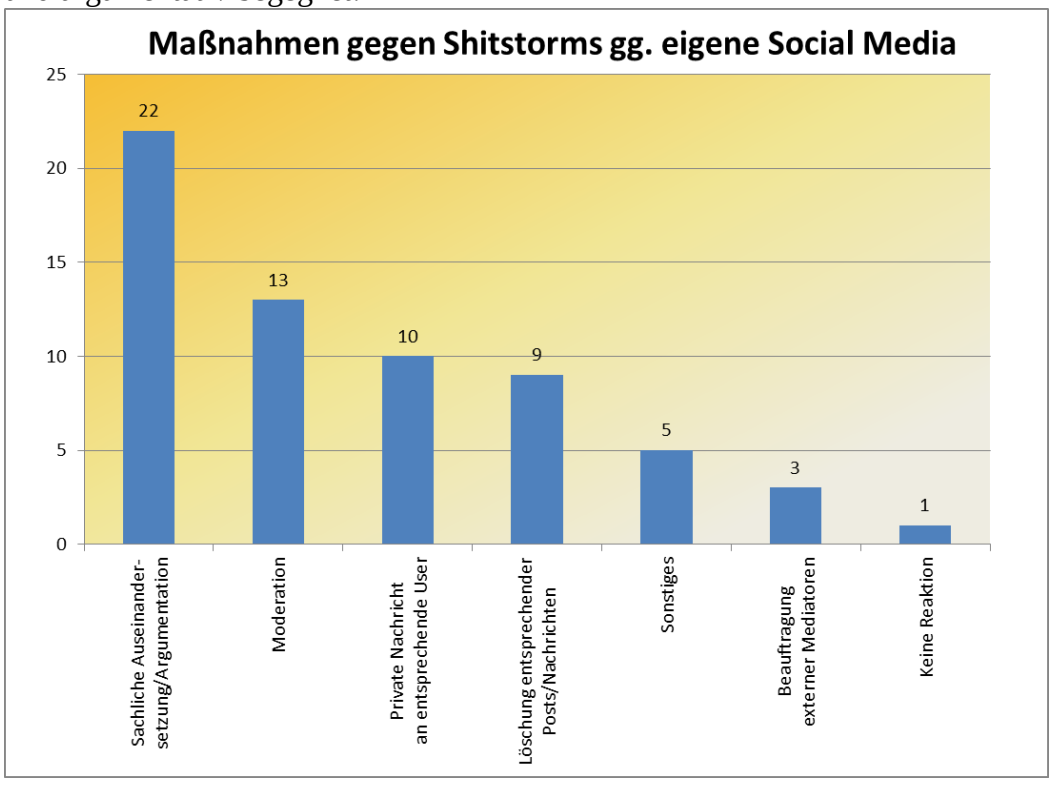
Es lässt sich feststellen, dass je größer das Unternehmen ist, desto mehr Beschäftigte sind in der Pflege und Betreuung der Social Media-Auftritte beschäftigt. Sieben und mehr Beschäftigte finden sich insbesondere in Einrichtungen mit mehr als 5.000 Beschäftigten.



Frage 12: Verfügen diese Mitarbeiter über eine spezielle Schulung oder Ausbildung im Umgang mit bzw. in der Kommunikation über Social Media? (Mehrfachnennung möglich)
Die Frage danach, ob diese Beschäftigten speziell für die Betreuung sozialer Medien geschult wurden und/oder speziell für diese Aufgabe eingestellt wurden, beantworteten die befragten Einrichtungen wie folgt:

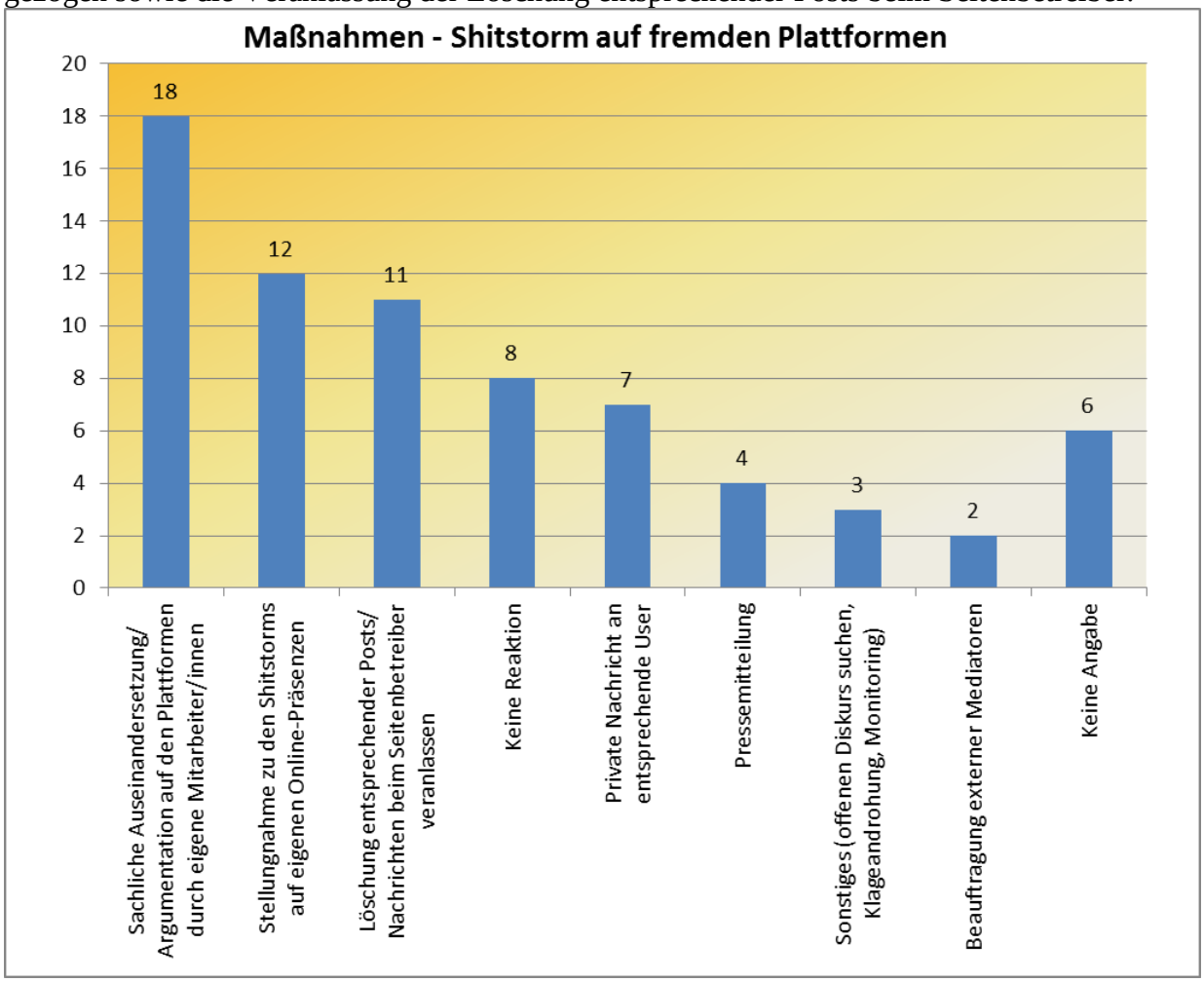


Frage 16: Welche Maßnahmen verfolgt Ihr Unternehmen zum Konfliktmanagement bei ausufernden Kommentaren bzw. sich anbahnenden Shitstorms auf den eigenen Social Media-Plattformen? (Mehrfachnennung möglich)
Auf den eigenen Social Media-Auftritten wurde bzw. wird diesen Shitstorms in erster Linie sachlich und argumentativ begegnet:



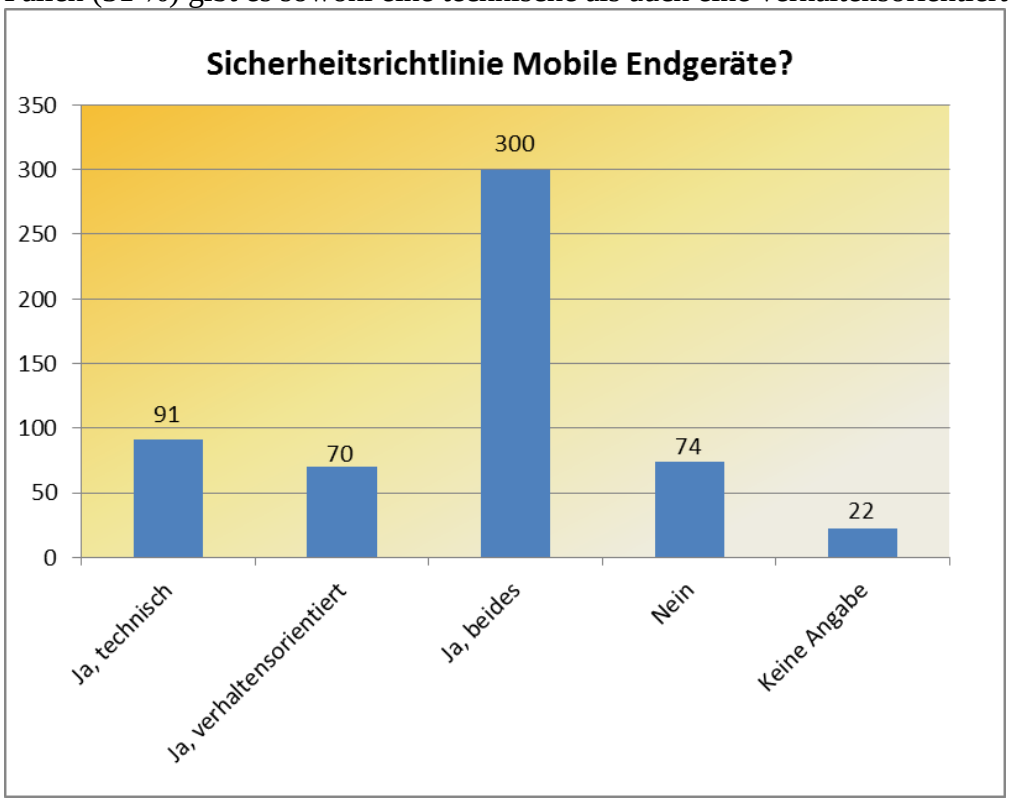
Frage 17: Welche Maßnahmen verfolgt Ihr Unternehmen zum Konfliktmanagement bei ausufernden Kommentaren, sich anbahnenden Shitstorms außerhalb der eigenen Online-Präsenzen? (Mehrfachnennung möglich)

Auch auf Shitstorms auf einrichtungsfremden sozialen Medien wird durch Argumentation und sachliche Auseinandersetzung durch die eigenen Beschäftigten reagiert. Aber auch die Stellungnahme zu diesen Shitstorms auf der eigenen Online-Präsenz wird von den befragten Einrichtungen in Betracht gezogen sowie die Veranlassung der Löschung entsprechender Posts beim Seitenbetreiber.

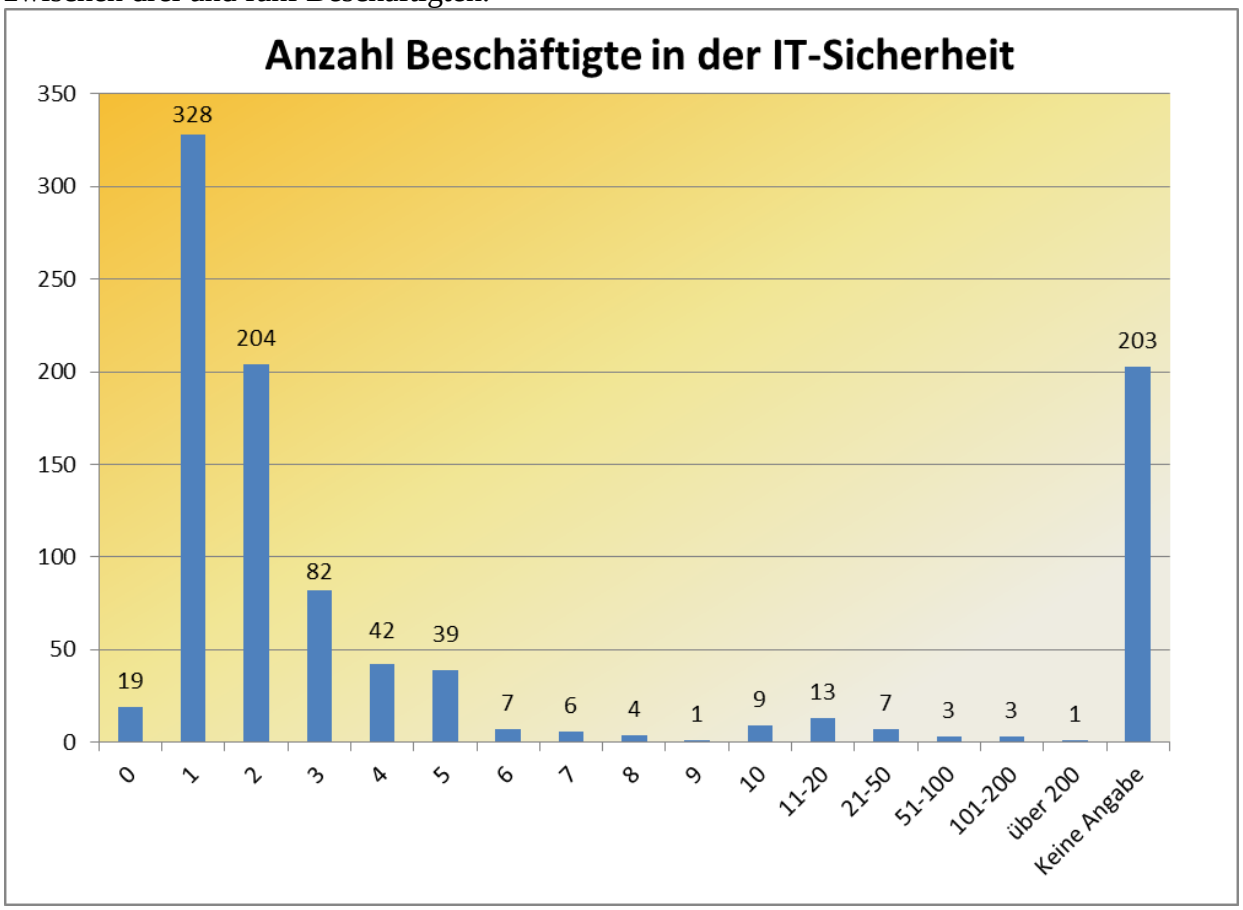


Teil 3: IT- und Informationssicherheit

Frage 20: Besteht für den Umgang mit mobilen Endgeräten eine Sicherheitsrichtlinie?
Für den Fall, dass Beschäftigte per mobilem Endgerät von außerhalb auf das Unternehmensnetzwerk zugreifen können, besteht in 91 Fällen eine technische Sicherheitsrichtlinie für den Umgang mit mobilen Endgeräten, in 70 Fällen existiert eine verhaltensorientierte Sicherheitsrichtlinie und in 300 Fällen (31 %) gibt es sowohl eine technische als auch eine verhaltensorientierte Sicherheitsrichtlinie.

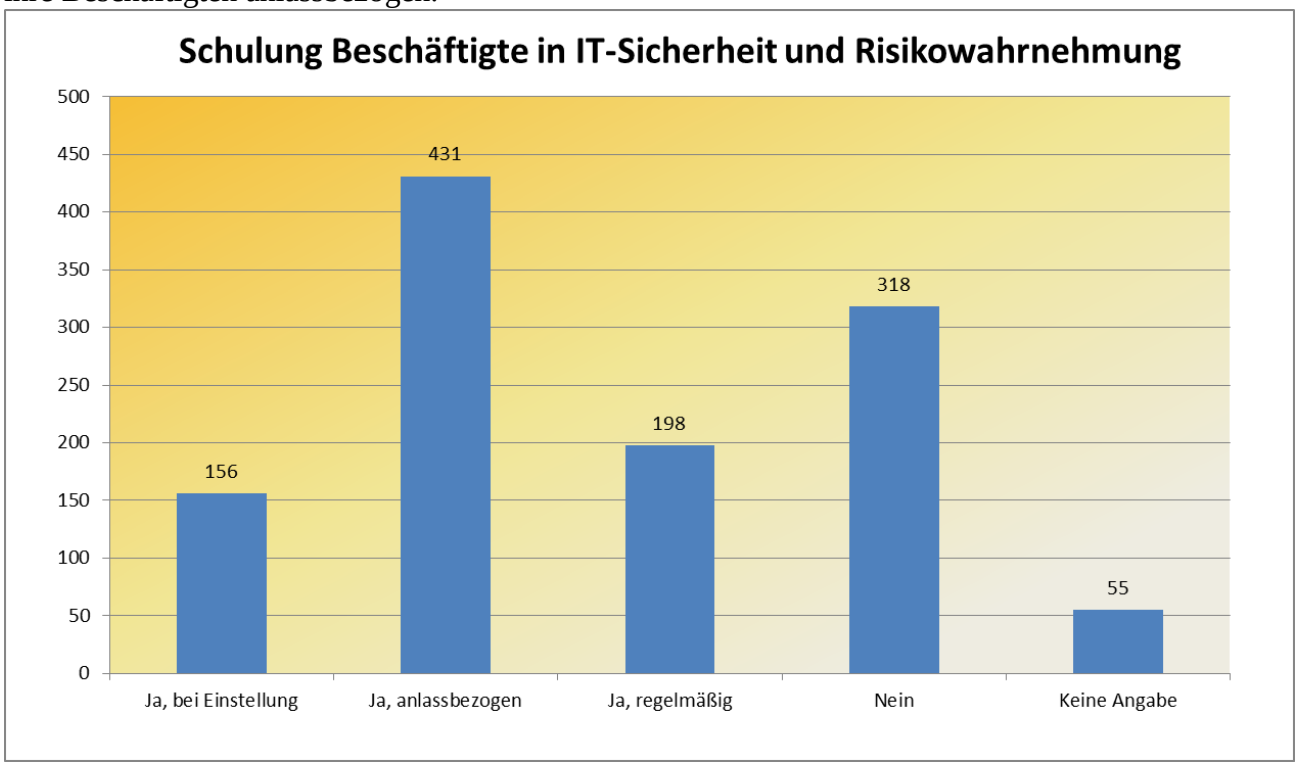


Frage 21: Wie viele Mitarbeiter sind in Ihrem Unternehmen mit Aufgaben der IT-Sicherheit befasst?
Zu der Frage nach der Anzahl der in der IT-Sicherheit Beschäftigten gaben 34 % der befragten Einrichtungen einen Beschäftigten an, 21 % haben in diesem Bereich zwei Beschäftigte und 17 % zwischen drei und fünf Beschäftigten.



Frage 22: Werden Ihre Mitarbeiter hinsichtlich IT-Sicherheit und Risikowahrnehmung (Bedrohung durch Cybercrime) geschult? (Mehrfachnennung möglich)

318 der befragten Einrichtungen gaben an, dass die Beschäftigten nicht hinsichtlich IT-Sicherheit und Risikowahrnehmung (d. h. Bedrohung durch Cybercrime) geschult werden. Die Mehrheit (431) schult ihre Beschäftigten anlassbezogen.



4.2 Fragebogen

Unternehmensbefragung

Herzlich Willkommen zur Online-Befragung der Forschungs- und Beratungsstelle Cybercrime KI 16 beim BKA zum Thema Hacktivismus gegen Unternehmen!

Mit dieser Online-Befragung möchten wir im Rahmen eines Forschungsprojekts zu Hacktivismus ermitteln, wie Unternehmen das Internet und Social Media nutzen und welche Erfahrungen Sie dabei gesammelt haben. Ihre Antworten helfen uns dabei, die Gefährdungslage durch Hacktivismus für Unternehmen im Internet richtig einzuschätzen.

Die Befragung gliedert sich in insgesamt fünf Abschnitte. Zur Beantwortung der Fragen benötigen Sie etwa 15 Minuten.

Wir bitten Sie, die Fragen vollständig zu beantworten, da wir nur so aussagekräftige Ergebnisse erhalten. Ihre Angaben werden zwischengespeichert, so dass eine Unterbrechung der Umfrage jederzeit möglich ist. Falls ein anderer Ansprechpartner einzelne Fragen besser beantworten kann, können Sie ihm dem Umfrage-Link weiterleiten und nach dessen Bearbeitung mit der Beantwortung fortfahren.

Ihre Daten werden selbstverständlich diskret behandelt und nicht an Dritte weitergegeben. Sowohl die Erhebung als auch die Auswertung werden vollkommen anonym durchgeführt.

Wir danken Ihnen vorab herzlich für Ihre Unterstützung.
Für Rückfragen stehen Ihnen gerne Frau Füllgraf (0611-55-11811) und Herr Koch (0611-55-14821) zur Verfügung. Bei Interesse an den Ergebnissen der Befragung und/oder des Forschungsprojekts schicken Sie bitte eine E-Mail mit dem Betreff „Hacktivismus – Unternehmensbefragung" an das neutrale Postfach der Forschungs- und Beratungsstelle KI 16: ki16@bka.bund.de.

Mit freundlichen Grüßen

Teil 1: Allgemeine Fragen zum Unternehmen

1. Wie viele Mitarbeiter (einschließlich Teilzeitkräften) sind derzeit in Ihrem Unternehmen beschäftigt?
- o < 10
- o 11 – 50
- o 51- 100
- o 101 – 250
- o 251 - 500
- o 501 – 1.000
- o 1.001 – 5.000
- o > 5.000
- o keine Angabe

2. In welcher Branche ist Ihr Unternehmen hauptsächlich tätig?

- o Land- und Forstwirtschaft
- o Fischerei und Fischzucht
- o Bergbau und Gewinnung von Steinen und Erden
- o Verarbeitendes Gewerbe
- o Energie- und Wasserversorgung
- o Baugewerbe
- o Handel; Instandhaltung und Reparatur von Kraftfahrzeugen und Gebrauchsgütern
- o Verkehr und Lagerei
- o Gastgewerbe
- o Information und Kommunikation
- o Verkehr und Nachrichtenübermittlung
- o Kredit- und Versicherungsgewerbe
- o Grundstücks- und Wohnungswesen, Vermietung beweglicher Sachen
- o Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen
- o Erbringung von sonstigen wirtschaftlichen Dienstleistungen
- o Öffentliche Verwaltung, Verteidigung, Sozialversicherung
- o Erziehung und Unterricht
- o Gesundheits-, Veterinär- und Sozialwesen
- o Kunst, Unterhaltung und Erholung
- o Erbringung von sonstigen öffentlichen und persönlichen Dienstleistungen
- o Private Haushalte mit Hauspersonal
- o Exterritoriale Organisationen und Körperschaften
- o keine Angabe

3. Ist Ihr Unternehmen börsennotiert?
- o Ja (mit US-Börse)
- o Ja (ohne US-Börse)
- o Nein
- o keine Angabe

4. Hat Ihr Unternehmen einen internationalen Vertrieb?
- o Ja
- o Nein
- o keine Angabe

5. Betreibt Ihr Unternehmen einen oder mehrere Onlineshops?
- o Ja
- o Nein
- o keine Angabe

6. Ist Ihr Unternehmen durch Niederlassungen im Ausland international vertreten? (Mehrfachnennung möglich)
- o In der EU
- o In europäischen Ländern außerhalb der EU (z.B. Norwegen, Schweiz)
- o In Asien
- o In Afrika
- o In Nordamerika
- o In Mittel- oder Südamerika

- o In Australien
- o In Ozeanien
- o Nein, unser Unternehmen hat keine Niederlassungen im Ausland *(exklusiv)*
- o keine Angabe *(exklusiv)*

7. Wie viele Standorte hat Ihr Unternehmen weltweit? Bitte geben Sie die Anzahl an Standorten an
- o _____
- o keine Angabe

[Progr. Nur ganze Zahlen zulassen; Plausibilitätscheck<0]

Im folgenden Hauptteil der Untersuchung geht es darum, wie Ihr Unternehmen das Internet nutzt, und welche Erfahrungen Sie dabei gemacht haben.

Teil 2 Social Media

8. Soziale Netzwerke bzw. Social Media sind Plattformen im Internet, auf denen sich Personen ein eigenes Nutzerprofil anlegen und mit anderen Nutzern austauschen können wie zum Beispiel Facebook, LinkedIn oder Instagram. Nutzt Ihr Unternehmen Social Media Plattformen zum Beispiel für die eigene Öffentlichkeitsarbeit oder das Marketing?

- o Ja
- o Nein
- o keine Angabe

Filter: Falls Q8=1 (Social Media-Nutzung)

9. Welche Social Media-Plattformen nutzt Ihr Unternehmen?
(Mehrfachnennung möglich)
- o Facebook
- o Google Plus
- o LinkedIn
- o Xing
- o vimeo
- o flickr
- o Foursquare
- o Myspace
- o Instagram
- o Pinterest
- o Qype
- o tumblr.
- o Twitter
- o Youtube
- o Sonstige (bitte nennen): _____
- o Sonstige (bitte nennen): _____
- o Sonstige (bitte nennen): _____
- o keine Angabe *(exklusiv)*

Filter: Falls Q8=1 (Social Media-Nutzung)

10. Wer ist in Ihrem Unternehmen für die Social Media-Auftritte zuständig?
(Mehrfachnennung möglich)
- o Die Marketing-Abteilung
- o Die Presse-/Öffentlichkeitsarbeits-Abteilung
- o Die IT-Abteilung
- o Externe Dienstleister (Outsourcing)
- o Sonstige (bitte nennen): _____
- o keine Angabe *(exklusiv)*

Filter: Falls Q8=1 (Social Media-Nutzung)

11. Wie viele Mitarbeiter betreuen und pflegen die Social Media-Auftritte Ihres Unternehmens?
- o _____
- o keine Angabe

[Progr. Nur ganze Zahlen zulassen; Plausibilitätscheck<0]

Filter: Falls Q8=1 (Social Media-Nutzung)

12. Verfügen diese Mitarbeiter über eine spezielle Schulung oder Ausbildung im Umgang mit bzw. in der Kommunikation über Social Media?
(Mehrfachnennung möglich)
- o Ja, der/die Mitarbeiter wurde(n) speziell dafür eingestellt
- o Ja, der/die Mitarbeiter wurde(n) speziell geschult
- o Nein
- o keine Angabe

Filter: Falls Q8=1 (Social Media-Nutzung)

13. Zu welchen Zwecken nutzt Ihr Unternehmen Social Media?
(Mehrfachnennung möglich)
- o Kommunikation aktueller Entwicklungen und Ereignisse
- o Werbung
- o Kundenbetreuung
- o technischer Support
- o Gewinnspiele
- o Kundenfeedback
- o Sonstiges (bitte nennen):_____
- o keine Angabe *(exklusiv)*

Kein Filter (Alle Befragten)

Die folgenden Fragen beziehen sich auf sog. Shitstorms, ein Begriff, der sich am ehesten mit „Sturm der Entrüstung übersetzen lässt". Unter einem Shitstorm wird ein Internetphänomen verstanden, bei dem in kurzer Zeit sehr viele beleidigende oder empörte Beiträge auf Internetplattformen wie Sozialen Netzwerken, Internetforen oder Blogs gegen Unternehmen, Personen des öffentlichen Lebens, Verbände oder Einzelpersonen geäußert werden.

14. War Ihr Unternehmen schon einmal von beleidigenden Kommentaren im Internet, d.h. von Shitstorms betroffen?
- o Ja, aber nur einmal
- o Ja, mehrmals
- o Nein, noch nie
- o Weiß nicht/keine Angabe

Filter: Falls Q14=1 oder 2 (Betroffenheit vom Shitstorm)

15. Auf welchen Internetplattformen war Ihr Unternehmen schon einmal von Shitstorms betroffen?
- o Auf unserem eigenen Social Media-Auftritt
- o In Social Media außerhalb unseres eigenen Auftritts
- o In Internetforen
- o In Blogs
- o Auf Twitter
- o Sonstiges (bitte nennen): _____
- o keine Angabe

Filter: Falls Q15=1 (Betroffenheit vom Shitstorm auf der eigenen Social Media-Präsenz)

16. Welche Maßnahmen verfolgt Ihr Unternehmen zum Konfliktmanagement bei ausufernden Kommentaren bzw. sich anbahnenden Shitstorms auf den eigenen Social Media-Plattformen?
(Mehrfachnennung möglich)
- o Moderation
- o sachliche Auseinandersetzung/Argumentation
- o private Nachricht an entsprechende User
- o Löschung entsprechender Posts/Nachrichten
- o Beauftragung externer Mediatoren
- o keine Reaktion
- o Sonstiges (bitte nennen):_____
- o keine Angabe *(exklusiv)*

Filter: Falls Q15=2,3,4,5 oder 6 (Betroffenheit vom Shitstorm außerhalb der eigenen Social Media-Präsenz)

17. Welche Maßnahmen verfolgt Ihr Unternehmen zum Konfliktmanagement bei ausufernden Kommentaren, sich anbahnenden Shitstorms außerhalb der eigenen Online-Präsenzen?
(Mehrfachnennung möglich)
- o Stellungnahme zu den Shitstorms auf eigenen Online-Präsenzen
- o Pressemitteilung
- o sachliche Auseinandersetzung/Argumentation auf den entsprechenden Seiten bzw. in den entsprechenden Foren durch eigene Mitarbeiter
- o Beauftragung externer Mediatoren
- o private Nachricht an entsprechende User
- o Löschung entsprechender Posts/Nachrichten beim Seitenbetreiber veranlassen
- o keine Reaktion
- o Sonstiges (bitte nennen):_____
- o keine Angabe *(exklusiv)*

Kein Filter (alle Befragten)

Teil 3 IT- und Informationssicherheit

18. Ist oder war Ihr Unternehmen schon einmal von digitalen Angriffen über das Internet auf IT-Systeme betroffen?
- o Ja, aber nur einmal
- o Ja, mehrmals
- o Nein, noch nie
- o keine Angabe

19. Greifen Mitarbeiter von außerhalb auf das Unternehmensnetzwerk zu?
(Mehrfachnennung möglich)
- o Ja (per mobile Endgeräte)
- o Ja (via Home Office)
- o Nein *(exklusiv)*
- o keine Angabe *(exklusiv)*

Filter: Falls Q19=1

20. Besteht für den Umgang mit mobilen Endgeräten eine Sicherheitsrichtlinie?
- o Ja, technisch
- o Ja, verhaltensorientiert
- o Ja, beides
- o Nein
- o keine Angabe

Kein Filter (alle Befragten)

21. Wie viele Mitarbeiter sind in Ihrem Unternehmen mit Aufgaben der IT-Sicherheit befasst?
- o _____
- o keine Angabe

[Progr. Nur ganze Zahlen zulassen; Plausibilitätscheck<>0]

22. Werden Ihre Mitarbeiter hinsichtlich IT-Sicherheit und Risikowahrnehmung (Bedrohung durch Cybercrime) geschult?
(Mehrfachnennung möglich)
- o Ja, bei Einstellung
- o Ja, anlassbezogen
- o Ja, regelmäßig
- o Nein *(exklusiv)*
- o keine Angabe *(exklusiv)*

23. Welche Maßnahmen ergreift Ihr Unternehmen zur Gewährleistung der Sicherheit Ihrer IT-Infrastruktur?

technische Maßnahmen:
- o Firewall
- o Spam-Filter
- o Schutzsoftware (Antivirenprogramme)
- o regelmäßige Software-Updates
- o Monitoring von Log-Dateien auf Unternehmens-IT
- o Verschlüsselungstechniken
- o Erstellung von Sicherungskopien
- o erweiterte IT-Zugangsbeschränkungen durch Benutzeridentifikation (z. B. Biometrie)
- o Passwortschutz auf allen Geräten
- o Beschränkung des Zugriffs auf Unternehmensdaten vom Home-Office
- o Intrusion Detection Systeme (Einsatz von Sensoren in der Unternehmens-IT zur Früherkennung von digitalen Einbrüchen)
- o Unser Unternehmen ergreift keine technischen Sicherheitsmaßnahmen. *(exklusiv)*
- o keine Angabe *(exklusiv)*

nicht-technische Maßnahmen:
- o Richtlinien zum Umgang mit IT (z. B. Verbot privater Massenspeicher an Unternehmens-IT; Absicherung gegen Datenweitergabe von innen, Regelungen für den Umgang mit sensiblen Daten etc.)
- o Passwort Richtlinien
- o Mitarbeiter Schulungen
- o regelmäßige Sicherheitsaudits durch Externe
- o Unser Unternehmen ergreift keine nicht-technischen Sicherheitsmaßnahmen. *(exklusiv)*
- o keine Angabe *(exklusiv)*

24. Wie hoch war der Anteil für IT-Sicherheitsmaßnahmen am Gesamtbudget des Unternehmens im Jahr 2014?
- o _____ in Prozent
- o keine Angabe

Teil 4 Aktivismus

25. Wie hoch schätzen Sie die Gefährdung Ihres Unternehmens ein, Ziel von politisch oder ideologisch motivierten Aktivitäten, wie z. B. Demonstrationen, Informationskampagnen und mutwillige Sachbeschädigunge zur Erreichung ideologischer Ziele, zu werden?
- o sehr gering
- o gering
- o hoch
- o sehr hoch
- o keine Angabe

26. Ist Ihr Unternehmen bereits Ziel von politisch oder ideologisch motivierten Aktivitäten geworden?
(Mehrfachnennung möglich)
- o Ja, einer Demonstration:
- o Ja, einer Informationskampagne (Flugblätter, Flyer, Informationsstände)
- o Ja, einer Bedrohung
- o Ja, einer Sachbeschädigung (Graffiti etc.)
- o Ja, einer sonstigen Aktivität (bitte nennen):_____
- o Nein *(exklusiv)*
- o keine Angabe *(exklusiv)*

Teil 5 Hacktivismus

Die folgenden Fragen drehen sich um Hacktivismus. Der Begriff „Hacktivismus" stellt eine Wortkreuzung aus den beiden Wörtern „Aktivismus" und „Hacker" dar. Hierbei handelt es sich um eine ideologische Protestform, die mittels Online-Tools durchgeführt wird. Es existieren diverse Angriffsformen von Hacktivismus. Hintergrund solcher Taten ist oft ein ideologischer Ausdruck von Protest und Propaganda und keine Profitorientierung.

27. Wie hoch schätzen Sie die Gefährdung Ihres Unternehmens ein, Ziel von hacktivistischen Aktivitäten zu werden?
- o sehr gering
- o gering
- o hoch
- o sehr hoch
- o keine Angabe

28. Ist oder war Ihr Unternehmen bereits Opfer hacktivistischer Angriffe?
- o Ja, aber nur einmal
- o Ja, mehrmals
- o Nein, noch nie
- o keine Angabe

Filter: Falls Q28=1 oder 2 (Opfer hacktivistischer Angriffe)

29. Von welchen Arten hacktivistischer Angriffe ist oder war Ihr Unternehmen bereits Opfer? Bitte geben Sie jeweils auch die Anzahl der Vorfälle an.

Art des hacktivistischen Angriffs	Anzahl der Vorfälle	Keine Angabe
Webdefacement: Ein Webdefacement ist eine unberechtigte Manipulation des sichtbaren Bereichs einer Webseite. Meist werden politische oder ideologische Nachrichtenbanner positioniert bzw. ganze Webseiten ersetzt.	_____	
DDoS-Angriff: DDoS-Angriffe sind ebenfalls oft ideologisch motivierte Angriffe. Hierbei werden absichtlich Server überlastet durch eine nicht zu bewältigende Menge an Anfragen von einer Vielzahl an Geräten. Dies führt von einer extremen Verlangsamung bis hin zum Absturz des Servers.	_____	
Schwarzes Fax: Der Angreifer sendet fortlaufend	_____	

schwarze Seiten an das Faxgerät des Opfers, um somit zum einen das Faxgerät des Opfers zu blockieren und zum anderen materielle Schäden durch den Verbrauch von Papier und Toner zu verursachen.		
E-Mail Spam	_____	
Leaking von internen Daten: Das inoffizielle bzw. unerlaubte Veröffentlichen von internen, geheimen Informationen des Opfers durch Dritte oder interne Täter. Die Informationen wurden im Vorfeld meist durch digitale Angriffe ausgespäht und/oder gestohlen.	_____	
Shitstorm: Sog. „Sturm der Entrüstung" als Internetphänomen, bei dem in kurzer Zeit sehr viele beleidigende oder empörte Beiträge auf Internetplattformen veröffentlicht werden.	_____	
Bedrohung	_____	
sonstige:	**Freitext**	

Filter: Falls Q28=1 oder 2 (Opfer hacktivistischer Angriffe)

30. Welche Folge(n) hatte(n) der/die hacktivistischer/n Angriff(e)?

(Mehrfachnennung möglich)

- o Sachschaden (z.B. unmittelbare Schäden an Hardware, Verbrauchsmaterialien etc.)
- o Systemabsturz
- o Serverausfall
- o Infektion des Systems mit Schadsoftware
- o Datenverlust (durch Beschädigung, Manipulation, Löschen)
- o unerwünschte Presseberichterstattung
- o Reputationsverlust
- o Umsatzeinbußen
- o Beeinflussung Aktienkurse
- o Erpressung mit gestohlenen Daten
- o Sonstige Folgen (bitte nennen):_____
- o keine Folgen *(exklusiv)*
- o keine Angabe *(exklusiv)*

Filter: Falls Q28=1 oder 2 (Opfer hacktivistischer Angriffe)

31. Sind Ihrem Unternehmen durch hacktivistische Angriffe finanzielle Schäden entstanden? Unter finanziellen Schäden sind auch Ausfälle, Mehraufwand für Informationstechnik, Wiederherstellungskosten und zusätzliche Arbeitsbelastung zu verstehen.

- o Ja
- o Nein
- o keine Angabe

Filter: Falls Q31=1 (Finanzieller Schaden durch Angriffe)

32. Welche finanziellen Schäden sind Ihrem Unternehmen durch hacktivistische Angriffe entstanden?

(Mehrfachnennung möglich)

- o Behebung der Störung/Wiederherstellung des Systems
- o Ausfall der Produktion
- o zusätzlicher Arbeitsaufwand
- o zusätzliche Investitionen in Informationstechnik
- o Verlust von Profiten
- o (Zer-)störung von Informationstechnik
- o Beeinflussung Aktienkurse
- o Kosten für Rechtsstreitigkeiten
- o Sonstiges (bitte nennen): _____
- o keine Angabe *(exklusiv)*

Filter: Falls Q28=1 oder 2 (Opfer hacktivistischer Angriffe)

33. Welche Maßnahmen wurden als Reaktion auf die Angriffe getroffen?

(Mehrfachnennung möglich)

- o Anzeige erstattet
- o Schäden intern behoben
- o Schäden von externen Auftragnehmern behoben
- o Investition in Sicherheitsmaßnahmen
- o Disziplinarische Maßnahmen gegen Mitarbeiter
- o Schulungen zur IT-Sicherheit
- o Sonstige Maßnahmen (bitte nennen): _____
- o Keine Maßnahmen *(exklusiv)*
- o keine Angabe *(exklusiv)*

Filter: Falls Q33<>1 (keine Anzeige erstattet)

34. Aus welchen Gründen haben Sie nach dem hacktivistischen Angriff auf Ihr Unternehmen keine Anzeige erstattet?

(Mehrfachnennung möglich)

- o Zweifel am Erfolg
- o Schutz von Betriebsgeheimnissen
- o zu großer Aufwand
- o schlechte Erfahrungen mit Ermittlungsbehörden
- o kein Vertrauen gegenüber Ermittlungsbehörden
- o laufender Betrieb zu sehr belastet
- o Reputations- und Imageverlust befürchtet
- o wegen entsprechender Unternehmenspolitik
- o zuständiger Ansprech-/Kontaktpartner nicht bekannt
- o keine Angriffsfolgen
- o Sonstiges (bitte nennen): _____
- o keine Angabe *(exklusiv)*

Filter: Falls Q28=1 (Opfer hacktivistischer Angriffe)

35. Wurde nach dem hacktistischen Angriff polizeilich und/oder außeramtlich (d.h. nicht polizeilich z.B. durch Privatdedektive) ermittelt?

- o Ja und der/die Täter wurden ermittelt
- o Ja und der/die Täter wurden nicht ermittelt
- o Nein
- o keine Angabe

Filter: Falls Q28=1 (Opfer hacktivistischer Angriffe)

36. Mit welchen Sicherheitsverbänden oder -behörden hat Ihr Unternehmen bezüglich der Angriffe Kontakt aufgenommen?

(Mehrfachnennung möglich)

- o Arbeitsgemeinschaft für Sicherheit in der Wirtschaft (ASW)
- o Bundesamt/Landesamt für Verfassungsschutz (BfV/LfV)
- o Bundesamt für Sicherheit in der Informationstechnik (BSI)
- o Nationales Abwehrzentrum Cybercrime (NCAZ)
- o Allianz für Cyber-Sicherheit (ACS)
- o BITKOM
- o Sonstige (bitte nennen): _____
- o Sonstige (bitte nennen): _____
- o Mit keinen Verbänden oder Behörden *(exklusiv)*
- o keine Angabe

Vielen Dank für Ihre Teilnahme!