Bundesministerium
des Innern
und für Heimat

Empfehlungen der BLoAG Hybrid | 11. Dezember 2023

Sensibilisierung im Umgang mit hybriden Bedrohungen einschließlich Desinformation

Empfehlungen der BLoAG Hybrid zur Sensibilisierung im Umgang mit hybriden Bedrohungen einschließlich Desinformation

Zur Weitergabe an Länderministerien und Kommunen

Hybride Bedrohungen bezeichnen verschiedene Formen illegitimer Einflussnahme auf Staaten durch fremde Staaten. Dabei versuchen diese Staaten, auch mittels nichtstaatlicher Akteure, durch den koordinierten Einsatz verschiedener Instrumente ihre Ziele gegen unsere Interessen und Werte offen oder verdeckt durchzusetzen. Sie beabsichtigen hierbei, unsere Demokratie zu schwächen und zu destabilisieren. Zu den eingesetzten Instrumenten gehören beispielsweise Desinformation, Cyberangriffe auf staatliche Stellen und Unternehmen, Spionage und Wirtschaftsspionage, Diebstahl von geistigem Eigentum, wirtschaftliche Einflussnahme, z.B. durch Investition in Schlüsselindustrien, Sabotage von Kritischen Infrastrukturen und Einflussnahme auf freie Wahlen. Aus sicherheitspolitischer Sicht ist Desinformation den hybriden Bedrohungen zuzuordnen, wenn sie direkt oder indirekt durch fremde Staaten gesteuert wird.[1] Dabei ist zu beachten, dass Desinformation auch von inländischen Akteuren absichtlich zur Destabilisierung eingesetzt und verbreitet wird.

Hybride Bedrohungen betreffen alle politischen und gesellschaftlichen Ebenen. Dabei können verschiedene Mittel kombiniert werden, sodass eine koordinierte Kampagne entsteht. Mitunter ist es schwierig, einzelne Ereignisse als Teil einer größeren Kampagne zu erkennen und so rechtzeitig zu reagieren.

Ein bekanntes Beispiel für Desinformation mit Potenzial zur Spaltung der Bevölkerung ist der „Fall Lisa“[2] aus dem Jahr 2016. Ein weiteres Beispiel ist der Fall des vermeintlich zu Tode geprügelten Jugendlichen in Euskirchen 2022.[3] Als Beispiel für ausländische Manipulation und Einflussnahme im Informationsraum kann die sogenannte „Doppelgänger“-Kampagne[4] angeführt werden. Als Beispiel für Cyberangriffe sind die Phishing-Attacken des Cyberakteurs „Ghostwriter“ zu nennen.[5] Auch Vereine, Kulturinstitute oder Städtepartnerschaften können zur illegitimen Einflussnahme genutzt werden.[6] Die unlängst berichtete Ausspähung polnischer

[1] Vgl. https://www.bmi.bund.de/DE/themen/heimat-integration/wehrhafte-demokratie/abwehr-hybrider-bedrohungen/abwehr-hybrider-bedrohungen-node.html. Hier handelt es sich um eine Charakterisierung hybrider Bedrohungen einschließlich Desinformation

[2] https://www.bpb.de/themen/migration-integration/russlanddeutsche/271945/der-fall-lisa/
https://www.sueddeutsche.de/panorama/urteil-in-berlin-fall-lisa-endet-mit-bewaehrung-1.3553054

[3] https://www.ruhrnachrichten.de/regionales/ukrainer-pruegeln-jugendlichen-in-nrw-zu-tode-polizei-warnt-vor-fake-video-w1737591-2000483586/. Vgl. auch Mascolo, Georg „Die neuen Waffen“ (Süddeutsche Zeitung, 10.06.2023)

[4] https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/2023/article/statement-by-ms-catherine-colonna-foreign-digital-interference-france-s
https://euvsdisinfo.eu/de/eines-dieser-dinge-ist-nicht-wie-die-anderen/

[5] https://www.spiegel.de/politik/deutschland/russischer-hack-erneute-attacke-hack-auf-bundestag-sieben-abgeordnete-betroffen-a-75e1adbe-4462-4e30-bd94-96796aed6b8a

[6] https://merics.org/de/studie/stadt-land-fluss-im-blick-beijings-chinas-subnationale-diplomatie-deutschland
https://www.welt.de/politik/ausland/article235115984/Staedtepartnerschaften-Foederalismus-spielt-China-in-die-Haende.html
https://www.faz.net/aktuell/politik/inland/china-die-strategie-hinter-den-staedtepartnerschaften-18832083.html

Bahnstrecken wäre grundsätzlich auch in Deutschland denkbar.[7] Ein Beispiel für Wissensabfluss ist der Vorfall an der Universität Heidelberg im Jahr 2019.[8]

Die große Herausforderung besteht darin, hybride Bedrohungen zu erkennen und abzuwehren, Maßnahmen zu koordinieren sowie die Resilienz von Staat und Gesellschaft zu stärken. Dies kann durch folgende Maßnahmen gefördert werden:

1. Informationsaustausch

Informieren Sie Ihre Mitarbeitenden über hybride Bedrohungen einschließlich Desinformation. Identifizieren Sie beispielhaft Bereiche in Ihren Arbeitseinheiten, in welchen fremde Staaten Einfluss nehmen könnten, und sorgen Sie dafür, dass Ihre Mitarbeitenden über die Risiken und über konkrete Werkzeuge der Einflussnahme gut informiert sind. Richten Sie eine zuständige Stelle /Ansprechperson für hybride Bedrohungen ein und führen Sie regelmäßig Informationsveranstaltungen durch. Ermutigen Sie Ihre Mitarbeitenden, sich bei Unsicherheiten an Ihre zuständige Stelle/verantwortliche Person zu wenden.

2. Öffentlichkeitsarbeit

Intensivieren Sie die proaktive themenbezogene Öffentlichkeitsarbeit im Rahmen der eigenen Zuständigkeit. Hierdurch kann die öffentliche Unterstützung für Maßnahmen zur Bekämpfung hybrider Bedrohungen und Desinformation erhöht werden.

3. Umgang mit Desinformation

Fördern Sie den Austausch zwischen Ihren Pressestellen und den Fachbereichen, u.a. um gezielt verbreiteten falschen oder irreführenden Informationen entgegenzuwirken. Kommunizieren Sie stets proaktiv, transparent und faktenbasiert. Stellen Sie Falschinformationen, die Sie direkt betreffen, zügig richtig.

4. Schutz Kritischer Infrastrukturen

Identifizieren Sie in Ihrem Fachbereich relevante Kritische Infrastrukturen. Tauschen Sie sich mit den Betreibern regelmäßig zu deren betrieblichen Risikoanalysen aus. Sensibilisieren Sie die KRITIS-Betreiber dafür, basierend auf den Risikoanalysen geeignete Resilienzmaßnahmen zur Aufrechterhaltung ihrer Funktionsfähigkeit zu treffen. Um die Versorgung der Bevölkerung auch bei Angriffen aufrechtzuerhalten, können Sie gemäß DIN SPEC 91390:2019-12 mit den KRITIS-Betreibern in Form eines Integrierten Risikomanagements (IRM) zusammenarbeiten. Berücksichtigt werden sollten die vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichten Schutzkonzepte und Empfehlungen.

[7] https://www.rnd.de/politik/polen-russischer-spionagering-soll-polnische-bahnstrecken-ausgespaeht-haben-versteckte-kameras-PQNYUEW5RS347HYZXI4D5JHYYE.html

[8] https://correctiv.org/aktuelles/china-science-investigation/2023/06/13/wie-die-uni-heidelberg-teil-von-chinas-quantenstrategie-wurde/

5. Cybersicherheit

Machen Sie sich mit den konkreten Vorgaben zur IT-Sicherheit Ihrer Länder- oder Kommunalverwaltungen vertraut und nutzen Sie das Beratungsangebot der jeweils zuständigen IT-Sicherheitsorganisation. Sorgen Sie insbesondere für eine ausreichende IT-Sicherheit, indem Sie Ihre Systeme, Daten und Netzwerke grundsätzlich auf einem sicheren Niveau betreiben, regelmäßig auf Schwachstellen überprüfen und diese schließen. Nutzen Sie starke Passwörter und Zwei-Faktor-Authentifizierungsverfahren sowie Verschlüsselung, um die Sicherheit Ihrer Daten zu erhöhen. Beziehen Sie alle Endgeräte in Büros, bei Telearbeit und Homeoffice in ein robustes Zugangsmanagement ein. Sensibilisieren Sie ihre Mitarbeitenden und stellen Sie Ansprechpersonen zur Verfügung.

6. Notfallpläne

Erstellen Sie für mögliche Szenarien anschlussfähige, verständliche Notfallpläne und Krisenreaktionsstrategien, um schnell und effektiv handeln zu können. Testen Sie diese regelmäßig, wo möglich unter Realbedingungen, um sicherzustellen, dass sie im Ernstfall funktionieren.

7. Wirtschafts- und Wissenschaftsschutz

Der Schutz von Unternehmen und Forschungseinrichtungen vor Spionage und Sabotage muss ein Thema für die Führungsebene sein. Sorgen Sie für ein offenes Arbeitsklima und schaffen Sie eine positive Fehlerkultur, denn zufriedene Mitarbeitende werden seltener zu Innentätern. Führen Sie eine Risikoanalyse durch. Identifizieren Sie ihre schützenswerten materiellen und immateriellen Güter, überlegen Sie, welche Akteure daran Interesse haben könnten und wie schädigendes Verhalten, z.B. Diebstahl oder Manipulation, möglich wäre. Leiten Sie darauf aufbauend Schutzmaßnahmen ab. Klassifizieren Sie entsprechende Daten nach Vertraulichkeitsklassen und legen Sie fest, wer darauf Zugriff haben muss. Prüfen Sie bei neuen Kooperationen genau, mit wem Sie zukünftig zusammenarbeiten. Recherchieren Sie am besten in der Sprache Ihres potenziellen Geschäfts-/Kooperationspartners. Weiterführende Informationen zum Thema finden Sie auf den Seiten des Bundesamtes für Verfassungsschutz.

8. Zusammenarbeit

Identifizieren Sie die für Kooperationen geeigneten und erforderlichen Organisationen, Behörden, Institutionen und Interessenvertretungen. Schaffen Sie Netzwerkstrukturen mit den erforderlichen Organisationen und Arbeitseinheiten und tauschen Sie sich regelmäßig über Bedrohungen aus, um gemeinsam Lösungen zu finden.

9. Aus- und Fortbildung

Schaffen Sie regelmäßig aktualisierte Informations- sowie Aus- und Fortbildungsangebote für Ihre Mitarbeitenden zum Umgang mit hybriden Bedrohungen einschließlich Desinformation. Identifizieren Sie die Organisationseinheiten in Ihren Häusern, die besonders intensiv fortgebildet werden sollten. Ermutigen Sie Ihre Mitarbeitenden, regelmäßig Kurse zu

Medienkompetenz zu besuchen, um auch mit der schnellen Entwicklung neuester Medien Schritt zu halten und Desinformation frühzeitig erkennen zu können.

10. Qualifikation von Mitarbeitenden

Mitarbeitende, die u.a. im Bereich der Internationalen Beziehungen tätig sind, sollten über die jeweils erforderlichen Qualifikationen verfügen, wie beispielsweise entsprechende Sprachkenntnisse, Umgang mit sozialen Medien oder fachspezifische Lehrgänge, oder entsprechend weiterqualifiziert werden und für die spezifischen Risiken in der Zusammenarbeit mit den entsprechenden Staaten sensibilisiert werden.

11. Sicherheitsempfindliche Tätigkeiten von Mitarbeitenden

Machen Sie sich mit den Vorschriften zum personellen Geheim- und Sabotageschutz vertraut und wenden Sie sich in Zweifelsfällen an die für Sie zuständige Stelle im Bereich Geheimschutz. Identifizieren Sie sicherheitsrelevante Organisationseinheiten und Tätigkeitsbereiche (z.B. IT-Bereich, Leitstelle Schriftgutverwaltung). Führen Sie sorgfältige Hintergrundprüfungen durch, bevor Sie neue Mitarbeitende in sensiblen Bereichen einstellen. Neben der Sicherheitsüberprüfung im personellen Geheim- und Sabotageschutz kann insbesondere das sog. Pre-Employment Screening eine sicherheitsorientierte Personalauswahl unterstützen.

Diese Empfehlungen sind nicht abschließend und sollten je nach Branche, Größe und Art der Organisation angepasst werden. Es ist notwendig, regelmäßig zu überprüfen, ob die Maßnahmen noch aktuell sind. Konkrete funktionale Erreichbarkeiten der zuständigen Stelle / Ansprechperson (E-Mail, Tel., etc.) sollten ebenfalls aktuell zur Verfügung gestellt werden.

Impressum

Herausgeber
Bundesministerium des Innern und für Heimat, 11014 Berlin
Internet: www.bmi.bund.de

Stand
Dezember 2023

Artikelnummer: BMI24013

Weitere Publikationen der Bundesregierung zum Herunterladen und zum Bestellen finden Sie ebenfalls unter: www.bundesregierung.de/publikationen