KONRAD ADENAUER STIFTUNG

IDEEN FÜR WOHLSTAND UND GERECHTIGKEIT

Hybride Bedrohungen koordiniert abwehren

Es wird ein Abwehrzentrum gegen hybride Bedrohungen aufgebaut.

Ferdinand Gehringer

kas.de

Die Menschen in Deutschland machen sich Sorgen um die Sicherheit. Sie fürchten sich vor einer weiteren Eskalation zwischen der Ukraine und Russland und einem unmittelbaren Angriff Russlands auf Deutschland. Doch Angriffe gibt es bereits heute. Staatliche und nicht-staatliche Akteure versuchen tagtäglich auf die Innere Sicherheit in Deutschland einzuwirken und gefährden diese.

Um die Sicherheit in Deutschland zu gewährleisten und diese Angriffe besser zu erkennen sowie abzuwehren, wird ein Abwehrzentrum gegen hybride Bedrohungen eingerichtet. Durch dieses Abwehrzentrum können hybride Bedrohungen[1] frühzeitig erkannt, in einen Zusammenhang gesetzt und schnell abgewehrt werden.

Deutschland ist Ziel hybrider Bedrohungen

Deutschland ist bereits seit längerem Ziel von hybriden Einflussnahmen staatlicher und nicht staatlicher Akteure. Ganz gleich, ob der Cyberangriff durch eine russische Hackergruppe auf die Parteizentrale der SPD 2023[2], der Angriff chinesischer Hacker auf das Bundesamt für Kartographie und Geodäsie (BKG) 2021[3], pro-russische Desinformationskampagnen wie die Doppelgänger-Kampagne[4], Sabotageakte an Lichtwellenleiterkabeln der Deutschen Bahn[5], Fälle mutmaßlicher Spionage für Russland beim Bundesnachrichtendienst[6], Drohnenflüge über kritischer Infrastruktur[7] oder russische Forschungsschiffe in der Ostsee, die den Meeresboden kartographieren[8]: Die Anzahl und Dichte der hybriden Einflussnahmen auf Deutschland haben zugenommen.

Hybride Bedrohungen umfassen den kombinierten Einsatz verschiedener Mittel wie Cyberangriffe, gezielte Propaganda und Desinformation, Sabotage, Spionage, Angriffe auf kritische Infrastrukturen, wirtschaftlichen Druck und Migration.[9] Diese Bedrohungen zielen darauf ab, die Schwachstellen liberaler Gesellschaften, der sozialen Marktwirtschaft, der demokratischen Willensbildung und digitalisierter Prozesse auszunutzen. Die Hauptziele bestehen darin, staatliche Interessen zu beeinträchtigen, Gesellschaften zu verunsichern und zu destabilisieren sowie die öffentliche Meinung zu beeinflussen. Deutschland steht dabei besonders im Fokus Russlands, aber auch China und der Iran zeigen zunehmende Aktivitäten in diesem Bereich.

Sicherheitsstrukturen sind auf hybride Bedrohungen nicht ausgerichtet

Bestehende Sicherheitsstrukturen und föderale Zuständigkeitsverteilungen in Deutschland ermöglichen es häufig nicht oder erst sehr spät, einzelne Einflussnahmen in Zusammenhang zu setzen sowie schnell auf diese zu reagieren. Die behördlichen Zuständigkeiten lassen sich zum Zeitpunkt des Angriffs nicht immer klar bestimmen und schließen eine schnelle Reaktion aus. Bei einem Angriff ist es für Sicherheitsbehörden nicht sofort ersichtlich, ob es sich um eine militärische, nachrichtendienstliche Operation eines Staates oder um Aktivitäten privater bzw. krimineller Gruppen aus dem Inland oder aus dem Ausland handelt. Vor allem staatliche Angreifer nutzen private und kriminelle Gruppen, um die Herkunft des Angriffs zu verschleiern.[10]

Derzeit gibt es kein Zentrum, in dem Informationen über Desinformationskampagnen, Cyberangriffe, Angriffe auf Kritische Infrastrukturen, Sabotage und Spionage in Echtzeit gebündelt zusammenlaufen und ausgewertet werden. Ein bundesweit einheitliches Lagebild zu hybriden Bedrohungen gibt es

nicht. Die Sicherheitsbehörden in Deutschland haben ihre eigenen Lagebilder, die sich in größten Teilen doppeln und überlagern. So wurden die Task Force gegen Desinformation im Bundesministerium des Innern und für Heimat und ein Gemeinsamer Koordinierungsstab Kritische Infrastruktur (GEKKIS) in den letzten beiden Jahren eingerichtet. Zudem gibt es bspw. mit dem Nationalen Cyberabwehrzentrum (Cyber-AZ), dem Kommando Cyber- und Informationsraum der Bundeswehr, dem Bundes Security Operations Center (BSOC) Organisationsstrukturen auf Bundesebene, die ihre Lagebilder und Erkenntnisse aus dem Cyberraum nur bedingt austauschen.

Abwehrzentrum besteht aus Lage- und Analysezentrum

Das Abwehrzentrum gegen hybride Bedrohungen besteht aus einem Lage- und einem Analysezentrum. Es ist im Geschäftsbereich des Bundeskanzleramtes als Bundesoberbehörde angesiedelt. Alle relevanten und notwendigen Behörden sind mit einem Vertretenden im Abwehrzentrum angedockt – das Bundeskriminalamt, die Bundespolizei, das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst, der Militärische Abschirmdienst, die Bundeswehr, das Bundesamt für Sicherheit in der Informationstechnik, das Bundesamt für Migration und Flüchtlinge, das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, die Bundesnetzagentur, das Zollkriminalamt, die Landeskriminalämter, die Landesämter für Verfassungsschutz und die Generalbundesanwaltschaft. Die Leitung des Zentrums obliegt dem Bundeskanzleramt.

Vernetzung und Analyse der Lage ermöglichen schnelles Handeln

Im Lagezentrum werden die erheblichen Vorfälle in einem dynamischen Echtzeit-Lagebild-Dashboard dargestellt. Informationen der einzelnen Mitgliedsorganisationen und die verschiedenen Lagebilder laufen in dem Zentrum in Echtzeit zusammen. So können eine gemeinsame Gesamtlage festgestellt und notwendige operative Maßnahmen zur Bekämpfung oder Reaktion getroffen werden. Angreifer werden künftig Cyberangriffe, Sabotage oder Spionage und Informationsoperationen noch gezielter und koordinierter ausführen. Das Dashboard umfasst Cyberangriffe, Desinformationskampagnen, vorherrschende Narrative in Medien und sozialen Netzwerken sowie die wesentliche Grundversorgung in Deutschland (bspw. Energie-, Wasser-, Gesundheits-, Nahrungsmittelversorgung und Internet).

Aktuelle Vorfälle und gegenwärtige Versorgungslage werden im Analysezentrum ausgewertet und die Intensität des Vorfalles wird bestimmt. Durch die Anwesenheit sämtlicher erforderlicher und thematisch betrauter Behörden ist eine interdisziplinäre Analyse der Lage möglich. Je nach Intensität des Vorfalls stehen unterschiedliche Krisenreaktionsmechanismen für die zuständigen Behörden zur Verfügung. Zudem erstellt das Analysezentrum Profile der Aktivitäten der Angreifer und identifiziert Merkmale bestimmter Angriffe. Die Angriffsmuster und Eigenschaften der Angreifer werden in einer Analysedatenbank erfasst und gespeichert. So lassen sich bei Vorfällen schneller Angriffsmuster erkennen und die Zuordnung auf bestimmte Akteure kann ohne größeren Zeitverlust erfolgen.

Außerdem werden die eigenen systemischen Schwachstellen der Bundesrepublik Deutschland fortlaufend analysiert. Unter anderem derzeit vorherrschende Narrative mit Polarisierungs- und Spaltungspotenzialen, Schwachstellen in IT-Systemen, instabile Versorgungsleistungen oder gestörte Lieferketten sowie gesetzgeberische Lücken oder regulatorische Unklarheiten fallen unter mögliche Schwachstellen, die für die Angreifer von Interesse sind.

Das im Koalitionsvertrag vorgesehene Lagezentrum im Bundeskanzleramt, in dem ressortübergreifend ein Gesamtlagebild entstehen soll, kann die Grundlage für das Abwehrzentrum bilden. Zwingend ist allerdings neben dem Lagezentrum auch das dazugehörige Analysezentrum.

Durch das Abwehrzentrum können hybride Bedrohungen und eigene systemische Schwachstellen frühzeitig erkannt, in einen Zusammenhang gesetzt und schnell abgewehrt werden. Die Fähigkeit, diese Bedrohungen schnell zu erkennen und abzuwehren, ist ein entscheidender Faktor für die nationale Sicherheit sowie die Widerstandsfähigkeit von Staat und Gesellschaft.

---

[1] Hybride Bedrohungen bezeichnen eine Kombination aus verschiedenen Taktiken, die von staatlichen oder nichtstaatlichen Akteuren eingesetzt werden, um ein Ziel zu destabilisieren oder zu beeinflussen. Diese Taktiken umfassen oft eine Mischung aus militärischen, wirtschaftlichen, politischen und informationstechnischen Maßnahmen. Beispiele hierfür sind Cyberangriffe, Desinformationskampagnen, wirtschaftlicher Druck und sogar verdeckte militärische Operationen

2 https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/05/aktuelle-Cyberangriffe.html [letzter Abruf: 05.05.2025].

[3] https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/07/cyberangriff-bkg.html [letzter Abruf: 05.05.2025].

[4] https://www.auswaertiges-amt.de/blob/2660362/73bcc0184167b438173e554ba2be2636/technischer-bericht-desinformationskampagne-doppelgaenger-data.pdf [letzter Abruf: 05.05.2025].

[5] https://www.tagesschau.de/wirtschaft/bahn-schutz-sabotage-100.html [letzter Abruf: 05.05.2025].

[6] https://www.mdr.de/nachrichten/deutschland/panorama/prozess-gegen-bnd-mitarbeiter-russland-spionage-100.html [letzter Abruf: 05.05.2025].

[7] https://www.ndr.de/nachrichten/schleswig-holstein/Drohnen-ueber-Brunsbuettel-Man-moechte-Unsicherheit-schaffen,drohnen402.html [letzter Abruf: 05.05.2025].

[8] https://www.tagesschau.de/investigativ/ndr-wdr/russland-ostsee-spionage-100.html [letzter Abruf: 05.05.2025].

[9] https://www.bmvg.de/de/themen/sicherheitspolitik/hybride-bedrohungen/was-sind-hybride-bedrohungen--13692 [letzter Abruf: 05.05.2025].

[10] https://www.computerworld.ch/security/microsoft/kriminelle-gruppen-staatliche-hacker-arbeiten-haeufig-2937086.html [letzter Abruf: 05.05.2025].

Der Autor

Ferdinand Gehringer
Referent Cybersicherheit
Geheimschutzbeauftragter
Analyse und Beratung

Impressum

Konrad-Adenauer-Stiftung e. V.
Ferdinand Gehringer
Referent Cybersicherheit
ferdinand.gehringer@kas.de

kas.de

Herausgeberin: Konrad-Adenauer-Stiftung e. V., 2025, Berlin
Satz: Konrad-Adenauer-Stiftung e. V.