European
Repository of
Cyber Incidents

EuRepoC
Cyberkonflikt Briefing

Q3 2026

Kerstin Zettl-Schabath
Lena Rottinger
Callahan Shelley
Erik Kellenter



Beobachtungen zur Gesamtlage

Im Q3 2026 wurden **227 öffentlich bekannt gewordene Cyber-Operationen** in die EuRepoC-Datenbank aufgenommen. Ein substanieller Anstieg (40.1%) gegenüber dem Vorquartal und 36 Operationen mehr als die insgesamt durchschnittlich verzeichnete Aktivität von 191 Cyber-Operationen pro Quartal im Gesamtzeitraum (2000-2026).

Mit **64 Vorfällen** bleiben die Vereinigten Staaten das am häufigsten angegriffene Land. **EU-Mitgliedstaaten waren in 67 Vorfällen betroffen**: Frankreich war mit 25 Vorfällen im Q3 (im Vergleich zu 11 Vorfällen im Q2) das häufigste Ziel; gefolgt von Deutschland (11) und Spanien (8).

Besonders berichtenswert ist der Angriff der „ShinyHunters" auf das US Federal Bureau of Investigation (FBI), bei dem mehr als 3 TB an Daten über FBI-Mitarbeiter gestohlen wurden. Gleichzeitig forderte ShinyHunters einen Bericht über die Gruppe zurückzuziehen. Kurz darauf folgte eine koordinierte Aktion von US-amerikanischen und internationalen

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).**

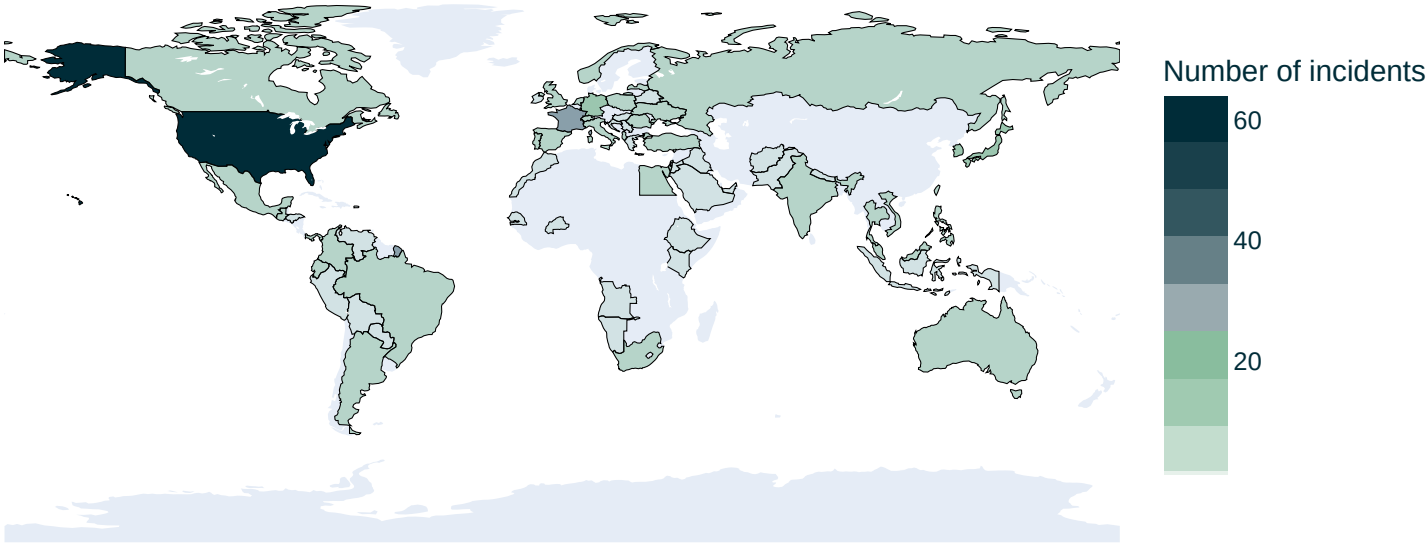
Die deutsche Ausgabe erscheint in Kooperation mit dem **Tagesspiegel Cybersecurity Background.**

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 3. Quartal 2026



Behörden, die zur Festnahme mehrerer Verdächtiger führte. Der der militärische Konflikt um den Iran spielte weiterhin eine gewichtige Rolle im US-amerikanischen Cyber-Ökosystem: es wurden mehrere Vorfälle verzeichnet, die auf Wasserversorgungssysteme in einigen Bundesstaaten, darunter New Jersey und Minnesota, zielten.

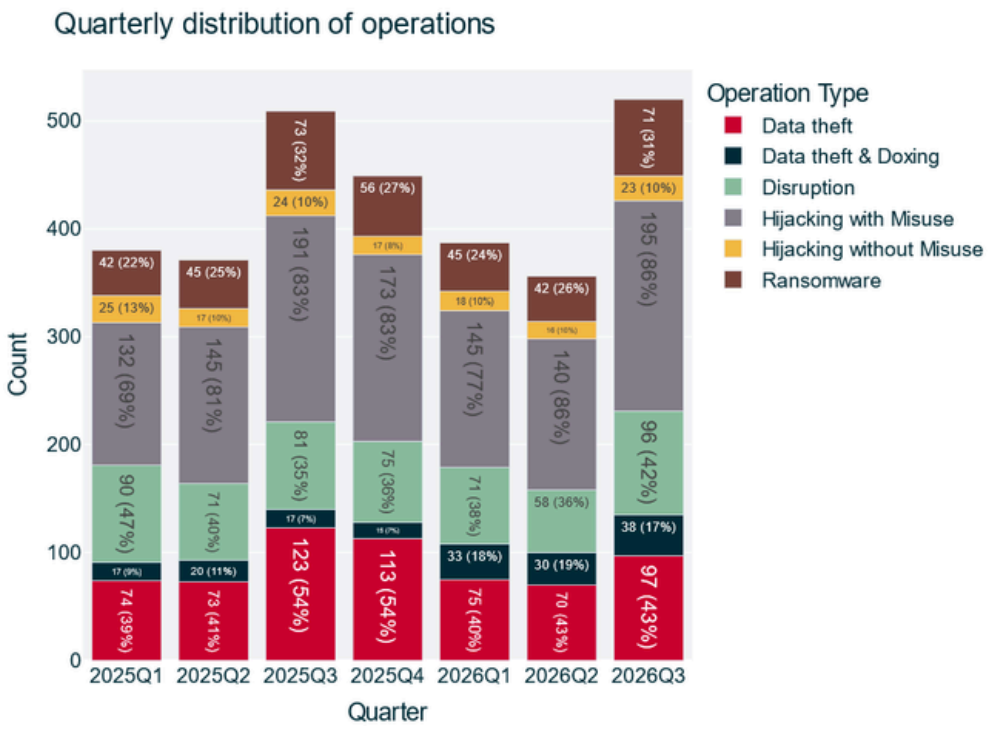
In Frankreich kam es im August zu Angriffen auf das französische Wohnungsbauministerium und das Ministerium für ökologischen Wandel. Ende Juli drangen unbekannte Akteure in das Bildungsministerium ein, was zur Entwendung personenbezogener Daten von Ministerialmitarbeitern führte. In Deutschland wurden, neben dem Diebstahl von Informationen aus dem Berliner Senat durch die Ransomwaregruppe „Rhysida“, Einrichtungen in den Sektoren Telekommunikation, Gesundheitswesen, Energie, Forschung und Verkehr angegriffen, während in Spanien das Gesundheitswesen, der Forschungssektor und der Verkehrssektor betroffen waren.

Brennpunkte und Zielmuster

Die relative Verteilung der Operationstypen ist gegenüber dem letzten Quartal weitgehend konstant geblieben. Der größte Teil der erfassten Cyberangriffe (86%) fallen unter die Kategorie "Hijacking with Misuse". Das heißt, ein Angreifer hat sich nicht nur Zugang zu IT-Systemen verschafft, sondern hat auch Schaden verursacht – meist durch die Entwendung und/oder Verschlüsselung von vertraulichen Daten und/oder das Lahmlegen von Systemen. Bei knapp einem Drittel dieser erfassten Cyberangriffe handelte es sich um Ransomware-Angriffe. Der Anteil der Vorfälle mit Datendiebstahl ("Data Theft") liegt in diesem Quartal insgesamt bei 60%, wobei in 17% der Fälle die gestohlenen Daten veröffentlicht wurden ("Data Theft & Doxing").

In 42% der erfassten Vorfälle hatte der Cyberangriff eine Störung der Systeme des Opfers zur Folge ("Disruption"): Eine Steigerung um 6 % gegenüber dem letzten Quartal und der höchste Wert seit Anfang 2025. In den meisten Fällen ist ein Ausfall von Systemen eine Konsequenz einer erfolgreichen Kompromittierung. Nur in 6 % der Fälle wurde die Störung durch einen DDoS-Angriff verursacht; ein deutlicher Rückgang, denn im Vorjahrsquartal betrug der Anteil der DDoS-Angriffe noch 20%.

Verteilung der Arten von Cyberoperationen



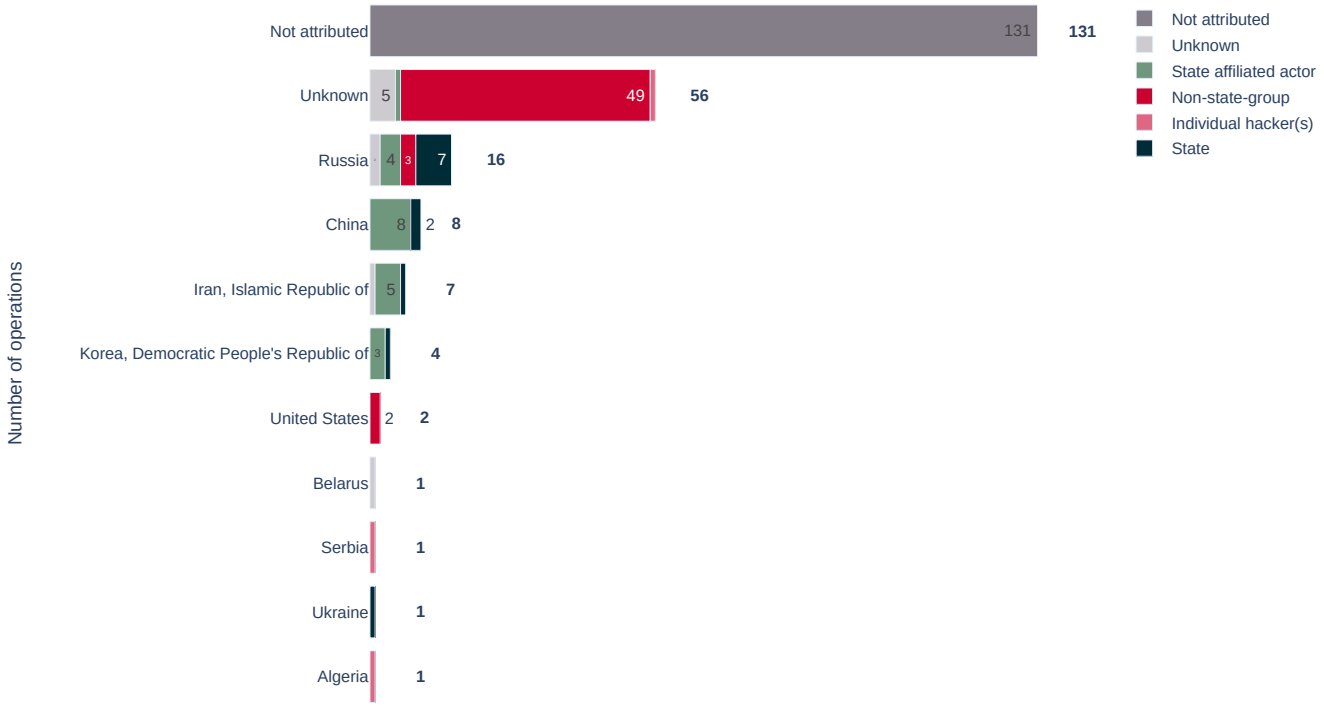
Im letzten Berichtsquartal gab es einen besonders schwerwiegenden Angriff auf die rumänische Katasterbehörde ANCPI, bei dem sensible Daten gestohlen und mutmaßlich die gesamte Grundbuchdatenbank des Landes gelöscht wurde. Auch wenn die Datenbank Berichten zufolge später aus einem Backup wiederhergestellt werden konnte, waren für einige Tage alle Immobilientransaktionen blockiert, sodass Notare keine Verkäufe beglaubigen und Bürger keine Grundbuchauszüge erhalten konnten.

Angreiferprofile und Attributionen

In Q3 wurden über die Hälfte der öffentlich berichteten Cybervorfälle (53%) nicht attribuiert. Wie auch in den vorherigen Quartalen führen Russland, China, Iran und Nordkorea die Liste der attribuierten Staaten an. Im Gegensatz zum Vorquartal, verzeichnet nicht Iran, sondern Russland die meisten Vorfallszuschreibungen, wobei mehrere Cyberangriffe dem Zentrum 16 des russischen Inlandsgeheimdienstes (FSB) angelastet wurden.

Laut der gemeinsamen offiziellen Attribution des Vereinigten Königreichs (VK) und der EU vom 13. Juli 2026 ist das Zentrum 16 nicht nur für den Angriff auf den polnischen Energiesektor Ende Dezember 2025 verantwortlich, sondern auch für eine ganze Reihe weiterer Angriffe auf EU-Mitgliedstaaten wie Frankreich, Deutschland, Zypern, die Niederlande, Österreich, die Slowakei, Rumänien und Finnland, sowie auf EU-Partnerstaaten (insbesondere der Ukraine). Das Zentrum 16 seit mindestens 2010 aktiv und greift vornehmlich staatliche Einrichtungen und verschiedene KRITIS Sektoren darunter Energie, Luftfahrt, Wasser sowie industrielle Fertigung an. Es ist die erste EU-Erklärung, in der das Zentrum 16 expressis verbis als Bedrohungsakteur genannt wurde. Bemerkenswert an der europäischen Reaktion ist das Ausmaß der Koordination und Informationen, der begleitenden Maßnahmen, sowie die offensichtliche Abwesenheit der USA als tonangebender Akteur.

Verteilung der Arten von Cyberoperationen



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

Neben der EU-Erklärung und der britischen Attribution haben Deutschland, Frankreich und Polen eigenständige Statements veröffentlicht, die sich erkennbar hinsichtlich ihrer Spezifität und ihres Tons unterscheiden. Frankreich legte in einem separaten Statement offen, dass das TURLA (Subgruppe des Zentrum 16) seit 2017 das Ministerium für Streitkräfte, 2018 die französische Botschaft in Moskau, 2019 den Justizsektor und 2026 eine Forschungseinrichtung mit Spezialisierung auf sensible Technologien angegriffen hatte. Keiner dieser Vorfälle war bislang in der EuRepoC-Datenbank dokumentiert worden; was bedeutet, dass sie nun erstmals öffentlich bekannt gemacht wurden. Damit handelt es sich um die zweite offizielle politische Attribution Frankreichs zu russischen staatlichen Cyberaktivitäten und könnte auf eine neue selbstbewusstere französische Cyberattributionspolitik hindeuten.

Die begleitenden deutschen und polnischen Presseerklärungen fielen deutlich verhaltener aus und lieferten keine neuen Informationen über die Cyberaktivität des Zentrum 16. Es wurde lediglich bestätigt, dass die Gruppe erfolgreich Einrichtungen in beiden Ländern kompromittierte, aber genaueres dazu wurde nicht bekannt gegeben (auch nicht auf Nachfrage in der Bundespressekonferenz).

Dieses Bündel an Reaktionen, was durch die Einbestellung russischer Botschafter in mehreren europäischen Ländern, einem britisch-europäischen Cybersanktionspaket, sowie einen Joint Advisory zu Routersicherheit ergänzt wurde, deutet auf eine Europäisierung der internationalen Cyberdiplomatie hin. Bis zur zweiten Trump Administration wurden entsprechende westliche Reaktionen stark von US-amerikanischer Initiative geprägt. Insgesamt ist dieses koordinierte Reaktionsbündel ein deutliches Signal, das zeigt, dass gemeinsames Handeln – auch ohne die Führung der USA – möglich ist.

KI und Angreiferprofile

Künstliche Intelligenz gewinnt als Hilfsmittel für Angreifer und als Angriffsziel weiter an Bedeutung. In Q3 gab es eine zunehmende Integration von KI in Angriffszyklen sowie einen neuen Typ von Angreifern: autonome KI-Agenten (siehe Hugging Face-Vorfall). Zu beobachten sind dabei vor allem zwei Trends: Erstens können weniger professionelle und mit Ressourcen ausgestatte Akteure zunehmend komplexere Cyberangriffe durchführen, da KI-Modelle bei der Zielauswahl, der Schwachstellenidentifikation und Penetration fremder Netzwerke schneller, effizienter und weitreichender arbeiten können als Menschen. Zudem werden gestohlene API-Schlüssel zur Erschließung zusätzlicher KI-Rechenkapazitäten während des laufenden Angriffs eingesetzt wurden. Die Nutzung von KI-Agenten wird dabei nachweislich sowohl von russischen (z.B. Midnight Blizzard), chinesischen, iranischen als auch nordkoreanischen Akteuren mit Verbindungen zum jeweiligen Staat vorangetrieben. Zweitens nimmt der Autonomiegrad der KIs stetig zu, sodass Cyberoperationen immer mehr KI-geleitet als „nur“ KI-assistiert sind. Anfängliche Behauptungen über vollständig autonome (Ransomware-)Angriffe müssen jedoch differenziert betrachtet werden. So musste das über den angeblich voll autonomen KI-Agenten JADEPUFFER berichtende Unternehmen im Nachgang einräumen, dass dieser nicht so autonom agierte, wie es für seine Ransomware-Aktionen zunächst dargestellt worden war.

Entwicklungen im Bereich der Cyberkriminalität

In Q3 waren u.a. folgende Entwicklungen im Cyberkriminalitätsbereich bemerkenswert:

- Im dritten Quartal setzten neue Gruppen wie Gammax und Orova verstärkt auf „double extortion“, bei der zunächst Daten exfiltriert und anschließend die Systeme verschlüsselt werden. Gestohlene Informationen werden dabei zunehmend mehrfach monetarisiert, beispielsweise durch die Erpressung betroffener Kunden des Primäropfers. Gleichzeitig verbleiben die Grenzen zwischen finanziell motivierter Cyberkriminalität und staatlichen Aktivitäten unscharf. Die beobachteten Überschneidungen zwischen der Ransomware-Gruppe Gunra und Lazarus verdeutlichen diese Entwicklung, belegen jedoch nicht automatisch eine staatliche Steuerung einzelner Operationen. Flexible Akteursnetzwerke, regionale Teilstrukturen und wechselnde Kooperationen erschweren die Attribution weiterhin. Festnahmen mutmaßlicher Mitglieder von ShinyHunters und TeamPCP zeigen zudem, dass Strafverfolgungsmaßnahmen zwar Wirkung entfalten, die zugrunde liegenden Netzwerke jedoch persistent und komplex bleiben.
- Auf taktischer Ebene blieb Device-Code-Phishing ein bedeutender Initial-Access-Vektor. Kommerzielle Phishing-as-a-Service-Angebote wie Greatness, DEBULL und ARToken ermöglichen skalierbare Angriffe und kombinieren zunehmend Microsoft-Authentifizierungsverfahren mit Adversary-in-the-Middle-Techniken. Da hierfür keine klassischen gefälschten Anmeldeseiten erforderlich sind, können die Angriffe für Beschäftigte schwieriger

zu erkennen sein. Daneben gewann Vishing in Kombination mit Mail Bombing an Bedeutung, insbesondere zur Erlangung des initialen Zugriffs. Die DCSO hat die Technik in mehreren IR-Einsätzen in Q3 beobachtet: Angreifer überlasten zunächst die Postfächer ihrer Opfer und geben sich anschließend telefonisch als IT-Support aus, um über legitime Fernwartungswerkzeuge Zugriff auf Unternehmenssysteme zu erhalten. Gefälschte Recruiting-Anfragen und weiterentwickelte ClickFix-Techniken erweitern das Spektrum. Bei ClickFix werden Opfer dazu verleitet, Befehle direkt in die Adresszeile des Browsers einzugeben; entsprechende Angriffsketten führen häufig zur Installation von Infostealern wie Amatera und Remus. Insgesamt werden Social Engineering und die Bereitstellung von Angriffswerkzeugen weiter professionalisiert und an bestehende Abwehrmaßnahmen angepasst.

- Dass sich Kriminelle entgegen dem vorherrschenden Muster auch zu Beginn ihrer „Karriere“ auf Krypto-Betrug fokussieren und erst im Laufe der Zeit Ransomware-Operationen durchführen können, bewies die Gruppe CRPx0, die gemäß dem White-Label-Ransomware-as-a-Service-Modell agiert und ihre Dienste sehr öffentlichkeitswirksam, u.a. über YouTube und Spotify, bewirbt. Das Zahlen von Lösegeld an solche Akteure ist keine zu empfehlende Reaktion: So wurden laut Proofpoint 2026 weltweit im Durchschnitt 37 % der erfassten Ransomware-Opfer trotz Lösegeldzahlungen erneut erpresst. Neben Führungskräften geraten Beschäftigte aus den Bereichen Finanzwesen, Personalwesen und Vertrieb gezielt ins Visier von Kriminellen. Softwareentwickler sowie Software-Ökosysteme wie npm, bleiben ebenfalls relevante Angriffsziele, speziell für Supply-Chain-Angriffe wie im Falle der sich selbst verbreitenden Operation „ChainDrop“.
- Mehrere Vorfälle verdeutlichten die potentiellen Auswirkungen auf kritische Betriebsabläufe sowie auf öffentliche Institutionen: Ein Ransomware-Angriff auf das Health Sciences Centre in Winnipeg beeinträchtigte neben weiteren Gebäudesystemen auch Türsicherungen sowie Heizungs- und Klimaanlagen. Bei Ernst & Young wurde ein Datendiebstahl behauptet, der auch dessen Kunden einer möglichen Folgeerpressung aussetzen könnte. In Liechtenstein wurden rund 31.000 Datensätze aus einem Register wirtschaftlich Berechtigter entwendet, was im Kontext der Bekämpfung von Geldwäsche und Terrorismusfinanzierung brisant ist.
- Besonders schwerwiegend war die Veröffentlichung von 5,8 TB an vertraulichen Daten nach dem obengenannten Angriff der Gruppe Rhysida auf den Berliner Senat. Zudem wurden bislang unveröffentlichte Schwachstellen in SonicWall-SMA-1000-Systemen von Ransomware-Angreifern ausgenutzt. Die verkürzten Zeitfenster zwischen Erstzugriff und Weitergabe durch den Initial Access Broker erschweren es in solchen Fällen, bereits erfolgte Kompromittierungen allein durch nachträgliches Patchen einzudämmen. Dies war mutmaßlich auch für drei ab Ende September als Zero-Day-Exploits ausgenutzte Citrix NetScaler-Schwachstellen der Fall.

International kam es zu den bereits genannten Festnahmen mutmaßlicher Mitglieder von ShinyHunters und TeamPCP, sowie zu Maßnahmen gegen mutmaßliche Mitglieder russischer Hacktivistengruppen, sowie auch von Scattered Spider.

Gleichzeitig wirft die neue präsidiale Direktive der USA vom 12. August zur Ermächtigung privater Vertragsnehmer im Kontext der Bekämpfung von „cyber-enabled transnational crime“ Fragen zu den damit verbundenen Risiken auf. Gleiches gilt für die von FBI-Chef Kash Patel angekündigte verstärkte Zusammenarbeit der USA mit China und Russland im Umgang mit sensiblen Informationen sowie die damit verbundenen sicherheitspolitischen Risiken.

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.

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

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

Follow us on social media

@EuRepoC

linkedin/EuRepoC

contact@eurepoc.eu

https://eurepoc.eu