TAGESSPIEGEL
BACKGROUND

Cybersecurity

Auswärtiges Amt finanziert Datenbank für Cybervorfälle

Die Bundesregierung fördert den Aufbau einer öffentlichen Datenbank zu Cybersicherheitsvorfällen. Das Europäische Repositorium für Cybervorfälle (EuRepoC) soll nicht nur aktuelle Fälle listen, sondern die Grundlage für schnellere politische Reaktionen schaffen.

von **Paul Dalg**

veröffentlicht am 23.02.2022

Als Startfinanzierung für die ersten drei Jahre stellt das **Auswärtige Amt** 1,2 Millionen Euro zur Verfügung, weitere Mittel kommen vom **dänischen Außenministerium**. Die Förderung wird heute bekannt gegeben und verteilt sich auf ein **Konsortium der Universitäten Heidelberg, Innsbruck und der Stiftung Wissenschaft und Politik**.

Die drei Kooperationspartner bringen jeweils ihren eigenen Forschungsblick ein: **Sebastian Harnisch** vom **Institut für Politische Wissenschaft der Universität Heidelberg** übernimmt die politische Analyse und fungiert als Projektverantwortlicher; **Annegret Bendiek und Matthias Schulze** von der **Stiftung Wissenschaft und Politik (SWP)** liefern die außenpolitischen und europäischen Implikationen von Cybervorfällen. **Matthias C. Kettemann** vom **Institut für Theorie und Zukunft des Rechts der Universität Innsbruck (UIBK)** ist im Projekt für die völkerrechtliche Einschätzung zuständig.

Durch die Bundesförderung werden bei den drei Projektpartnern zehn neue Stellen geschaffen. Sowohl mit weiteren Geldgebern als auch mit weiteren Forschungspartnern laufen EU-weit bereits Gespräche.

Wissensdatenbank und Monitor für Cyberangriffe

Laut Sebastian Harnisch soll das Projekt weitaus mehr werden als nur eine **Open-Source-Datenbank für Cyberangriffe**: „Das Ziel ist es, erstmals ein offenes, wissenschaftliches und gesamteuropäisches Lagebild zu erstellen, um die **EU-Cyberdiplomatie** und die **zivilgesellschaftliche Resilienz** zu stärken." Die Forscher:innen müssen nicht bei Null anfangen, da mit dem Heidelberg **Cyberkonfliktdatensatz** bereits im Institut ein Datensatz *mit über 1.000 Cybervorfällen (https://heidata.uni-heidelberg.de/dataset.xhtml?persistentId=doi:10.11588/data/KDSFRB)* vorliegt, auf dem nun aufgebaut werden kann.

Auf Basis der bisherigen Daten und Einschätzungen soll auch bei neuen Cyberangriffen eine schnelle Einordnung möglich werden. Es sei angedacht, im Falle eines aktuellen Vorfalls möglichst rasch wissenschaftlich fundierte Einschätzungen bereitzustellen, erklärt Matthias Kettemann von der Universität Innsbruck im Gespräch mit Tagesspiegel Background: „Wir wollen die Debatte mit frei verfügbaren Fakten unterstützen."

Ad-hoc-Einschätzungen: Welche Relevanz hat der aktuelle Angriff?

Das **Repositorium** sei sowohl für die interessierte Öffentlichkeit, für Journalist:innen, aber auch für politisch Verantwortliche gedacht. Bisher falle es einigen dieser Stakeholder und Multiplikatoren mitunter schwer, **unterschiedliche Formen von Cybervorfällen** gemäß der tatsächlichen Schwere und Relevanz richtig einzuordnen.

„Es gibt sehr viele unterschiedliche Arten von Angriffen und Täter:innen mit sehr unterschiedlicher Motivation", erklärt Kettemann. „Hier ist es für die politische und öffentliche Debatte wichtig, schnell eine mehrdimensionale Bewertung bereitzustellen: politisch, rechtlich und technisch." Längst nicht jede **Distributed-Denial-of-Service-Attacke (DDoS)** müsse als Cyberangriff gewertet werden, auf den politisch wie rechtlich reagiert werden muss, sagt er. Und im Gegenzug könne eine technisch vergleichsweise simple **Desinformationskampagne** im Vorfeld einer demokratischen Wahl sehr wohl als schwerer Cyberangriff eingestuft werden.

Vom Ausspähen bis zu Cyberkriegshandlungen

Der Fokus auf Cybervorfälle ist daher weit gewählt, sagt Kettemann. Aus der Perspektive des Rechtswissenschaftlers gehe es auch um die Frage, „ob erfasste Cyberangriffe gegen Staaten als Kriegshandlung eingestuft werden können" und wie die EU dann darauf antworte. Doch auch **Spähangriffe** gegen einzelne

Personen sollen in die Datenbank aufgenommen werden. „Hier bewirken wir eine Humanisierung der Cybersicherheitsforschung."

Von **mehr Transparenz in der globalen Konfliktlandschaft** im Cyberraum spricht auch Matthias Schulze von der Stiftung Wissenschaft und Politik: „Keine leichte Aufgabe in Anbetracht der Schwierigkeit der Attribution von Urheberinnen und Urhebern." Gerade deswegen sei es wichtig, den Überblick zu behalten, ergänzt Annegret Bendiek, Expertin für Cyberpolitik an der SWP. Für das Projekt sind am Standort Berlin *bereits seit gestern drei Stellen ausgeschrieben (https://www.swp-berlin.org/karriere)*.

Der Diskussion um Attribution eine neue Tiefe geben

In der medialen Berichterstattung endet die Frage der Täter:innen noch zu oft bei dem Klischee „mutmaßlich chinesische oder russische Hacker". Auch hier hoffen die Forschenden, das ihre Analysen Journalist:innen und politische Entscheider zu besseren Unterscheidungen befähigen: Handelt es sich bei der Tat eher um einen rein **finanziell motivierten Einbruch** mit Täter:innen aus dem Milieu der „digitalen Kleinkriminellen"? Oder gibt es Anzeichen, die auf eine g**roßangelegte Aktion durch eine ausländische Macht** oder eine hochprofessionelle Tätergruppe hinweisen?

Die Frage, ob man es im Cyberraum mi**t organisierter Kriminalität, staatlich-orchestrierten Taten oder Einzelfällen** zu tun habe, ist dabei mehr als eine wissenschaftliche Leidenschaft zur Kategorisierung. „Nur wenn wir wissen, mit was es zu tun haben, können wir Maßnahmen umsetzen, die nicht an den Ursachen vorbeigehen", sagt Kettemann. Er erwartet einen deutlichen Mehrwert durch die neuen Analysekapazitäten – sowohl für die **europäische Regulierungsdebatte bei Cybersicherheit** als auch im Hinblick auf **diplomatische Handlungsfähigkeiten**.

Die Debatte um **global einheitliche Cybernormen** laufe bereits seit mehr als zehn Jahren, sagt er. Doch im Vergleich mit Auseinandersetzungen zu Land oder zu See stehe man noch am Anfang. Obwohl **völkerrechtswidriges Verhalten auch im Cyberraum** schwer zu ahnden ist, sagt Kettemann: „Eine öffentliche Ächtung ist nicht sinnlos." Umso mehr Staaten sich auf ein internationales Regelwerk einigen, desto leichter werde es, Cyberangriffe zu ächten und über Sanktionen zu diskutieren. Auch selbstständige Verpflichtungen auf eine gute **Cyberpolicy**, wie sie derzeit in Schweden oder

Neuseeland vorbereitet werden, hätten mittel- bis langfristig einen messbaren Effekt.