

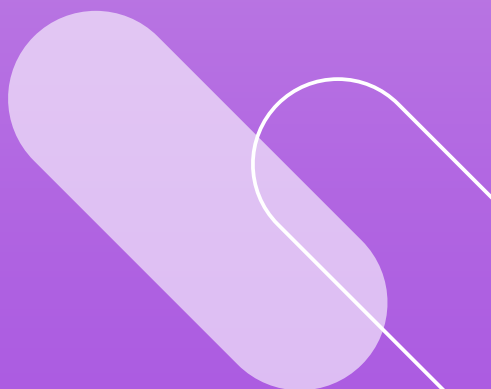


Hate Aid

Engagement in Gefahr?

Ein Krisenplan für alle Engagierten

Handlungsmöglichkeiten und Schutzstrategien bei digitaler Gewalt auf kommunaler Ebene. Vom Sportverein bis zur Integrationshilfe.



Inhalt

1 Was ist eine Krise?	4
1.1 Wie können Sie mit einer Krisensituation umgehen?	6
1.2 Was sind potenzielle Krisen? – Einige Gefahrenszenarien	7
2 Wer ist Ihr Krisenteam?	9
2.1 Rollen und Aufgaben im Krisenteam	9
2.2 Krisenmanagement	10
2.3 Analoge und digitale Sicherheit	11
2.4 Kommunikation	13
2.5 Rechtssichere Screenshots erstellen	15
2.6 Ein Statement veröffentlichen	16
3 Erkennen Sie die unterschiedlichen Phasen einer Krise	18
4 Akut betroffen – konkrete Schritte im Umgang mit einer Krise	22
5 Kontakt	24
6 Weitere Hilfsangebote	26
7 Anmerkungen	28

1 Was ist eine Krise?

Sie beteiligen sich an einer Diskussion zum Klimaschutz, organisieren eine Gesprächsrunde für Geflüchtete oder teilen online ab und zu Bilder über Ihre Arbeit? Die Reaktionen können heftig sein. Sie müssen nicht häufig auf Social Media aktiv sein oder ein politisches Amt ausüben, um per E-Mail, SMS oder Messenger angefeindet zu werden. Solche Angriffe sind für viele politisch Engagierte Alltag und können eine Krise auslösen.

So kann eine Krise zum Beispiel verlaufen:

Zunächst werden Sie kritisiert.



Wir brauchen eine Lösung, keine weitere Veranstaltung!

Kritik entwickelt sich zu **Hass, Beleidigungen und Bedrohungen**.



Du A****! Du hast keine Ahnung, wie es den Menschen wirklich geht.

Plötzlich erhalten Sie innerhalb von wenigen Tagen **Unmengen von Hassmails mit Gewaltfantasien oder eine Person veröffentlicht Ihre Wohnadresse** auf Facebook.



Ich weiß, wo du wohnst! Wenn du nicht damit aufhörst, stanno wir dir einen Besuch ab

Unwahre Informationen über Sie oder gefälschte (Nackt-)Fotos werden im Internet veröffentlicht und verbreiten sich rasend schnell. Das Ziel: Sie und Ihre Arbeit diffamieren.



Habt ihr schon das neuste Nacktfoto von der Alten gesehen? Sie sollte lieber in die Küche an den Herd und keine Politik machen.

Die Folgen: Sie fühlen sich bedroht und haben Angst um Ihre Sicherheit und die Ihrer Familie. Sie können die reale Gefahr dieser Gewaltandrohung nicht einschätzen. Sie sind überfordert und wissen nicht, wie Sie Ihre Arbeit weiterführen und mit der Situation umgehen sollen. Sie stehen vor einer Krise oder sind schon mittendrin.



Eine Krisensituation ist ein akuter Zustand von Überforderung, Spannung oder Bedrohung, bei dem die Anforderungen der Situation die eigenen Ressourcen und Möglichkeiten überschreiten.¹

Krisen können sowohl in der **analogen** als auch in der **digitalen** Lebenswelt ausgelöst werden.

Oftmals gehen digitale Anfeindungen ins Analoge über: Sie werden etwa online beschimpft und dann im Supermarkt auf das Streitthema angesprochen und erneut angegriffen. Auch können sich Konflikte und Auseinandersetzungen aus dem analogen Leben ins Netz verlagern.

Die Fremdwahrnehmung zeigt: **76 % der Befragten nehmen wahr, dass politisch Engagierte am häufigsten von Hatespeech betroffen sind.**² Neueste Studienergebnisse belegen, dass sich Hass im Netz am häufigsten auf die politischen Ansichten der Betroffenen bezieht.³

13 % der in der Kommunalpolitik Tätigen haben schon darüber nachgedacht, sich aus Sorge um ihre Sicherheit und die ihrer Familie aus der Politik zurückzuziehen.⁴

Bereiten Sie sich auf Krisensituationen und Anfeindungen vor!

1.1 Wie können Sie mit einer Krisensituation umgehen?

Auch wenn Ihnen ein solches Szenario unwahrscheinlich erscheint, hat es den Ursprung in einer Meinungsverschiedenheit. Diese kann sowohl digital als auch analog eskalieren. **Krisen können alle Menschen treffen – plötzlich, unerwartet und unvorbereitet.**

Ein Krisenplan gibt Ihnen in einer Akutsituation ein Mindestmaß an Kontrolle über die Situation und kann Ihnen dabei helfen, die Krise gut zu bewältigen.

Für den Plan beantworten Sie folgende Fragen:

- 1 Was sind für Sie Gefahrenszenarien und somit potenzielle Krisen?
- 2 Wer gehört zu Ihrem Krisenteam?
- 3 Welche konkreten Schritte folgen im Umgang mit einer Krise?

Handlungsempfehlungen wie „Bewahre Ruhe!“ oder „Lass dich nicht provozieren!“ werden im Umgang mit Krisensituationen häufig gegeben. Das ist oft leichter gesagt als getan. **Was wirklich hilft: Erstellen Sie präventiv einen Krisenplan und bereiten Sie sich damit auf eine mögliche Krisensituation vor.** So sind Sie im Ernstfall vorbereitet.

1.2 Was sind potenzielle Krisen? – Einige Gefahrenszenarien

- Über Sie kursieren falsche Informationen im Netz, die rufschädigend sind.
- Sie erhalten Drohungen via E-Mail.
- Sie bekommen Hasskommentare oder Hassnachrichten auf Social Media oder sogar einen Shitstorm.
- Es werden sexualisierte Deepfakes von Ihnen erstellt, um Sie zu diskreditieren.
- Mit Ihren Daten werden Fake-Profil auf Social Media erstellt oder E-Mail-Adressen angelegt. Damit werden Inhalte verbreitet und Falschaussagen getätigt.
- Eine Person stalkt Sie.⁵
- Ihre E-Mail-Adresse wird gehackt und Sie können sich nicht mehr mit Ihrem Passwort einloggen oder bemerken ungewöhnliche Aktivitäten auf Ihrem Account.
- Sie erhalten Phishing-Mails, um Ihnen z. B. finanziell zu schaden.
- Ihre sensiblen, personenbezogenen Daten, wie Ihre Wohnadresse, private Fotos oder Informationen über Angehörige, werden veröffentlicht.
- Ihr Name oder Foto taucht auf Feindeslisten auf und es wird zu Gewalt gegen Sie aufgerufen.⁶
- ...

Ab wann für Sie eine Krise beginnt, ist sehr individuell und hängt sowohl vom Arbeitsumfeld als auch von den eigenen Ressourcen im Umgang mit Anfeindungen ab.

Krisensituationen / Gefahrenszenarien

Welche Szenarien würden Ihre persönlichen und beruflichen Ressourcen übersteigen und könnten für Sie somit eine Gefahr darstellen? **Definieren Sie Ihre potenziellen Krisenszenarien.** Nutzen Sie dafür die zuvor genannten Krisenszenarien als Orientierung und finden Sie weitere Beispiele, die Ihnen einfallen.

2 Wer ist Ihr Krisenteam?

Eine Krise nimmt viele Ressourcen in Anspruch. Um sich präventiv auf eine Krisensituation vorzubereiten, ist es sinnvoll, ein Krisenteam zusammenzustellen. Dieses Team übernimmt während und nach einer Krise bestimmte Aufgaben und Rollen. Im besten Fall stellen Sie dieses Krisenteam schon vor Eintreten der Krise auf und können es dann sofort aktivieren. So verfügen Sie über Handlungssicherheit und können Ihre eigenen Kräfte in der akut herausfordernden Krisensituation schonen. Sollten Sie zu diesem Zeitpunkt noch kein Krisenteam haben, organisieren Sie sich zuallererst eines. Noch ist es nicht zu spät.

Ihr Krisenteam sollte zum Beispiel aus Ihnen, Ihren Vorgesetzten und Ihrem Team bestehen. Es können auch engagierte Personen im Team sein, die Sie kurzfristig unterstützen – etwa Ehrenamtliche, Menschen im Praktikum oder in Ausbildung oder Menschen aus Ihrem privaten und beruflichen Umfeld.

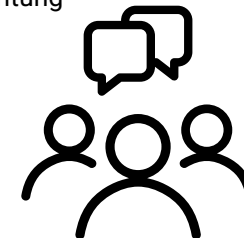
2.1 Rollen und Aufgaben im Krisenteam

Krisenmanagement:

- Krisenkoordination
- Angriffsbeobachtung

Analoge und digitale Sicherheit:

- Sicherheitsmanagement
- Schutz von Privatsphäre und Daten
- IT-Sicherheitsmanagement



Kommunikation:

- Safeguard für Netiquette
- Community Management
- Kommunikation mit der Presse

2.2 Krisenmanagement

Eine oder mehrere Personen behalten den Überblick über die Krisensituationen und bringen dadurch Ruhe ins Team. Zudem sind sie für die Verteilung der Rollen verantwortlich. **Folgende Rollen sollen dabei erfüllt werden:**



Krisenkoordination

- Die Rolle steuert das Krisenteam.
- Beruft Meetings ein, vergibt die Rollen für eine Krisensituation und informiert das Team über die nächsten Schritte des Krisenplans.
- Präventive Vorbereitung: Bereitet eine Liste mit potenziellen Unterstützenden, Organisationen und Fachleuten vor, die im Team fehlen und in einem Krisenfall kontaktiert werden. Die Rolle erstellt außerdem einen Verteiler aus dieser Liste.
- In akuter Situation: Kontaktiert die Unterstützenden aus dem Verteiler, erklärt die Situation und schildert konkrete Schritte. Außerdem informiert diese Person das Umfeld, z. B. die Nachbarperson im Büro, über den Angriff und bespricht Unterstützungsmaßnahmen.
- Nachbereitung: Reflektiert gemeinsam mit dem Team die Krisensituation und überlegt, was gut lief und was beim nächsten Mal besser gemacht werden kann.



Angriffsbeobachtung

- Die Rolle beobachtet und verfolgt die Entwicklung der Krise, die sich vor allem auf den Social-Media-Kanälen sehr rasant entwickeln kann.
- Evaluiert und schätzt die Situation konstant ein.
- Legt einen Kommunikationskanal fest, über den alle regelmäßig informiert werden (E-Mail, Chat o. Ä.).
- Informiert die für die Krisenkoordination verantwortliche Person und das Team über den Verlauf der Krise.
- Alarmiert das Team, falls große Veränderungen und/oder Eskalationen stattfinden (z. B. wenn diffamierende Behauptungen auf weiteren Social-Media-Plattformen verbreitet werden).

2.3 Analoge und digitale Sicherheit

Eine oder mehrere Personen beschäftigen sich mit Maßnahmen zur analogen Sicherheit und zum digitalen Schutz der Betroffenen. **Folgende Rollen und Aufgabenbereiche gibt es:**



Sicherheitsmanagement

- Die Rolle protokolliert und analysiert Angriffe und schätzt ein, welche Gefahrenszenarien eingetreten sind.
- Kontaktiert die Strafverfolgungsbehörden, schildert die Situation und bittet um Unterstützung. Kontaktiert eine geeignete Beratungsstelle für eine Gefahrenereinschätzung und Schutzmaßnahmen (z. B. HateAid, Mobile Beratungsteams gegen

Rechtsextremismus oder Aktion Zivilcourage). Auf der Webseite stark-im-amt.de finden Sie eine Übersicht an Beratungsangeboten und Unterstützungsmöglichkeiten für kommunal Engagierte.

- Erhält rechtssichere Screenshots vom Community Management und erstattet in Absprache mit der betroffenen Person Strafanzeige bei einer Polizeistation vor Ort oder bei einer Onlinewache bzw. einer Meldestelle für digitale Gewalt.

Bitte beachten Sie:

Es gibt eine Reihe von Delikten, z. B. Beleidigung, üble Nachrede und Verleumdung, bei denen neben einer Strafanzeige auch ein sog. Strafantrag notwendig ist. Ein Strafantrag ist eine ausdrückliche Erklärung der angegriffenen Person, dass sie die Strafverfolgung wünscht. Ohne einen Strafantrag kann die Staatsanwaltschaft das Verfahren grundsätzlich nicht mehr fortsetzen. Er muss innerhalb von drei Monaten gestellt werden. Die Frist beginnt an dem Tag, an dem die angegriffene Person erstmals von der Tat und der Tatperson erfahren hat.

Wenn Sie Sorge haben, dass Sie die Angabe Ihrer Adresse bei der Anzeigeerstattung gefährden könnte, sieht das Gesetz gewisse Schutzmöglichkeiten vor. Unter bestimmten Voraussetzungen können Sie eine andere Adresse als Ihre private angeben, an der Sie zuverlässig erreichbar sind (z. B. Ihre Büroadresse).



Schutz von Privatsphäre und Daten

- Die Rolle checkt mithilfe von Suchmaschinen, welche sensiblen, personenbezogenen Daten über die angegriffene Person und ihr Umfeld im Netz zu finden sind. Das können z. B. Wohnadresse, Arbeitsplatz, Telefonnummer, private Fotos etc. sein.
- Wenn sensible, personenbezogene Daten gefunden werden: Kontaktiert die Verantwortlichen, z. B. die Betreibenden von Webseiten oder Suchmaschinen⁷, und unterstützt ggf. bei der Löschung der Daten.⁸
- Überprüft auf den Social-Media-Plattformen, welche Informationen über die angegriffene Person für Dritte einsehbar sind, und verstärkt die Privatsphäre-Einstellungen (z. B. Konto vorübergehend auf „privat“ stellen oder Kommentarfunktion ausschalten). Weitere Informationen finden Sie in unserem Online-Artikel zu Privatsphärechecks unter hateaid.org/privatsphaere-check

Wer bestimmte personenbezogene Daten von Ihnen hat, kann Ihre aktuelle private Anschrift ganz leicht herausfinden. Das geht mithilfe einer sog. einfachen Melderegisterauskunft, die (online) beim Meldeamt beantragt werden kann. Um sich davor zu schützen, können Sie die Eintragung einer Melderegisterauskunftssperre beantragen.

Dafür müssen Sie einen Antrag bei der zuständigen Meldebehörde stellen. In diesem führen Sie aus, wieso eine Auskunft Ihrer Privatadresse an Dritte eine Gefahr für Sie darstellen würde. Nachweise, die dies belegen, z. B. von Ihnen erstattete Strafanzeigen, aber auch ein Schreiben Ihres Arbeitgebers, eines Vereins oder einer Beratungsstelle, können hilfreich sein. **Im besten Fall können Sie so die Eintragung einer Melderegisterauskunftssperre schon präventiv erreichen.**

HateAid kann Sie hierbei unterstützen.



IT-Sicherheitsmanagement

- Die Rolle informiert das Team über Hacking⁹- und Phishing¹⁰-Angriffe. Falls in Ihrem Team oder Umfeld niemand über Fachwissen dazu verfügt, suchen Sie Unterstützung, z. B. durch eine IT-Fachberatung.
- Führt einen Passwortmanager und die Zwei-Faktor-Authentifizierung für alle Personen im Team ein.
- erinnert das Team regelmäßig an die Nutzung von starken Passwörtern. (Hinweise zur Erstellung starker Passwörter finden Sie in unserem Leitfaden.)
- erinnert das Team regelmäßig, Updates auf den Arbeitsgeräten durchzuführen und Daten mithilfe von Backups zu sichern.
- Bei Hacking-Verdacht: Alarmiert das Team, ändert alle Passwörter, bewahrt alte Geräte auf (wichtig für die Beweissicherung des Hacking-Angriffs). Institutionen und Unternehmen beauftragen ein sogenanntes Cyber-Incident-Response-Unternehmen¹¹.

2.4 Kommunikation

Im Umgang mit digitalen Anfeindungen spielt Kommunikation nach innen und außen eine besonders wichtige Rolle. **Wenn Sie allein oder mit einem kleinen Team arbeiten, überlegen Sie präventiv, wer Sie in Krisensituationen unterstützen kann.** Das können etwa Ehrenamtliche, (ehemalige) Mitarbeitende, andere Organisationen oder Menschen aus Ihrem beruflichen und privaten Umfeld sein. Diese Menschen sind Ihr Solidaritätsnetzwerk. Informieren Sie es im Vorfeld einer akuten Krise und besprechen Sie, wer welche Rolle übernimmt. So sparen Sie Zeit und Arbeit in der akuten Krisensituation. Besetzen Sie folgende Aufgaben und Rollen im Bereich Kommunikation.



Safeguard für Netiquette

- Die Rolle definiert Regeln, wie auf den eigenen Social-Media-Kanälen kommuniziert werden soll und veröffentlicht diese Regeln als Netiquette¹².
- Bearbeitet die Netiquette ständig und sorgt dafür, dass diese regelmäßig aktualisiert wird.



Community Mangement

- Die Rolle setzt die Regeln der Netiquette durch, filtert Kommentare und beantwortet, blockiert, meldet oder löscht sie.
- Erstellt rechtssichere Screenshots der gewaltvollen Inhalte (s. Absatz rechtssichere Screenshots erstellen).
- Meldet gewaltsame Inhalte richtig. Hier gibt es zwei Möglichkeiten: entweder die Meldung eines Verstoßes gegen die Regeln der Plattform selbst („Community-Richtlinien“ bzw. AGBs) oder eine Meldung von rechtswidrigen Inhalten auf Grundlage des Digital Services Acts. Nur bei einer Meldung auf Grundlage des Digital Services Acts haben die Plattformen bestimmte gesetzliche Pflichten, wie z. B. zu prüfen, ob der gemeldete Inhalt rechtswidrig ist, und diesen ggf. zu löschen.



Kommunikation mit der Presse

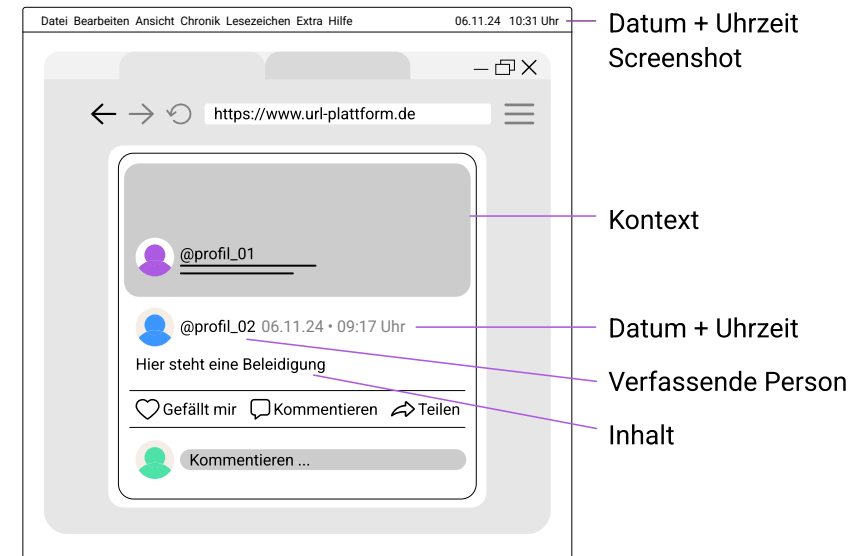
In einem kleinen Team haben Sie vielleicht niemanden, der für die Kommunikation mit der Presse verantwortlich ist. Diese Rolle muss allerdings in Krisensituationen besetzt werden. Sie ist zuständig für die externe Kommunikation. Die Person, die diese Aufgabe übernimmt, sollte präzise schreiben und kommunizieren können.

- Erstellt in Krisenfällen einen Entwurf für ein öffentliches Statement.
- Fertigt Textbausteine an, auf die das Team zurückgreifen kann.
- Informiert das Team über das Statement, sodass alle einer einheitlichen Kommunikationslinie folgen.
- Steht für öffentliche Anfragen zur Verfügung.

2.5 Rechtssichere Screenshots erstellen

Ein rechtssicherer Screenshot ist eine Bildschirmaufnahme, bspw. eines Postings oder Kommentars auf Social Media, auf der bestimmte wichtige Informationen ersichtlich sind. Diese Informationen sind:

- die URL des dazugehörigen Links,
- Datum (TT.MM.JJJJ) und Uhrzeit (Stunde:Minute) des anfeindenden Inhalts,
- Abbildung der Tatpersonen
- sowie der Kontext, in dessen Rahmen die Anfeindung stattgefunden hat.



Beispiel eines rechtssicheren Screenshots

Sowohl im „Leitfaden zum Umgang mit digitaler Gewalt“ als auch auf der HateAid-Webseite finden Sie Anleitungen, wie Sie einen rechtssicheren Screenshot erstellen können. Mit diesen Screenshots können Vorfälle schnell und dauerhaft dokumentiert werden. Dies ist essenziell, wenn Sie sich dazu entscheiden, rechtlich gegen bestimmte Inhalte vorgehen zu wollen.

2.6 Ein Statement veröffentlichen



Warum sollten Sie ein Statement veröffentlichen?

- Es dient dazu, falsche Informationen über Sie oder Ihre Organisation richtigzustellen.
- Es ermöglicht Ihnen, sich zu einer Thematik zu positionieren und Verantwortung zu übernehmen.
- Sie können die Strategien der Angreifenden offenlegen.
- Sie kommunizieren nach außen, wie Sie sich in Anbetracht der akuten Krise verhalten, zum Beispiel ob Sie sich vorerst zurückziehen oder eine Veranstaltung absagen.
- Es hilft, Unterstützung und Solidarität aus Ihrem Netzwerk und von anderen wichtigen Personen zu erhalten.



Wo veröffentlichen Sie Ihr Statement?

- Veröffentlichen Sie es auf Ihrer Webseite, z. B. auf der Seite der Kommune.
- Teilen Sie es auf Ihrem Social-Media-Konto.
- Teilen Sie es in regional bedeutsamen Gruppen auf Social-Media-Plattformen, z. B. in einer Facebook-Ortsgruppe.
- Senden Sie es direkt an Ihr Netzwerk, Ihr Kollegium und relevante Personen in Amt und Mandat.
- Geben Sie es im Rahmen von Pressemitteilungen an die Medien weiter.



Wann veröffentlichen Sie Ihr Statement?

- Nehmen Sie sich Zeit, beobachten Sie die Situation und schätzen Sie ein, welche Strategien die Angreifenden verfolgen.
- Machen Sie eine digitale Pause und geben Sie danach bekannt, dass Sie nun wieder online sind, wenn Sie sich bereit fühlen.
- Bedanken Sie sich für digitale Zivilcourage und Unterstützung aus Ihrer Community, wenn Sie diese erfahren.



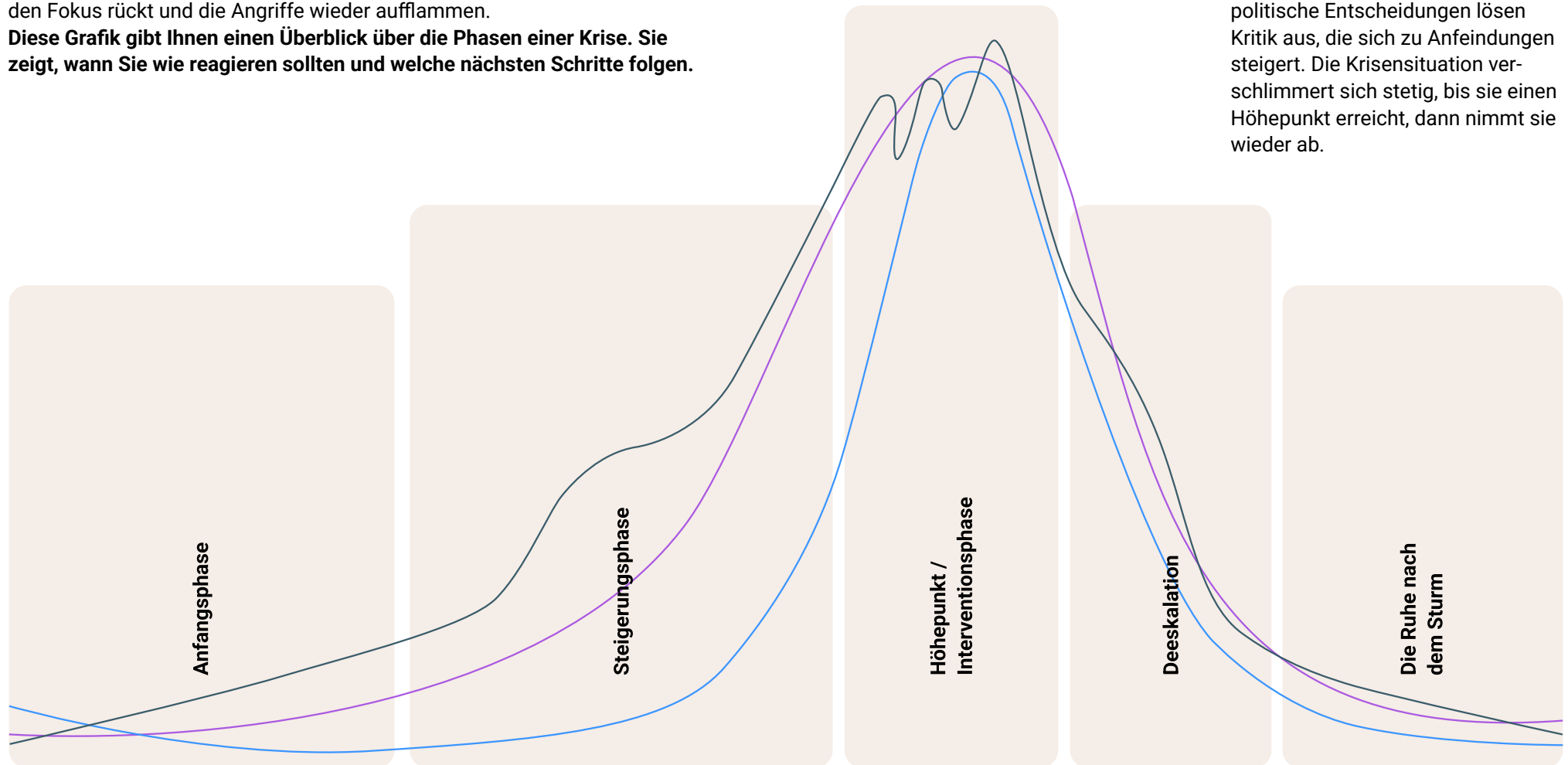
Wie formulieren und verbreiten Sie ein gelungenes Statement?

- Um eine Wirkung zu erreichen, soll das Statement auf dem Kanal verbreitet werden, mit dem Sie Ihre Zielgruppe erreichen.
- Fassen Sie sich kurz, formulieren Sie präzise und betonen Sie Ihre Position.
- Geben Sie den Anfeindungen oder Diffamierungen wenig Raum.
- Aktivieren Sie Ihre digitale Community und werben Sie für Solidarität und Unterstützung.
- Seien Sie in Ihrem Statement ehrlich und transparent.
- Vermeiden Sie Aussagen, die im Widerspruch zu Ihren eigenen Werten stehen.
- Wenn Sie etwas bedauern, dann entschuldigen Sie sich dafür. Nehmen Sie keine Verteidigungsposition ein, sondern eine aufklärende Haltung.
- Weitere Hinweise zur Veröffentlichung eines Statements finden Sie in unserem Leitfaden für Informationen und Maßnahmen zum Schutz vor digitaler Gewalt gegen kommunal Engagierte.

3 Erkennen Sie die unterschiedlichen Phasen einer Krise

Eine Krise entsteht durch mehrere gezielte Angriffe und verläuft oft in **Wellen**. Ein Ereignis, wie z. B. eine politische Entscheidung, kann zunächst Kritik auslösen, die sich rasch zu Anfeindungen steigert. Diese erreichen einen Höhepunkt und ebbens meist wieder ab, bevor das Thema erneut in den Fokus rückt und die Angriffe wieder aufflammen.

Diese Grafik gibt Ihnen einen Überblick über die Phasen einer Krise. Sie zeigt, wann Sie wie reagieren sollten und welche nächsten Schritte folgen.



Ein bestimmtes Ereignis löst eine Krisensituation aus. Die Anfeindungen passieren plötzlich und schnell, erreichen einen Höhepunkt und nach kurzer Zeit beruhigt sich die Situation wieder.

Die Krise bezieht sich nicht nur auf eine Situation, sondern mehrere Einzelangriffe. Höhepunkte einer solchen Krise werden mehrmals erreicht, sobald das Angriffsthema wieder präsent ist. Hasswellen verlaufen oft ähnlich wie diese Grafik.

Ein Ereignis oder bestimmte politische Entscheidungen lösen Kritik aus, die sich zu Anfeindungen steigert. Die Krisensituation verschlimmert sich stetig, bis sie einen Höhepunkt erreicht, dann nimmt sie wieder ab.

Anfangsphase

- Sie werden heftig kritisiert und angegangen. Die Kritik ist jedoch nicht feindlich oder bedrohlich Ihnen gegenüber.
- **Präventive Maßnahmen umsetzen:** persönliche Informationen im Netz minimieren, Privatsphäreinstellungen überprüfen, Adresse schützen (z. B. durch Sensibilisierung im sozialen Umfeld), sich nicht provokant äußern.

Steigerungsphase

- Die Anfeindungen nehmen zu, weiten sich auf andere Plattformen aus (wie z. B. Facebook oder die Kommentarspalte von lokalen Zeitungen) und können gewaltvoller werden.
- Schnelle Entwicklung innerhalb von wenigen Tagen oder sogar Stunden.
- **Das Krisenteam aktivieren.**
- Unterstützungsnetzwerk aktivieren.

Höhepunkt / Interventionsphase

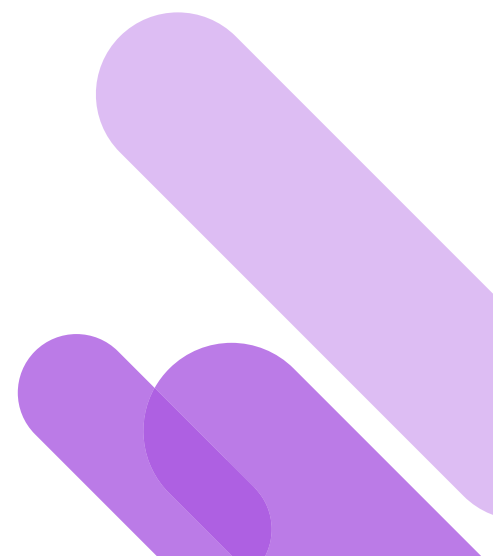
- Ihre vorformulierten Gefahrenszenarien treffen ein.
- Der Höhepunkt einer Krise kann ein einmaliges Ereignis sein (z. B. die Veröffentlichung der privaten Wohnadresse) oder mehrere Vorfälle dieser Art umfassen.
- Sie erhalten innerhalb weniger Stunden unzählige Kommentare auf Ihren Social-Media-Kanälen.
- **Sie setzen Maßnahmen für Ihre analoge und digitale Sicherheit um.**
- Bewahren Sie Ruhe und nehmen Sie sich Zeit.

Deeskalation

- Die Anfeindungen nehmen ab und Sie sind nicht mehr stark im Fokus.
- Sie formulieren und veröffentlichen ggf. ein Statement zu der Situation.
- **Vorsichtig bleiben!**
- Ressourcen schonen, weil die Krise noch nicht vorbei ist.
- Es kann weitere Höhepunkte geben, weil das Thema, zu dem Sie angefeindet werden, immer wieder aufkommt.

Die Ruhe nach dem Sturm

- Sie können Ihren Alltag wieder normal führen.
- **Sie können über die Krise reflektieren und Ihren Umgang damit evaluieren.**
- Sie bedanken sich bei allen, die Sie unterstützt haben.
- Ggf. setzen Sie Veränderungen um.



4 Akut betroffen – konkrete Schritte im Umgang mit einer Krise

Schritt 1: Ruhe bewahren

Eine Krisensituation kann emotional sehr belastend sein und starke Gefühle auslösen.

- Suchen Sie sich Unterstützung und sprechen Sie mit Ihnen nahestehenden Personen darüber, wie Sie sich in dieser Situation fühlen.
- Führen Sie Gespräche mit Fachpersonal von Beratungsstellen oder mit therapeutischem Fachpersonal, das Sie emotional auffangen und stabilisieren kann.
- Schaffen Sie einen Ausgleich für sich und unternehmen Sie bewusst Aktivitäten, die Ihnen Kraft geben. Machen Sie sich vorab Gedanken, welche Aktivitäten das sein können: ein Treffen mit befreundeten Personen, Sport, andere Hobbys.
- **Setzen Sie sich einen zeitlichen (z. B. maximal zwei Stunden am Tag) und örtlichen (z. B. nur draußen im Park) Rahmen, in dem Sie sich mit der Krise befassen.** Durch die zeitliche Eingrenzung schaffen Sie Distanz zu der akuten Situation und Belastung.

Schritt 2: Das Krisenteam aktivieren

Die für die Krisenkoordination verantwortliche Person organisiert ein Meeting und informiert das Krisenteam über den Inhalt der Krise, den Hintergrund und die Rolle jeder Person. Je nach Teamgröße tragen einige Personen unterschiedliche Rollen. **Falls im Team Kompetenzen fehlen, sollten Sie für externe Unterstützung sorgen: z. B. durch HateAid.** Je früher Beratungsstellen oder die Polizei informiert und involviert sind, desto besser können sie Handlungsempfehlungen geben.

Schritt 3: Nicht erstarren, sondern handeln!

Auch wenn eine Krise extrem überfordernd sein kann, können und sollten Sie handeln. Damit es Ihnen leichter fällt, finden Sie im Anhang dieser Broschüre ein Krisenplan-Poster. **Verteilen Sie anhand dessen die Aufgaben in Ihrem Krisenteam.**

Schritt 4: Aus der Krise lernen!

Sie konnten Maßnahmen ergreifen, um aktiv mit der Situation umzugehen. Die Anfeindungen nehmen langsam ab, die Situation normalisiert sich. Sobald Ihr Alltag zurückgekehrt ist, nehmen Sie sich Zeit, um die Krise zu verarbeiten. Sprechen Sie gemeinsam mit dem Krisenteam über die Krisensituation und werten Sie aus, wie Sie mit ihr umgegangen sind.

Stellen Sie sich folgende Fragen und halten Sie die Antworten fest:

- Wer hat Sie unterstützt? Bei wem wollen Sie sich bedanken?
- Was ist gut gelaufen? Was hat Ihnen Stärke gegeben?
- Was lief schlecht? Welche Hilfe und Unterstützung haben Sie sich gewünscht, aber nicht erhalten?
- Was wollen Sie ändern, um zukünftig besser vorbereitet zu sein?
- Was ist vor der Krise (bzw. in der Anfangsphase) passiert, das Ihnen als Warnsignal für kommende Krisensituationen dienen kann?

Eine Zusammenfassung der Handlungsmöglichkeiten und einen Krisenplan zum individuellen Ausfüllen finden Sie am Ende dieser Broschüre.

5 Kontakt zur HateAid-Beratung

Digitale Gewalt erfolgreich abwehren.

Ob in akuten Krisensituationen oder zur Prävention – die HateAid-Beratung bietet praxisnahe Unterstützung an.

→ **Kurzfristig, kostenlos und anonym.**

Wir helfen weiter bei Fragen zur digitalen Sicherheit, zur Kommunikation und zum psycho-sozialen Umgang mit Hass und Desinformation im Netz.



Alle unsere Beratungsangebote finden Sie unter: hateaid.org/beratung

Dort können Sie



telefonische Beratungstermine buchen,



unsere offene Telefon-Sprechstunden nutzen,



schriftliche Beratung per E-Mail in Anspruch nehmen,



rechtswidrige Inhalte melden



sowie auf unser umfangreiches Hintergrundwissen zugreifen.

6 Weitere Hilfsangebote

Stark im Amt

Die Initiative Stark im Amt ist spezifisch mit kommunalpolitisch Engagierten erstellt worden. Auf der Webseite stark-im-amt.de finden Sie Informationen und Material zum Schutz und Umgang mit Hass und Gewalt gegen kommunalpolitisch Aktive, aber auch eine Auflistung diverser Beratungsstellen und Organisationen, die Sie unterstützen.

Starke Stelle

Die starke Stelle ist eine bundesweite, unabhängige Ansprechstelle für in der Kommunalpolitik Tätige, die dabei hilft, die für Sie passenden Unterstützungsangebote aus den Bereichen der Sicherheitsbehörden, Justiz und Zivilgesellschaft zu finden.

Sie erreichen die starke Stelle per E-Mail über info@starkestelle.de

☎ 0800 – 300 99 44

Bundesverband Mobile Beratung e. V.

Bundesweit gibt es rund 50 Mobile Beratungsteams, die Sie zum Umgang mit Rechtsextremismus, Rassismus, Antisemitismus, Antifeminismus und Verschwörungserzählungen beraten. Auf der Webseite des Bundesverbandes Mobile Beratung (BMB e. V.) finden Sie eine Liste aller Beratungsstellen und ihren Standort: bundesverband-mobile-beratung.de/mobile-beratung/#Beratungsteams

Amadeu Antonio Stiftung

Bei der Amadeu Antonio Stiftung (AAS) erhalten Sie Informationen zu Hatespeech, Desinformation und zu digitaler Gewalt im Allgemeinen. Hier finden Sie mehr Informationen zu den Angeboten der AAS: amadeu-antonio-stiftung.de

VBRG

Der VBRG setzt sich für Betroffene rechter, rassistischer und antisemitischer Gewalt ein und ist bundesweit über unterschiedliche Anlaufstellen zu erreichen. Hier finden Sie eine Übersicht der Beratungsstellen: verband-brg.de/beratung

Aktion Zivilcourage e. V.

Aktion Zivilcourage e. V. entwickelt Schutzkonzepte für kommunal Engagierte, vor allem in Fällen hybrider Angriffe, bei denen Betroffene Hass im Netz und im analogen Raum erleben. Hier finden Sie mehr Infos: aktion-zivilcourage.de/angebote/verwaltung/schutzkonzepte

Anmerkungen

1 Vgl. „Psychosoziale Krise“. Online Lexikon für Psychologie und Pädagogik. URL: <https://lexikon.stangl.eu/16034/psychosoziale-krise>

2 Vgl. forsa (2023): Hate Speech. Forsa-Studie 2023. Zentrale Untersuchungsergebnisse. URL: https://www.medienanstalt-nrw.de/fileadmin/user_upload/NeueWebsite_0120/Themen/Hass/forsa_LFMNRW_Hassrede2023_Praesentation.pdf (13.05.2024)

3 Vgl. Das NETTZ, Gesellschaft für Medienpädagogik und Kommunikationskultur, HateAid und Neue deutsche Medienmacher*innen als Teil des Kompetenznetzwerks gegen Hass im Netz (Hrsg.) (2024): Lauter Hass – leiser Rückzug. Wie Hass im Netz den demokratischen Diskurs bedroht. Ergebnisse einer repräsentativen Befragung. Berlin. https://kompetenznetzwerk-hass-im-netz.de/download_lauterhass.php

4 Vgl. forsa (2024): Die Situation ehrenamtlicher Bürgermeisterinnen und Bürgermeister. Ergebnisse einer Befragung für die Körber-Stiftung. URL: <https://koerber-stiftung.de/projekte/demokratie-beginnt-vor-ort>

5 Die Beratungsstelle Stop-Stalking Berlin beschreibt Stalking als „das vorsätzliche und beharrliche Nachstellen und Belästigen einer Person, welches diese nicht möchte und als unangenehm erlebt“. Formen des Stalkings im digitalen Raum sind z. B. wiederholte Nachrichten auf Social Media, per SMS oder E-Mail. Stop-Stalking Berlin oder das Anti-Stalking-Projekt unterstützen Sie (auch telefonisch) in Fällen von Stalking.

6 Der Bundesrat definiert Feindeslisten als eine „Sammlung personenbezogener Daten, die beispielsweise durch ausdrückliche oder subtile Drohungen in einem Zusammenhang verbreitet werden, den die Betroffenen und die Öffentlichkeit als einschüchternd oder bedrohlich empfinden können“. (Online verfügbar unter: <https://www.bundesrat.de/DE/plenum/bundesrat-kompakt/21/1004/55.html>)

7 Geben Sie den Namen der Suchmaschine und „Löschantrag nach DSGVO“ in der Suchmaschine ein. In den Suchergebnissen finden Sie die jeweiligen Online-Formulare, mit denen Sie die Löschung beantragen können.

8 Weiterführende Informationen zu Ihrem Recht auf Löschung und den Voraussetzungen finden Sie hier: https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Betroffenenrechte/Betroffenenrechte_L%C3%B6schung_Vergessenwerden.html

9 Hacking bezeichnet in der Regel den Prozess, in dem Geräte, Softwares oder Netzwerke technisch angegriffen werden. Das Ziel dabei ist oft, die Personen, die die Geräte, Dateien oder Programme besitzen, zu schädigen.

10 Phishing bezeichnet den Versuch, Daten (wie Passwörter oder Kreditkartennummern) mittels gefälschter Webseiten, E-Mail-Adressen oder Kurznachrichten abzugreifen. Mehr Informationen finden Sie in der Broschüre „Leitfaden zum Umgang mit digitaler Gewalt“.

11 Cyber Incident Response bezeichnet den Prozess, bei dem auf IT-Bedrohungen wie Cyberangriffe oder IT-Sicherheitsbedrohungen reagiert wird. Auf der Seite des Bundesamtes für Sicherheit in der Informationstechnik finden Sie Unterstützung und Beratung zu Stellen, die Sie beim Prozess der Cyber Incident Response unterstützen können.

12 Beispielhaft können Sie sich an der Netiquette von HateAid orientieren: hateaid.org/netiquette

Impressum

Herausgegeben von

HateAid gGmbH
Greifswalder Straße 4
10405 Berlin

E-Mail: kontakt@hateaid.org
hateaid.org

Sitz der Gesellschaft: Berlin
Registergericht: Amtsgericht
Charlottenburg

Handelsregisternummer:
HRB 203883 B
USt-IdNr.: DE322705305

Geschäftsführerinnen:

Anna-Lena von Hodenberg und
Josephine Ballon

V. i. S. d. P.: Anna-Lena von
Hodenberg (HateAid gGmbH)

Redaktion: Basma Bahgat,
Katharina Heffe, Anna-Lena von
Hodenberg, Samara Feldmann, Eva
Pasch, Anna Wegscheider, Stefanie
Zacharias

Gestaltung: Regina Buschmeier

Druck: Umweltdruck Berlin GmbH

Haftungsausschluss

Die Hinweise in diesem Bericht wurden nach bestem Wissen und Gewissen formuliert. Diese Handreichung ersetzt keine individuelle (juristische) Beratung. Für die Richtigkeit, Vollständigkeit und Aktualität der Informationen übernehmen die Herausgebenden keine Gewähr.

Die erste Auflage dieser Publikation wurde im Rahmen der Förderung des „Kompetenznetzwerkes Hass im Netz“ durch das Bundesprogramm „Demokratie leben!“ des Bundesministeriums für Familie, Senioren Frauen und Jugend im Jahr 2022 entwickelt und gedruckt.

Die vorliegende Neuauflage wurde eigenverantwortlich grundlegend von HateAid gGmbH im Jahr 2026 überarbeitet und herausgegeben.

Spenden

Als gemeinnützige Organisation sind wir auf Spenden angewiesen.

Machen Sie das Internet zu einem besseren Ort und unterstützen Sie HateAid mit einer Dauerspende.

Ihre regelmäßige Spende fließt direkt in unsere tägliche Arbeit – und damit in die Meinungsvielfalt unserer Demokratie.

Schon mit 10 Euro pro Monat machen Sie deutlich:
Menschenrecht gilt auch digital.

Spendenkonto:

Kontoinhaberin: HateAid
Bank: GLS Bank
IBAN: DE04 4306 0967 1231 5982 03
BIC: GENODEM1GLS

hateaid.org/spenden

Krisenplan zum Ausfüllen

Die Zusammenfassung der Handlungsmöglichkeiten und den Krisenplan zum individuellen Ausfüllen können Sie [hier herunterladen](#).

Nicht erstarren, sondern handeln!

Was können Sie tun, um in einer Krisensituation handlungsfähig zu bleiben und sich sicher zu fühlen?
Und wer übernimmt welche Aufgaben?

Analoge Sicherheit

Was sollten Sie tun? Was erreichen Sie damit und wer ist verantwortlich?

Polizeistation vor Ort kontaktieren und ein Sicherheitsgespräch verlangen
Eine Einschätzung der Gefahrensituation durch Fachleute gibt Ihnen Kontrolle und Handlungsfähigkeit.
Sicherheitsmanagement:

In Absprache mit Angriffsbewachung:

Rechtssichere Screenshots erstellen
Rechtssichere Screenshots dokumentieren den Verlauf und die Inhalte dauerhaft. Dies ist wichtig, wenn Sie sich auch rechtlich zur Wehr setzen wollen, z. B. durch eine Anzeige bei der Polizei. Weitere Informationen und Anleitungen finden Sie auf unserer Website.
Community Management:

Meldungsinteresse kurzfristig beantragen
Mehr Informationen hierzu finden Sie im Hauptteil des Krisenplans. Bedenken Sie, dass Ihre Adresse eventuell an weiteren Stellen in Erfahrung gebracht werden kann, und informieren Sie sich frühzeitig über Schutzmöglichkeiten.
Person für Schutz von Privatsphäre und Daten:

Routinen verändern und Altszenen vermeiden
Verlieren Sie Ihre täglichen Abläufe, um schwerer auffindbar zu sein, und bleiben Sie möglichst in Begleitung, besonders an öffentlichen Orten.
Selbstständig organisieren

Übernachtungsort kurzfristig wechseln
Sie können Sie vorübergehend Schutz und Distanz bei akuten Drohungen schaffen und analoge Angriffe vermeiden. Erstellen Sie präventiv eine Liste an Menschen, die Ihnen nahehaben und bei denen Sie für eine Übergangszeit unterkommen können.
Selbstständig organisieren

Soziales Umfeld informieren und sensibilisieren
Sie sensibilisieren Ihr soziales Umfeld, z. B. Familie, Bekannte und Nachbarschaft, für Ihre Situation und bekommen ggf. emotionale Unterstützung. Sensibilisieren Sie auch Bildungseinrichtungen Ihrer Familienmitglieder, besonders vorsichtig mit Ihren personenbezogenen Daten umgehen.
Eigene Nachbarschaft selbstständig informieren
Nachbarnperson im Büro übernimmt die Krisenkoordination:

Bei Veranstaltungen, auf denen Sie als Gast eingeladen sind, Anmeldeliste verlangen, Sicherheitspersonal organisieren und Hausregeln aufleiten lassen
Sie erhalten einen Überblick, wer an Veranstaltungen teilnimmt, können sich vorbereiten und ggf. Gefahren abwenden.
Selbstständig in Absprache mit Safeguard für Netiquette:

Konsequent Safearbeitszeile erstellen
Durch Anzeigen wird die Polizei über Ihre Situation informiert und kann ggf. Sicherheitsmaßnahmen ergreifen. Darüber hinaus können unbekannte Täterpersonen durch geeignete Ermittlungsmaßnahmen ggf. identifiziert und in der Folge zur Rechenschaft gezogen werden.
Sicherheitsmanagement ggf. zusammen mit der Person, gegen die sich die Angriffe richten:

Ihren Standpunkt vertreten

Was sollten Sie tun? Was erreichen Sie damit und wer ist verantwortlich?

Statement veröffentlichen
Sie können Ihre eigene Position klar darstellen.
Für die Kommunikation mit der Presse verantwortlich:

Lokalzeitung kontaktieren
Sie können Ihre eigene Position in unterschiedlichen Zielgruppen vertreten und dem Thema mehr Glaubwürdigkeit und Wichtigkeit verleihen.
Für die Kommunikation mit der Presse verantwortlich:

Digitale Sicherheit

Was sollten Sie tun? Was erreichen Sie damit und wer ist verantwortlich?

Passwörter ändern
Starke Passwörter verringern das Hacking Risiko. Ein Passwort Manager kann Sie dabei unterstützen. Dabei handelt es sich um ein Tool, das sichere Passwörter generiert und diese in einer Datenbank für Sie speichert.
Selbstständig in Absprache mit IT-Sicherheitsmanagement:

Zwei Faktor-Authentifizierung einstellen
Die Zwei Faktor-Authentifizierung erschwert Hacking Angriffe, weil Sie sich nicht nur mit Ihrem Passwort, sondern mit einer zusätzlichen Information einloggen. Die Authentifizierung kann z. B. über einen Code erfolgen, der Ihnen per Mail zugesandt wird.
Selbstständig mit Unterstützung von IT-Sicherheitsmanagement:

Sensible Informationen in Netz suchen und ggf. löschen
Sie schützen die eigene Privatsphäre.
Person für Schutz von Privatsphäre und Daten:
(ggf. HateAid zur Unterstützung kontaktieren)

Bei Hacking Verdacht externe IT Expertise einbeziehen
Hacking Angriffe können unterschiedlich gefährlich sein. Mit externer Unterstützung können Sie die eigene IT Sicherheit wiederherstellen und die Aufklärung des Vorfalls vorantreiben.
IT-Sicherheitsmanagement:

Social-Media-Kommunikation

Was sollten Sie tun? Was erreichen Sie damit und wer ist verantwortlich?

Kommentarfunktion auf den eigenen Social-Media Kanälen einschränken
Passen Sie die Kommentareinstellungen in der Kommentarfunktion an (z. B. „öffentlich“ – „privat“ oder Blockade für bestimmte Begriffe).
Community Management:

Bei Bedarf Social-Media Konten für eine kurze Zeit deaktivieren
Ihr Konto wird nicht gelöscht, sondern für eine Zeit unsichtbar geschaltet. Wenn Sie Ihr Konto nach der Krise wieder verwenden wollen, müssen Sie sich in der Regel neu erneut einloggen. Damit endet die Deaktivierung. Das Konto teilweise zu deaktivieren, kann zu mehr Entlastung und Abgrenzung beitragen.
Community Management:

Inhalte auf Social-Media Plattformen melden
Wenn bereits rechtssichere Screenshots (siehe links) erstellt wurden, können Sie die Inhalte melden. Gemeldete Inhalte werden im besten Fall von den Plattformen gelöscht.
Community Management:

Angehefts auf Social-Media Plattformen blockieren
Wenn Sie die Profile der AngreiferInnen „melden“ und für sich „blockieren“, sehen diese Personen nicht, was Sie zukünftig veröffentlichen, und können Sie nicht kontaktieren.
Community Management:

Kommentare, die der Hetzseite widerprechen, konsequent löschen
Sie zeigen Grenzen auf und schaffen einen sicheren Ort für Menschen, die regelmäßig mit Ihnen und mit anderen interagieren wollen.
Community Management:

In Absprache mit Safeguard für Netiquette:

Unterstützende aktivieren
Auf diese Weise können Sie auf Ihren Kanälen Unterstützung und Solidarität suchen und aktivieren, z. B. in Form von öffentlichem Zuspruch durch Ihr Netzwerk oder Gegenrede.
Krisenkoordination:



