European
Repository of
Cyber Incidents

EuRepoC

Cyber Conflict Briefing

Februar 2024

Jakob Bund
Kerstin Zettl-Schabath
Martin Müller
Camille Borrett (Data Support)

Beobachtungen zur Gesamtlage

Im **Februar 2024** wurden 107 Cyber-Operationen in die EuRepoC-Datenbank aufgenommen. Das sind 24,4% mehr als im Vormonat und 36 Operationen mehr als die insgesamt durchschnittlich verzeichnete Aktivität von 71 Cyber-Operationen pro Monat im Gesamtzeitraum.

Die **durchschnittliche Intensität** der im Februar erfassten Operationen beträgt 3.25 und liegt somit über dem historischen Durchschnitt (2,79). Der auffällige Anstieg der Operationen seit Februar 2023 lässt sich vor allem auch dadurch erklären, dass EuRepoC ab diesem Zeitpunkt Cyberangriffe gegen Kritische Infrastrukturen grundsätzlich miteinschließt und nicht wie zuvor davon abhängig macht, ob diese Aktivitäten mit politischen beziehungsweise staatlichen Angreifern oder Opfern verknüpft sind.

Über das Briefing

Analysen für das Cyber Conflict Briefing werden von EuRepoC erstellt. Die deutsche Ausgabe wird in Zusammenarbeit mit dem **Tagesspiegel Cybersecurity Background** veröffentlicht.
Das Briefing fasst die zentralen Trends, Dynamiken und Befunde zu den von EuRepoC in einem bestimmten Monat erfassten Cybervorfällen zusammen. Diese müssen nicht notwendigerweise im Februar stattgefunden haben, sondern können bereits zu einem früheren Zeitpunkt begonnen haben. Dabei stehen technische, politische sowie rechtliche Aspekte im Vordergrund.

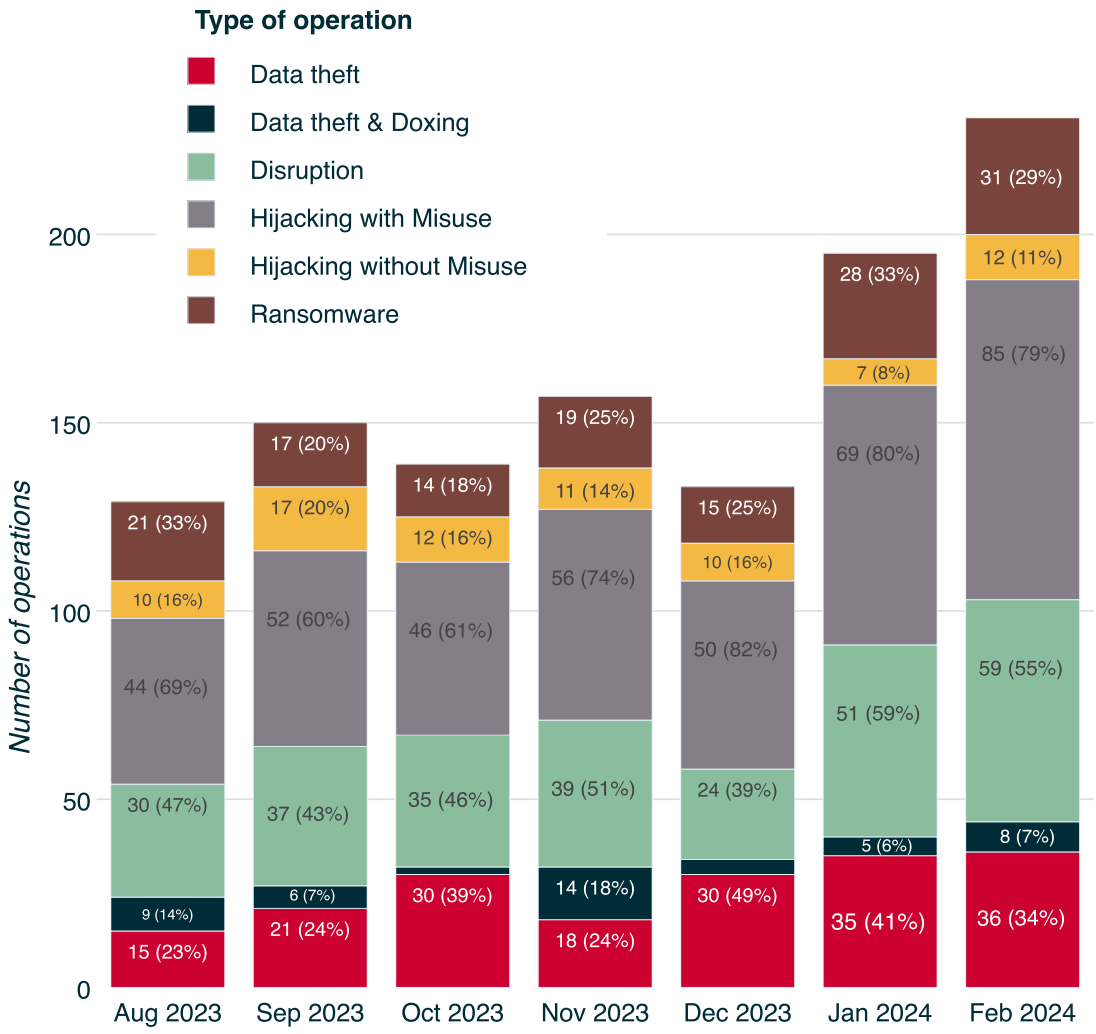
Über EuRepoC

Das European Repository of Cyber Incidents ist ein europäisches Forschungsprojekt mit dem Ziel, Informationen und Wissen über Cyber-Konflikte sichtbar zu machen. Es wird geleitet von der Universität Heidelberg, in Kooperation mit der Universität Innsbruck, der Stiftung Wissenschaft und Politik und dem Cyber Policy Institute (Estland). Es wird aktuell durch das Auswärtige Amt und das dänische Außenministerium gefördert.

Nähere Informationen zum EuRepoC-Projekt finden Sie hier.

Die im Februar 2024 erfassten Vorfälle verteilen sich auf folgende **Operationstypen**:

Monthly distribution of operations



Hinweis: Einzelne Cybervorfälle können mehrere Operationstypen in Kombination aufweisen.

Der größte Anteil umfasst „Hijacking with Misuse"-Operationen mit 85 Fällen (79%). Als Sammelbegriff fasst dies Aktionen, bei denen es Angreifern gelungen ist, in Systeme und Netzwerke einzudringen, um dort bereits unbefugt üblicherweise schädliche Aktionen auszuführen. Diese Aktivitäten werden, sofern erkennbar, weiter nach ihrer Absicht differenziert und können Datendiebstahl oder Betriebsstörungen umfassen.

In einem Jahr, in dem die Bevölkerungen in über 60 Ländern zur Abstimmung aufgerufen sind, zeichnen sich wahlbeteiligte Organisationen als ein Schwerpunkt nicht nur für mögliche staatliche Beeinflussungsversuche und Spionageoperationen, sondern auch für finanziell motivierte Kriminalität ab. Der Einfluss, den Störungen im Wahlablauf und Verzögerungen in der Stimmenauszählung auf die Anerkennung der Ergebnisse haben könnten, kann Ransomware-Gruppen als Druckmittel dienen. Erpressungsversuche zu diesem Zweck könnten sich das Ziel setzen, Systeme zu lähmen oder Datenbanken zu verschlüsseln, die für die reibungslose Durchführung von Wahlen notwendig sind.

Darüber hinaus stellen vertrauliche Informationen von Kandidaten und Kandidatinnen ein attraktives Ziel dar. Von der tatsächlichen oder auch nur angedrohten Veröffentlichung interner Unterlagen geht in Wahlkampfzeiten ein erhebliches Druckpotential aus, von dem kriminelle Gruppen versuchen zu profitieren. In diesem dynamischen Umfeld könnten staatliche Akteure anstreben, eigene Aktionen in der Absicht kompromittierende Informationen zu erbeuten und in Umlauf zu bringen als Ransomware zu tarnen.

Die Ransomware-Gruppe Knight behauptete, Ende Januar Daten aus Netzen des rumänischen Abgeordnetenhauses, der unteren Kammer des Parlaments, erlangt zu haben.

In dem verhältnismäßig kleinen Datensatz von 300 MB waren allerdings Personalausweiskopien des Ministerpräsidenten und mindestens eines weiteren hochrangigen Politikers enthalten.

Die insgesamt 316 Dateien umfassten neben öffentlich einsehbare Informationen auch interne Dokumente von weiteren Abgeordneten. Anfängliche Berichte sprachen unter anderem von darin enthaltenen Bankinformationen und Patientendaten. Für die Löschung der Daten forderte Knight umgerechnet rund 30.000 Euro. In Rumänien finden 2024 Wahlen gleich in vier Runden statt, für das Präsidentenamt, das Parlament, das Europaparlament und auf kommunaler Ebene.

Um den Einsatz von Ransomware gegen wahlwichtige Organisationen zu verhindern, ging das US-Cyberkommando bereits 2020 gegen das Trickbot-Botnet vor, das zur Verbreitung von Schadsoftware genutzt wurde.

Dieses Einschreiten im Vorfeld der US-Präsidentschaftswahlen war die erste öffentlich berichtete Defend-Forward-Operation.

Der zweithäufigste im Februar 2024 festgestellte Operationstyp war „Disruption"-Operationen (55%). Darunter verstehen sich Operationen mit dem Ziel, einen informationstechnischen Dienst außer Betrieb zu setzen. Eine Disruption oder Störung beeinträchtigt entsprechend dessen Verfügbarkeit. Störaktionen sind in aller Regel von vorübergehender Wirkung. Im Fall von Ransomware kann der blockierte Zugriff auf betriebswichtige Daten allerdings auch über einen längeren Zeitraum für Ausfälle sorgen. Von diesen Operationstypen sind für Februar 59 durch das Repositorium erfasst.

Mitte Februar wurde etwa das börsennotierte Unternehmen Izumi Co. Ltd., das in ganz Japan Supermärkte und Einkaufszentren betreibt, Ziel eines Ransomwareangriffs. Läden des Unternehmens blieben in Folge für vier Tage geschlossen. Die für Anfang März geplante Öffnung einer neuen Geschäftsstelle musste auf Ende April verschoben werden. Der umfänglich eingeschränkte Zugang zu Buchhaltungsdaten und Bestellsystemen sorgt weiterhin für anhaltende Lieferschwierigkeiten. Eine ebenfalls für März angestrebte IT-Integration im Rahmen der Geschäftszusammenführung mit einem anderen Lebensmitteleinzelhändler verzögert sich aufgrund der Wiederherstellungsbemühungen voraussichtlich um drei Monate.

Obwohl die Geschäftsführung die finanziellen Auswirkungen des Ransomwarevorfalls als gering einschätzt, behindert die Verschlüsselung betriebswichtiger Daten die für April

geplante Fertigstellung des Geschäftsberichts für das Finanzjahr 2023. Die Vorlage des Berichts musste auf unbestimmte Zeit verschoben werden.

Ähnliche Zwangslagen hatten auch in Deutschland das Berichtswesen von mindestens zwei Börsenunternehmen beeinträchtigt. Seit die Deutsche Börse von Unternehmen, die in den großen deutschen Aktienindizes gelistet sind, bis April die Einreichung von geprüften Geschäftsberichten fordert, haben Hindernisse, dieser Berichtspflicht nachzukommen, das Potential zu Verwerfungen an den Finanzmärkten.

Im vergangenen Jahr schied das Biotechnologieunternehmen Evotec zeitweilig aus dem Mittelwertindex MDax aus, nachdem es im Zuge der Bewältigung eines Ransomwareangriffs die Geschäftszahlen nicht fristgerecht vorlegen konnte. Der Batteriehersteller Varta versäumte dieses Jahr ebenfalls aufgrund eines nicht näher benannten Cyberangriffs den Stichtag und droht seinen Platz im SDax zu verlieren.

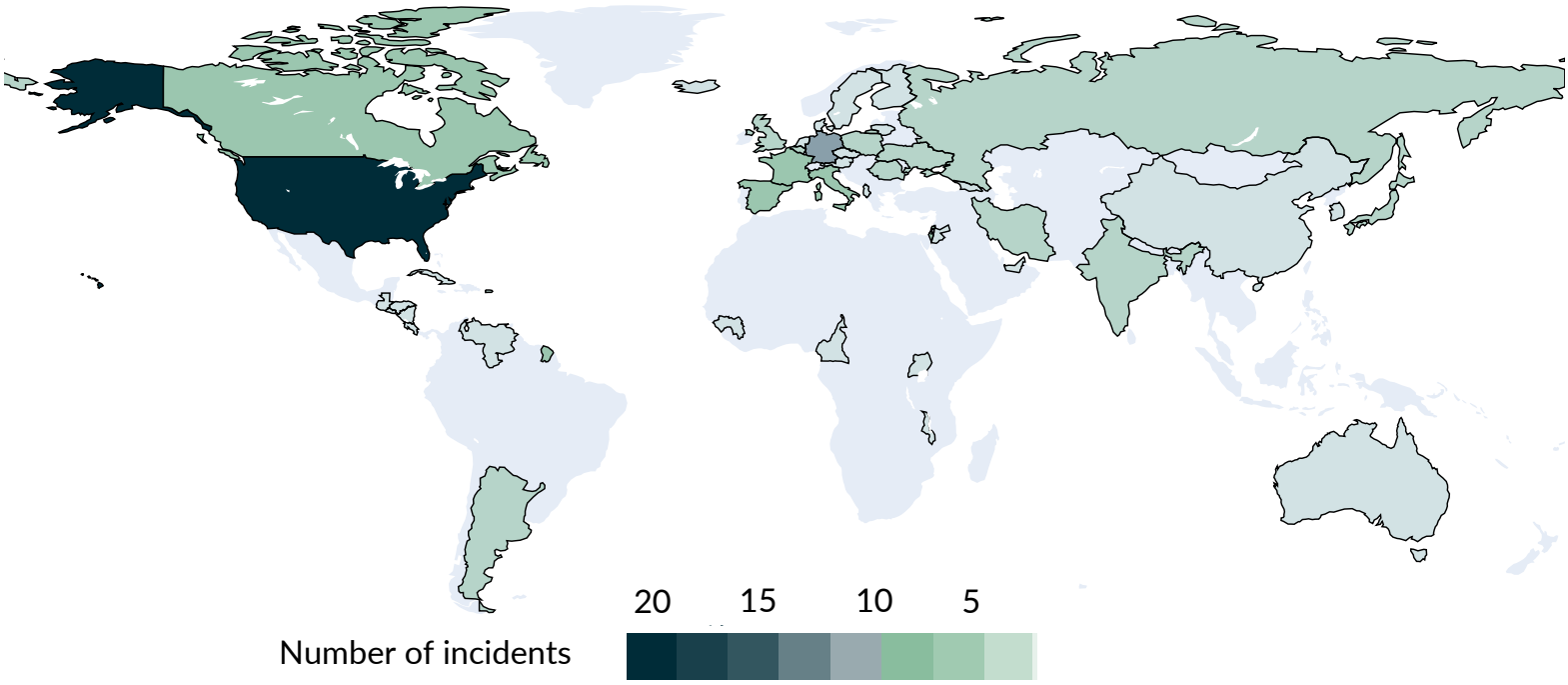
Diese Fälle deuten auf finanzielle Konsequenzen von betriebsstörenden Cyberoperationen hin, die für die betreffenden Unternehmen über kurzfristige Lieferschwierigkeiten hinausreichen. Die Kosten eines so forcierten Ausstiegs aus einem marktweisenden Index können längerfristig den Schaden von Betriebsausfällen übersteigen. Investmentfonds, die Indizes nachbilden, passen ihr Portfolio an Veränderungen in deren Zusammensetzung an und verkaufen Anteile, wenn Unternehmen einen Referenzwert verlassen. Als Auslöser für solche Verkäufe in großem Umfang können Abgänge aus Indizes den Aktienwert der Unternehmen nachhaltig beeinflussen.

Brennpunkte und Zielmuster

Wie in den Vormonaten waren auch im Februar 2024 erneut Unternehmen der Kritischen Infrastruktur der am häufigsten betroffene Sektor. Mit 56 Fällen beziehungsweise 52% der neu aufgenommenen Fälle handelt es in absoluten Zahlen um eine geringe Steigerung, angesichts der insgesamt zugenommenen Fallzahl aber um einen relativen Rückgang um zehn Prozentpunkte. An zweiter Stelle stehen erneut staatliche Institutionen, welche in 47 Fällen respektive 44% betroffen waren. Auch hier handelt es sich um eine minimale Steigerung um zwei Fälle im Vergleich zum Vormonat, der relativ aber einen Rückgang um 5 Prozentpunkte darstellt.

Wenngleich nicht in der gleichen Intensität wie kritische Infrastruktur und staatliche Institutionen, wurden für den Februar jeweils neun Fälle gegen Endnutzer und andere nicht-staatliche Gruppierungen sowie den Bildungssektor aufgenommen, was eine deutliche Steigerung zu den Vormonaten darstellt. Bei den erstgenannten stechen zum einen Operationen der Vereinigten Staaten gegen kriminelle Akteure heraus, die im Folgenden genauer dargestellt werden, zum anderen Iran sowie der Hamas zugeschriebene Aktionen gegen israelische Ziele, die durch einen Bericht der Google Threat Analyis Group und Mandiant bekannt wurden. Im Bildungssektor waren insbesondere europäische Universitäten und nordamerikanische Schulen betroffen, die von EuRepoC je nach ihrer innerstaatlichen Organisation teils auch als staatliche Institutionen oder auch als kritische Infrastruktur - die NIS2-Richtlinie erfasst etwa auch Forschungseinrichtungen - eingestuft werden.

Geographic distribution of operations



Bei der Verteilung betroffener Staaten stehen erneut die Vereinigten Staaten an erster Stelle. Die für den Februar neu aufgenommenen 24 Fälle schlagen sich in einem Anteil von etwa 22% nieder, ein Rückgang im Vergleich zu den Vormonaten. An zweiter Stelle sind zwölf Vorfälle mit Betroffenen in Deutschland aufgenommen worden. Da in dritter Stelle mit jeweils sechs Vorfällen neben Israel mit Frankreich und Spanien auch zwei andere Mitgliedsstaaten der Europäischen Union stehen, ergibt sich für den Februar entgegen der Vormonate ein deutlicher Überhang von betroffenen EU-Staaten (insgesamt 39 Fälle) gegenüber den Vereinigten Staaten.

Innerhalb der kritischen Infrastrukturen war der Gesundheitsbereich mit 16 Vorfällen am häufigsten betroffen. Die Verteilung liegt etwa jeweils hälftig zwischen Nordamerika und Europa. Auffällig waren im Februar mehrere Angriffe auf Dienstleister im Sektor, die teils weitreichende Folgen hatten: So sorgte ein Cybervorfall bei ChangeHealth, einer Tochter des US-Versicherungsunternehmen UnitedHealth, für weitreichende Probleme in Apotheken bei der Verschreibung von Medikamenten. In Frankreich waren die Zahlungsdienstleister Viamedis und Almerys von Diebstählen mit den Daten von etwa 33 Millionen betroffenen Personen, also der Hälfte der Einwohner Frankreichs, betroffen. Ebenfalls sorgte ein Ransomwarevorfall bei einem rumänischen IT-Dienstleister im Krankenhaussektor für großflächige Ausfälle in 25 Krankenhäusern, in weiteren 75 wurde die Systeme sicherheitshalber abgeschaltet. Die Vorfälle zeigen im Einzelnen die Abhängigkeiten im medizinischen Bereich, welche angesichts des Einsatzes verschiedener technischer Dienstleister bei allen Akteuren (Krankenkassen, Krankenhäuser, Praxen usw.) für besonders weitreichende, kaskadenartige Folgen von Cyberangriffen in diesem Sektor sorgen. Hinzu kommen die häufig besonders sensiblen Gesundheitsdaten, die den Bereich insbesondere für kriminell agierende Ransomwaregruppen attraktiv machen, was sich in Vorfällen bei einzelnen Einrichtungen gleichsam bemerkbar macht.

Ebenfalls häufig betroffen waren der Finanzsektor mit zwölf und der Telekommunikationssektor mit zehn Vorfällen. Für den Bereich Finanzen waren im Februar vermehrt klassische Institute

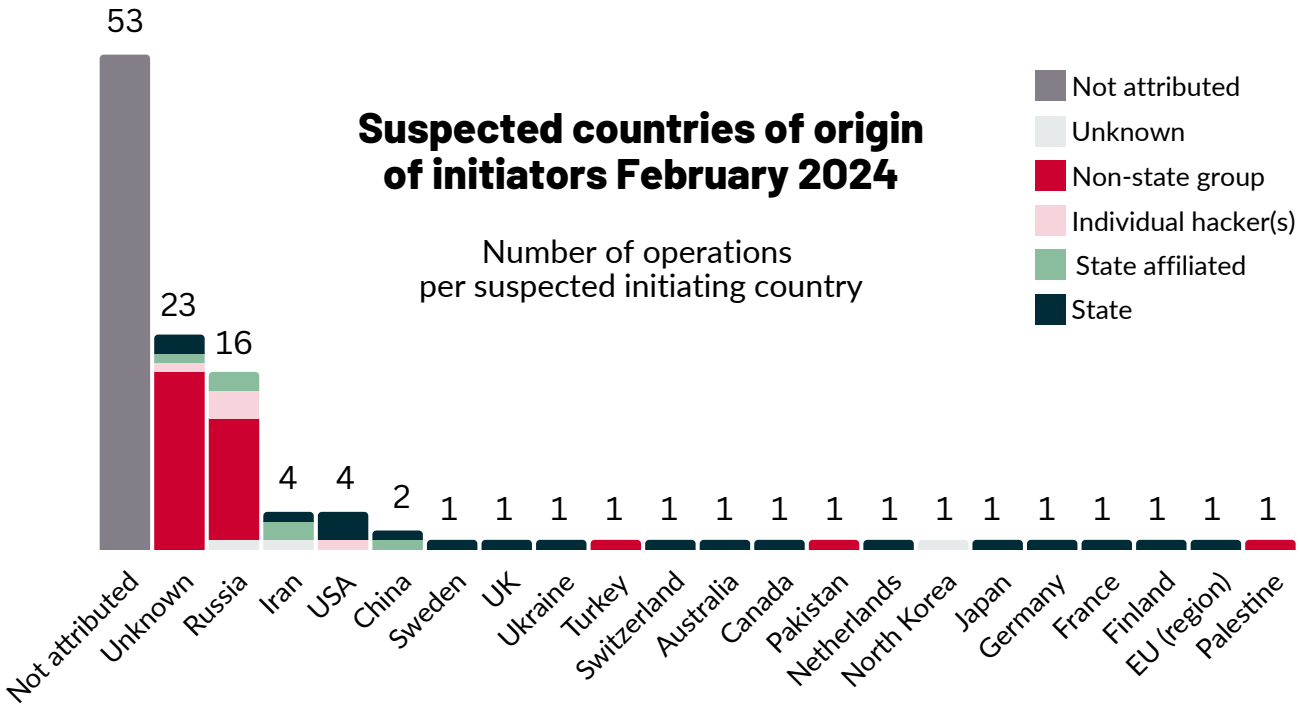
betroffen, die wie andere Unternehmen der kritischen Infrastruktur verstärkt von Ransomwarevorfällen und/oder Datendiebstählen betroffen sind. Für den Kryptobereich konzentrierten sich Aktionen im Vergleich auf unmittelbar finanziell motivierte “Crypto-Heists”.
Für den Bereich staatlicher Institutionen zeigt sich erneut eine überwiegende Betroffenheit im Bereich der Verwaltungsbehörden mit 31 Vorfällen. Neben den bereits genannten Bildungsinstitutionen waren erneut Verwaltungsbehörden auf lokaler und regionaler Ebene betroffen. Auf technischer Seite waren etwas mehr als die Hälfte der Vorfälle disruptiver Natur, für insgesamt acht wurde der Einsatz von Ransomware bekannt.

Angreiferprofile und Attributionen

Auch im Februar beträgt der Anteil der Cybervorfälle, die weder einem konkreten Land, noch einem Angreifertyp zugesprochen werden konnten, mit 53 Fällen die Hälfte der verzeichneten Operationen. Im Vergleich zum Januar machen dagegen solche Operationen, die hinsichtlich des Angreifertyps attribuiert wurden, nicht aber bezüglich des Ursprungslandes, mit 19% (21 Fälle) lediglich 4 % weniger am Gesamtsample aus als im Vormonat. Auffällig ist beim Blick auf die Liste der attribuierten Herkunftsländer, jeweils weiter ausdifferenziert nach den attribuierten Akteurstypen, die scheinbar auffällig große Vielfalt an Ländern, von denen offensive Aktivitäten ausgingen, mit jeweils einem zugesprochenen Vorfall im Februar. Beim Blick in die Daten wird jedoch schnell klar, dass hierfür hauptsächlich eine spezielle Cyberoperation, mit zudem weniger offensiver, denn defensiver Intention verantwortlich ist: der Takedown von Infrastruktur der Lockbit Ransomware-Gruppierung im Rahmen der “Operation Cronos”, die neben der Übernahme der Ransomware-Website auch die Beschlagnahmung von Servern sowie die Verhaftung zweier Personen umfasste. Hieran nahmen neben den USA zehn weitere, vor allem europäische Länder mit ihren Strafverfolgungsbehörden teil, hinzu kommt Europol in einer vor allem koordinierenden Rolle - einer Aufgabe, welcher angesichts der mehr als 20 beteiligten Behörden sowie den ergriffenen Maßnahmen besondere Bedeutung zukommt.

Operationen mit attribuierter nichtstaatlicher Verantwortlichkeit (z.B. Hacktivisten, Cyberkriminelle, individuelle Hacker) sind im Vergleich zum Vormonat um 10%, auf 37% gestiegen. Davon waren 18 kriminell motivierte Operationen. Im Verhältnis zum Gesamtsample ist der Anteil an Cyber-Crime-Vorfällen mit ca. 18% somit im Vergleich zum Januar nahezu konstant geblieben, gleiches gilt für die 13% der Cybervorfälle vom Februar, die stärker ideologisch/politisch motivierten Akteuren (Hacktivisten; patriotische Hacker) zugesprochen wurden. Der Anteil der sogenannten “Proxy-Operationen”, also durchgeführt von staatlich-affilliierten Akteuren, ist von 7% im Januar geringfügig auf 6% gefallen.

Klammert man alle Länder aus, die in der Liste aufgrund der Operation Cronos erscheinen, bleibt die Prominenz der USA mit vier Operationen auffällig. Hinzu kommt, dass hiervon sogar drei staatlichen Akteuren zugeschrieben wurden. Alle drei reihen sich ein in die immer größer werdende Zahl an US-geführten Operationen, die zwar die technischen Inklusionskriterien EuRepoCs erfüllen, nämlich mindestens ein Element der sogenannten CIA-Triade der



Informationssicherheit betreffen (Confidentiality; Integrity; Availability), von ihrer funktionalen Ausrichtung her jedoch defensiver Natur sind. So richteten sich neben der groß angelegten Kampagne gegen Lockbit noch zwei weitere US-Handlungen gegen Bedrohungsakteure, die vor allem in den USA in den letzten Jahren für Aufsehen gesorgt haben. In dem einen Fall erlangten das Department of Justice und FBI Zugriff auf das von der russischen Gruppe APT28 (aka Fancy Bear) kontrollierte Moobot Botnet, kopierten und löschten Daten der infizierten Router und blockierten ebenso den Fernzugriff des Botnetzes auf besagte Router ("Operation Dying Ember"). Beim zweiten Fall handelte es sich ebenfalls um einen Schlag gegen ein Botnetz, bestehend aus infizierten small-office/home-office (SOHO)-Routern. Dieses wurde seitens der chinesischen Gruppe Volt Typhoon kontrolliert, deren Infiltrationen amerikanischer kritischer Infrastrukturen in einer Anhörung des "Select Committee on the Chinese Communist Party of the US House of Representatives" am Tag der Operationsverkündung vom FBI Direktor Christopher Wray in den direkten Zusammenhang sogenannter "prepositioning"-Operationen gestellt wurden.

So können Botnetze eben nicht nur zur Spionage missbraucht werden, sondern auch den initialen Einfallspunkt für Angreifer bieten, um darüber geführte Infiltrationen von kritischen Netzen zu tarnen und Zugänge für mögliche Sabotage-Akte zu einem späteren Zeitpunkt zu sichern. Gerade im Hinblick auf eine mögliche Verschärfung des Konflikts um Taiwan wurden die Aktivitäten von Volt Typhoon seitens der US-Administration als eine solche Vorbereitungshandlung gewertet.

Blickt man auf diese zunehmend praktizierte Selbst-Attribution staatlicher "Cyber-Gegenmaßnahmen", wird das Selbstverständnis demokratischer Staaten wie der USA im Vergleich zu autokratisch geführten Ländern deutlich. So gehen erstgenannte mit ihren abwehrorientierten Operationen an die Öffentlichkeit, einerseits sicherlich um deren (mutmaßlichen) Erfolg gegenüber der einheimischen Bevölkerung zu demonstrieren, andererseits aber auch, um das eigene Handeln als normativ richtig im Vergleich zu den auf Schaden abzielenden Operationen autokratischer Cyberangreifer darzustellen. Hinzu kommt, dass diese Operationen durch entsprechende Gerichtsentscheide auch durch das nationale Recht legitimiert

werden. So bezeichnete die stellvertretende US-Generalstaatsanwältin, Lisa O. Monaco, das Volt-Typhoon Vorgehen als Bedrohungen für die nationale Sicherheit, das “in Echtzeit” gestört worden sei. Gleiches gilt für das Vorgehen gegen das APT28-gekaperte Moobot-Botnet, welches ebenfalls als Gefahr für die nationale Sicherheit der USA, im Rahmen der Presseerklärung jedoch auch im Kontext des russischen Vorgehens gegen die Ukraine adressiert wurde. Beide Presseerklärungen bezeichneten das jeweilige autokratische Verhalten im Cyberspace als destabilisierend und Bedrohung der nationalen Sicherheit, ohne sich jedoch fehlten direkt auf seitens der UN-Mitglieder anerkannte (freiwilligen) Normen verantwortlichen Staatenverhaltens im Cyberspace zu beziehen. Gleiches gilt für potenzielle Rechtsverletzungen der autokratischen Cyberoperationen, die ebenfalls seitens der reagierenden Partei, in diesem Falle der USA, hätten öffentlich adressiert werden können, vor allem in Kombination mit den jeweils vorgenommenen Attributionen staatlicher Verantwortlichkeit. Erklären lässt sich diese strategische Ambivalenz der generellen Anerkennung von Normen sowie der Gültigkeit internationalen Rechts im Cyberspace auf der einen, gegenüber der fehlenden öffentlichen und konkreten Identifizierung von Normbrüchen/Rechtsverletzungen auf der anderen Seite, durch das Eigeninteresse von Demokratien mit weit entwickelten Cyberfähigkeiten, wie den USA, die sich hierdurch auf längere Sicht in ihrem eigenen Vorgehen nicht selbst beschränken wollen. Dass die Frage, wie genau das Völkerrecht im Falle von Cyberkonflikten Anwendung finden soll, nach wie vor eine der drängendsten auf internationaler Ebene ist, machte nicht zuletzt die siebte Session der Open-Ended-Working-Group (OEWG) der UN deutlich, die diesem Thema regelmäßig einen eigenen Sitzungsblock einräumt, mit bislang jedoch nur mäßigem Fortschritt.

Autokratische Staaten treten mit ihren Cyberoperationen gegen andere Staaten dagegen bislang noch nicht proaktiv an die Öffentlichkeit. Dies steht im Gegensatz zu digitalen Repressionsmaßnahmen auf nationaler Ebene, etwa gegen Dissidenten oder Oppositionelle, die jedoch (ähnlich wie die Maßnahmen demokratischer Staaten gegen autokratische Angreifer-Infrastruktur) oft durch entsprechende Gesetze/Gerichtsentscheide zumindest im nationalen Rahmen legitimiert werden, dann zumeist im sprachlichen Kontext von Anti-Terror-, Anti-Kinderpornografie- oder Anti-Drogen-Maßnahmen.

Im Februar wurden insgesamt elf Cybervorfälle bestehenden konventionellen Konflikten des HIIK-Konfliktbarometers zugeordnet. An erster Stelle rangiert weiterhin der russische Krieg gegen die Ukraine, mit fünf zugeordneten Fällen, gefolgt von zwei Operationen im Kontext des Konflikts zwischen Israel und der Hamas. Drei der verbliebenen vier Fälle teilen sich auf weitere, seit längerem bestehende Dyaden auf, mit jedoch deutlich geringerer Konfliktintensität als die beiden erstgenannten (China - Japan; China - USA; Indien - Pakistan). Hinzukommt eine Cyberoperation, die in inner-iranischen Spannungen zwischen dem Regime und Oppositionellen verortet wird.

Mehr von EuRepoC

EuRepoC informiert mit einem täglich kuratierten Cyber Incident Tracker über neu in die Datenbank aufgenommene Cybervorfälle. Diesen können Sie hier abonnieren.

Über die Autor:innen

Jakob Bund ist Wissenschaftler an der Stiftung Wissenschaft und Politik (SWP).

Kerstin Zettl-Schabath ist Wissenschafterin am Institut für Politische Wissenschaft (IPW) der Universität Heidelberg.

Martin Müller ist Universitätsassistent und Dissertant am Institut für Theorie und Zukunft des Rechts an der Universität Innsbruck.

Camille Borrett ist Datenanalystin an der Stiftung Wissenschaft und Politik (SWP).

Follow us on social media

@EuRepoC

linkedin/EuRepoC

contact@eurepoc.eu

https://eurepoc.eu