TAGESSPIEGEL
BACKGROUND

Cybersecurity

„Wir wollen Cybersicherheitsinformationen zugänglicher machen“

Matthias Schulze, Kerstin Zettl-Schabath und Matthias Kettemann (v. l.). (Fotos: Stiftung Wissenschaft und Politik, Universität Heidelberg, Universität Innsbruck)

Mit dem Europäischen Repositorium für Cybervorfälle wollen die Projektpartner der Wissenschaft, staatlichen Stellen und der Öffentlichkeit systematisch Informationen zu politisch relevanten Cyberangriffen zur Verfügung stellen. Ein Interview über Zielstellung und Ausrichtung des Projekts.

von **Johannes Steger** veröffentlicht am 07.11.2022

*Wenn heute das Europäische Repositorium für Cybervorfälle (https://eurepoc.eu/) (**EuRepoC**) live geht, soll damit nicht nur eine bessere Übersicht über aktuelle Zwischenfälle entstehen, gleichzeitig kann so auch eine Grundlage für schnellere politische Reaktionen geschaffen werden. Als Startfinanzierung für die ersten drei Jahre hatte das Auswärtige Amt Anfang des Jahres 1,2 Millionen Euro zur Verfügung gestellt (Background*

berichtete (https://background.tagesspiegel.de/cybersecurity/auswaertiges-amt-finanziert-datenbank-fuer-cybervorfaelle)), weitere Mittel kamen vom dänischen Außenministerium. Das Projekt wird realisiert und betreut von einem Konsortium der Stiftung Wissenschaft und Politik und der Universitäten Heidelberg und Innsbruck. Im Interview geben die Projektbeteiligten Matthias Schulze, Kerstin Zettl-Schabath und Matthias Kettemann einen Überblick zur Funktionsweise von EuRepoC.

Welche initiale Motivation steht hinter dem Projekt EuRepoC?

Matthias Schulze: Wenn ich mir zum Beispiel das Phänomen von bewaffneten Konflikten oder Kriegen anschaue, existieren eine ganze Menge an empirischen Daten und es gibt zahlreiche Datenbanken, die etwa aufzeigen, welche Arten von Kriegen es gibt, wo sie stattfanden und wie viel Menschen dabei gestorben sind. Was sind die Auslöser? Und gibt es historische Trends? All diese Fragen kann ich mithilfe von Daten beantworten. Im Bereich des Cyberkonflikts sind wir ehrlicherweise blank, wenn es um quantitative und statistische Daten geht.

Wofür brauchen wir diese Datengrundlage?

Schulze: Wenn keine Daten vorliegen, ist die Analyse immer gezwungen sich auf Einzelfälle zu konzentrieren – dann landen wir schnell bei Themen wie „Stuxnet“ oder „Notpetya“. Das ist natürlich interessant, lässt aber keine generalisierten Aussagen zu und man kann die Fälle auch schlecht vergleichen. Es gibt also wenige Möglichkeiten herzuleiten, welcher Vorfall die größeren Auswirkungen hatte. Die politische Bewertung, ob und wie eine Reaktion erfolgen soll, ist also schwierig. Es braucht eine Messlatte, die die Intensität einer Reaktion festhält und so für zukünftige Fälle eine Vergleichbarkeit schafft. Das ist in Deutschland und der Europäischen Union bislang nicht möglich, weil dieser Maßstab fehlt.

Nun geht das von einem Fall aus, in dem sehr klar ist, welche Akteure welche Operationen durchgeführt haben. Nun gab es etwa einen *Vorfall wie in Montenegro (https://background.tagesspiegel.de/cybersecurity/was-steckt-hinter-dem-cyberangriff)*, bei dem weder klar wurde, was eigentlich

passiert ist noch ist wirklich aufgeklärt, ob das nun ein Akt von Kriminellen oder einer staatlichen APT-Gruppe gewesen ist. Wie sähe so ein Vorfall im EuRepoC aus?

Kerstin Zettl-Schabath: Die Unterscheidung nehmen wir entsprechend der vorliegenden Attribution vor. Wir können sehr detailliert erfassen, welche Akteure zu welchem Zeitpunkt, in welcher Form eine Attribution vorgenommen haben. Selbst wenn uns eine Attribution nicht hundertprozentig einleuchtend erscheint, nehmen wir diese auf, weil sie für das Gesamtverständnis eines Vorfalls relevant ist. Allerdings können wir einer Attribution auch Metainformationen hinzufügen, um etwa kenntlich zu machen, aus welcher Quelle sie stammt und diese Urheberschaft einordnen.

Bei dem *Cyberzwischenfall in Albanien (https://background.tagesspiegel.de/cybersecurity/cisa-veroeffentlicht-neue-erkenntnisse)* gab es etwa eine Attribution des Landes selbst gen Iran – was den Abbruch der diplomatischen Beziehungen zur Folge hatte, die US-Regierung verhängte Sanktionen. EU und Nato hielten sich indes mit einer Attribution zurück. Wie werden solche Fälle abgebildet?

Matthias Kettemann: Der Albanien-Fall ist insofern auch interessant, weil wir nicht nur Daten über die Vorfälle selbst erfassen, also welches Land zu welchem Zeitpunkt, mit welcher Art von Cyberangriff betroffen gewesen ist, sondern auch den Lebenszyklus des Vorfalls und der Nachwirkungen. Wir ergänzen also etwa Aspekte wie politische Folgen, Effekte auf Politik und Wirtschaft oder Daten aus Unternehmensquellen. Das bedeutet, dass Fälle nicht statisch in der Datenbank vorliegen, sondern in Feedback-Schleifen weiter ergänzt werden und somit ein möglichst komplettes Bild über einen Zwischenfall vorliegt.

Zettl-Schabath: Wir stehen natürlich vor dem Dilemma, dass wir nicht alle Fälle erfassen können. Eine Studie hat etwa im ersten Halbjahr diesen Jahres knapp sechs Millionen DDoS-Angriffe gezählt. Das können wir natürlich überhaupt nicht abbilden und brauchen Selektionskriterien. Insofern können wir nur Cybervorfälle erfassen, die eine politische

Wirkung entfalten – etwa in Form eines überbordenden Schadens oder politischen Reaktionen wie im Fall Albanien. Das schließt einen gewissen Teil von Cyberkriminalität aus, inkludiert aber bestimmte Fälle, wo Cyberkriminalität politisiert wird.

Aus welchen Quellen stammen die Daten für das EuRepoC?

Zettl-Schabath: Wir haben Quellen identifiziert, aus denen viel automatisiert in die Datenbank gespeist und dann von uns validiert wird. Das ist ein Set an Quellen wie beispielsweise Medien, aber auch die Threat Intelligence von Unternehmen, staatlichen Webseiten und Twitter-Accounts von Experten in diesem Bereich – zusammengenommen sind es über 200 Quellen. Wir haben dabei nicht den Anspruch jede Quelle zu kennen und zu integrieren, wir wollen ein möglichst breites Bild der öffentlich bekannten Fälle abdecken. Dabei bleibt es nicht statisch, sondern unser Team überprüft täglich, ob neue Quellen hinzugekommen sind – und ergänzt dann Informationen zu den einzelnen Fällen.

Schulze: Und es gibt ja beispielsweise in den USA schon ähnliche Projekte, allerdings sind die oft sehr tabellarisch und wenig geeignet abseits von wirklich wissenschaftlichem Fachpublikum. Auf der anderen Seite gibt es die schicken Grafiken der Sicherheitsunternehmen, denen es aber oft an wissenschaftlicher Genauigkeit fehlt. Insofern wollten wir das Beste aus beiden Welten zusammenbringen. Zudem fehlt beiden Welten oft der Kontext – etwa vor welchem Hintergrund ein Cyberzwischenfall oder eine besonders hohe APT-Aktivität stattfindet. Aus diesem Grund haben wir zudem über 60 Kategorien definiert, die einen Vorfall bewerten können – etwa technische oder rechtliche.

Welche sind das zum Beispiel?

Zettl-Schabath: Eine Kategorie betrifft etwa die Attribution: Wer hat sie in welcher Form vorgenommen. Auch Verschränkungen zwischen Cyberraum und anderen Dimensionen werden abgebildet. Dann kommen Kategorien von politischen Reaktionen hinzu, etwa wer sich äußert, welche Länder und Institutionen betroffen sind. Auf technischer Ebene etwa auch die Art des Zwischenfalls und die Auswirkungen. Auch die völkerrechtlichen Dimensionen werden als eigene Kategorien abgebildet.

Das Projekt läuft unter der Idee von Open Access. Warum?

Kettemann: Für uns ist besonders wichtig, dass wir ein Gegenmodell aufbauen zu den bestehenden Cybervorfall- und Analysedatenbanken, die man für Geld abonnieren muss. Wir möchten eine Demokratisierung des Zugangs zu Cybersecurity-Informationen schaffen. Daher haben wir neben staatlichen Stellen eben auch die Öffentlichkeit im Blick. Daher gibt es auch verschiedene Darstellungsformen der Informationen – etwa einen Newsletter, der über wesentliche Ereignisse berichtet aber auch ein digitales Dashboard, das ein tieferen Einblick gewährt – das alles unter dem Gedanken der freien Verfügbarkeit.

Neben dem Auswärtigen Amt fördert auch das dänische Außenministerium das Projekt. Sind weitere Förderer und auch Partner geplant?

Schulze: Wir haben das Interesse europäischer zu werden und sind offen für weitere Partner. Das Interesse an dem Thema ist groß, doch die Bereitschaft Dritter, jetzt schon als Partner einzusteigen, ist eben auch verbunden mit großem Einsatz an personellen Kapazitäten – da herrscht noch viel Zurückhaltung. Gleichzeitig hatten wir auch noch kein fertiges Produkt, dass man vorzeigen kann. Was wir bereits allerdings aufbauen, ist ein wissenschaftliches Board, in dem wir uns mit Kolleg:innen aus projektfremden Institutionen austauschen. Gleichzeitig wollen wir im kommenden Jahr eine Konferenz in Österreich ausrichten, mit der wir den akademischen Prozess und die Beteiligung mit anderen Instituten weiter vorantreiben. Auch mit weiteren Förderern sind wir bereits im Austausch, etwa in Österreich.