LEITFADEN

Wie können gemeinwohlorientierte Organisationen
besser auf Angriffe reagieren?

ZUKUNFT DEMOKRATIE, 2026

Einführung

Dieses Dokument ist ein Leitfaden für zivilgesellschaftliche Organisationen, die mit Angriffen aus rechtsextremen und verschwörungsideologischen Milieus umgehen müssen – oder sich darauf vorbereiten wollen. Es bündelt Erfahrungswissen, typische Muster und konkrete Handlungsoptionen in drei Bereichen: Angriffsstrategien, Gegenmaßnahmen und kommunikative Praxis.

Ziel ist eine einfache, praxisnahe Handreichung, die dabei hilft, Angriffe früh zu erkennen, richtig einzuordnen und zu entscheiden, ob und wie die eigene Organisation reagieren sollte.

Der erste Teil beschreibt die häufigsten **Angriffsformen**: organisierte Empörungswellen, Doxing, Social Engineering, Leaks, sowie Anfragen von Medienaktivisten und viele weitere. Zu jeder Form werden typische Abläufe und Warnsignale erklärt, damit Angriffe schneller erkannt werden können.

Der zweite Teil sammelt konkrete **Gegenmaßnahmen**. Dazu gehören Bedrohungsanalysen, Monitoring und Dokumentation, Notfallmaßnahmen, der Schutz sensibler Daten sowie Hinweise zu rechtlichen Schritten. Ziel ist es, vorbereitet zu sein und im Ernstfall nicht erst Strukturen und Zuständigkeiten klären zu müssen.

Der dritte Teil richtet den Blick auf **Kommunikation**. Er zeigt, wie Organisationen Haltung zeigen können, ohne sich zu rechtfertigen, wie typische Vorwürfe eingeordnet und entkräftet werden können und wie Pressearbeit, Community-Kommunikation und Vernetzung in Angriffssituationen sinnvoll genutzt werden.

Hinweis zur Nutzung: Im Text sind **Hyperlinks** eingebaut. Ein Klick auf die Links führt direkt zu weiterführenden Informationen, Tools oder Beispielen an der jeweils passenden Stelle.

Überblick

01 Strategien

02 Gegenmaßnahmen

03 Kommunikationsempfehlungen

04 Annex mit Vorlagen und Beispielen

STRATEGIEN

Wie zivilgesellschaftliches Engagement gezielt angegriffen wird

Zivilgesellschaft ist nicht hilflos. Wer sich in Deutschland für das Gemeinwohl einsetzt, sollte dies mit Hingabe weiter tun können.

1 Strategien

Seit Jahren intensivieren sich rechtsextreme und verschwörungsideologische Angriffe auf zivilgesellschaftliche Akteure. Schon längst betreffen diese Angriffe nicht mehr nur Organisationen, die die Demokratie gegen Angriffe einschlägiger Akteure verteidigen. Zunehmend sind auch Organisationen, die sich für Inklusion, Gesundheit, Klimaschutz oder andere gemeinnützige Zwecke stark machen, von Anfeindungen und Angriffen betroffen.

Die Ziele sind klar: Die Angreifenden streben ein Ende öffentlicher Förderung und damit auch ein Ende zivilgesellschaftlicher Organisation in vielen Bereichen an. Neben Druck auf Mittelgeber werden Akteure auch gezielt eingeschüchtert, bedroht und in einigen Fällen auch physisch angegriffen. Dahinter steckt auch der Wunsch, zivilgesellschaftlich organisierten Widerspruch gegen antidemokratische Bestrebungen im Keim zu ersticken.

Dadurch ergibt sich auch die Möglichkeit eines Chilling Effects: Nicht nur die Angegriffenen selbst, sondern auch andere Organisationen sollen eingeschüchtert und bedroht werden. Das ist Teil der Kalkulation: Zivilgesellschaft soll so weit eingeschüchtert werden, dass sie sich aus Sorge vor Angriffen selbst zensiert, aus Debatten zurückzieht oder ihre Arbeit einstellt.

Als zentraler Akteur tritt hier die rechtsextreme AfD in Erscheinung. Sie hat es sich zur Aufgabe gemacht und Strategien entwickelt, um einen angeblichen “NGO-Sumpf” zu bekämpfen. Dazu erfolgt sowohl eine offizielle als auch implizite Zusammenarbeit mit Medienaktivisten, rechtsextremen Aktivisten aus dem Vorfeld sowie verschwörungsideologischen Akteuren.

Die folgenden Kapitel bieten einen umfassenden Überblick über die Strategien extrem rechter Akteure, um zukünftige Angriffe schneller und besser zu erkennen.

1.1 (Organisierte) Großangriffe

Zu den wichtigsten Instrumenten der extremen Rechten gehört der mehr oder weniger organisierte Großangriff. Häufig kommt hierfür der Begriff „Shitstorm“ zum Einsatz, der aber unzureichend zwischen ernsthafter Kritik, beispielsweise an Unternehmen, oder rechtsextremen Empörungskampagnen, unterscheidet.

Ein solcher Großangriff ist dadurch gekennzeichnet, dass Influencer, Medienaktivisten, Politiker und andere Akteure durch tage- oder wochenlange Skandalisierung Anfeindungen, Beleidigungen und Drohungen auslösen. Als Auslöser hierfür können ganz unterschiedliche Ereignisse herhalten. Einige Beispiele aus den vergangenen Jahren:

- Ein Pfarrer wird nach einem verkürzenden Artikel in der Lokalzeitung beschuldigt, christliche Traditionen abschaffen zu wollen und erhält über längere Zeit Morddrohungen, nachdem auch rechtsextreme Medienaktivisten das Thema aufgegriffen und skandalisiert haben.
- Eine Interviewszene einer Kommunalpolitikerin wird aus dem Zusammenhang gerissen und immer wieder genutzt, um sie und die Partei anzufeinden. Seit mehr als sechs Jahren wird das Video im Abstand von Wochen oder Monaten immer wieder verbreitet.
- Ein Museum bietet im Rahmen eines Projektes zum Thema Kolonialismus Führungen an, die sich explizit an Menschen richten, die von Rassismus betroffen sind. Das Angebot wird erheblich von Rechtskonservativen bis Rechtsextremen skandalisiert. Das Museum erhält Drohungen, der Staatsschutz ermittelt.

Auch Ankündigungen von Events, Projekten oder Publikationen können als Anlass dienen. Häufig werden Informationen aus ihrem Zusammenhang gerissen oder stark verkürzt. Solche Angriffe können sowohl Auslöser als auch Anfangspunkt anderer Angriffsformen sein, darunter Doxing oder Desinformation. Manchmal werden Betroffene immer wieder aufs Neue angegriffen oder ältere Geschichten nach Jahren wieder verbreitet, um erneut Wut, Beleidigungen und Bedrohungen zu erzeugen.

Großangriffe fußen nicht immer auf kleinteiliger Organisation, oder werden von einem einzelnen Akteur gesteuert. Gerade in der rechtsextremen und verschwörungsideologischen Szene ist tägliche Empörung erprobt, die Verbreitung erfolgt auch durch einfaches Posten und Reposten von Inhalten. Folgende Szenarien sind möglich:

- Ein Influencer greift eine Meldung auf oder erhält einen Hinweis von einem Anhänger, und verbreitet sie unter Verwendung eines in der Szene gängigen Narrativs. Auf diese erste Story steigen Medienaktivisten und Influencer ein. Dadurch entsteht eine regelrechte Empörungswelle.
- Die Skandalisierung als Teil einer größeren, explizit formulierten Strategie, bestimmte zivilgesellschaftliche Akteure anzugreifen. In diesem Zusammenhang ist es plausibel, dass sämtliche Veröffentlichungen, Wortmeldungen und Posts genau beobachtet werden, um potenziell Skandalisierbares zu identifizieren, das dann verbreitet wird, damit andere Akteure eine Meldung und Behauptung aufgreifen.

Es lässt sich aber auch nachweisen, dass Großangriffe im Geheimen organisiert werden. Zum Beispiel schlossen sich vor 2017 tausende Aktivisten in Chats unter dem Namen „Reconquista Germanica“ zusammen, um die AfD vor der bevorstehenden Bundestagswahl zu stärken. In konzertierten Aktionen wurden damals Hashtags auf Twitter (heute X) zu Kanzlerduellen geflutet, Fake Accounts angelegt und politische Gegner sowie Journalisten angegriffen. Unter den Mitgliedern der Gruppe auf der Plattform Discord waren sowohl Mitglieder der AfD als auch der Identitären Bewegung.

Im Jahr 2023 planten Verschwörungsgläubige und Verbündete eine Kampagne gegen den Tagesspiegel-Journalisten Sebastian Leber. Ein Leak zeigte damals, dass die Beteiligten gleichzeitig Artikel veröffentlichten, in denen Leber unter anderem mit Adolf Hitler verglichen und seine Entlassung gefordert wurde.

Gegenmaßnahmen

- Bedrohungsanalyse
- Beratungsangebote nutzen
- Dokumentation
- Monitoring
- Notfallmaßnahmen
- Self-Doxing

1.2 Strategisches Auskundschaften

Extrem rechte und verschwörungsideologische Akteure betreiben häufig strategische Recherchen, wenn zivilgesellschaftliche Organisationen oder deren Gründer, Vertreter und Mitarbeitende bereits im Fokus der öffentlichen Aufmerksamkeit stehen. Solche Situationen entstehen typischerweise durch öffentliche Stellungnahmen, organisierte Veranstaltungen oder laufende Projekte. Sie können also Folge von Großangriffen sein, ihnen aber auch vorausgehen.

Hinter dieser Strategie stehen in der Regel zwei mögliche Ziele. An erster Stelle steht die Suche nach Posts, Fotos oder anderen Inhalten, die sich für eine Skandalisierung eignen. Das Alter und der Kontext von Äußerungen oder Fotos spielt hierbei maximal eine untergeordnete Rolle, auch Uralt-Posts und -Kommentare längst stillgelegter oder vergessener Accounts können zur Skandalisierung genutzt werden. Das zweite mögliche Ziel sind Doxings (siehe 1.3).

Gegenmaßnahmen

- Self-Doxing
- Sperrung der Meldeadresse

1.3 Doxing

Als Doxing (auch: Doxxing) bezeichnet man die Veröffentlichung privater Daten, wie der (privaten) Anschrift oder Telefonnummer, aber auch Mail-Adressen oder Geburtsdaten. Die Veröffentlichung der Privatadresse oder Telefonnummer ist bereits als Bedrohung zu verstehen, kann aber auch dazu führen, dass diese Daten von anderen Akteuren für Drohschreiben oder -anrufe genutzt werden oder die Adressdaten für Online-Bestellungen auf den Namen der Angegriffenen genutzt werden.

Gegenmaßnahmen

- Self-Doxing
- Monitoring
- Suchergebnisse entfernen
- Anzeige erstatten

1.4 Social Engineering

Unter Social Engineering versteht man gezielte Manipulationen, wie das Vortäuschen einer falschen Identität, mit dem Ziel, an Informationen zu gelangen. Der Zweck eines solchen Angriffs könnte sein, an persönliche Adressen, E-Mail- und Telefonkontakte, Termindaten oder andere sensible Informationen zu gelangen.

Denkbar ist zum Beispiel, dass Angreifer sich in Mails, Sprachnachrichten oder Telefonaten als Journalisten, Mitarbeiter von Behörden oder sogar als Mitarbeiter der eigenen Organisation ausgeben. Im Jahr 2022 wurde ein Mann verurteilt, der über Jahre extreme Drohschreiben unter dem Pseudonym „NSU 2.0“, benannt nach den Rechtsterroristen des selbsternannten „Nationalsozialistischen Untergrunds“, verschickt hatte. Der Täter gab sich unter anderem als Polizist aus, um bei der Polizei und mindestens einem Medium Daten zu erbeuten.

Es ist denkbar, dass künftig auch vermehrt künstliche Intelligenz zum Einsatz kommt, um Anrufe oder Sprachnachrichten für solche Zwecke zu erzeugen. Kriminelle nutzen diese Tools bereits für Betrugsanrufe. Schon heute reicht etwa eine Minute Tonmaterial aus, um eine Stimme zu klonen. In Zeiten, in denen auch zivilgesellschaftliche Organisationen auf TikTok, YouTube und Instagram Präsenz zeigen, muss man häufig nicht lange suchen, um entsprechendes Tonmaterial von Mitarbeitenden zu finden.

Gegenmaßnahmen

- **Schutz vor Social Engineering**

1.5 Leaks

Die Veröffentlichung interner Daten und Kommunikation dient in der Regel zur Skandalisierung. Leaks können beispielsweise interne Mails oder Chats oder auch interne Dokumente wie Richtlinien oder projektbezogene Daten sein.

Als Quelle für Leaks kommen sowohl externe Akteure in Frage, die Daten durch Social Engineering oder andere Angriffe erbeuten. Aber auch unzufriedene oder ehemalige Mitglieder oder Mitarbeitende könnten solche Daten weitergeben.

Gegenmaßnahmen

- **Monitoring**
- **Suchergebnisse entfernen**

1.6 Desinformation

Als Desinformation beschreibt man Falschbehauptungen oder Fakes, hinter denen die Absicht steckt, Menschen zu täuschen. Ob Lügen, manipulierte Bilder oder KI-generierte Fakes – dahinter ist immer Intention.

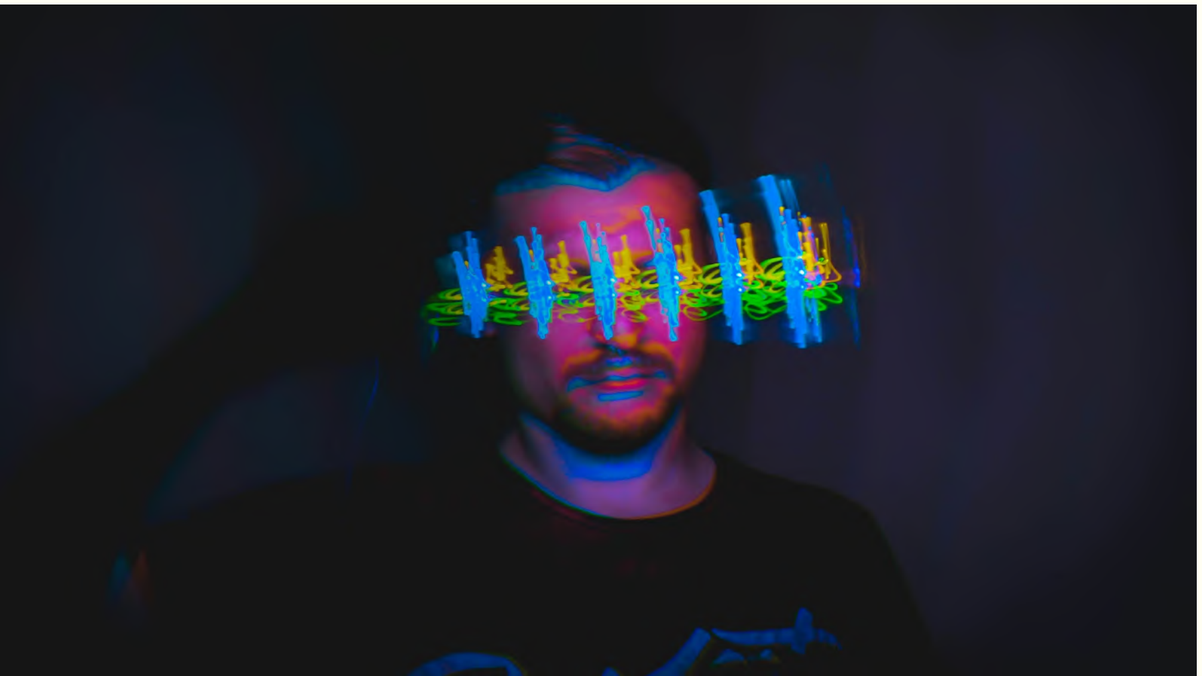
Mögliche Desinformationsnarrative betreffen häufig das Arbeitsfeld einer zivilgesellschaftlichen Organisation. Wer also zum Thema Klima arbeitet, wird häufig mit Falschbehauptungen konfrontiert, die mit der Leugnung der Klimakrise einhergehen. Wer mit Geflüchteten arbeitet, wird häufig mit rassistischen, muslimfeindlichen oder antiziganistischen Narrativen zu tun haben.

Andere Desinformationsnarrative können sich auf Finanzierungen, Tätigkeiten oder den Wertekanon einzelner Mitarbeitende oder Mitglieder, Veröffentlichungen oder Events beziehen oder Kooperationspartner betreffen.

Desinformation wird auch als Zeitfresser eingesetzt, zum Beispiel in Direktnachrichten und E-Mails oder in Kommentaren. Wer immer wieder dieselbe Falschbehauptung in den Kommentaren verbreitet, will wahrscheinlich eher keinen Faktencheck lesen, sondern die Arbeitszeit von Mitarbeitenden verschwenden.

Gegenmaßnahmen

- Monitoring
- Desinformation begegnen & Prebunking
- Suchergebnisse entfernen
- Anzeige erstatten



1.7 Einbindung in Verschwörungserzählungen

Seit Jahren binden extrem rechte und insbesondere verschwörungsideologische Akteure zivilgesellschaftliche Akteure in Verschwörungserzählungen ein. Besonders geläufig ist die Erzählung, dass bestimmte Organisationen ein Teil eines sogenannten „Deep State“ oder “Staat im Staate” seien, einer geheimen Elite, die den Staat und seine Regierung im Verborgenen lenkt und in die demokratische Willensbildung eingreift.

Andere Verschwörungserzählungen beschäftigen sich mit dem „Great Reset“, einer Erzählung von einer angeblich geheim geplanten Neuordnung der Gesellschaft durch Überwachung und Sklaverei, in den häufig auch Organisationen eingebunden werden, die sich mit der Klimakrise beschäftigen. Sie werden unter anderem deshalb zum Teil der großen Verschwörungserzählung, weil sie angeblich die Grundlage für „Klima-Lockdowns“ schaffen, die Regierungen zur Kontrolle der Bevölkerung einführen wollen.

Gegenmaßnahmen

- Monitoring
- Umgang mit Verschwörungserzählungen

1.8 Fake Accounts

Fake Accounts werden zu verschiedenen Zwecken eingesetzt. Sie dienen einerseits zu einer künstlichen Verstärkung von Narrativen. In diesem Sinne werden Fake Accounts für Reposts, Likes oder wahlweise zustimmende oder provozierende Kommentare genutzt.

Fake Accounts können aber auch genutzt werden, um Mitarbeitende oder Mitglieder nachzuahmen und in deren Namen oder im Namen der Organisation problematische Posts zu verbreiten. Solche Fake Accounts werden zum Beispiel eingesetzt, um abstoßende Kommentare über Gewalt- und Terrorakte oder Lügen über Wahlen zu verbreiten.

Gegenmaßnahmen

- **Monitoring**
- **Umgang mit Fake Accounts**

1.9 Deep Fakes

Wie bereits beschrieben, können geklonte Stimmen zum Beispiel beim Social Engineering zum Einsatz kommen. Deep Fakes können aber auch zur Verbreitung von Desinformation genutzt werden. Geklonte Stimmen wurden in der Vergangenheit zum Beispiel genutzt, um in der Slowakei ein Fake-Telefonat zwischen einem Kandidaten und einer Journalistin zu verbreiten, die vermeintlich gemeinsam an einem Plan zum Wahlbetrug arbeiteten. Deep Fakes können auch in Form von Bildern oder Videos eingesetzt werden, die falsche Behauptungen mit Bezug auf zivilgesellschaftliche Organisationen und deren Tätigkeiten verbreiten.

Ein erschreckend riesiger Anteil von Deep Fakes wird jedoch genutzt, um Fake-Pornografie zu erstellen. Betroffen sind davon in erster Linie Frauen, und auch Frauen, die in der Öffentlichkeit stehen, darunter Politikerinnen und Aktivistinnen. Deep Fakes dieser Art werden gezielt eingesetzt, um Bedrohungen und Belästigungen auszulösen und Frauen aus ihrer Arbeit zu verdrängen.

Gegenmaßnahmen

- **Monitoring**
- **Umgang mit Deep Fakes**
- **Suchergebnisse entfernen**

1.10 Anfragen von Medienaktivisten

Spätestens seit den 2000er Jahren sind in Deutschland verschiedene medienaktivistische Projekte in Erscheinung getreten, wie zum Beispiel NiUS, Apollo News und viele weitere. Zwar bezeichnen sich die Macher selbst als Journalisten, haben aber mit klassischer journalistischer Arbeit in der Regel wenig gemein. Medienaktivismus zeichnet sich häufig durch die systematische Missachtung journalistischer Standards aus. In der Regel beschränken sich Medienaktivisten aus dem rechten und verschwörungsideologischen Spektrum auf einen kleinen Themenbereich, Sprache und Themenwahl dienen in erster Linie der negativen Emotionalisierung. Stories über politische Gegner und verhasste Minderheiten sollen Angst, Wut oder Neid erzeugen.

Anfragen von Medienaktivisten sind dementsprechend mit Vorsicht zu begegnen, weil nicht von einer offenen Anfrage mit dem Ziel des Erkenntnisgewinns auszugehen ist. Insbesondere Anfragen an zivilgesellschaftliche Organisationen, die vielfach zu politischen Feinden erklärt werden, dienen konsequent der Erzeugung von Wut oder Neid, unterstellen fehlende politische Neutralität und sollen die betroffenen Organisationen lächerlich machen oder als gierig, inkompetent, politisch fragwürdig oder Teil einer Verschwörung bloßstellen.

Abseits von schriftlichen Anfragen nutzen Medienaktivisten aus dem Spektrum vermehrt Straßenumfragen nach dem Vorbild seriöser Medien. Dabei ist ihre Absicht nicht immer auf den ersten Blick zu erkennen. Üblich sind zudem kurzfristige Interviewanfragen auf Veranstaltungen, wie Demonstrationen oder anderen politischen Events. Auch die Einladung zum spontanen gemeinsamen Selfie sollte hinterfragt werden. Medienaktivisten kommunizieren dabei nicht immer den Namen ihres Blogs oder Kanals.

Gegenmaßnahmen

- Dokumentation
- Monitoring
- Umgang mit Medienaktivisten

1.11 Parlamentarische Anfragen

Die AfD nutzt seit Jahren Anfragen in Parlamenten, um Informationen über zivilgesellschaftliche Organisationen zu erfragen. Dabei fungiert schon die Anfrage selbst als Einschüchterungsversuch, der den betroffenen Organisationen signalisieren soll, dass sie in den Fokus der Partei geraten sind. Zugleich sollen die erfragten Informationen zum Aufbau von Informationssammlungen und gegebenenfalls auch zur Skandalisierung genutzt werden. Diese Angriffe haben seit Jahren System und wurden zuletzt weiter professionalisiert, etwa durch eine eigene Arbeitsgruppe für solche Anfragen in der AfD-Bundestagsfraktion.

Gegenmaßnahmen

- Umgang mit parlamentarischen Anfragen

1.12 Veranstaltungsanmeldungen/besuche

Personen aus extrem rechten oder verschwörungsideologischen Kreisen melden sich häufig zu Veranstaltungen an, die sie als Plattform nutzen wollen oder die von Organisationen oder Personen organisiert wurden, die Rechtsextreme zu Feinden erklärt haben.

Bereits eine Anmeldung zu einer Veranstaltung kann als Versuch der Einschüchterung verstanden werden. Nehmen solche Akteure tatsächlich an einer Veranstaltung teil, sind unterschiedliche Verhaltensweisen beobachtbar, von Störversuchen über provozierende Publikumsfragen bis hin zu Filmaufnahmen zum Zwecke der Skandalisierung.

Gegenmaßnahmen

- Bedrohungsanalysen
- Umgang mit Veranstaltungsanmeldungen und -besuchen

GEGEN-MASSNAHMEN

Wie zivilgesellschaftliche Organisationen reagieren können

2.1 Bedrohungsanalysen

Um sich gegen mögliche Bedrohungen zu wappnen, sollte man sich zunächst fragen, welche konkreten Gefahren und Folgen es für die eigene Arbeit, aber auch für konkrete Kampagnen oder Events gibt. Das Wissen um potenzielle Angriffe im Rahmen der eigenen Tätigkeit hilft dabei, diese besser zu identifizieren und sinnvolle Präventions- und Gegenmaßnahmen zu ergreifen.

Es lohnt sich, Bedrohungsanalysen bereits in der Planungsphase von größeren Projekten oder Events zu berücksichtigen. In dieser Phase besteht kein akuter Zeit- und Handlungsdruck. In Situationen, in denen Kampagnen und Aktionen bereits in Gange sind, sind dagegen teilweise schnelle Entscheidungen und Reaktionen erforderlich. Wer vorbereitet ist, kann in solchen Fällen strukturierter und besonnener agieren.

Mögliche Fragen für eine Bedrohungsanalyse sind:

- Was muss ich schützen? (Büroadresse, Kommunikation, Daten von Mitarbeitenden, Kommunikation)
- Vor wem muss ich mich, meine Organisation, Mitarbeitenden und Daten schützen?
- Welche Konsequenzen sind zu erwarten, wenn meine Schutzmaßnahmen scheitern?
- Wie wahrscheinlich sind Angriffe? Welche Angriffe sind wahrscheinlicher als andere?
- Welche Schutzmaßnahmen sind angemessen, sinnvoll und umsetzbar? Wo und bei wem liegt in der Organisation die Verantwortlichkeit für die Planung und Durchführung?

2.2 Prebunking

Desinformation, also die absichtliche Verbreitung von Falschinformationen um andere zu täuschen, können Organisation sowohl präventiv als auch reaktiv begegnen. Eine Form der präventiven Herangehensweise wird als Prebunking bezeichnet. Dabei geht es darum, im Vorfeld über Mechanismen und Narrative von Desinformation aufzuklären. Solche Maßnahmen können sowohl organisationsintern als auch für die externe Kommunikation hilfreich sein. Die Forschung zeigt, dass Prebunking wie eine Art Impfung gegen Desinformation wirken kann.

Im Vorfeld von Events oder Veröffentlichungen, die potenziell ein hohes Maß an Aufsehen erregen, könnte man beispielsweise ein Dokument mit den wichtigsten Fragen und Antworten erarbeiten und dabei auch gängige Desinformationsnarrative berücksichtigen, die kontextbezogen von Bedeutung sind. Beispiele für häufige Desinformationsnarrative sind Erzählungen über Geldgeber oder das Tätigkeitsfeld. Oft werden Organisationen auch in bestehende populäre Desinformationsthemen, wie Klimawandelleugnung, Kulturkampfnarrative oder queerfeindliche Desinformation einbezogen.

Außerdem sind häufig Mitarbeitende oder Mitglieder betroffen, zum Beispiel indem gefälschte oder aus dem Kontext gerissene Aussagen von ihnen verbreitet werden. Viele Narrative, die zur Verbreitung von Desinformation genutzt werden, sind wiederkehrend. Ist erst einmal ein Prebunking-Dokument verfügbar, können Organisationen auch künftig darauf zurückgreifen und beliebig erweitern.

Nützliche Ressourcen

Einen **ausführlichen Guide zum Thema Prebunking** gibt es von der Universität Cambridge, der BBC und der Google-Tochter Jigsaw:
https://prebunking.withgoogle.com/docs/A_Practical_Guide_to_Prebunking_Misinformation.pdf

2.3 Desinformation begegnen

Wird eine Organisation, Mitglieder oder Mitarbeitende mit Desinformation konfrontiert, die beispielsweise die eigene Arbeit, Finanzierung oder Mitarbeitende betrifft, steht an erster Stelle die Frage, ob eine Reaktion sinnvoll oder sogar schädigend sein kann. Dazu gilt es zunächst einige wichtige Fragen zu beantworten:

Wen hat die Desinformation erreicht und wen erreicht sie potenziell noch?
Die Verbreitungswege von Desinformation können stark variieren, aber häufig nehmen sie den Weg von abseitigeren oder kleineren Kommunikationsräumen und verbreiten sich von dort aus auf unterschiedlichen Plattformen. Im schlimmsten Fall wird Desinformation unkritisch und unhinterfragt von Massenmedien oder Politikern aufgegriffen und erreicht so ein riesiges Publikum.

Nicht jede Falschmeldung erreicht viele Menschen. Umso wichtiger ist die Frage, wie viele Menschen schon erreicht wurden und noch erreicht werden könnten. Dazu lohnt sich der Blick auf unterschiedliche Plattformen und Reaktionen. Ist der Empfängerkreis überschaubar, lohnt es sich, die Entwicklung gegebenenfalls weiter zu beobachten, statt zu reagieren. Gerade Organisationen mit großer Reichweite sollten darauf achten, dass sie für sich festlegen, ab wann eine Falschbehauptung groß genug ist, um öffentlich auf sie zu reagieren, damit sie sie durch ihre Reichweite nicht sogar weiter verbreiten und größer machen, als sie ist.

Verbreitet sich ein Desinformationsnarrativ zunehmend, hat aber noch keine hinreichende Reichweite, lohnt es sich, eine Reaktion schon einmal vorzubereiten, um sie für den Fall griffbereit zu haben, dass zum Beispiel größere Influencer oder Medienaktivisten mit großer Reichweite das Thema aufgreifen.

Welche Gefahr geht von diesem Narrativ/dieser Desinformation aus?
Desinformation kann Folgen haben. Sie kann Beleidigungen und Bedrohungen für die eigene Organisation oder konkret betroffene Mitarbeitende auslösen. In solchen Fällen lohnt sich eine Richtigstellung in jedem Fall und sollte zuerst dort ausgespielt werden, wo sie kursiert und gegebenenfalls Menschen erreicht, die sich nicht nur in rechtsextremen oder verschwörungs-ideologischen Kommunikationsräumen bewegen. Eine Richtigstellung auf Telegram wird eher wenig Effekt haben, als ein Post auf Facebook oder TikTok, der auch Unterstützer erreicht.

Manchmal werden Falschbehauptungen und Fakes auch genutzt, um Geldgeber unter Druck zu setzen, sich von der Organisation zu distanzieren oder sogar das Funding einzustellen. Hier lohnt es sich auf jeden Fall, eine Reaktion vorzubereiten und ggf. Geldgeber zu informieren, bevor sie von Dritten unter Druck gesetzt werden.

Wer auf Desinformation reagieren will, muss mehrere Dinge beachten:
Schnelles Reagieren ist wichtig - aber nur, wenn die Richtigstellung wasserdicht ist
In den allermeisten Fällen lohnt es sich nicht, auf eine Falschmeldung zu reagieren, die ihren Peak schon längst überschritten hat, also deren Reichweite in Form von Posts, Reposts, Klicks und Kommentaren schon wieder sinkt und die schon seit mehreren Tagen oder sogar Wochen kursiert. In solchen Fällen sorgt man im schlimmsten Fall dafür, dass der Fake erneut kursiert.

Die große Herausforderung ist also, einer Falschmeldung offensiv zu begegnen, wenn sie nicht noch zu klein ist, aber auch noch nicht Massenmedien, eine breite Öffentlichkeit und demokratische Politiker erreicht hat. Im Zweifelsfall lohnt es sich hier auch, sich eine Einschätzung von Fachleuten einzuholen, ob und wann sich eine Reaktion lohnt.

Das Allerwichtigste ist: Die Widerlegung von Desinformation muss in jedem Fall richtig sein und die Falschaussage nachvollziehbar entkräften. Wer eine Richtigstellung nach der Veröffentlichung noch einmal korrigieren muss, schafft sich neue, zusätzliche Probleme. Solange es Unsicherheit gibt, sollte man Desinformation entweder noch nicht kommentieren, oder transparent machen, dass eine Aufarbeitung oder Untersuchung stattfindet und noch abgeschlossen werden muss.

Das Wahrheitssandwich

Wer einer Falschmeldung mit einer Richtigstellung begegnen will, sollte darauf achten, wie die Falschbehauptung eingebettet ist. Die Wiederholung falscher Behauptungen kann auch zu ihrer Verbreitung beitragen, deshalb ist es wichtig, dass Falschnachricht oder Fake in einem Statement nicht zu allererst wiederholt werden.

Der Linguist George Lakoff empfiehlt deshalb das sogenannte „truth sandwich“: Wer eine Falschmeldung widerlegen will, sollte in einem Artikel oder anderweitigen Beitrag dazu erst die Tatsachen benennen, dann auf die falsche Behauptung eingehen und dann wieder auf die Fakten zurückkommen. So verhindert man, dass der erste oder letzte Eindruck bei Rezipientinnen der Fake ist, den man eigentlich gerade zu widerlegen versucht.

2.4 Dokumentation

In Zeiten zunehmender Attacken auf gemeinwohlorientierte Organisationen ist es für jede einzelne Organisation wichtig, den Überblick zu behalten und seltsame bis bedrohliche Vorkommnisse zu dokumentieren. So lassen sich auch Eskalationen zu einem späteren Zeitpunkt nachvollziehen.
Es lohnt sich, ein eigenes Dokument als Protokoll einzurichten, auf das alle relevanten Teammitglieder zugreifen können.

Beispiele für Ereignisse, die dokumentiert werden sollten, sind:

- Telefonanrufe, bei denen Fremde Informationen erfragen oder beleidigend werden;
- auffällige oder nicht bestellte Briefe oder Päckchen, oder unangekündigte Besuche fremder Personen;
- beleidigende oder bedrohende Social-Media-Inhalte gegenüber der Organisation und Mitarbeitenden oder Mitgliedern.

Eine gute Dokumentation ist außerdem wichtig für mögliche Anzeigen, beispielsweise wegen Beleidigungen, Bedrohungen oder Doxings. Hierfür können auch Archivierungstools wie web.archive.org oder archive.is genutzt werden. Wichtig ist allerdings: Diese Archivierungen sind öffentlich und auch noch verfügbar, wenn die betreffenden Posts oder Inhalte gelöscht wurden. Wurden sensible Daten oder Fotos verbreitet, sollten diese nicht über Archivierungstools gesichert werden.

Statt webbasierter Archivierungstools können Inhalte auch lokal archiviert werden, zum Beispiel als Screenshots oder als vollständig archivierte Seiten. Wichtig ist hier natürlich, die archivierten Screenshots und Dateien entsprechend auffindbar abzulegen.

Einige Beispiele für nützliche Tools und Anleitungen:

- Wie man rechtssichere Screenshots erstellt, beschreibt HateAid in dieser Anleitung
- Wenn man ganze Seiten mit Kommentaren etc. archivieren möchte, geht das mittels Browser-Erweiterungen wie
  - Fireshot (für Chrome und Firefox) kann Screenshots ganzer Browserfenster erstellen, die als Bild oder PDF-Datei gespeichert werden können.
  - SingleFile (für Chrome und Firefox) ermöglicht das Speichern ganzer Seiten als HTML-Datei. Der Vorteil: Die Seiten werden sehr originalgetreu gespeichert und können später einfach durchsucht und kopiert werden.

2.5 Monitoring

Monitoring kann sowohl im Alltag als auch im akuten Angriffsfall äußerst hilfreich sein um:

- Bedrohungen und Kampagnen früh zu identifizieren
- Das Ausmaß einer Bedrohungslage einzuschätzen und daraus Entscheidungen abzuleiten, ob und welche Maßnahmen sinnvoll sind
- Justiziable Bedrohungen und Beleidigungen zu identifizieren und zur Anzeige zu bringen.

Viele professionelle Monitoring- oder Social-Listening-Tools kosten tausende Euro im Jahr und sind selten auf die Bedarfe von NGOs oder Vereinen zugeschnitten. Es gibt aber auch einige Möglichkeiten, Monitoring-Aufgaben kostenlos oder für deutlich geringere Kosten zu automatisieren.

Google Alerts

https://www.google.de/alerts

Google Alerts können ein extrem sinnvolles und kostenloses Monitoring-Werkzeug sein, wenn sie richtig eingesetzt werden. Für jede Organisation sind individuelle Einstellungen sinnvoll. Das liegt auch daran, dass die Ergebnisse erheblich variieren können, wenn die eigene Organisation häufig online erwähnt wird, weil sie beispielsweise häufig Thema in den Medien ist.

Wichtig: Google Alerts nutzen als Grundlage für Benachrichtigungen Suchergebnisse, die bei Google indexiert werden. Manchmal kann einige Zeit vergehen zwischen der Veröffentlichung eines Artikels oder Beitrags und der Indexierung durch Google, dann verzögert sich auch der Alert. Außerdem eignet sich Google nur begrenzt für Alerts für Social Media Plattformen, weil nicht jeder einzelne Post im Index von Google landet.

Google Alerts erlaubt die Nutzung von Suchoperatoren, also Sonderzeichen oder einzelnen Ergänzungen, die die Suche einschränken.
Ein paar Beispiele für sinnvolle Alerts:

- „Name der Organisation“
  - Die Anführungszeichen sorgen dafür, dass der Name der eigenen Organisation in exakt dieser Wortreihenfolge gesucht wird
  - Diese Suche eignet sich nur dann, wenn die eigene Organisation nicht ständig in Medien zitiert wird oder anderweitig häufig Einträge oder Artikel im Netz erzeugt
  - Es lohnt sich hier außerdem, sämtliche möglichen Schreibweisen der Organisation sowie übliche Schreibfehler aufzuführen. Hierzu kann man neben den Anführungszeichen auch den Suchoperator OR nutzen. Dann würde im Feld für den Google Alert folgendes stehen: „Name der Organisation“ OR „Name-der-Organisation“ OR „fehlerhafte Schreibweise der Organisation“
  - Um ein Wort von den Suchergebnissen auszuschließen kann man in der Suchanfrage ein Minuszeichen (-) vor das auszuschließende Wort setzen
  - Gerade hier ist es sinnvoll, mit den Alert-Einstellungen von Google zu experimentieren, um nicht zu viele, aber auch nicht zu wenige Alerts zu erhalten. Gegebenenfalls lohnt sich auch die Einrichtung einer eigenen Mailadresse für Monitorings, auf die mehrere Kolleg:innen zugreifen können - solange diese Adresse dann nicht in Vergessenheit gerät.
- „Büro- oder Impressumsadresse“
  - Auch dieser Alert ergibt nur Sinn, wenn die Adresse nicht ständig im Netz genannt wird, etwa weil im Haus zahlreiche Büros verschiedener Firmen, Organisationen etc. ansässig sind
  - Wie bereits beim Namen lohnt sich auch hier die Suche verschiedener Schreibweisen. Zum Beispiel könnte eine Adresse in der Bahnhofstraße 15 in Berlin für folgenden Alert genutzt werden: („Bahnhofstraße 15“ OR „Bahnhofstr. 15“ OR „Bahnhofstr 15“) Berlin
- Mailadressen, insbesondere von Kolleginnen und Kollegen, die eher in der Öffentlichkeit stehen oder bereits zuvor persönlich angegriffen wurden
- Auch Namen von Publikationen, Events oder Kampagnen können wir oben beschrieben für Google Alerts genutzt werden

Im Fall kampagnenartiger Angriffe können die Ergebnisse für Alerts auch auf konkrete Websites, zum Beispiel von rechtsextremen Medienaktivisten, beschränkt werden. Ein Alert, der über Erwähnungen der Organisation oder angegriffener Kolleg:innen informiert, könnte in dem Fall folgendermaßen aussehen:

- (site:website1.de OR site:website2.de) „Name der Organisation“ OR „Vorname Nachname“

Talkwalker Alerts

https://alerts.talkwalker.com/

Talkwalker ist ein Unternehmen, dass kommerzielle Monitoring-Tools anbietet. Technisch funktionieren diese Alerts genauso wie Google Alerts, allerdings kann Talkwalker auch Ergebnisse für X einbeziehen. Seit der Übernahme von Twitter durch Elon Musk hat die Plattform, die jetzt X heißt, noch einmal zusätzlich an Bedeutung für rechtsextreme und verschwörungsideologische Akteure gewonnen und wird oft als Startpunkt oder zur Weiterverbreitung von Kampagnen, Desinformation etc genutzt.

Website-Monitoring mit Follow that Page

https://www.followthatpage.com/

Dieses Tool lohnt sich nur, wenn man konkrete einzelne Artikel oder Seiten beobachten möchte, die selten geändert werden, also wenn man nachverfolgen möchte, ob eine Behauptung in einem Blogpost oder eine Kontaktadresse in einem Impressum geändert wurde. Dazu gibt man die konkrete Adresse und eine Mailadresse ein.
Achtung: Dieses Tool eignet sich nicht um die Startseiten von Blogs oder medienaktivistischen Projekten zu monitoren. Außerdem ist die Zahl der Seiten, die man angeben kann, begrenzt.

Manuelles Monitoring

Manuelles Monitoring ist zeitintensiv und oft im Alltag nicht umsetzbar. Es kann aber gerade in Notfallsituationen helfen, Bedrohungen schnell zu identifizieren. Tipps für manuelles Monitoring sind deshalb im Abschnitt „Notfallmaßnahmen“ aufgeführt.

2.6 Umgang mit Medienaktivisten

Unter dem Begriff "Medienaktivisten" sind hier Autoren, Kolumnisten, Reporter und Talkshow-Hosts von unseriösen, pseudojournalisten und rechtspopulistischen News- und Meinungsportalen gemeint.

Medienaktivisten nehmen zunehmend verschiedene zivilgesellschaftliche Organisationen, Vereine, Stiftungen und Begünstigte öffentlicher und Spendengelder in den Blick. Dazu gehören telefonische und schriftliche Anfragen ebenso wie angemeldete oder unangemeldete Besuche bei Events oder eher zufällige Begegnungen durch Straßenumfragen oder Interviews bei externen Veranstaltungen. Weil generell nicht davon auszugehen ist, dass Anfragen von Medienaktivisten durch Erkenntnis-gewinn motiviert sind, sollten Anfragen aller Art grundsätzlich abgelehnt werden. Darüberhinaus gibt es aber Situationen, in denen die Anfragenden sich nicht sofort zu erkennen geben.

Einige Aktivisten haben sich in den vergangenen Jahren eigene „Presseausweise" angefertigt, die sie nutzen, um zu suggerieren, sie seien seriöse Journalisten. Hier hilft der genaue Blick auf die ausstellende Organisation. Wegen dieser Entwicklungen wurde der bundeseinheitliche Presseausweis ins Leben gerufen, der von folgenden Verbänden ausgestellt wird:

- Bundesverband Digitalpublisher und Zeitungsverleger (BDZV)
- Deutsche Journalistinnen- und Journalisten-Union in Ver.di (dju)
- Deutscher Journalisten-Verband (DJV)
- Medienverband der freien Presse (MVFP)
- Fotografenverband FREELENS
- Verband Deutscher Sportjournalisten (VDS)

Bei einer Anfrage sollte grundsätzlich erfragt werden, für welches Medium die Anfrage erfolgt.
Außerdem hilft eine Suchmaschinensuche im Zweifelsfall dabei, einzuschätzen, wie seriös eine Anfrage ist.

Wichtig: Keinerlei Kommunikation mit Medienaktivisten ist als vertraulich einzuschätzen - dazu gehören Telefonate ebenso wie Mails, Nachrichten auf Social-Media-Plattformen und Messengern oder Videoaufnahmen. Entscheidet man sich zu einer Reaktion auf eine Anfrage, einen Kommentar oder eine Nachricht, sollte dieser Aspekt immer mitgedacht werden.

Viele Straßenumfragen oder Anfragen bei externen oder internen Events oder Demonstrationen müssen nicht geplant auf Mitarbeitende oder Mitglieder ausgerichtet sein. Trotzdem können Arbeitgeber oder Organisation im Nachhinein identifiziert und mit den erfolgten Aufnahmen verbunden werden.
Bei Straßenumfragen lohnt sich zunächst der Blick auf das Mikrofon. Ist dort kein Logo zu erkennen, sollte an erster Stelle die Frage stehen, zu welchem Medium oder Kanal der oder die Filmende gehört. Überdies sollte man darauf bestehen, sich Medium oder Kanal oder vorherige Arbeiten des Interviewers zeigen zu lassen.

Straßenumfragen von rechten oder verschwörungsideologischen Medienaktivisten oder Streamern dienen nicht dem Erkenntnisgewinn, sondern sind darauf ausgelegt, die eigene Ideologie zu unterstreichen, zu skandalisieren oder die Gefilmten verächtlich zu machen. In diesen Fällen sollte man Filmaufnahmen klar und deutlich widersprechen und auf das Recht am eigenen Bild hinweisen. Eine Einwilligung muss vorliegen, damit die Bilder später benutzt werden können. Wenn man allerdings in die Kamera spricht und eine Frage auf welche Weise auch immer beantwortet, kann das als Einwilligung verstanden werden. (Bei Demonstrationen sind Aufnahmen der Teilnehmenden grundsätzlich erlaubt.)

Wichtig ist in jedem Fall: Ruhe bewahren und auf mögliche Provokationen nicht eingehen.
Zunehmend kommen auch Smart Glasses zum Einsatz, bei denen nicht auf den ersten Blick erkennbar ist, dass es sich um eine Brille mit Kamerafunktion handelt. Die Brillen werden genutzt, um Menschen ohne Einverständnis zu filmen, ohne dass die Gefilmten merken, dass eine Kamera läuft. Bei ungewöhnlichen Begegnungen lohnt sich hierbei der Blick auf die Brille. Kameras lassen sich teilweise erkennen und in vielen Fällen zeigt ein Licht an, dass die Kamera läuft. Diese Lichter lassen sich allerdings teilweise auch deaktivieren.

2.7 Sperrung der Meldeadresse

Eine Melderegisterauskunft ist vergleichsweise unkompliziert und kostet nicht viel. Wer von Bedrohungen betroffen ist oder in einem Bereich arbeitet, bei dem Anfeindungen vorhersehbar sind, kann diese Melderegisterauskunft sperren lassen.
Einige nützliche Links dazu:

- Netzpolitik.org hat zusammengetragen, in welchen Fällen eine Melderegisterauskunft bedrohlich sein kann
- HateAid fasst die wichtigsten Informationen zusammen und hilft auch bei der Beantragung einer Auskunftssperre
- Der Verband der Beratungsstellen für Betroffene rechter, rassistischer und antisemitischer Gewalt stellt eine Mustervorlage für eine Beantragung zur Verfügung

2.8 Schutz vor Social Engineering

Unter Social Engineering versteht man eine Form der psychologischen Manipulation, bei der Menschen dazu gebracht werden, vertrauliche Informationen preiszugeben oder unsichere Aktionen durchzuführen, um bspw. an sensible Daten zu gelangen. Organisationen sind besonders häufig von Social Engineering betroffen, wenn bereits Aufmerksamkeit auf sie gerichtet ist, also bei großen Veröffentlichungen, Events oder wenn gerade schon ein Großangriff läuft. Manchmal wird Social Engineering aber auch als Vorbereitung für Doxings oder Großangriffe genutzt.
Ein paar Dinge helfen, sich vor Social Engineering zu schützen:

- Klare Regeln, welche Daten auf welchem Weg freigegeben werden;
- Für die Herausgabe sensibler Daten auch unter Kollegen oder Mitgliedern ein Passwort vereinbaren, ohne das keine Daten übermittelt werden;
- Wenn Medien, Behörden oder andere Organisationen anrufen und Daten abfragen und der Anrufende nicht bekannt ist, sollte man sich die Anfrage grundsätzlich per Mail bestätigen lassen;
- Auch Partner und Familie sollten im Fall wahrscheinlicher Angriffe sensibilisiert werden.

2.9 Umgang mit Verschwörungserzählungen

Die Einbettung zivilgesellschaftlicher Organisationen in Verschwörungserzählungen hat sich in den letzten Jahren intensiviert. Ob Organisationen mit Klimathemen, Geflüchteten oder Gesundheit zu tun haben - sie alle wurden in Verschwörungserzählungen eingebettet. Ob sich eine Reaktion lohnt, hängt von der Reichweite der Erzählung ab. Im Zweifelsfall lieber einen externen Rat einholen. Wer reagieren möchte, sollte die Umstände klar benennen, nämlich dass es sich um eine Verschwörungserzählung handelt, warum das der Fall ist, wem diese Erzählung nützt und welche Gefahren dahinter stecken. Viele Verschwörungserzählungen sind im Kern antisemitisch - auch das gilt es, wenn es zutrifft, zu benennen.

2.10 Umgang mit Fake Accounts

Fake Accounts, die vorgeben, ein offizieller Account der Organisation, von einzelnen Mitarbeitenden oder Mitgliedern zu sein, können bei allen Social-Media-Plattformen gemeldet werden. Hierzu muss meistens ein Nachweis, zum Beispiel über den Upload des Fotos vom Personalausweis oder Ähnlichem, erbracht werden, dass das Profil Identitätsklau betreibt.
Fake Accounts sollten vor der Meldung dokumentiert werden (siehe **Dokumentation**). Außerdem können ggf. rechtliche Schritte geprüft werden.

2.11 Umgang mit Deep Fakes

Der Vorgang ist hier derselbe wie bei Fake Accounts.
Deep Fakes aller Art sollten vor der Meldung dokumentiert werden (siehe **Dokumentation**). Außerdem können ggf. rechtliche Schritte geprüft werden. Für Deep Fakes gibt es in Deutschland keine speziellen rechtlichen Regelungen, es können jedoch Verletzungen von Persönlichkeitsrechten, der Datenschutzverordnung oder Kennzeichnungspflichten zur Anzeige gebracht werden.

2.12 Suchergebnisse entfernen

Unter bestimmten Umständen kann man Suchergebnisse bei Suchmaschinen wie Google oder Bing entfernen lassen. Das gilt zum Beispiel für sensible Daten, private Bilder oder ähnliche Inhalte. Google und Bing haben dafür eigene Formulare, über die die Entfernung von Suchergebnissen angefragt werden kann.
Diese Maßnahmen können auch genutzt werden, wenn sensible Daten oder Kommunikation durch Leaks verbreitet werden.

2.13 Umgang mit parlamentarischen Anfragen

Die AfD nutzt parlamentarische Instrumente wie Kleine Anfragen seit Jahren zum Informationsgewinn und als Mittel zur Einschüchterung und Delegitimation politischer und zivilgesellschaftlich organisierter Gegner. Wer sich selbst als Organisation (oder Verbündete) in einer Kleinen Anfrage wiederfindet, sollte die Erwähnung und den damit verknüpfen Angriff auf die Organisation nicht persönlich nehmen, sondern als Teil einer strategischen Kampagne begreifen – und entsprechend professionell, besonnen und solidarisch reagieren.

In der Regel betreffen Kleine Anfragen Informationsgesuche zur Finanzierung, Berichtspflicht und Verwaltung von öffentlich geförderten Projekten (wobei mehrere Anfragen auch schon komplett spendenfinanzierte Organisationen und gemeinnützige GmbHs tangiert haben). Bei allen Nachfragen zur Finanzierung durch öffentliche Mittel ist eine enge Abstimmung mit der zuständigen Verwaltungs- oder Förderstelle zentral und unbedingt empfehlenswert. Antworten sollten sachlich, knapp und nur im rechtlich notwendigen Umfang erfolgen. Es gilt, personenbezogene Daten konsequent zu schützen, juristischen Rat einzuholen und tendenziöse Unterstellungen klar zurückzuweisen. Wichtig ist, Ruhe zu bewahren, den durch Regierung oder Ministerien legitimierten Auftrag in den Mittelpunkt zu stellen und sich nicht auf Provokationen einzulassen.

Darüber hinaus sollten interne Handlungspläne vorbereitet werden, um im Ernstfall souverän reagieren zu können. Solidarität und Vernetzung mit anderen Betroffenen stärkt die Handlungsfähigkeit, ebenso wie eine aktive, selbstbewusste Kommunikation nach außen: Wer angegriffen wird, weil er für Demokratie eintritt, sollte dies klar benennen und als Teil demokratischer Haltung sichtbar machen. Damit befasst sich auch der zweite Teil dieses Leitfadens.

Zum Umgang mit Angriffen sind die folgenden Leitfäden zu empfehlen, die sich diesem Thema noch ausführlicher widmen:

- Druck aus den Parlamenten – Zum Umgang sozialer Organisationen mit Anfeindungen von rechts (Der Paritätische, Mobile Beratung gegen Rechtsextremismus Berlin und vdk)
- Umgang mit Angriffen von Rechtspopulismus und Rechtsextremismus – FAQ (Arbeitskreis deutscher Bildungsstätten)

2.14 Umgang mit Veranstaltungsanmeldungen und Besuchsankündigungen

Organisierte Rechtsextreme und Medienaktivisten nutzen Veranstaltungen für Einschüchterungsversuche und Raumnahme. Ein Ausschluss ist nicht in jedem Fall möglich und je nach Veranstaltung und Ankündigung oder Anfrage sollte der Einzelfall entscheiden. Dazu gehört auch die Frage, ob es sich beim potenziellen Besucher um einen bekannten Aktivisten, Influencer oder Medienaktivisten oder um eine Privatperson mit einschlägigen Ansichten handelt. Auch hier lohnt es sich im Zweifelsfall, externe Expertise zu konsultieren, bspw. von der Mobilen Beratung.

Außerdem lohnt sich Abwägen: Welche Risiken bestehen durch den Ausschluss einer Person im Vergleich zu Risiken bei ihrer Teilnahme. Ein paar Überlegungen dazu:

- Der Ausschluss von einer Veranstaltung kann skandalisiert werden. Allerdings ist das eher selten der Fall, die Risiken bei einer Teilnahme von organisierten Rechtsextremen und Verschwörungsideologen sind allerdings häufig größer.
- Auch die Frage auf einen rechtlichen Anspruch auf eine Teilnahme ist zu prüfen, bspw. über die Durchsetzung des Hausrechts..
- Bei einer Teilnahme ist gerade bei bekannten Akteuren mit Störversuchen, Einschüchterung und Raumnahme zu rechnen.
- Andere Besuchende können sich durch die Teilnahme einschlägiger Akteure zurückziehen oder auf eine aktive Teilnahme verzichten.
- Zunehmend filmen Influencer und Aktivisten zudem auf Veranstaltungen aller Art, um die Gefilmten schließlich bloßzustellen oder für skandalisierende Berichte zu nutzen.

Wo möglich, sollten Veranstaltungen, bei denen Störversuche und Skandalisierung möglich sind, Anmeldungen erfordern und verbindliche Regeln und Ausschlussklauseln für die Veranstaltung formuliert werden, die bei Bedarf durchgesetzt werden können. Für die Durchsetzung müssen im Vorfeld ein klarer Prozess sowie Verantwortliche bestimmt werden. Gegebenenfalls können auch Beratungsstellen wertvolle Hilfe liefern.

Nützliche Ressourcen

Aktuelle Leitfaden zum Thema gibt es außerdem bei der **Mobilen Beratung gegen Rechtsextremismus Berlin** und der **Gesellschaft für Medienpädagogik und Kommunikationskultur**.

2.15 Anzeige erstatten

In Fällen von Beleidigungen, konkreten Bedrohungen, Desinformation oder Doxings kann eine Anzeige sinnvoll sein. Wenn die Organisation oder ihre Mitarbeitenden konkret angegriffen werden, können Beratungsstellen oder Anwälte helfen. Organisationen wie Hate Aid und verschiedene Beratungsstellen helfen bei Anzeigen und der entsprechenden Betreuung in diesen Fällen.
In anderen Fällen äußern Angreifer auf Social-Media-Plattformen Hassrede, die zum Beispiel als Volksverhetzung oder auch Holocaustleugnung eingeordnet werden kann. Solche Fälle kann man bei Meldestellen einreichen, die mögliche rechtliche Schritte prüfen und ggf. Anzeigen erstatten. Dazu gehören zum Beispiel:

- die **Meldestelle Respect**
- **Hessen gegen Hetze**
- **die Zentralstelle zur Bekämpfung von Hasskriminalität im Internet**

Außerdem sind in den meisten Bundesländern Anzeigen per **Internetwache** möglich.

2.16 Notfallmaßnahmen

Präventive Maßnahmen

Die wichtigste Präventivmaßnahme um für einen Großangriff vorzusorgen, ist die Klärung von Zuständigkeiten und Vertretungen. Ein paar wichtige Fragen hierzu:

- Wer kümmert sich um Monitoringaufgaben?
- Wer trifft Entscheidungen über Statements?
- Wer entscheidet über konkrete Schutzmaßnahmen?
- Wer dokumentiert?

Dasselbe gilt für Abstimmungsprozesse und Kommunikationsabläufe sowie Klarheiten für alle Mitarbeitenden darüber, wer über sicherheitsrelevante Vorfälle zu benachrichtigen ist.
Außerdem lohnt es sich, nützliche Keywords für manuelles Monitoring (beispielsweise Namen und Adressen) zu erstellen. In der Hektik eines Großangriffs kann diese Arbeit viel unnötige Zeit erfordern.

Maßnahmen im Notfall

Wenn der Angriff läuft, gilt es schnell und bedacht zu handeln. Folgende Maßnahmen können hilfreich sein:

1/ Dokumentation

- Siehe Kapitel „**Dokumentation**“
- Notiert werden sollten sämtliche wichtigen Informationen über entsprechende Anrufe, Anfragen, Mails oder Social-Media-Inhalte inkl. Screenshots und ggf. Videos

2/ Google Alerts überprüfen und ergänzen

- Laufende Alerts sollten, wenn genügend Kapazitäten vorhanden sind, so eingestellt werden, dass jedes neue Suchergebnis eine neue Mail auslöst
- Außerdem sollten neue Google Alerts zur aktuellen Situation angelegt werden, die Schlagworte oder Namen zum konkreten Vorfall oder zur Kampagne enthalten

3/ (Private) Social-Media-Kanäle schließen

- Wenn ein Großangriff läuft, ist davon auszugehen, dass sämtliche Social-Media-Profile auf skandalisierbare Inhalte oder mögliche Kontakte für Social-Engineering-Versuche durchleuchtet werden. Das gilt für die Profile der Organisation ebenso wie für Mitarbeitende oder Mitglieder, die akut angegriffen werden. Das gilt aber auch für andere Mitarbeitende, die beispielsweise auf der Team-Seite der Website oder im Zusammenhang mit Veranstaltungen genannt werden.
- Privatprofile sollten geschlossen werden, wenn:
  - unklar ist, ob skandalisierbare Posts oder Kommentare vorhanden sind. Das gilt leider auch für ironische Bemerkungen.
  - Rückschlüsse auf Wohnort, Familienmitglieder oder Kontakte verfügbar sind
- Das gilt auch für LinkedIn-Profile. Hier lohnt sich ein Blick darauf, welche Informationen von welchen Usern abgerufen werden können.

4/ Kommentarspalten schließen

- Wenn eine Moderation durch zu hohes Kommentaraufkommen verunmöglicht wird, sollten Kommentarbereiche geschlossen werden. Einen Hinweis auf den Grund der Abschaltung kann zum Beispiel im aktuellsten Post ergänzt werden.

5/ Sensibilisierung für Social Engineering

- Ein - unaufgeregter - Hinweis an Mitarbeitende und ggf. auch deren Umfeld bezüglich der Möglichkeit von Social-Engineering-Versuchen kann bei der Abwehr helfen.

Monitoring im Notfall

Zunächst sollte die vorgefertigte Keywordliste (siehe „Präventive Maßnahmen“) wenn nötig um Begriffe oder Namen, die im Kontext der aktuellen Kampagne relevant sind, ergänzt werden. Diese Begriffe können für Suchen auf verschiedenen Plattformen genutzt werden:

X/Twitter

- Auf X können alle Suchbegriffe in einer Suchanfrage verwendet werden. Eine Suchanfrage sieht dann so aus: „Keyword1“ OR „Keyword2“ OR „Vorname1 Nachname1“ OR „Vorname2 Nachname“
- Wichtig: Man sollte auf der Ergebnisseite immer auf „Latest“ klicken, um sich alle aktuellen Posts anzeigen zu lassen.
- Eine einmal eingegebene Suche kann als URL aus dem Adressfeld des Browsers kopiert und in die Keywordliste oder ein anderes Dokument kopiert werden. Für das oben aufgeführte Beispiel sähe das folgendermaßen aus: https://x.com/search?q=Keyword1%E2%80%9C%20OR%20%20%E2%80%9EKeyword2%E2%80%9C%20OR%20%E2%80%9EVorname1%20Nachname1%E2%80%9C%20OR%20%E2%80%9EVorname2%20Nachname%E2%80%9C&src=typed_query&f=live
- Es ist außerdem möglich, sich nur Posts anzeigen zu lassen, die ein Minimum an Likes oder Reposts aufweisen. Dazu lässt sich die Suche für Likes um min_faves=50 (oder eine beliebige Zahl) und für Reposts um min_retweets=50 (oder eine beliebige Zahl) ergänzen.

YouTube

Zwei Wege eignen sich zur Suche von YouTube-Videos:

- Zunächst lohnt es sich, die Keywords auf YouTube selbst zu suchen. Wichtig ist dabei, bei den Suchergebnissen oben rechts auf „Filter“ und dann unter „Sortieren nach“ den Punkt „Uploaddatum“ auszuwählen, um sich die neuesten Ergebnisse anzeigen zu lassen
- Außerdem können Suchergebnisse via Google gesucht werden. Hierzu lautet die Suche dann: site:youtube.com „Keyword1“ OR „Keyword2“. Wichtig ist auch hier die richtige Sortierung. Dazu klickt man auf „Suchfilter“ und wählt unter „Beliebige Zeit“ den gewünschten Zeitraum aus. Wenn gerade ein Großangriff läuft, sollte die Wahl auf einen Zeitraum zwischen der letzten Stunde und der letzten Woche fallen.

Andere Plattformen

Auch auf TikTok, Instagram und Facebook können Keywords gesucht werden. Die Suchergebnisse schließen allerdings häufig nicht sämtliche Posts zum Keyword ein und sind nicht immer transparent sortiert oder eingrenzbar.

2.16 Self-Doxing

Beim Self-Doxing handelt es sich um eine Sammlung präventiver Maßnahmen, die dabei helfen, künftige Doxings zu verhindern. Dazu werden verschiedene Suchanfragen ausgeführt, um zu testen, welche Informationen online zur eigenen Person verfügbar sind.
Alle Mitarbeitenden sollten diese Maßnahmen in regelmäßigen Abständen selbst durchführen, um mögliche neue Suchergebnisse rechtzeitig identifizieren zu können. Auch neue Mitarbeitende sollten ein Self-Doxing durchführen. Da diese Maßnahmen auch Suchergebnisse beinhalten können, die Mitarbeitende nicht zwingend mit ihrem Arbeitgeber teilen möchten, sollten sie diese jeweils für sich selbst durchführen. Die Organisation sollte dann benachrichtigt werden, wenn beim Self-Doxing Ergebnisse auftreten, die für die Organisation relevant sein könnten.

1/ Suchmaschinen

Im ersten Schritt sollten relevante Suchbegriffe zur eigenen Person aufgeschrieben und auf unterschiedlichen Suchmaschinen (zum Beispiel Google, Yandex und Bing) gesucht werden. Da jede Suchmaschine unterschiedlich funktioniert, können die Suchergebnisse sich jeweils erheblich unterscheiden. Beispiele für Suchbegriffe sind:

- Der Name in Varianten
  - “Vorname Nachname“ (wenn es sich um einen Namen handelt, der sehr häufig vorkommt, sollte hier noch ein weiterer Begriff zur Eingrenzung der Suchergebnisse genutzt werden, beispielsweise der Wohnort=
  - “Vorname zweiter Vorname Nachname”
- Die private Anschrift
  - “Musterstraße 12”
  - “Musterstr 12”
  - “Musterstr. 12”
- “Mailadresse”
- Telefonnummer

Man kann außerdem nach veralteten Informationen suchen, die nicht mehr aktuell sind. Dazu gehören zum Beispiel veraltete Mail-Adressen oder Usernamen, die nicht mehr benutzt werden. Außerdem sollten bei der Suche nach dem Namen zudem die Ergebnisse aus der Bildersuche überprüft werden.
Sollten Suchergebnisse angezeigt werden, die sensible Daten oder Fotos enthalten, deren Veröffentlichung nicht zugestimmt wurde, kann der Ausschluss dieser Ergebnisse aus der Suche beantragt werden (siehe „Suchergebnisse entfernen“).

2/ Bildersuchen

Bildersuchen helfen, ggf. Doxings oder beleidigende Inhalte zu identifizieren. Dabei gibt es verschiedene Suchmöglichkeiten.

Bilderrückwärtssuchen

Bilderrückwärtssuchen erfüllen im Grunde zwei Funktionen: Sie suchen zum einen Uploads desselben Fotos auf verschiedenen Websites und zum anderen nach optisch ähnlichen Fotos. Dazu lädt man ein Bild von sich auf Suchmaschinen wie Google, Bing und Yandex hoch und untersucht die Suchergebnisse nach möglichen problematischen Uploads.

Wichtig: Google hat die Rückwärtsbildersuche für Gesichter inzwischen weitestgehend eingeschränkt. Daher sollte man in jedem Fall auch weitere Suchmaschinen konsultieren.

Die Browsererweiterung „Search by Image“ für Chrome und Firefox ermöglicht die gleichzeitige Suche eines Bildes auf mehreren Suchmaschinen.

Gesichtserkennungstools

Rechtsextreme Aktivisten nutzen zunehmend auch KI-Gesichtserkennungstools wie Pimeyes, um an Informationen zu kommen. Pimeyes sucht per Gesichtserkennung nach Suchergebnissen und erzielt in der Regel deutlich mehr Suchergebnisse als herkömmliche Suchmaschinen (außer der oder die Suchende ist selbst nicht online unterwegs und nicht auf irgendwelchen öffentlich einsehbaren Fotos von Veranstaltungen, Versammlungen oder Accounts von Familienmitgliedern abgebildet).
Pimeyes ist in allen wichtigen Funktionen kostenpflichtig im monatlichen Abonnement. Es lohnt sich daher, eine sinnvolle Lösung für einen solchen Account zu finden.

Wichtig: Pimeyes könnte hochgeladene Fotos auch dazu nutzen, die eigene Technik zu verbessern. Ein Upload eines Fotos sollte deshalb allen freigestellt sein.

Es ist möglich, sich selbst aus den Suchergebnissen von Pimeyes auszuschließen (das Formular ist hier zu finden). Dazu muss man ein eigenes Foto und ein Foto des Personalausweises oder anderen Dokuments hochladen. Damit werden anderen Usern künftig keine Suchergebnisse angezeigt. Allerdings kann es sich lohnen, die Suche vor diesem Schritt wenigstens einmal durchzuführen, um mögliche relevante Ergebnisse zu identifizieren.

Metadaten überprüfen

Smartphones und viele Kameras speichern beim Fotografieren und Filmen Metadaten. Diese bieten unter anderem Aufschluss darüber, wo ein Foto aufgenommen wurde. Social-Media-Plattformen wie Instagram, Facebook und TikTok entfernen diese Metadaten beim Upload, auch bei WhatsApp werden sie entfernt. Betreibt man allerdings einen eigenen Blog oder eine eigene Website, haben hochgeladene Fotos gegebenenfalls noch alle Metadaten und können Aufschluss über den Ort der Aufnahme und damit vielleicht die Büroadresse oder die eigene Anschrift geben.

Fotos, die online abrufbar sind, können mit einem Tool wie https://www.metadata2go.com/ überprüft werden. Das Tool kann außerdem Metadaten von Fotos und Videos entfernen, damit bei künftigen Uploads auf der privaten Website oder der Organisationsseite keine Metadaten abgerufen werden können.

3/ Web-Archive

Selbst wenn eine Website nicht mehr im Netz ist, ist es möglich, dass noch archivierte Versionen davon abrufbar sind. Dazu sollten relevante Keywords wie Name, Mailadresse und Adresse in den gängigen Web-Archiven gesucht werden. Die wichtigsten Archive sind:

- web.archive.org
- archive.is

Wenn man zum Beispiel nach alten Tweets suchen möchte, kann man auf beiden Seiten mit dem Suchoperator * suchen, der als Platzhalter funktioniert. Ein Beispiel für eine solche Suche wäre: www.twitter.com/username/*. Auch nach alten, nicht mehr verfügbaren Websites und Unterseiten kann man auf diese Weise suchen: www.websitename.de/*

4/ Datenleaks suchen

Online-Shops, Social-Media-Plattformen oder Apps, bei denen man sich mit Mail/Nutzernamen und Passwort anmelden muss, fallen regelmäßig Hackerangriffen zum Opfer. Dann werden Daten von Nutzenden, wie die Mail-Adresse, teilweise auch Anschriften, Telefonnummern, Konto- und Kreditkartendaten oder Passwörter veröffentlicht. Rechtsextreme nutzen solche Dienste zunehmend, um Zugang zu privaten Informationen zu erhalten.

Es gibt mehrere Tools, die man nutzen kann, um zu überprüfen, ob die eigenen Daten in solchen Leaks veröffentlicht wurden. Der bekannteste kostenlose Dienst ist **Have I Been Pwned.**
Dort kann man die eigene Mailadresse (oder mehrere Mailadressen) angeben und überprüfen, ob und in welchen Datensätzen sie auftaucht. Bei allen diesen Diensten sollten die Passwörter, falls noch nicht geschehen, schnellstmöglich geändert werden. Falls dasselbe Passwort außerdem für andere Websites oder Apps genutzt wurde, sollten auch diese Passwörter geändert werden.

2.17 Beratungsangebote

Bei rechtsextremen Angriffen helfen Beratungsorganisationen, die sich auf die Unterstützung bei rechtsextremen, verschwörungsideologischen, rassistischen oder antisemitischen Angriffen spezialisiert haben. Diese Organisationen kennen sich zudem häufig gut mit lokalen Akteuren und ihren Netzwerken aus.

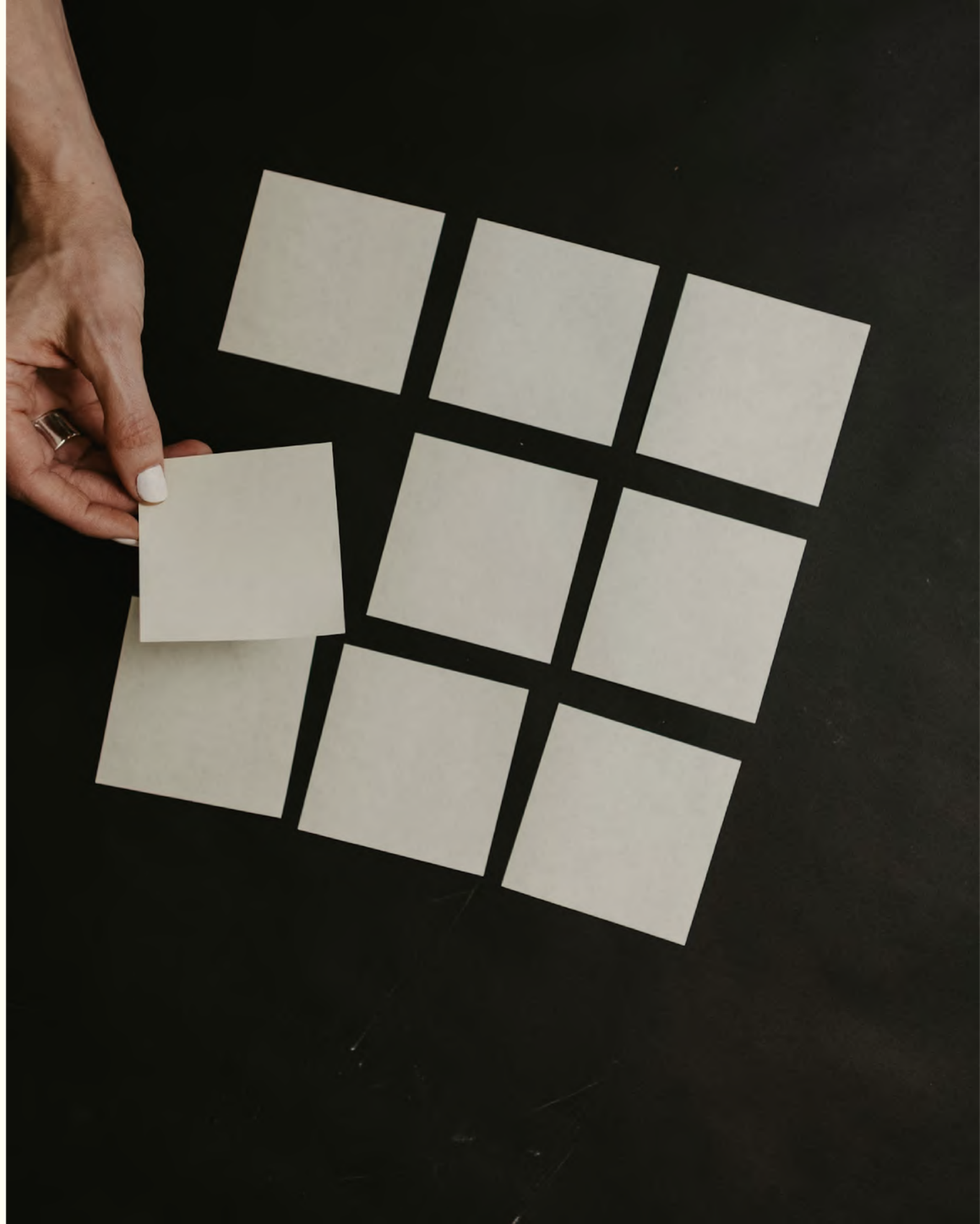
Der Verband der Beratungsstellen für Betroffene rechter, rassistischer und antisemitischer Gewalt führt eine **Liste von Beratungsstellen in allen Bundesländern**.

Außerdem unterstützt auch die Organisation **HateAid** bei rechtlichen Fragen.

Weitere nützliche Ressourcen

Ratgeber der Amadeu Antonio Stiftung - Social Media-Tipps für die Zivilgesellschaft

HateAid Initiative Gegenrechtsschutz - Beratung bei Rechtsmissbrauch



KOMMUNIKATIONS-EMPFEHLUNGEN

Bei Angriffen effektiv kommunizieren

3 Kommunikationsempfehlungen

Angriffe gegen gemeinwohlorientierte Organisationen sind längst kein Randphänomen mehr. Parlamentarische Anfragen, mediale Kampagnen, gezielte Desinformation, persönliche Angriffe auf Mitarbeitende und Versuche der politischen Instrumentalisierung gehören für viele Organisationen inzwischen zum Alltag.
Was dabei oft als „Kritik“, „Transparenzforderung“ oder „journalistische Recherche“ daherkommt, folgt in Wirklichkeit einer klaren politischen Logik: Zivilgesellschaft soll delegitimiert, verunsichert und langfristig geschwächt werden.

Diese Angriffe zielen nicht primär auf einzelne Projekte oder Förderprogramme ab. Sie sollen bewirken, dass die Einflussnahme von Zivilgesellschaft insgesamt eingeschränkt wird. Sie stellen in Frage, ob gemeinwohlorientiertes Engagement legitim ist, ob Zivilgesellschaft sich „einmischen“ und ob sie Haltung zeigen und sich für eine wehrhafte Demokratie einsetzen darf. Genau hier liegt der eigentliche Konflikt: **Es geht um die Deutungshoheit darüber, was Demokratie bedeutet – und wer sie gestalten darf.**

Viele Organisationen reagieren darauf verständlicherweise mit Erklärungen, Rechtfertigungen und dem Versuch, Vorwürfe sachlich zu entkräften. Doch rein reaktive Maßnahmen greifen zu kurz und lassen nur begrenzt zu, dass die Kommunikation effektiv gestaltet werden kann. Dieses Kapitel setzt genau hier an. Es verbindet politische Einordnung, kommunikative Haltung und praktische Handlungsfähigkeit.

Denn Angriffe zielen auf Vereinzelung, Verunsicherung und Erschöpfung. Eine wirksame Antwort setzt auf Klarheit, Zusammenhalt und strategische Kommunikation. Sie hält den Fokus nicht auf den Vorwürfen, sondern auf dem, was auf dem Spiel steht: demokratische Resilienz, gesellschaftlicher Zusammenhalt und das Recht, sich für Gemeinwohl, Menschenrechte, Umwelt, Teilhabe und Gerechtigkeit einzusetzen.

Die folgenden Abschnitte bieten dafür einen Werkzeugkasten: von der inneren Haltung über konkrete Sprachbausteine, von der Reaktion auf Anfragen und Kampagnen bis zur Mobilisierung der eigenen Community und dem Aufbau von Allianzen. Ziel ist nicht, auf jede Attacke zu antworten. **Ziel ist, handlungsfähig zu bleiben, Deutungshoheit zu behalten und sichtbar zu machen, dass Einschüchterung nicht wirkt.**

Haltung zeigen,
Deutungshoheit behalten,
handlungsfähig bleiben.

3.1 Eigene Narrative setzen

Beim Der Name deiner Organisation findet sich in einer parlamentarischen Anfrage der Opposition wieder? Du erhältst unerwartet einen Fragenkatalog von einer pseudojournalistischen oder medienaktivistischen Plattform und sollst Stellung beziehen? Ein Programm, über das deine Organisation Förderung bezieht, steht plötzlich in der Kritik, einseitige politische Einflussnahme zu betreiben? In diesen Fällen ist adäquates Reagieren, das Haltung und Selbstbewusstsein ausdrückt, äußerst wertvoll.

Wer sich von solchen Angriffen in die Defensive und damit in eine ungünstige Rechtfertigungsposition drängen lässt, hat schon einen Teil des Konflikts verloren. Besser ist es, die Problembeschreibung und Deutungshoheit des Angreifers gar nicht erst zu übernehmen.

Stattdessen braucht es eine klare Haltung: **Zivilgesellschaft ist demokratische Infrastruktur, sie ist gesetzlich legitimiert, auf das Gemeinwohl ausgerichtet, gesellschaftlich unverzichtbar und Ausdruck gelebter Grundrechte.** Angriffe entlarven sich so als Angriffe auf die Demokratie selbst – und nicht als legitime Kritik an Organisationen, Projekten oder Personen. Haltung bedeutet, den eigenen normativen Anspruch zu betonen, anstatt sich in eine Rechtfertigung zu verlieren, die vom eigentlichen Konflikt ablenkt. Konternarrative und Perspektivwechsel können ebenfalls eingesetzt werden, um die destruktiven Strategien demokratiefeindlicher Akteure klar zu entlarven.

Der eigentliche Konflikt dreht sich darum, dass von rechtsaußen Anspruch auf die Deutungshoheit demokratischen Engagements erhoben wird und Organisationen systematisch geschwächt und delegitimiert werden sollen, die teils über Jahrzehnte unverzichtbare Beiträge für die Erfüllung der freiheitlich demokratischen Grundordnung geleistet haben. Extrem rechte Akteure versuchen, diesen Konflikt zu verschleiern. **Kurz gesagt: Der eigentliche Konflikt ist der zwischen demokratischer Resilienz und autoritärer Unterwanderung.**

Checkliste: Haltung statt Rechtfertigung

1/ Framing nicht übernehmen

Übernimm rechtspopulistische Labels, Unterstellungen und Deutungen nicht in deiner Kommunikation — auch nicht, um diese zu verneinen oder zu widerlegen.

2/ Demokratische Rolle betonen

Zivilgesellschaft ist keine Lobby, sondern Teil der demokratischen Grundordnung und gesetzlich abgesichert.

3/ Positive Selbstbeschreibung wählen

Spreche über „Infrastruktur“, „Zusammenhalt“, „Engagement“, „Verantwortung“ – nicht über Abwehr von Vorwürfen.

4/ Angriff entlarven

Mach sichtbar, dass es der Gegenseite nicht um Aufklärung oder Transparenz geht, sondern um Einschüchterung und Delegitimierung nach autoritärem Muster.

5/ Normative Stärke zeigen

Haltung heißt, einstehen für Grundrechte, Gemeinwohlorientierung, Teilhabe und Resilienz – und das ist nicht verhandelbar.

Konter-Narrative

In den meisten Fällen ist die Anti-NGO Argumentation der Gegenseite empirisch kaum haltbar, oder sie verwendet bewusst strategische Verkürzungen. So sollen unbequeme Stimmen mundtot gemacht oder zur Bedrohung stilisiert werden, während beispielsweise wirtschafts- und politiknahe Akteure und Lobbygruppen unerwähnt bleiben.

Nachfolgend sind einige Narrative aufgeführt, die sich gezielt entkräften lassen.

Vorwurf: „NGOs verschwenden unser Steuergeld."
Antwort: Zivilgesellschaft spart dem Staat Milliarden, weil Millionen Menschen ehrenamtlich Verantwortung übernehmen. Jeder Euro wirkt mehrfach zurück in die Gesellschaft.
Fakt: In Deutschland engagieren sich rund 29 Millionen Menschen freiwillig und unentgeltlich für das Gemeinwohl, das ist jeder Vierte ab 14 Jahren.

Vorwurf: „NGOs sind linke Lobbygruppen."
Antwort: Unter den über 660.000 Organisationen in Deutschland gibt es eine Vielfalt an politischen Orientierungen, von konservativ bis progressiv.
Fakt: Eingetragene Vereine machen 94 Prozent der zivilgesellschaftlichen Organisationen in Deutschland aus. Am liebsten organisieren sich die Deutschen in Sportvereinen mit über 25 Millionen Aktiven.

Vorwurf: „NGOs sind keine rechtlich oder institutionell anerkannten Akteure."
Antwort: Zivilgesellschaftliche Organisationen sind rechtlich klar verankert. Sie agieren auf Basis des Vereins-, Stiftungs- oder Gemeinnützigkeitsrechts und unterliegen denselben Transparenz- und Rechenschaftspflichten wie andere juristische Personen.
Fakt: Eingetragene Vereine, Stiftungen und GmbHGs sind nach deutschem Recht rechtsfähige Organisationen.

Vorwurf: „Zivilgesellschaftliche Organisationen haben zu viel Macht."
Antwort: Gemeinwohlorientierte Akteure haben keine Gesetzgebungsmacht. Sie bringen Expertise und Stimmen in den Diskurs ein, die sonst oft ungehört bleiben.
Fakt: NGOs dürfen keine verbindlichen Entscheidungen treffen. Ihre Einflussnahme erfolgt ausschließlich über öffentliche Debatten, Kampagnen oder Anhörungen.

Vorwurf: „Profit und Selbstbereicherung stehen bei NGOs im Vordergrund."
Antwort: Die Arbeit in diesem Sektor ist oft prekär, Gehälter sind gering. Die Finanzierung erfolgt überwiegend durch Mitgliedsbeiträge und Spenden.
Fakt: Berichte zeigen, dass Gehälter im Non-Profit Sektor deutlich unter denen in gewinnorientierten Unternehmen liegen und sich NGOs finanziell vor allem auf Spenden, Mitgliedsbeiträge und Stiftungsförderungen stützen.

Vorwurf: „NGOs arbeiten intransparent."
Antwort: Zivilgesellschaftliche Organisationen unterliegen strengen Nachweispflichten. Viele setzen freiwillig auf Transparenzinitiativen.
Fakt: Seit 2022 müssen sich viele zivilgesellschaftliche Organisationen, die regelmäßig Lobbyarbeit betreiben, in ein Lobbyregister eintragen und dort unter anderem Lobbyaktivitäten, finanzielle Aufwendungen und größere Spenden offenlegen, was die bestehenden Transparenzpflichten deutlich stärkt.

Vorwurf: „NGOs betreiben Zensur und Cancel Culture."
Antwort: Kritik an Diskriminierung ist keine Zensur, sondern ein elementarer Bestandteil der demokratischen Gegenrede.
Fakt: Mit Zensur ist die Kontrolle oder das Verbot von Meinungen durch Akteure, die über Kommunikationsräume bestimmen, gemeint. Kritische Gegenrede, das was NGOs betreiben, ist Teil der geschützten Meinungsfreiheit.

Vorwurf: „Umwelt-NGOs vertreten nur eigene Interessen, die die Bürgerinnen und Bürger nicht mittragen.“

Antwort: Bestrebungen zum Umwelt- und Klimaschutz genießen breite Unterstützung in der deutschen Bevölkerung.

Fakt: Für den Natur- und Umweltschutz setzen sich in Deutschland über 16 Millionen Menschen ehrenamtlich ein. Große Umweltverbände wie NABU, BUND oder Greenpeace verzeichnen jeweils deutlich mehr Mitglieder bzw. Förderer als die mitgliederstärksten Parteien des demokratischen Spektrums.

Die **Maecenata Stiftung** hat in einer Studie näher beleuchtet, wie gezielte Narrative die Arbeit der Zivilgesellschaft delegitimieren und warum uns das alle angeht. Die Studie kann hier eingesehen werden:

https://www.maecenata.eu/2025/09/10/das-anti-ngo-narrativ-wie-versucht-wird-die-zivilgesellschaft-zu-delegimitieren/

Perspektivwechsel

Neben Haltung und Konter-Narrativen ist es entscheidend, einen kommunikativen Perspektivwechsel zu unternehmen, denn Angriffe auf die Zivilgesellschaft sind keine Aneinanderreihung von Einzelfällen oder zugespitzten Nachfragen. Sie sind Ausdruck einer systematischen Strategie. Wer nur auf einzelne Vorwürfe reagiert, bleibt im Takt des Gegners. Wer den Blick weitet, deckt die dahinter liegenden Muster, Interessen und Zielsetzungen auf und gewinnt Deutungshoheit zurück.

Perspektivwechsel bedeutet, nicht länger über die Vorwürfe der Gegenseite zu sprechen. Es bedeutet, die Frage nicht zu beantworten, *ob* eine Organisation legitim ist, sondern sichtbar zu machen, *warum* sie angegriffen wird. Nicht Rechtfertigung, sondern Einordnung. Nicht Verteidigung, sondern Entlarvung. Ein Perspektivwechsel verschiebt damit die kommunikative Logik weg von der Frage „Stimmt der Vorwurf?“ hin zur Frage „Welche Strategie steckt dahinter?“. Damit rückt die Kommunikation weg von der Selbstbeschreibung und hin zur politischen Einordnung des Angreifers.

Als einfache Anleitung gilt:
Taktik enttarnen – Muster aufzeigen – Verantwortung markieren

→ Die folgenden Beispiele sollen als Inspiration und Anleitung für die eigene Kommunikation dienen. Sie fokussieren sich auf die AfD als Hauptakteur der Angriffe gegen die Zivilgesellschaft. Es ist anzuerkennen und von der Maecenata Stiftung bewiesen, dass die CDU-Fraktion mit ihren 551 Fragen eine Negativ-Lawine in der Berichterstattung über NGOs losgetreten hat, und dass auch andere Parteien (etwa auf Landtagsebene) zivilgesellschaftliche Organisationen unter Druck setzen. In ihrer Fülle und Systematik ist die AfD jedoch mit keiner anderen Partei vergleichbar.

Kleine Anfragen der AfD

Taktik enttarnen

Die AfD nutzt Scheintransparenz, um Angst zu verbreiten. Wer den Regierungen auf Landes- und Bundesebene so viele Anfragen in so kurzer Zeit stellt, hat mit parlamentarischer Kontrolle nichts am Hut – es ist eine organisierte Einschüchterungskampagne.

Muster aufzeigen

Die AfD hat eigens eine Arbeitsgruppe gebildet, um Vereine und Initiativen mit Anfragen und Klagen systematisch unter Druck zu setzen.

Verantwortung markieren

Wenn Kräfte der politischen Mitte diese Taktik übernehmen, machen sie sich zum Spielball der AfD. Wer unsere Demokratie stärken will, muss unsere Zivilgesellschaft verteidigen.

Internationales Playbook / AfD erfindet nichts selbst

Taktik enttarnen

Die AfD hat eigens Arbeitsgruppen gebildet, um Vereine und Initiativen mit Anfragen und Klagen systematisch unter Druck zu setzen. Damit erfindet die AfD nichts Neues.

Muster aufzeigen

Das ist Teil eines internationalen Playbooks. Die AfD kopiert Strategien von Orbán, Trump und Co: Zuerst Zweifel säen, dann Mittel kürzen, am Ende Strukturen zerstören. Wer diese Muster kennt, erkennt sofort, was hier bezweckt wird: Die Abschaffung etablierter Träger, die wirtschaftsliberalen Interessen Paroli bieten.

Verantwortung markieren

Bund und Länder haben die Pflicht, gemeinwohlorientiertes Engagement im Sinne einer wehrhaften Demokratie zu verteidigen. Einmal verlorengegangene Strukturen sind schwer wieder aufzubauen, wie Entwicklungen in anderen Ländern beweisen.

Verschwendung von Steuergeldern? Garantiert durch die AfD.

Taktik enttarnen

Die AfD stellt endlose Fragen zur Arbeit der Zivilgesellschaft.

Muster aufzeigen

Während also Ehrenamtliche Millionen Stunden von gemeinnütziger Arbeit leisten, gibt die AfD unser Steuergeld aus, um genau diese Menschen zu drangsalieren.

Verantwortung markieren

Das ist kein Dienst an den Bürgerinnen und Bürgern, sondern eine Veruntreuung öffentlicher Mittel für parteipolitische Zwecke. Die AfD muss zu ihrer Mittelverwendung Rechenschaft ablegen.

Attacke auf den Kern der Gesellschaft

Taktik enttarnen

Die AfD versucht, die Lebensadern der Gesellschaft anzugreifen: Sozialdienste, Unterstützung für die Schwächsten, Umweltschutzbestrebungen, Jugend- und Bildungsarbeit, Kulturinitiativen.

Muster aufzeigen

So wird Misstrauen gegenüber elementar wichtigen Strukturen gesät und Dauerempörung ausgelöst statt Lösungen angeboten.

Verantwortung markieren

Wo bleiben die Antworten auf die echten Probleme in Krankenhäusern und Bildungseinrichtungen, beim Klimaschutz oder im ländlichen Raum? Diese Anfragen sind keine Aufklärung, sondern Ablenkung vom eigenen Versagen.

Neutralitätsanspruch an die Zivilgesellschaft

Taktik enttarnen

Rechtspopulistische Akteure behaupten, zivilgesellschaftliche Organisationen müssten sich „politisch neutral“ verhalten – und unterstellen ihnen bei jeder klaren Haltung einen Verstoß gegen dieses angebliche Neutralitätsgebot.

Muster aufzeigen

Diese Forderung ist gezielt irreführend. Es gilt kein Neutralitätsgebot, sondern ein Demokratiegebot. Zivilgesellschaft ist nicht dazu da, wertfrei neben Menschenfeindlichkeit, Rassismus, Umweltsünden oder Bevorteilung zu stehen. Sie ist Ausdruck von Grundrechten, von Meinungsfreiheit, Vereinigungsfreiheit und gesellschaftlicher Teilhabe.

Verantwortung markieren

Akteure in Politik, Verwaltung und Förderpraxis müssen klarstellen: Eine demokratische Gesellschaft ist nicht neutral. Menschenwürde, Grundrechte und Vielfalt sind nicht verhandelbar. Vereine und zivilgesellschaftliche Organisationen haben nicht nur das Recht, sondern die Verantwortung, sich an diesen Prinzipien auszurichten und sie zu verteidigen.

3.2 Prävention und Vorbereitung

Gezielte Desinformationskampagnen, parlamentarische Anfragen oder mediale Angriffe können jede Organisation treffen – unabhängig von Größe oder Bekanntheit. Auch wenn ihr bislang verschont geblieben seid, ist es wichtig, vorbereitet zu sein: Die Zahl der Angriffe auf zivilgesellschaftliche Akteure steigt stetig.
Ein klarer Notfallplan hilft, im Ernstfall handlungsfähig zu bleiben – ohne erst in der Krise entscheiden zu müssen, wer spricht, wer handelt und wann Schweigen die bessere Strategie ist. Überlegt im Vorfeld, wo eure roten Linien liegen – also, wann ihr reagieren wollt oder müsst, und wann bewusst nicht.

Ein guter Plan gibt euch Orientierung in fünf Punkten:

- ☐ **Klare Zuständigkeiten:** Wer entscheidet, wer spricht, wer dokumentiert - intern und extern.
- ☐ **Schnelle Kommunikationswege:** Welche Kanäle werden genutzt (Telefon, Signal, E-Mail).
- ☐ **Abgestimmte Botschaften:** Eine Stimme nach außen, kein Durcheinander.
- ☐ **Sicherheit & Fürsorge:** Schutz für betroffene Personen und euer Team.
- ☐ **Reflexion:** Nach der Krise: Was lief gut? Was kann verbessert werden?

Ein Beispiel für einen Krisenplan findet sich im Annex.

3.3 Anfragen von Alternativmedien

Viele Organisationen sahen sich in jüngster Vergangenheit der folgenden Situation ausgesetzt: Plötzlich landet ein umfangreicher Fragenkatalog von *NiUS* mit extrem kurzer Fristsetzung in der Inbox – erkennbar mit dem Ziel, den Verein und seine Arbeit in ein schlechtes Licht zu rücken.

Die Kombination aus Detailfragen und Zeitdruck zeigt, dass es hier nicht um Aufklärung, sondern um das Sammeln von Material für Angriffe und Diffamierung geht. Das Einzelbeispiel einer Organisation bedient lediglich das größere bereits vorgefertigte Narrativ der Gegenseite.

Die empfohlene Antwort in solchen Fällen ist: **nicht reagieren**. Es handelt sich hier nicht um seriöse journalistische Recherche - die bisher veröffentlichten Beiträge von Plattformen wie NiUS, Apollo, Compact und Co machen deutlich, dass es sich um politische Kampagnen handelt (siehe auch **Umgang mit Medienaktivisten**).

Parallel sollte intern das Team vorbereitet werden: mit Monitoring kann überprüft werden, wie die Berichterstattung verläuft und ob andere Medien das Thema aufgreifen. Eine einheitliche Sprachregelung (FAQ) sollte festgelegt werden für mögliche Nachfragen.

Erfahrungen zeigen, dass diese Angriffe meist auf die eigenen Kanäle der Angreifer beschränkt bleiben und nur selten größere Resonanz entfalten, obwohl sich das auch aktuell ändert. Ihre Wirkung entsteht vor allem durch Verunsicherung – dem lässt sich durch Ruhe, Geschlossenheit und Klarheit begegnen. Sollten seriöse Medien das Thema aufgreifen, ist es wichtig, aktiv zu werden → siehe **Großangriff**.

Empfehlungen für Organisationen:

- **Medium prüfen:** Handelt es sich um ein etabliertes bzw. seriöses Medium (Presserat kann hier helfen) oder ein Kampagnenportal wie *NiUS* oder *Compact*?
- **Monitoring einschalten:** Beobachte, ob und wie die Inhalte über rechtspopulistische Kanäle hinaus aufgegriffen werden.
- **Sprechfähigkeit intern sichern:** Einheitliche Sprachregelungen festlegen, klare Kernbotschaften vorbereiten, keine Rechtfertigungen, **Notfallplan** aktivieren.
- **Optional: Community informieren:** Deutlich machen, dass es sich um einen politischen Angriff handelt, der Teil eines bekannten rechtsextremen, illiberalen Playbooks ist.

3.4 Akuter Großangriff – wie reagieren?

Zu den wichtigsten Instrumenten der extremen Rechten gehört der mehr oder weniger organisierte kommunikative Großangriff. Häufig kommt hierfür der Begriff „Shitstorm“ zum Einsatz, der aber unzureichend zwischen ernsthafter Kritik, beispielsweise an Unternehmen, oder rechtsextremen Empörungskampagnen unterscheidet. Ein solcher Großangriff ist dadurch gekennzeichnet, dass Influencer, Medienaktivisten, Politiker und andere Akteure durch tage- oder wochenlange Skandalisierung Anfeindungen, Beleidigungen und Drohungen auslösen.

Ob und wann ihr öffentlich reagieren solltet, hängt stark von der Situation ab – ein Patentrezept gibt es nicht. Wichtig ist vor allem: Ruhe bewahren, die Lage beobachten und externe Einschätzungen einholen. Selbst erfahrene Personen können in der Dynamik eines Angriffes den Überblick verlieren. Ein Blick von außen hilft, aus dem Tunnel herauszukommen und die Tragweite realistischer einzuschätzen.

Grundregel: Keine Gegenkampagne aus Panik starten. Eine unüberlegte Reaktion kann eine kleine Welle erst groß machen. In manchen Fällen ist es besser, eine Attacke einfach auszusitzen. Wenn aber absehbar ist, dass ein Angriff langfristige Folgen haben könnte, sollte aktiv gegengesteuert werden – etwa wenn:

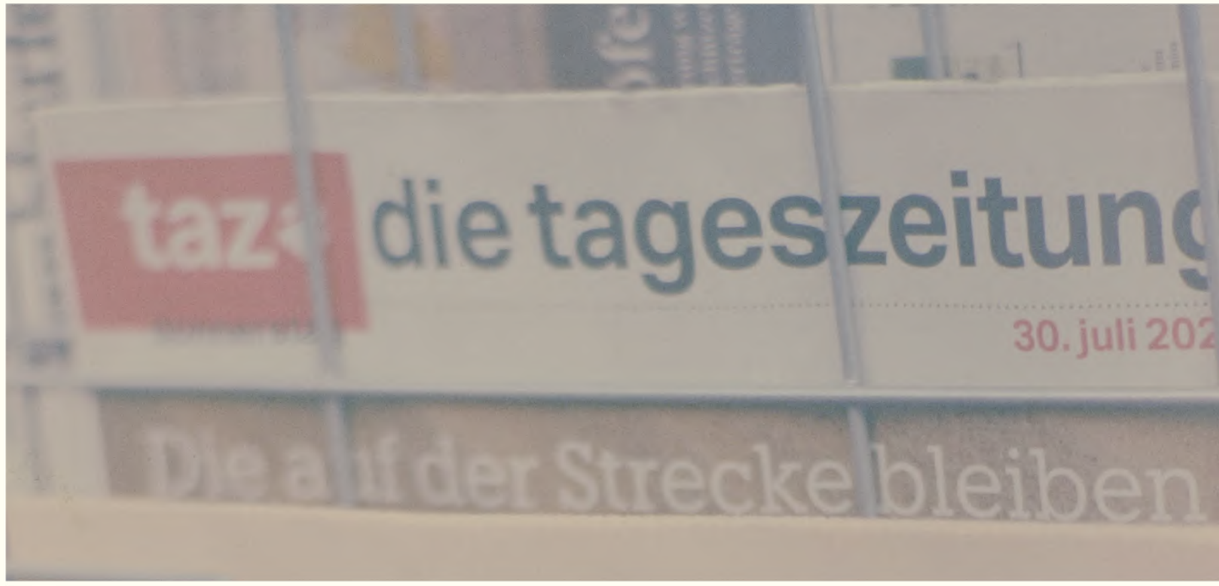
- Geldgeber*innen oder Partnerorganisationen sich verunsichert zeigen,
- euer Arbeitgeber direkt angegriffen wird (im Falle von Angriffen gegen Einzelpersonen), oder
- Berichterstattung in seriösen konservativen Medien (z. B. Welt, FAZ), die die Kampagne und die Frames der Angreifer übernehmen.

Beobachtet die Lage sorgfältig im Laufe des ersten Tages: Wie stark verbreitet sich die Kritik, wer teilt sie, und welche Akteure springen auf? Wenn sich die Situation zuspitzt, solltet ihr am Folgetag über eine öffentliche Reaktion entscheiden. Holt euch aber in jedem Fall Rat von außerhalb.

Wie reagieren? Proaktive Pressearbeit

Wenn ihr euch entschieden habt, zu reagieren, kann proaktive Pressearbeit eine wirkungsvolle Gegenstrategie sein: Sie hilft, Angriffe abzuwehren und gleichzeitig die eigene Arbeit und Haltung sichtbar zu machen. Eine gut platzierte Berichterstattung stärkt eure Glaubwürdigkeit und zeigt, dass ihr seriös arbeitet. Außerdem kann sie eure Community mobilisieren und Solidarität in der Öffentlichkeit fördern.

Wichtig dabei: Journalist:innen schreiben nicht automatisch eine Geschichte, nur weil ihr sie bittet. Für Journalist:innen wird es meist dann interessant, wenn ihr einen neuen Dreh oder eine größere Bedeutung anbieten könnt – etwa, wenn ihr ein Beispiel für eine größere Entwicklung seid oder eine orchestrierte Kampagne sichtbar machen könnt.
Entscheidend ist auch die Vernetzung: Es hilft, Kontakte zu Journalistinnen aufzubauen. Wenn ihr keine Kontakte habt, nutzt solidarische Kontakte: Wenn größere Accounts euch bereits unterstützt haben, könnt ihr sie bitten, Journalist:innen anzusprechen oder euch zu vernetzen.



Beispiele aus den letzten Jahren verdeutlichen, wie wirkungsvoll dieser Ansatz sein kann:

- **Amadeu Antonio Stiftung:** Nachdem eine Mitarbeiterin der Stiftung das rechtsextreme Hetzportal Apollo News öffentlich kritisiert hatte, erhielt sie Morddrohungen. Auch die FAZ griff zunächst die von Apollo News gesetzten Frames auf und trug so zur Eskalation bei. Durch aktive Pressearbeit gelang es der Amadeu Antonio Stiftung jedoch, ihre Perspektive in der taz und bei medidasres des Deutschlandfunks zu platzieren. Die dort erschienenen Beiträge, gestützt auf Screenshots und Stellungnahmen der Stiftung, setzen ein neues, faktenbasiertes Narrativ und korrigierten die einseitige Berichterstattung. Ein positiver Medienartikel ist auch wichtig, damit eure Kontakte ihn solidarisch in den sozialen Medien teilen können.
- **Pro Asyl:** Nach Angriffen durch rechte Medien und Unionspolitiker positionierte sich Geschäftsführer Karl Kopp in einem Interview mit der *taz* faktenbasiert und rechtsstaatlich („Wir lassen uns nicht einschüchtern“) und setzte so eigene Narrative.
- **CORRECTIV:** Nach einer massiven Gegenkampagne zur Potsdam-Recherche veröffentlichte CORRECTIV eine transparente FAQ-Seite zur eigenen Methodik, die Angriffslinien entkräftete und Vertrauen in die Arbeit stärkte.
- **Sea-Watch:** Standardvorwürfe gegen Seenotrettung werden seit Jahren in einem FAQ präzise beantwortet. Durch den Verweis auf internationale Rechtsnormen („Seenotrettung ist Pflicht“) setzt die Organisation einen klaren normativen Rahmen gegen rechte Narrative.
- **Zentrum ÜBERLEBEN, XENION und das Berliner Netzwerk BNS** haben eine Pressemitteilung veröffentlicht, in dem sie eine AfD-Anfrage öffentlich kritisieren, die ihre Arbeit mit traumatisierten Geflüchteten infrage stellte. Die Pressemitteilung entlarvt die Anfrage der AfD als gezielten Versuch der Diskreditierung und setzt diese direkt in einen größeren Kontext politischer Instrumentalisierung.

Empfehlungen für Organisationen

- FAQ und Stellungnahmen prominent auf Webseite und Social Media Seiten verlinken, um es für Journalist*innen einfach auffindbar zu machen.
- Kurze Q&A-Formate vorbereiten, um typische Angriffslinien strukturiert zu beantworten.
- Klare Kernbotschaften definieren und konsequent wiederholen, um ein konsistentes Bild zu vermitteln.
- Sprecher:innen im Vorfeld festlegen, die in Krisensituationen ansprechbar und medienerfahren sind.
- Wenn der Artikel über die Hasskampagne gegen euch online ist, dann fragt andere Organisationen und Accounts mit großer Followerzahl, den Artikel zu teilen im Sinne einer “Candy Shower” Solidarität mit euch zu zeigen.

Schau dir für mehr Inspiration auch die **Formulierungshilfen** für Anschreiben an Journalistinnen im Annex an. Wir haben eine **Candy-Storm Signalgruppe**. Schreib uns eine E-Mail info@zukunftdemokratie.org und wir laden dich ein.

Wie reagieren? Community einbeziehen

Rechtsextreme Angriffe zielen darauf, Organisationen zu isolieren und ihre Unterstützung im Umfeld zu schwächen. Wer in der Öffentlichkeit attackiert wird, soll sich allein fühlen und die eigene Community soll verunsichert oder demobilisiert werden. Genau deshalb ist es entscheidend, in solchen Momenten aktiv die eigene Community einzubeziehen. Sichtbare Solidarität und gemeinsames Handeln stärken nicht nur die Betroffenen, sondern senden auch ein starkes Signal nach außen: Wir lassen uns nicht spalten.

Organisationen können Angriffe gezielt nutzen, um Mitglieder, Unterstützer:innen und Verbündete zu mobilisieren, selbst aktiv zu werden - ob durch Spenden, Grußkarten verschicken oder Aufrufe teilen. Wenn die eigene Community versteht, dass Angriffe Teil einer politischen Strategie der Gegenseite sind, wächst das Bewusstsein und die Bereitschaft, gemeinsam zu reagieren, zeigen auch diese Beispiele:

- **Deutsche Umwelthilfe:** Die DUH adressiert gezielte Bedrohungen (inkl. Doxxing) offen, bittet um Unterstützung und verbindet das mit ihrer inhaltlichen Arbeit (Klagen für Klimaschutz).
- **Royal National Lifeboat Institution UK**: Die RNLI wurde zur Zielscheibe von Nigel Farage und anderen extremen Rechten, weil sie Migrant:innen aus dem Ärmelkanal rettet. Die Organisation ging in die Offensive und veröffentlichte ein Video, das ihre Arbeit selbstbewusst und emotional erklärte. Ergebnis: massive öffentliche Unterstützung und ein Spendenanstieg von rund 3000 Prozent.
- **SPD / Christian Ecke**: Nach der brutalen Attacke auf den Europaabgeordneten Matthias Ecke setzte sofort eine Welle der Solidarität ein und die SPD hat diese gut kommuniziert. Matthias Ecke erhielt über 8.000 persönliche Rückmeldungen – darunter unzählige Karten und Briefe. Diese massive, persönliche Unterstützung („Love-Shower“ oder “Candy Shower”) machte sichtbar: Die Betroffenen stehen nicht allein. Sie stärkte die Angegriffenen direkt, wirkte nach außen abschreckend und signalisierte gleichzeitig: Wer Einzelpersonen attackiert, greift die demokratische Gemeinschaft an.

Empfehlungen für Organisationen

- **Angriff als Chance begreifen**: Nutzt die Aufmerksamkeit, um neue Unterstützende zu gewinnen, eure Arbeit sichtbar zu machen und eure Community langfristig zu stärken. Angriffe sind auch Gelegenheiten, Haltung und Zusammenhalt öffentlich zu zeigen.
- **Playbook hinter Angriffen klarmachen:** Zeigen, dass Angriffe dieser Art keine Zufälle sind, sondern Teil einer gezielten Einschüchterungsstrategie rechtsextremer Akteure. Klar formulieren, was auf dem Spiel steht, für die Organisation, aber auch für demokratisches Engagement insgesamt.
- **Verbindung zur eigenen Arbeit herstellen**: Verknüpft eure Reaktion auf Angriffe mit eurer eigentlichen Mission. Zeigt, dass ihr euch durch Hass nicht einschüchtern lasst, sondern euer Engagement für [Thema einsetzen, z. B. Klimaschutz, Demokratie, Menschenrechte] fortsetzt.
- **Community aktivieren – mit klarem Call-to-Action**: Gebt eurer Community etwas zu tun: Spenden, solidarische Nachrichten, Social-Media-Unterstützung oder Teilen eurer Inhalte. So wird aus Empörung Handlung – und aus Ohnmacht Zusammenhalt.
- **Dringlichkeit klarmachen**: Eurem Publikum muss klar sein, warum es wichtig ist, dass es jetzt in diesem Moment etwas macht, zum Beispiel weil viel auf dem Spiel steht oder Spenden für juristische Maßnahmen gebraucht werden.
- **Dank und Sichtbarkeit:** Zeigt öffentlich Wertschätzung für Solidarität und Unterstützung. Das motiviert und stärkt eure Verbündeten – und sendet das Signal: Wir stehen zusammen.

Schau dir für mehr Inspiration auch die **Formulierungshilfen** für Community-Ansprache im Annex an.

Wie reagieren? Bande bilden

Angriffe gegen gemeinwohlorientierte Organisationen zielen darauf ab, zivilgesellschaftliche Akteure zu isolieren und sie ohne Rückhalt angreifbar zu machen. Umso wichtiger ist es, Allianzen zu bilden – mit anderen Initiativen, Vereinen, Netzwerken und lokalen Bündnissen. Gemeinsames Auftreten schafft Rückendeckung, geteilte Reichweite und Schutz, sowohl online als auch offline. Auch die Unterstützung durch Politik, Verwaltung oder prominente Stimmen kann entscheidend sein. Wer sich öffentlich an die Seite zivilgesellschaftlicher Akteure stellt, sendet ein klares Signal: **Angriffe auf eine Organisation sind Angriffe auf die demokratische Gemeinschaft insgesamt.**

- **“Dorfliebe für alle”**: Die Initiative wollte anfänglich einen AfD-Landrat verhindern und sah sich massivem Gegenwind (z.B. durch Freie Sachsen, Freies Thüringen) ausgesetzt. Parallel erreichte sie jedoch auch Rückenwind, durch Einladungen an Initiativen wie “Wir sind die Brandmauer” oder durch gemeinsame Auftritte auf CSDs. Auf Instagram zeigte sich Solidarität durch gemeinsame Posts: digitale Verstärkung des Zusammenhaltes.
- **Meißen**: Seit der Kommunalwahl 2024 hat sich die Stimmung in Meißen verschärft: Hass, Hetze und konkrete Drohungen, angeheizt durch den AfD-Stadtrat, führten zu Angriffen, Drohungen und finanziellen Kürzungen. Die Antwort darauf lautete enger Zusammenhalt, Solidarität über Vereinsgrenzen hinweg und neue Bündnisse, die öffentlich sichtbar machten: Wir lassen uns nicht einschränken.
- **Sachsen / Neulandgewinner**: Als die AfD im Landtag die Förderung des Programms Neulandgewinner stoppen wollte, mobilisierte die Initiative landlebtdoch Unterstützung, indem sie sich direkt an demokratische Abgeordnete wandte und öffentlich Rückendeckung einforderte. So entstand politische und öffentliche Solidarität, der Antrag wurde abgelehnt und das Programm fortgeführt. Ein Beispiel dafür, wie gezielte Kontakte zu Abgeordneten zivilgesellschaftlichen Initiativen Schutz und Rückhalt geben können.

Schau dir für mehr Inspiration auch die **Formulierungshilfen** für Ansprache an Verbündete und Abgeordnete im Annex an.

Wie reagieren: Kommunikation um juristisches Vorgehen

Es ist entscheidend, justiziable Angriffe auch vor Gericht zu bringen – und den juristischen Weg kommunikativ zu begleiten. Dabei gilt: Rechtliche Schritte sind auch eine Botschaft. Sie zeigen, dass Einschüchterung nicht hingenommen wird und dass demokratisches Engagement sich auf geltendes Recht stützt. Wichtig ist, Verfahren transparent und sachlich zu kommunizieren – etwa durch kurze Statements, Hintergrundinfos oder ein FAQ für Journalist:innen. So entsteht Vertrauen, und die Öffentlichkeit versteht, dass rechtliche Schritte keine Eskalation, sondern Verteidigung demokratischer Standards sind.

- **HateAid:** Nach falschen Behauptungen von NIUS erwirkte HateAid im September 2024 eine einstweilige Verfügung und kommunizierte das knapp, dokumentiert und ohne Polemik mit einem PDF-Pressestatement für Journalist:innen.
- **Mission Lifeline**: Die Seenotrettungs-NGO setzte rechtlich durch, dass nach Falschbehauptungen von NIUS Gegendarstellungen korrekt veröffentlicht werden müssen (Zwangsgeld/Androhung Zwangshaft; später bestätigt).

ANNEX & VORLAGEN

Beispiele für die Kommunikation

Notfallplan: Kommunikation bei Angriffen

1. Sofortmaßnahmen (innerhalb der ersten Stunden)

Ziel: Überblick gewinnen, Ruhe bewahren, Zuständigkeiten klären.

Monitoring starten:

- Überblick verschaffen: Wo wird über euch gesprochen (Social Media, Presse, Kommentare)?
- Screenshots sichern (auch gelöschte Posts, Drohungen etc.).
- Handelt es sich um vereinzelte Kritik, eine orchestrierte Kampagne oder gezielte Desinformation? Einschätzung von außen einholen!

Krisenteam aktivieren:

- Wer ist zuständig für:
  - Monitoring & Dokumentation
  - Presse & Öffentlichkeitsarbeit
  - Interne Kommunikation
  - Kontakt zu Partnern / Geldgebern / Jurist*innen
- Klare Kommunikationswege festlegen (Signal/Slack/Telefon)

Ruhe bewahren:

- Keine spontanen Posts oder Statements.
- Externe Einschätzung einholen (z. B. von Partnerorganisationen, Journalistinnen, Kommunikationsberaterinnen).

2. Lageeinschätzung (nach 6–12 Stunden)

Ziel: Entscheiden, ob und wie ihr reagiert.

Nicht reagieren, wenn:

- Es sich um kleinere, selbstlaufende Wellen handelt (ein paar Dutzend Kommentare).
- Kein Reputations- oder Sicherheitsrisiko besteht.
  Keine größeren Medien oder Multiplikatoren das Thema aufgreifen.

Reagieren, wenn:

- Qualitätsmedien oder Portale wie *NiUS* mehrfach berichten.
- Arbeitgeber, Partner oder Fördergeber angesprochen oder verunsichert werden.
- Die Kampagne finanzielle, rechtliche oder sicherheitsrelevante Folgen haben kann.

3. Kommunikationsstrategie (nach 12–24 Stunden)

Option 1 – Schweigen & Monitoring fortsetzen

- Wenn der Angriff abebbt oder keine Reichweite entwickelt.
- Signalisiert Souveränität und entzieht der Gegenseite Aufmerksamkeit.

Option 2 – Proaktive Reaktion

- Wenn ihr eigene Narrative setzen wollt oder euch schützen müsst.
- Wählt geeignete Formate:
  - Statement auf eurer Website
  - Interview oder Hintergrundgespräch mit vertrauenswürdigen Journalist*innen
  - Social Media Post, der klar benennt, warum die Angriffe agieren - eigenes Narrativ setzen!

Option 3 – Candy Storm organisieren

- Wenn ihr massiv angegriffen werdet: Solidarität aktivieren: Freundliche Organisationen, große linksliberale Accounts und Medienkontakte mobilisieren.
- Positive Botschaften posten lassen („Wir stehen hinter XY, weil…“).

Wichtig: Interne und Partnerkommunikation

Ziel: Vertrauen sichern, Team und Partner informieren.

Intern:

- Team kurz updaten: Was passiert, was tun wir, wer spricht nach außen?
- Belastete Personen schützen – ggf. Social Media pausieren, Unterstützung anbieten.

Extern:

- Enge Partner und Fördergeber früh informieren („Wir sind Ziel einer Kampagne, wir behalten Ruhe und prüfen die Lage.“).
- Wenn nötig: kurze, sachliche Mail an Unterstützer*innen oder Netzwerk.

4. Nachbereitung (nach 3–7 Tagen)

Ziel: Lernen und stärken.

Kurze interne Auswertung:

- Was hat funktioniert? Und wo müssen Abläufe oder Zuständigkeiten klarer werden?
- Krisen-Ordner aktualisieren (Kontaktliste, Mustertexte, Medienkontakte).
- Prüfen, ob Auskunftssperre oder digitale Sicherheitsmaßnahmen sinnvoll sind.
- Wenn nötig: kurze, sachliche Mail an Unterstützer*innen oder Netzwerk.

Anschreiben für Journalist*innen

Szenario 1: Angriff durch populistisches Meinungsportal

Sehr geehrte [Name],

derzeit läuft eine groß angelegte, orchestrierte Kampagne rechtsalternativer Medienportale – insbesondere von [Quelle/Plattform nennen] – gegen [eure Organisation/Mitarbeiter].

Seit Beginn der Kampagne erreichen uns täglich Hassnachrichten, Beleidigungen und Morddrohungen. Ziel ist es offenkundig, ein Exempel zu statuieren – um kritische zivilgesellschaftliche Stimmen einzuschüchtern und andere Akteur*innen davon abzuhalten, weiterhin öffentlich Haltung zu zeigen.

Wir sehen darin ein exemplarisches Beispiel für ein immer wiederkehrendes Muster: Orchestrierte Onlinekampagnen, die gezielt Empörung erzeugen, demokratische Organisationen delegitimieren und durch digitale Gewalt zum Schweigen bringen sollen. Auch [Beispiel nennen: der Fall Brosius-Gersdorf, jüngste Angriffe auf die Amadeu Antonio Stiftung oder HateAid] folgte einem ähnlichen Muster. Während derzeit vielfach über Angriffe auf zivilgesellschaftliches Engagement berichtet wird, wird zu selten beleuchtet, welche Akteure, Mechanismen und Netzwerke hinter solchen Angriffen stehen.

Gern stellen wir Ihnen dazu weiteres Material als Hintergrundinformation zur Verfügung:

- Screenshots von Hassnachrichten, Einschüchterungsversuchen und Morddrohungen (auf Anfrage)
- Aufnahmen der [Anlass: Veröffentlichung, Stellungnahme, Veranstaltung, etc.] die den Ausgangspunkt der Kampagne bildete
- Interviewmöglichkeiten mit betroffener Person / Politikexperten zur Einordnung / Geschäftsführung / Pressesprecher

Für Hintergrundgespräche, Interviews oder weiterführendes Material stehen wir gern zur Verfügung. Sie können mich auch gern telefonisch erreichen unter [+49 1234].

Mit freundlichen Grüßen

Szenario 2: Einordnung zum Neutralitätsvorwurf gegen zivilgesellschaftliche Organisationen

Sehr geehrte [Name],

aktuell wird gegenüber [Name der Organisation] öffentlich der Vorwurf erhoben, sie verstoße gegen ein angebliches Neutralitätsgebot. Als zivilgesellschaftliche Organisation, die selbst seit vielen Jahren im Bereich [z. B. Soziales / Umwelt / Bildung] tätig ist, möchten wir diese Darstellung klar einordnen.

Zivilgesellschaft ist nicht wertneutral, sondern verfassungsgebunden. Sie orientiert sich an Menschenwürde, Grundrechten und demokratischen Prinzipien. Das ist kein parteipolitisches Engagement, sondern demokratische Verantwortung.

Gerne stehen wir Ihnen für eine Einordnung zur Verfügung. Sie können uns dazu wie folgt zitieren:

„Eine demokratische Gesellschaft ist nicht neutral. Wer sich für Menschenwürde, Gleichwertigkeit und Zusammenhalt einsetzt, verstößt gegen kein Gebot, sondern erfüllt schlichtweg einen demokratischen Auftrag. Die Forderung nach ‚Neutralität' gegenüber Ausgrenzung und Demokratiefeindlichkeit ist keine Ausgewogenheit, sondern der Versuch, Engagement zum Schweigen zu bringen."

Wenn Sie Rückfragen haben oder weitere Hintergründe benötigen, melden Sie sich jederzeit gern.

Mit freundlichen Grüßen

E-Mail an Unterstützende / Mitglieder bzw. Newslettertext

Szenario: Kleine Anfrage der AfD in Bundes- oder Landtag über öffentlich geförderte oder durch Spenden finanzierte Organisation

Liebe*r <NAME>,

Menschen wie du sind der AfD ein Dorn im Auge. Weil du dich einmischst. Weil du Haltung zeigst. Weil du nicht schweigst, wenn Rechtsextreme versuchen, in Deutschland wieder an die Macht zu kommen.

Deswegen wollen sie uns jetzt mundtot machen. Dich, mich und alle, die für eine starke, vielfältige Demokratie arbeiten. Dafür hat die AfD einen Antrag im Bundestag gestellt, um der <DEINE ORGANISATION> die Förderung zu streichen.

Es ist eine neue Eskalationsstufe: Die AfD versucht, Menschen wie dich, die sich für eine demokratische Zivilgesellschaft engagieren, einzuschüchtern. Sie wollen ein Zeichen setzen.

Aber das lassen wir uns nicht gefallen - denn wir sind mehr.

Spende jetzt und setze ein Zeichen gegen die AfD.

<SPENDENBUTTON> Jetzt spenden!

Danke für deine Hilfe!

Herzlich,
xxx

E-Mail mit Gesprächseinladung an Abgeordnete in Bund/Land

Szenario: Angriffe auf gemeinwohlorientierte Organsationen im Allgemeinen

Sehr geehrte*r [Name],

die zunehmende Zahl Kleiner Anfragen und öffentlicher Vorwürfe der AfD gegen gemeinwohlorientierte Organisationen gibt uns Anlass zur Sorge. In immer kürzeren Abständen werden Vereine, Initiativen und Träger, die sich für Demokratie, sozialen Zusammenhalt, Umwelt- und Menschenrechte einsetzen, unter Generalverdacht gestellt und ihre Förderung infrage gestellt.

Diese Anfragen folgen erkennbar einem Muster: Sie zielen weniger auf Aufklärung als auf Delegitimierung, Verunsicherung und politischen Druck auf Träger, Fördermittelgeber und Engagierte. Viele Organisationen berichten von erheblicher Verunsicherung in ihren Teams, bei Ehrenamtlichen und in ihrem Umfeld. Was hier stattfindet, ist keine normale parlamentarische Kontrolle, sondern eine systematische Infragestellung zivilgesellschaftlicher Arbeit als solcher.

Als [Name der Organisation] sind wir seit [x] Jahren in [Themenfeld] tätig und erleben aktuell, wie stark diese Angriffe die Arbeitsfähigkeit, das Sicherheitsgefühl und die Planungssicherheit zivilgesellschaftlicher Akteure beeinträchtigen. Zivilgesellschaft ist jedoch keine Randerscheinung, sondern ein zentraler Pfeiler unserer demokratischen Infrastruktur. Wer sie schwächt, schwächt die Demokratie.

Vor diesem Hintergrund würden wir uns sehr über ein persönliches Gespräch mit Ihnen freuen. Uns geht es darum, Ihnen aus der Praxis zu schildern,

- wie diese Angriffe konkret wirken,
- welche Risiken wir für die demokratische Kultur sehen und
- welche politischen Schutzmechanismen aus unserer Sicht dringend notwendig sind.

Wir halten es für wichtig, dass demokratische Abgeordnete diese Entwicklung nicht nur zur Kenntnis nehmen, sondern aktiv Position beziehen und die Zivilgesellschaft sichtbar schützen.

Gerne richten wir uns terminlich nach Ihnen und kommen auch kurzfristig auf Sie zu.

Mit freundlichen Grüßen

E-Mail an Partnerorganisationen

Szenario: Kleine Anfrage der AfD in Bundes- oder Landtag über öffentlich geförderte Organisation

Liebe Mitstreiter*innen,
morgen debattiert der Bundestag den Antrag der AfD-Fraktion *„Staatliche Finanzierung der Zivilgesellschaft aus Bundesmitteln beenden“.*

Mit diesem Antrag will die AfD der Zivilgesellschaft sämtliche staatlichen Fördermittel entziehen – und nutzt den Bundestag als Bühne für ihre Kampagne gegen zivilgesellschaftliches Engagement.

Wir brauchen jetzt eure Unterstützung.
Zeigt öffentlich, dass ihr hinter unabhängiger Demokratiearbeit steht.
Bitte teilt, postet, sprecht darüber. Hier könnt ihr auf Talking Points und Social Media Material zugreifen:
<LINK ZU DOKUMENT FÜR PARTNER>

Die AfD greift uns an, weil wir wirksam und sichtbar sind – und weil wir für viele andere stehen. Die Bedrohungslage ist real: Büros werden ausgespäht, Feindeslisten erstellt, Gewalt angedroht.
Es trifft uns – aber gemeint sind wir alle.

Der Antrag ist die politische Zuspitzung einer massiven Einschüchterungskampagne: Auf Plattformen wie *Nius* oder *Apollo News* werden täglich Falschmeldungen über Demokratieprojekte verbreitet – nach dem bekannten Muster aus den USA oder Ungarn. Dieser Angriff richtet sich gegen die demokratische Öffentlichkeit – gegen alle, die Freiheit, Gleichheit und Vielfalt verteidigen.

Darum unsere Bitte: Steht jetzt sichtbar an unserer Seite. Jede Stimme, jeder Post, jedes Statement zählt.

Gemeinsam zeigen wir: Zivilgesellschaftliche Demokratiearbeit ist unersetzlich – und wir lassen uns nicht einschüchtern.

Herzliche Grüße

E-Mail an Fördermittelgeber

Szenario: Proaktive Information anlässlich einer parlamentarishen Anfrage der AfD

Sehr geehrte*r [Name],

wir möchten Sie proaktiv darüber informieren, dass [Name der Organisation] aktuell Ziel öffentlicher Angriffe und parlamentarischer Anfragen durch die AfD ist, in denen unsere Arbeit und die Förderung gemeinwohlorientierter Projekte grundsätzlich infrage gestellt werden.

Diese Angriffe erfolgen nicht isoliert, sondern sind Teil einer bundesweit zu beobachtenden Strategie, mit der zivilgesellschaftliche Akteure delegitimiert, verunsichert und unter politischen Druck gesetzt werden sollen. Ziel ist erkennbar, demokratisches Engagement als „parteiisch“, „aktivistisch“ oder „nicht neutral“ zu diskreditieren und Förderstrukturen zu untergraben.

Uns ist wichtig, Ihnen dazu eine klare Einordnung zu geben:
Unsere Arbeit ist rechtlich legitimiert, fachlich fundiert und am Gemeinwohl orientiert. Sie basiert auf den Grundwerten unserer Verfassung – Menschenwürde, Grundrechten, Demokratie und gesellschaftlichem Zusammenhalt. Das ist kein parteipolitisches Engagement, sondern Kernauftrag zivilgesellschaftlicher Arbeit. Wir sehen diese Angriffe nicht als Ausdruck berechtigter Kritik, sondern als Versuch, demokratische Infrastruktur zu schwächen. Entsprechend werden wir nicht in Rechtfertigungsschleifen gehen, sondern unsere Haltung klar vertreten und unsere Arbeit konsequent fortsetzen.

Gerade in dieser Situation ist die Verlässlichkeit von Förderpartnern entscheidend. Ihre Unterstützung gibt uns nicht nur finanzielle, sondern auch institutionelle Rückendeckung gegenüber Einschüchterungsversuchen.

Gerne stehen wir Ihnen für ein persönliches Gespräch zur Verfügung, um die Situation einzuordnen, Hintergründe zu erläutern und etwaige Fragen offen zu besprechen.

Vielen Dank für Ihr Vertrauen und die gute Zusammenarbeit.

Mit freundlichen Grüßen

Textbausteine für die Kommunikation

Angriff und Diskreditierungsstrategie entlarven

Die [Partei] missbraucht parlamentarische Instrumente, um gezielt zivilgesellschaftliche Arbeit zu diskreditieren. Das ist keine Kontrolle, sondern ein Angriff auf demokratische Infrastruktur.

Mit ihrer Anfrage entlarvt [die Partei/ die Publikation] sich selbst. Sie offenbart nicht nur fachliche Unkenntnis, sondern legt eine klare Geisteshaltung/ politische Haltung offen.

[Die Partei/ die Publikation] versucht, Zweifel zu säen und Misstrauen zu verbreiten, um demokratische Strukturen auszuhöhlen. Wer diese Strategie erkennt, versteht, dass es nicht um Fakten geht, sondern um Spaltung.

Diese Anfrage folgt einem bekannten Muster: erst Misstrauen schüren, dann den Rückzug der Zivilgesellschaft fordern. Das ist autoritäre Politik mit demokratischen Mitteln.

Rechtsstaatlichkeit betonen

Wir handeln im Rahmen klarer Gesetze und Richtlinien. Unsere Arbeit wird regelmäßig geprüft, hält gerichtlicher Überprüfung stand und ist ein fester Bestandteil unseres demokratischen Rechtsstaats.

Eine demokratische Gesellschaft ist nicht neutral. Wer sich für Menschenwürde, Grundrechte und Zusammenhalt einsetzt, ist nicht parteiisch – sondern demokratisch.

Professionalität hervorheben

Unsere Kolleg:innen arbeiten nach anerkannten wissenschaftlichen Standards und mit einem klaren Wertekompass. Wer daran Zweifel sät, ist nicht um Aufklärung bemüht, sondern betreibt Einschüchterung.

Gesellschaftlichen Nutzen sichtbar machen

Unsere Arbeit ist kein Luxus. Sie unterstützt Menschen, stabilisiert Familien und stärkt den gesellschaftlichen Zusammenhalt. Wer diese Strukturen schwächt, gefährdet unsere Demokratie im Kern.

Zivilgesellschaft schafft Werte, die sich nicht in wirtschaftlichen Kennzahlen messen lassen: Vertrauen, Sicherheit, Mitgefühl. Das ist das Fundament einer gesunden Demokratie.

Sportvereine, Nachbarschafts- und Umweltinitiativen, Jugendclubs oder Feuerwehr – all das ist Zivilgesellschaft. Menschen kommen dort zusammen, um das Miteinander unserer Gesellschaft zu gestalten.

In Vereinen, Initiativen und Projekten erleben Menschen jeden Tag, was Gesellschaft bedeutet: fairer Umgang, Respekt, Solidarität. Genau dafür stehen wir ein.

Verantwortung markieren

Die demokratische Mitte trägt Verantwortung, Angriffe auf zivilgesellschaftliches Engagement nicht zu normalisieren.

Demokratie lebt davon, dass Menschen Haltung zeigen. Wer Engagement zur Neutralität erzieht, schwächt die Demokratie – und stärkt ihre Gegner.

Wer die Arbeit von Ehrenamtlichen und Fachleuten politisch instrumentalisiert, schwächt das Vertrauen in staatliche Institutionen – und das trifft uns alle.

Es gibt kein Gebot, gegenüber Rassismus, Ausgrenzung oder autoritären Fantasien neutral zu bleiben. Im Gegenteil: Unsere Verfassung verpflichtet uns, die Würde jedes Menschen zu schützen. Daran orientiert sich unsere Arbeit.

Hier trainieren Kinder zusammen, hier helfen Ehrenamtliche, hier kommen Menschen aus ganz unterschiedlichen Hintergründen zusammen. Das ist gelebte Demokratie. Und die verteidigen wir.

Positive Selbstbeschreibung

Zivilgesellschaft ist gelebte Demokratie. Millionen Menschen engagieren sich ehrenamtlich, professionell und mit großer Verantwortung. Dieses Engagement ist Teil unserer demokratischen DNA.

Unsere Arbeit zeigt: Eine starke Gemeinschaft entsteht nicht durch Misstrauen, sondern durch Menschen, die sich umeinander kümmern.

Wir laden alle demokratischen Kräfte ein, über Lösungen zu sprechen – nicht über Spaltung. Unsere Türen stehen offen für Zusammenarbeit, nicht für Angriffe.

Deutschland steht vor großen Aufgaben – sozial, ökologisch, ökonomisch. Diese Aufgaben lösen wir nur gemeinsam, nicht gegeneinander.

Wir glauben an eine Gesellschaft, die sich gegenseitig stärkt – statt Angst zu verbreiten. Das ist unser Beitrag, jeden Tag.

Wir organisieren Sport, Bildung, Nachbarschaftshilfe und Engagement, damit unser Zusammenleben funktioniert. Das ist kein parteipolitisches Programm, sondern demokratische Normalität. Wer das delegitimieren will, greift den Kern unserer Gesellschaft an.

FRAGEN ODER ANREGUNGEN?

info@zukunftdemokratie.org