European
Repository of
Cyber Incidents

EuRepoC
Cyberkonflikt Briefing

Q2 2026

Kerstin Zettl-Schabath
Lena Rottinger
Erik Kellenter
Callahan Shelley

Beobachtungen zur Gesamtlage

Im zweiten Quartal 2026 (Q2) wurden **162 neue Cyberoperationen** verzeichnet: ein Rückgang von 14% im Vergleich zum letzten Quartal. Die Zahl der Operationen ist damit nach einem Aktivitätshöhepunkt Mitte 2025 weiter zurückgegangen und liegt 9 % unter dem langfristigen Quartalsdurchschnitt. Insgesamt ist Q2 stark geprägt von Cyberoperationen, die Kontext des Konflikts zwischen Iran, USA, Israel und den Golfstaaten, durchgeführt wurden.

Die Vereinigten Staaten sind mit 51 Vorfällen weiterhin das am häufigsten angegriffene Land und machen fast ein Drittel der erfassten Vorfälle aus. Der anhaltende Konflikt mit dem Iran geht dabei mit verstärkten Angriffen auf kritische Infrastrukturen der USA einher. Mit 37 Vorfällen ging die Zahl der Angriffe gegen EU-Mitgliedstaaten deutlich zurück; sie sank im Vergleich zum letzten Quartal um 18%. Am häufigsten waren Deutschland und Frankreich mit jeweils 11 Vorfällen betroffen, gefolgt von Spanien mit 4 Vorfällen; zusammen entfielen auf diese Länder zwei Drittel aller Angriffe auf EU-Mitgliedstaaten.

Über das Briefing

Das *Cyber Conflict Briefing* analysiert Entwicklungen in der Bedrohungslandschaft auf Grundlage der von **EuRepoC** erfassten Cybervorfällen. Für diese Auswertung stehen technische, politische sowie rechtliche Aspekte im Vordergrund. Seit Oktober 2025 veröffentlicht EuRepoC das Briefing quartalsweise in Zusammenarbeit mit der **Deutschen Cyber-Sicherheitsorganisation GmbH (DCSO).**

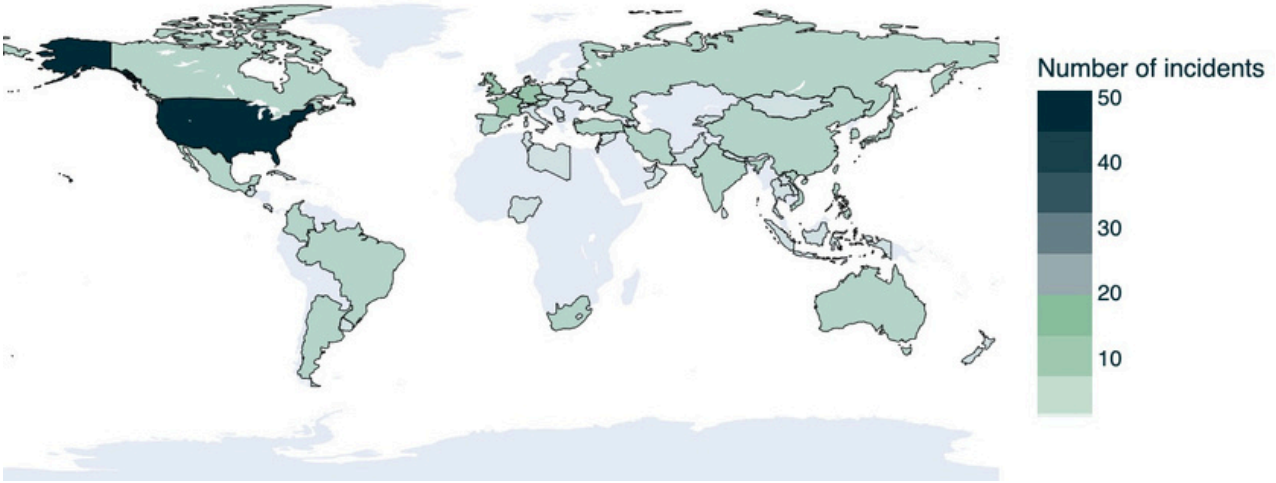
Die deutsche Ausgabe erscheint in Kooperation mit dem **Tagesspiegel Cybersecurity Background.**

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.

Weitere Informationen finden Sie unter https://eurepoc.eu

Geografische Verteilung von Cyberoperationen im 2. Quartal 2026



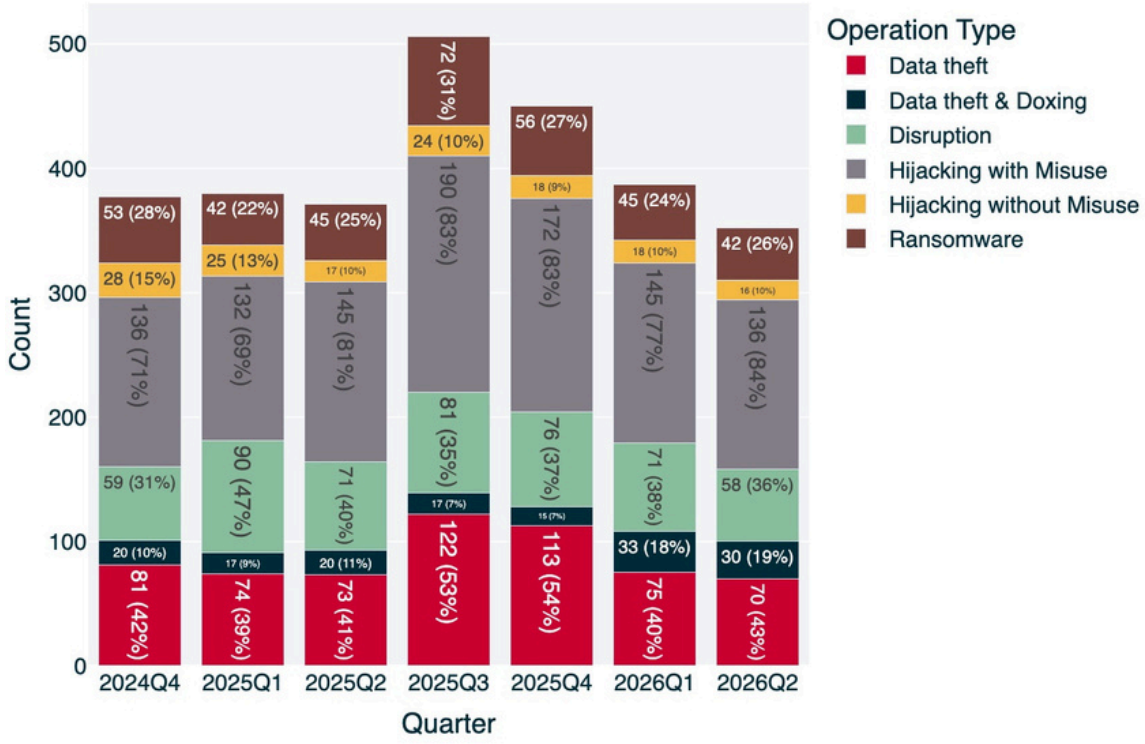
In Deutschland kam es Mitte April zu einem Hackerangriff auf einen externen medizinischen Dienstleister, bei dem personenbezogene Daten von rund 61.000 Patienten aus Krankenhäusern in der gesamten Bundesrepublik gestohlen wurden. Der Trend, dass französische Regierungsstellen Opfer von Angriffen wurden, setzte sich fort: Cyberkriminelle drangen über ein kompromittiertes Konto, das mit dem Bildungsministerium verknüpft war, in „Tchap“ ein, einen von der französischen Regierung genutzten Messaging-Dienst; anschließend entwendeten die Angreifer 643.459 Nachrichten von 73.467 Personen, darunter auch Nachrichten aus mehreren Ministerien. Das Vereinigte Königreich lag mit 11 Angriffen gleichauf mit Deutschland und Frankreich.

Brennpunkte und Zielmuster

Die relative Verteilung der Operationstypen ist gegenüber dem Vorquartal konstant geblieben. Der größte Anteil der Vorfälle (84%) entfällt auf die Kategorie „Hijacking with Misuse"; das wird kodiert, wenn ein Eindringen weitere schädliche Handlungen beinhaltet. In den meisten Fällen bedeutet dies Datendiebstahl oder Störungen der IT-Systemen, doch die Auswirkungen solcher Aktivitäten können vielfältig sein. Ende Mai manipulierte ein unbekannter Angreifer den KI-Support-Chatbot von Meta, um Zugriff auf die Instagram-Konten bekannter Persönlichkeiten zu erlangen, darunter das Konto eines Chief Master Sergeants der US-Space Force und ein inaktives Konto des ehemaligen US-Präsidenten Barack Obama, über die anschließend antiamerikanische Inhalte verbreitet wurden.

Die häufigste Folge von Cybervorfällen ist Datendiebstahl, der bei 62% der erfassten Vorfälle gemeldet wurde. Bei fast einem Drittel der Datendiebstähle kam es zu einem Datenleck. Die häufigste Ursache für Datenlecks ist Ransomware, die in 26% der erfassten Vorfälle eingesetzt wurde. Im Q2 war die Ransomware-Gruppe ShinyHunters erneut für schwerwiegende Sicherheitsverletzungen verantwortlich. Besonders hervorzuheben sind der Angriff auf die US-amerikanische Bildungsplattform Canvas im Mai 2026, von dem weltweit fast 9.000 Schulen und Universitäten betroffen waren, sowie die Ausnutzung der Zero-Day-Schwachstelle CVE-2026-35273 in der Unternehmenssoftware People Soft von Oracle. Laut Mandiant und der Google Threat Intelligence Group (GTIG) wurde die Zero-Day genutzt, um über 100 Organisationen weltweit anzugreifen, darunter die University of Nottingham und weitere Einrichtungen. Die Nutzung von Zero-Day-Schwachstellen durch

Verteilung der Arten von Cyberoperationen



Ransomware-Gruppen ist eine neue Entwicklung; darüber hinaus hat sich der Anteil der Vorfälle, bei denen mindestens eine Zero-Day-Schwachstelle eine Rolle spielte, im Vergleich zum letzten Quartal von 1,6% auf 3% verdoppelt.

Disruption ist der dritthäufigste Angriffstypus (36%). In den meisten Fällen folgt Disruption auf Hijacking (Hijacking mit Missbrauch); D. kann jedoch auch durch einen DDoS-Angriff erfolgen. Im Quartalsvergleich ist die Zahl der DDoS-Angriffe zurückgegangen. So sank der Anteil der DDoS-Angriffe von 7% auf 1% (zu Q1 2026), während EuRepoC im Q2 keine weiteren Vorfälle der berüchtigten russischen Hacktivisten-Gruppe NoName057(16) verzeichnete, nachdem in den vergangenen 12 Monaten mehrere internationale Strafverfolgungsmaßnahmen durchgeführt worden waren.

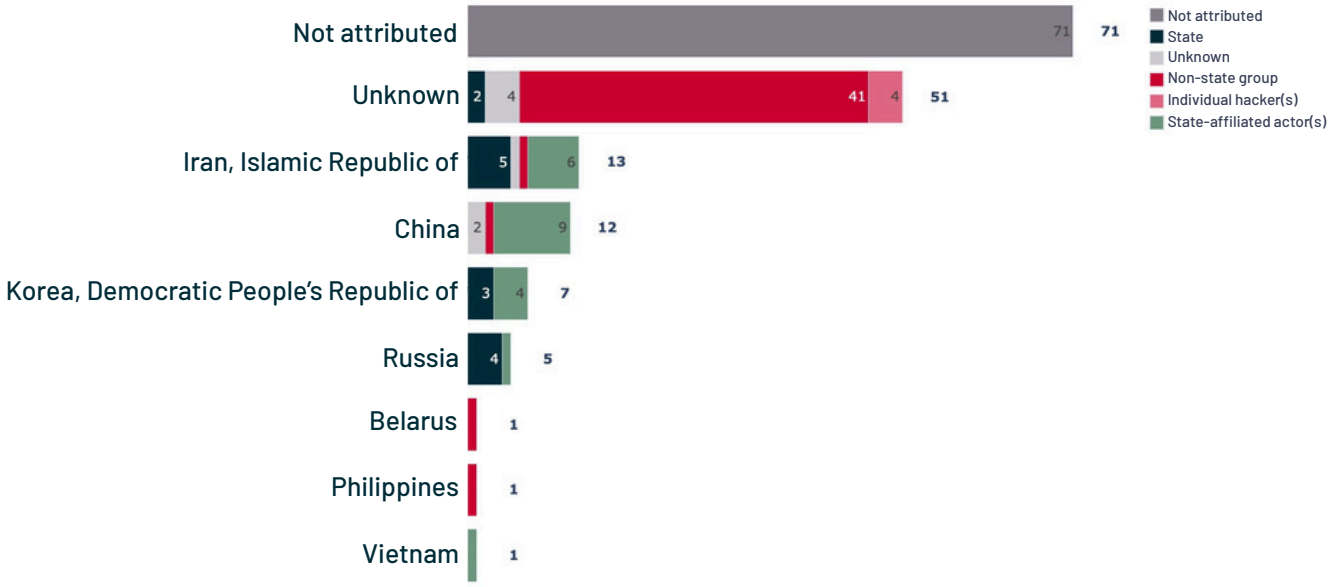
Hijacking without Misuse macht 10% der erfassten Vorfälle aus; dabei handelt es sich um Vorfälle, bei denen die Angreifer gestoppt wurden, bevor ernsthafter Schaden entstehen konnte, oder bei denen die Auswirkungen auf die Opfer unklar blieben. Dies ist typisch für lang andauernde Spionagekampagnen, die beispielsweise über Telemetriedaten aufgedeckt werden.

Angreiferprofile und Attributionen

Bisher sind im zweiten Quartal 2026 ca. 56% der öffentlich berichteten Cybervorfälle attribuiert worden, wobei die CRINK-Staaten (China, Russland, Iran und Nordkorea) erneut die Liste der Angreiferstaaten anführen. Während in vorherigen Quartalen meist Russland und China die meisten Attributionen zu verzeichnen hatten, führt dieses Quartal erstmals Iran die Liste mit dreizehn Vorfällen an.

Mehr als die Hälfte der von der iranischen Regierung ausgehenden dokumentierten Cybervorfälle gehen auf das Konto von Handala Hack. Wie der Name „Handala“ bereits andeutet, agiert die Gruppierung mit einem ideologisch aufgeladenen Widerstandsnarrativ, mit dem vorzugsweise anti-Westliche und anti-Israelische Botschaften verbreitet werden. In diesem Kontext kompromittierte Handala beispielsweise das Hilfszentrum für Holocaust-Opfer in Israel und das

Verteilung der Arten von Cyberoperationen



Note: Individual cyber incidents may have several operation types in combination

Medienoutlet für Exil-Iraner:innen „Iran Wire". Handala attribuiert sich oft während oder nach den Angriffen selbst, indem sie Informationen zum Angriff und gestohlene Daten über Telegram verbreiten. Nicht alle dieser Selbstzuschreibungen können verifiziert werden und EuRepoC dokumentiert nur diejenigen Fälle, bei der eine CIA-Triadenverletzung nachweislich vorliegt. Aber selbst nicht-verifizierte Reklamierungen eines Angriffs können Reputationsschäden bei den Opfern verursachen und den psychologischen Effekt der vermeintlichen Disruption und Destruktion aufrechterhalten. Im Juni drang Handala beispielsweise in die Netzwerke eines kalifornischen Wasserdienstleister (Cal Water) ein, stahl sensible Kundendaten und veröffentlichte diese im Nachgang. Handala erklärte zudem, es sei in der Lage, den Zugang zur Wasserversorgung zu beeinträchtigen, habe sich jedoch vorerst dagegen entschieden. Cybersicherheitsexpert:innen konnten indes keine Anhaltspunkte für ein erfolgreiches Eindringen in die Betriebstechnologie (OT) finden, wiesen aber darauf hin, dass Handala in früheren Angriffen erfolgreich maßgefertigte Wiper einsetzte, die die Netzwerke des Opfers weitestgehend lahmlegten (siehe Stryker-Vorfall).

Neben Handala nahmen auch weitere iranische Akteure kritische Infrastrukturen ins Visier. Angesichts des anhaltenden Konflikts zwischen den USA, Israel, dem Iran und Golfstaaten, warnten US-Behörden mehrfach im zurückliegenden Quartal vor iranischen Angriffen zur Ausnutzung von Schwachstellen in internetzugänglichen Betriebstechnologien (OT) und zur digitalen Manipulation von automatischen Tanküberwachungssysteme (Automatic Tank Gauge Systems, ATG). Letztere Aktivität wurde noch nicht offiziell von der US-Regierung attribuiert, Medienberichten zufolge ist sie jedoch auch auf die iranische Regierung zurückzuführen.

Neben iranischen Bedrohungsakteuren waren auch chinesische Akteure in Q2 besonders aktiv. Zwei Attributionen stechen dabei besonders hervor: Zum einen ein Hinweis der Five-Eyes-Nachrichtendienste zur gezielten Nutzung von Networkingseiten und Onlinejobplattformen zur Informationsgewinnung sowie die technische Attribution von

Google, die offenlegte, wie die (angeblich) chinesische Gruppierung UNC5221 Zeroday-Schwachstellen ausnutzte. Insgesamt zeigen die Fälle das bereits bekannte chinesische Angriffsmuster, Cyberoperationen zu nutzen, um wertvolle Informationen von staatlichen Einrichtungen und Wirtschaftsunternehmen zu stehlen.

Anfang April 2026 wurde durch ein britisches Advisory bekannt, dass die russische Bedrohungsgruppe APT28 vulnerable Router ausnutzen, um DNS-Hijacking-Operationen zu ermöglichen. Seit 2024 leitete APT28 dabei den Datenverkehr ihrer Opfer auf von ihnen kontrollierte DNS-Server um, sodass sie Passwörter, OAuth-Token und andere Zugangsdaten für Web- und E-Mail-Dienste abgreifen konnten. In diesem Kontext wurden auch US-Behörden operativ tätig, um den US-amerikanischen Teil des kompromittierten Netzwerks von Routern auszuschalten. APT28, auch bekannt als Forest Blizzard, Fancy Bear, STRONTIUM, wird dem russischen Militärgeheimdienst (GRU) zugerechnet und ist einer der aktivsten russischen Bedrohungsakteure.

Auch im April berichteten deutsche Medien, dass die Signalaccounts hochrangiger deutscher Politiker:innen erfolgreich kompromittiert wurde. Zu den Betroffenen zählten offenbar die Bundestagspräsidenten Julia Klöckner (CDU), Bildungsministerin Karin Prien (CDU) und Bauministerin Verena Hubertz (SPD). Bereits im Februar warnte das BSI und der BfV vor Phishingangriffen über die Messengerdienste Signal und WhatsApp und vermutete staatlich gesteuerte Akteure dahinter. Während niederländische Nachrichtendienste explizit Russland als verantwortlichen Staat nennt, hat die deutsche Bundesregierung bis heute den Vorfall nicht offiziell attribuiert.

Entwicklungen im Bereich der Cyberkriminalität

In Q2 waren folgende Entwicklungen im Cyberkriminalitätsbereich berichtenswert:

- Die Beziehungen und Rollenverteilungen innerhalb von Ransomware-as-a-Service (RaaS)-Strukturen werden zunehmend flexibler und komplexer: So konnte etwa die „FortiBleed"-Kampagne über einen gemeinsamen Affiliate mit den Gruppen Lynx und INC Ransom verknüpft werden, die regelmäßig auch deutsche Unternehmen ins Visier nehmen. Die zentrale Rolle von „TOXMAN" bei der technischen Entwicklung, der Ausführung sowie den Lösegeldverhandlungen deuten auf eine Aufgabenausweitung seitens einzelner Affiliates hin. Hierdurch können zwar aus Sicht der RaaS-Gruppen Risiken an diese ausgelagert werden, zugleich entstehen jedoch durch operative Überschneidungen neue Detektions- und Attributionsmöglichkeiten.
- Ein weiterer Hinweis auf die zunehmende Flexibilisierung des Cybercrime-Ökosystems ist ein Bericht von Microsoft zum „Malware-signing-as-a-Service" (MSaaS) Akteur „Fox Tempest": Dieser bietet Kriminellen, wie etwa Ransomware-Gruppen, kurzfristige, scheinbar legitime Software-Zertifikate an, wodurch ihr maliziöser Code Sicherheitsprozesse umgehen kann.
- Gleichzeitig kommt es immer häufiger vor, dass mehrere Akteure dasselbe Ziel kompromittiert haben. Ob koordiniert, wissentlich oder völlig unabhängig voneinander: In jedem Falle erschwert eine solche Mehrfachkompromittierung laufende Abwehr- sowie im Nachgang eines Vorfalls stattfindende Forensik- und Schadensbewertungsprozesse.

- Dass dabei scheinbar kriminelle Ransomware-Aktionen in Wahrheit das Werk staatlich-affiliierter Akteure sein können, verdeutlichte einmal mehr die hergestellte Verbindung zwischen Operationen der Chaos Ransomware mit der iranischen APT MuddyWater.
- Die aktuell aktivste RaaS-Gruppe ist „The Gentlemen“. Sie entwickelt und betreibt eine eigene EDR-Killer-Suite, die den Affiliates zur Verfügung steht. Im Gegensatz zu älteren RaaS wie Qilin oder Akira ist das Zielprofil jedoch internationaler und weniger auf die USA fokussiert. Gemeinsam haben sie jedoch die zahlreichen Angriffe gegen deutsche Unternehmen. Auch in Q2 stellten Ransomware sowie Erpressungen hierzulande ein erhebliches Risiko dar, ausgehend sowohl von etablierten RaaS-Akteuren, als auch “Newcomern” wie Settra und Krybit.
- Ähnliche „Globalisierungstendenzen“ deuteten in den letzten Monaten auch chinesische Cyberkriminelle wie TA4922 an, die zuletzt Ziele in Deutschland, Italien, Großbritannien und Südafrika ins Visier nahmen. Die u.a. auf Betrug durch Datendiebstahl sowie den Verkauf von Zugangsdaten abzielenden Operationen greifen dabei primär saisonal bedingte Themen rund um HR, Steuern und Gehaltsabwicklungen in ihren Social-Engineering-Taktiken auf.
- Auf taktischer Ebene ist ClickFix mitsamt den stetig neuen Untervarianten weiterhin der Favorit vieler führender Initial Access Broker. Konkret nutzte etwa KongTuke die Technik, um eine bislang unbekannte Backdoor namens Mistic auf den opportunistisch ausgewählten Zielsystemen zu platzieren, was u.a. zu Kompromittierung durch Qilin-Affiliates führte.
- Auch Open-Source-Supply-Chains stehen weiterhin im Fokus vieler Krimineller, etwa zur Verbreitung von Infostealern. Konkret visierten die Täter in einem Fall Claude- und Gemini-Nutzer an, wodurch sie gleich zwei besonders aktuelle Angriffsvektoren kombinierten.
- Allgemein nutzten kriminelle (sowie staatliche) Angreifer KI-Workflows und Anwendungen immer häufiger als potenzielles Einfallstor in Zielsysteme. So missbrauchten Angreifer in Q2 Schwachstellen in der „Skill“-Architektur von OpenClaw, wodurch ein Remote-Access-Trojaner verbreitet werden konnte. Nicht überprüfte Plugins von Drittanbietern können Angreifern somit Zugang zu KI-gestützten Systemen verschaffen.
- Jedoch diversifizierten Kriminelle wie die auf Erpressung ausgerichtete Gruppe FulcrumSec auch ihre eigene KI-Nutzung. So setzte die Gruppe KI-Agenten zur effizienteren Analyse gestohlener Daten ein
- Stellvertretend für die zahlreichen Strafverfolgungsmaßnahmen in Q2 erzielte die internationale „Operation Endgame“ weitere Erfolge, diesmal gegen die Malware SocGholish sowie Amadey und StealC. Im Falle von SocGholish wurden 106 Server und Domains abgeschaltet sowie rund 15.000 kompromittierte WordPress-Seiten bereinigt. Die Diskussion um die jeweilige rechtliche Grundlage für solche Aktionen dürfte weitergehen, insbesondere im größeren Kontext der aktuell laufenden Gesetzgebungsverfahren im Sicherheitsbereich in Deutschland.

Mehr von EuRepoC

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

About the authors

Kerstin Zettl-Schabath ist Senior Cyber Threat Intelligence Analyst bei dem Deutschen Cyber-Sicherheitsorganisation (DCSO).

Lena Rottinger ist Doktorandin der Universität Heidelberg und ist wissenschaftliche Mitarbeiterin im EuRepoC-Projekt; sie ist verantwortlich für die politische Kodierung von Cybervorfällen.

Erik Kellenter ist Studentischer Mitarbeiter bei der Stiftung Wissenschaft und Politik (Berlin) und studiert seinen Bachelor in Politikwissenschaft und Master in Computerwissenschaft.

Callahan Shelley ist wissenschaftlicher Mitarbeiter bei der Stiftung Wissenschaft und Politik (Berlin) in der Forschungsgruppe EU/Europa.

Follow us on social media

@EuRepoC

linkedin/EuRepoC

contact@eurepoc.eu

https://eurepoc.eu