2024

Bundeslagebild Cybercrime

Bundeskriminalamt

BKA

Allgemeine Informationen

Das Bundeslagebild Cybercrime wird durch das Bundeskriminalamt (BKA) in Erfüllung seiner Zentralstellenfunktion erstellt. Es enthält die aktuellen Erkenntnisse und Entwicklungen im Bereich der Cyberkriminalität in Deutschland und bildet insbesondere die diesbezüglichen Ergebnisse polizeilicher Strafverfolgungstätigkeiten ab.

Schwerpunkt des Bundeslagebildes Cybercrime sind die Delikte, die sich gegen das Internet und informationstechnische Systeme richten – sogenannte Cybercrime im engeren Sinne (CCieS).

Delikte, die lediglich unter Nutzung von Informationstechnik begangen werden und bei denen das Internet vorwiegend Tatmittel ist, werden als Cybercrime im weiteren Sinne (CCiwS) bezeichnet. Diese bleiben bei den Betrachtungen im Bundeslagebild Cybercrime weitestgehend unberücksichtigt.

Grundlage für den statistischen Teil des Lagebildes sind die Daten der Polizeilichen Kriminalstatistik (PKS). Da bei einem Großteil der Straftaten der CCieS Schäden in Deutschland verursacht werden, der Aufenthaltsort der Täter aber unbekannt ist oder der Angriff aus dem Ausland heraus ausgeführt wird, bedarf es zur ganzheitlicheren Beschreibung des Phänomens neben der Darstellung der Inlandstaten (Inlands-PKS) auch der Darstellung der Auslandstaten (Auslands-PKS)[1][2]. Hierzu werden in diesem Jahr erstmals absolute Zahlen ausgewiesen. Im Folgenden wird für diese Fälle weiter der Begriff „Auslandstat“ verwendet, auch wenn im Bereich Cybercrime bei einem weit überwiegenden Teil der Fälle der Handlungsort des Täters unbekannt ist.

Sowohl in der Inlands- als auch in der Auslands-PKS wird das sogenannte Hellfeld abgebildet, also die polizeilich bekannt gewordene Kriminalität. Valide Aussagen und Einschätzungen zu Art und Umfang des komplementären Dunkelfeldes, also den Straftaten, die der Polizei nicht bekannt sind, können aus den statistischen Grunddaten der PKS nicht abgeleitet werden. Im Bereich der Cyberkriminalität ist das Dunkelfeld weit überdurchschnittlich ausgeprägt, sodass es für eine quantitativ und qualitativ zutreffende Lagebeschreibung von besonderer Bedeutung ist, polizeiexterne Informationen einzubeziehen. Zu diesem Zweck fließen in das Bundeslagebild Cybercrime auch Erkenntnisse und Einschätzungen anderer Behörden sowie ausgewählter privatwirtschaftlicher oder wissenschaftlicher Einrichtungen und Verbände ein.

An verschiedenen Stellen des Bundeslagebilds Cybercrime 2024 finden Sie QR-Codes, über die Sie sich bei Bedarf ergänzende Informationen erschließen können. Zum besseren Verständnis der in den einzelnen Kapiteln beschriebenen Modi Operandi wird empfohlen, die QR-Codes zu Beginn des jeweiligen Kapitels zu nutzen.

[1] Die separate Erfassung von Auslandstaten in der PKS wurde zum 01.01.2020 eingeführt. Nach gemeinsamer Evaluation und Abstimmung mit den Bundesländern erfolgt für das Berichtsjahr 2024 erstmalig die Ausweisung der absoluten Zahlen.

[2] Fallerfassung in der PKS-Ausland, wenn alle Tathandlungen im Ausland oder an einem unbekannten Ort erfolgt sind und gleichzeitig ein Schaden/Taterfolg in Deutschland eingetreten ist.

Inhaltsverzeichnis

1. Cybercrime 2024 - Überblick

Nach einem weiteren Anstieg der Auslandstaten auf 201.877 Fälle übersteigen sie die Straftaten der Inlands-PKS deutlich.

Die Aufklärungsquote bei Cybercrime-Delikten beträgt 32 %.

Deutschlandweit wurden 950 Ransomware-Angriffe angezeigt.

Die weltweiten Ransomware-Zahlungen liegen bei über 800 Mio. US-Dollar.

Hacktivistische DDoS-Angriffe auf Ziele in Deutschland setzen sich fort.

KI wird zunehmend auch für cyberkriminelle Aktivitäten genutzt.

Der durch den Bitkom e.V. festgestellte Schaden durch Cyberattacken beträgt 178,6 Mrd. Euro.

International koordinierte Maßnahmen erfolgen in einer höheren Frequenz - die Strafverfolgung passt sich erfolgreich der gesteigerten Bedrohungslage an.

1.1 BEDROHUNGSLAGE

Überblick 2024

Die Bedrohungslage im Cyberraum war 2024 anhaltend hoch. Wie bereits 2023 prägten vor allem Ransomware-Angriffe sowie DDoS-Kampagnen hacktivistischer Akteure das Berichtsjahr. Daneben wurden vereinzelte Aktivitäten mutmaßlich staatlicher Akteure gegen Einrichtungen kritischer Infrastrukturen und politische Institutionen verzeichnet.

Phishing

Phishing ist und bleibt ein relevanter Eintrittsvektor. Besonders häufig wurden Versand- und Finanzdienstleister, aber auch Bundesbehörden als vermeintliche Absender von Phishing-Mails missbraucht.

Ransomware

Ransomware bleibt eine zentrale Bedrohung und verursacht weiterhin erhebliche Schäden bei Unternehmen und Privatpersonen.

DDoS

Die Bedrohung durch DDoS-Angriffe ist weiterhin auf einem sehr hohen Niveau. Zudem sind die Aktivitäten hacktivistischer Kollektive signifikant angestiegen.

Schäden

Die in Deutschland explizit durch Cyberattacken entstandenen Schäden betrugen gemäß einer im Jahr 2024 durchgeführten Erhebung des Bitkom e. V. 178,6 Mrd. Euro und sind damit im Vergleich zum Erhebungsjahr 2023 deutlich angestiegen (+ 30,4 Mrd. Euro). Dies stellt die bislang höchste gemessene Schadenssumme dar. Schäden durch Cyberangriffe machen drei Viertel der erfassten Gesamtschäden (266,6 Mrd. Euro) aus, die durch analogen und digitalen Diebstahl, Industriespionage oder Sabotage entstanden sind.

Bedrohungsszenarien

Digitalisierung geopolitischer Konflikte
Geopolitische Konflikte weiten sich zunehmend in den digitalen Raum aus. Dies zeigt sich vor allem in einem Anstieg hacktivistischer Aktivitäten gegen Ziele in Deutschland.

Künstliche Intelligenz (KI)
KI ergänzt das Repertoire cyberkrimineller Akteure. Zukünftig ist eine weitere Verschärfung KI-unterstützter Straftaten zu erwarten.

1.2 BEDEUTENDE ENTWICKLUNGEN

Januar
Hacktivistische Akteure beginnen diverse Kampagnen gegen Ziele in Deutschland. Unter anderem betroffen sind das Bundesamt für Logistik und Mobilität, diverse Verkehrsunternehmen wie der Rhein-Main-Verkehrsverbund, der Flughafen Stuttgart sowie die Bundeswehr und der Bundestag.

Februar
Das Universitätsklinikum Brandenburg an der Havel GmbH wird Ende Februar Ziel eines Cyberangriffs. Nachdem der Angreifer vermutlich über eine Phishing-Mail ins System gelangt, werden im Anschluss von den betroffenen Systemen massenhaft Spam-Nachrichten versendet.

März
Ein Forscherteam entwickelt den KI-Wurm Morris-II. Durch automatische Replikation kann dieser sich durch KI-Systeme bewegen, dort Malware ausführen oder Daten stehlen.

APT29, eine mutmaßlich staatliche Gruppierung, missbraucht Namen und Logo der CDU für eine Phishing-Kampagne, die zur Distribuierung von Malware verwendet wird.

April
Als Rechnung getarnt wird eine mittels KI modifizierte Version des Rhadamantys-Info-Stealers gegen ein deutsches Unternehmen eingesetzt. Gemäß Analysen eines IT-Dienstleisters könnte ein mittels KI erstelltes Skript Teil des Angriffes gewesen sein.

Mai
Eine Datenbank der europäischen Polizeibehörde Europol wird kompromittiert – dabei fließen primär personenbezogene Daten, aber auch Kontaktdaten und tätigkeitsbezogene Informationen ab. Ein mutmaßlich gestohlener Datensatz wird später im Darknet zum Verkauf angeboten.

Juni
Die IT-Infrastruktur der CDU wird kompromittiert. Eintrittsvektor war eine Schwachstelle in einem IT-Sicherheitsprogramm.

Juli
Ein fehlerhaftes Update des IT-Sicherheitsdienstleisters Crowdstrike führt weltweit zum Ausfall von Unternehmensnetzwerken. Der Vorfall wird in der Folge von Cyberkriminellen als Narrativ für Phishing-Kampagnen verwendet. Dabei setzen cyberkriminelle Akteure auch auf maliziöse Fake-Webseiten, die den IT-Dienstleister imitieren.

August
Die Deutsche Flugsicherung GmbH bestätigt, dass ihre Systeme kompromittiert wurden.

September
Die IT-Systeme mehrerer Schulen in Nordrhein-Westfalen werden mittels der Ransomware INC Ransom verschlüsselt.

Oktober
Die Deutsche Gesellschaft für Osteuropakunde (DGO) gibt öffentlich bekannt, dass E-Mail-Postfächer kompromittiert und sensible Informationen ausgespäht wurden.

November
Hacktivistische Akteure rufen die #OPGERMANY aus. Es beginnt eine neue DDoS-Kampagne gegen Ziele in Deutschland. Betroffen sind diesmal u. a. das BKA sowie die Flughäfen Dortmund und München.

Dezember
Die im November gestartete #OPGERMANY erreicht ihren Höhepunkt – es wird die höchste Anzahl an hacktivistischen Aktivitäten im gesamten Jahr verzeichnet.

Nachdem es im Vorjahr um den Cyberakteur Cl0p ruhiger wurde, tritt er Ende Dezember wieder in Erscheinung – die Gruppierung nutzt erneut eine IT-Schwachstelle aus, um Daten von Unternehmen zu exfiltrieren und die Betroffenen dann mit der Veröffentlichung der erbeuteten Daten zu erpressen.

1.3 BRANCHEN IM FOKUS

Das **verarbeitende Gewerbe** ist ein übliches Ziel von Ransomware- bzw. Double Extortion-Angriffen. Insbesondere kleine und mittelständische Unternehmen sind von Angriffen auf diese Branche betroffen.

Bei einem Ransomware-Angriff auf einen Landtechnikspezialisten in Bayern wurden mehrere Maschinen des Unternehmens verschlüsselt, wodurch der Produktionsbetrieb temporär gestoppt werden musste. Zudem kam es zur Ausleitung von Unternehmensdaten.

Einrichtungen des **Gesundheitswesens** wurden häufig angegriffen. Neben der Gefahr für Leib und Leben sind hierbei oftmals besonders sensible Daten betroffen.

Infolge eines Cyberangriffs auf einen Klinikverband in Nordrhein-Westfalen mussten mehrere Krankenhäuser des Kreises Soest von der Notfallversorgung abgemeldet werden. Zudem wurden Patientendaten sowie unternehmensinterne Informationen gestohlen.

Die Internetauftritte von **öffentlichen Verwaltungen und Behörden** standen zunehmend im Fokus von DDoS-Angriffen und hacktivistischen Aktivitäten.

Aufgrund von DDoS-Angriffen waren die Webseiten der Landesregierung, der Landespolizei sowie des Landesverfassungsschutzes von Mecklenburg-Vorpommern für mehrere Stunden nur eingeschränkt erreichbar. Die pro-russische hacktivistische Gruppierung NoName057(16) beanspruchte die Angriffe über Telegram für sich.

Verkehrsverbünde, Flughäfen und Häfen waren mehrfach Ziel von Cyberangriffen verschiedener Art.

Im Mai verschaffte sich der Akteur Just Evil Zugriff auf ein externes System des Hamburger Flughafens, das zur Dokumentierung von Wachrundgängen genutzt wird. Sensible Informationen wurden bei dem Angriff nicht erbeutet.

1.4 STRAFPROZESSUALE MAßNAHMEN 2024

Aus polizeilicher Sicht konnte im Berichtsjahr die dynamische Fallentwicklung im Bereich Cybercrime in Teilen erfolgreich eingedämmt werden. Den zahlreichen Aktivitäten cyberkrimineller Akteure wurde eine hohe Schlagzahl an polizeilichen Maßnahmen entgegengestellt, die sich gegen unterschiedliche cyberkriminelle Akteure und Phänomenbereiche richteten.

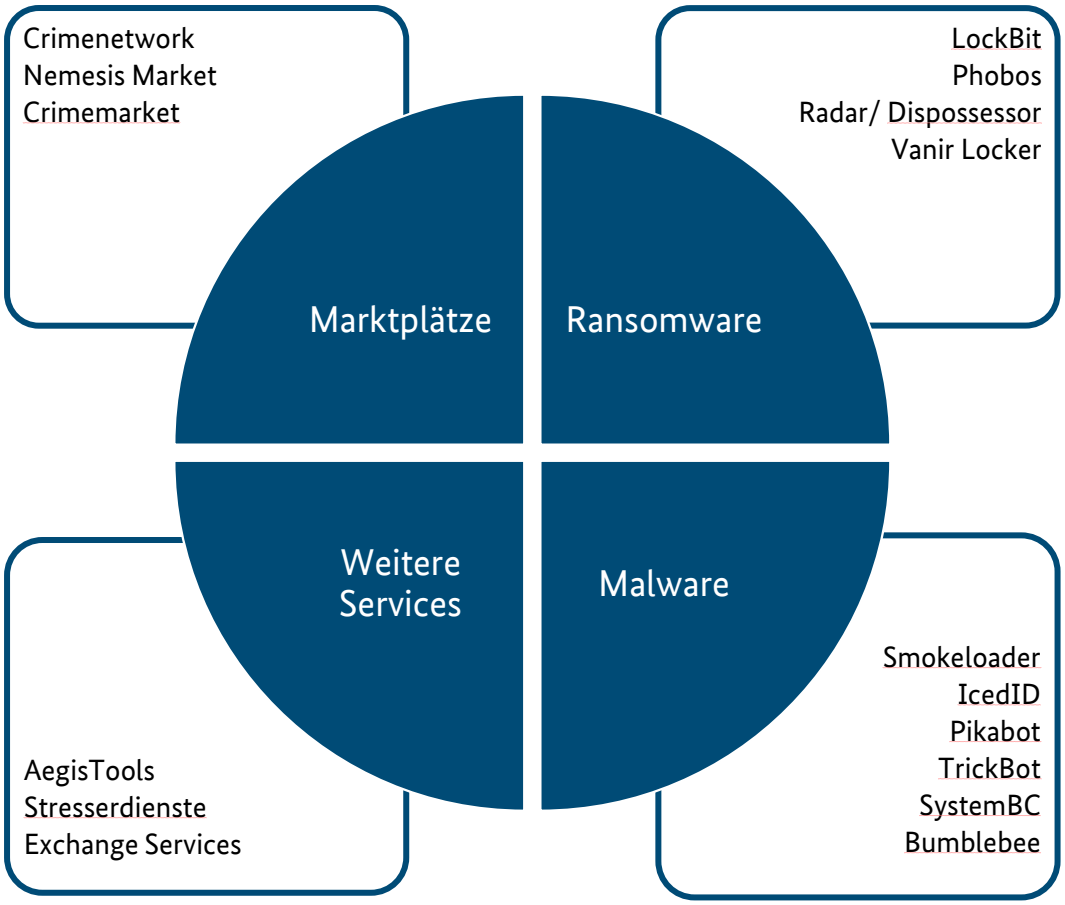


Abbildung 1: Ziele operativer Maßnahmen 2024.

2. Polizeiliche Kriminalstatistik

Vor dem Hintergrund eines sehr hohen Dunkelfeldes im Bereich Cybercrime ist die PKS vor allem als Datenbasis für Trendaussagen zur Entwicklung des Phänomenbereichs relevant.

Die cyberspezifischen Delikte werden in der PKS unter dem Summenschlüssel Cybercrime zusammengefasst. Nachdem im Jahr 2021 im Bereich der Cybercrime-Delikte ein Höhepunkt an registrierten Straftaten, bei denen der Handlungsort der Täter im Inland (Inlands-PKS) liegt, festgestellt wurde, ist diese Entwicklung seit 2022 rückläufig. Im Jahr 2024 konnte mit 131.391 Fällen ein weiterer leichter Rückgang (-2,2 %) an Cyber-Straftaten in der Inlands-PKS verzeichnet werden.
Die Aufklärungsquote ist hierbei ebenfalls leicht gesunken (31,9 %), liegt damit aber auf dem Niveau der letzten vier Jahre. Der Anteil von Cybercrime-Delikten an den registrierten Straftaten insgesamt nahm leicht zu und lag für das Jahr 2024 bei 2,3 % (vgl. 2023: 2,2 %).

Bei der detaillierteren Betrachtung der Einzeldelikte des Summenschlüssels Cybercrime liegt der größte Anteil der Fallzahlen mit weiterhin ca. 82 % im Bereich des Computerbetrugs, allerdings ist bei den absoluten Zahlen im Vergleich zum Vorjahr ein Rückgang feststellbar. Ebenfalls rückläufig sind die Fallzahlen des Ausspähens von Daten/Datenhehlerei, während bei den relevanten Einzeldelikten Fälschung beweiserheblicher Daten und Datenveränderung/Computersabotage ein leichter Anstieg zu verzeichnen ist.

Aber auch wenn die Fallzahlen der Inlands-PKS für das Jahr 2024 leicht rückläufig sind, ist dies kein Indiz für einen generellen Rückgang der registrierten Cyberstraftaten mit Auswirkungen auf Deutschland. Die Inlands-PKS hat hier nur eine begrenzte Aussagekraft, da vielfach das Agieren der Cybertäter nicht im Inland verortet werden kann. Ein realistischeres Bild der Kriminalitätsbelastung anhand der PKS ergibt sich erst bei der Betrachtung dieser Fallzahlen in Verbindung mit den Auslandstaten; den Fällen also, bei denen der Aufenthaltsort der Täter unbekannt ist oder diese sich nicht in Deutschland aufhalten und ein Schaden/Taterfolg in Deutschland eingetreten ist.
Hierzu können für 2024 erstmals absolute Zahlen in der PKS ausgewiesen werden: Mit einem weiteren Anstieg auf 201.877 Fälle (ca. + 6 %) sind im Phänomenbereich Cybercrime erheblich mehr Auslands- als Inlandstaten erfasst. Zudem setzen sie den bereits in den Vorjahren festgestellten Trend fort, dass die Auslandstaten im Cyberbereich ansteigen.

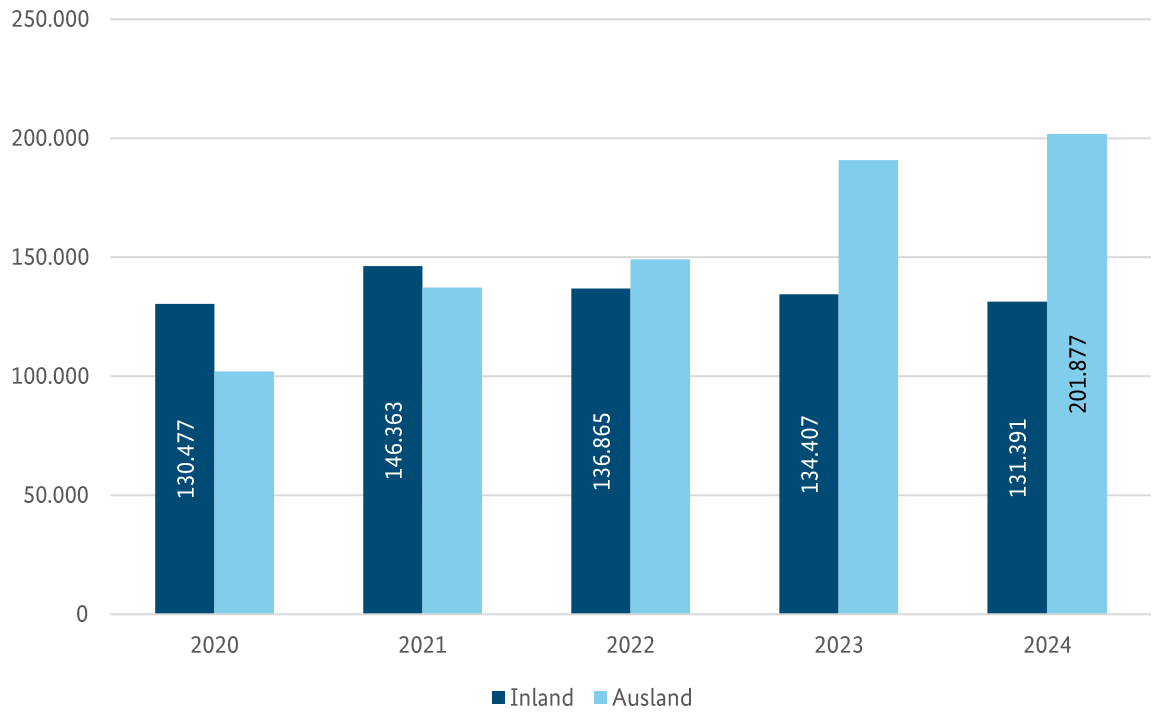


Abbildung 2: Erfasste Cybercrime-Fälle in Deutschland ohne Nennung der absoluten Zahlen bei den Auslands-Taten für die Jahre 2020-2023.

Vergleicht man den Anteil an Cybercrime-Delikten der Inlands- und Auslands-PKS, wird die hohe Relevanz der Auslandstaten für diesen Deliktsbereich deutlich: Während Cybercrime-Delikte in der Inlands-PKS nur einen Anteil von 2,3 % an den Gesamtstraftaten darstellen, machen sie in der Auslands-PKS beinahe ein Drittel aller Taten aus (31,4 %).

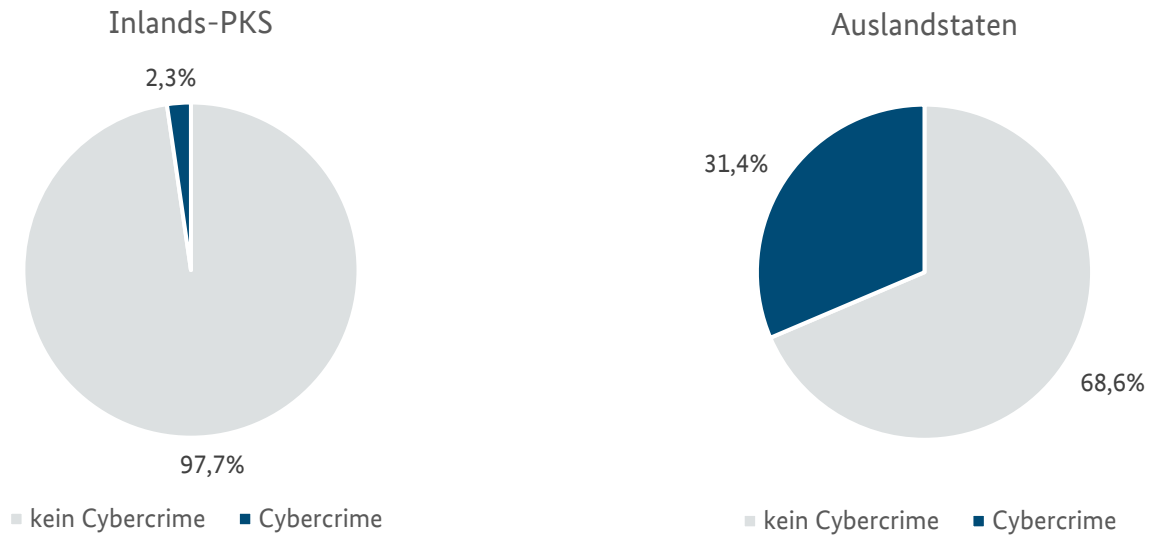


Abbildung 3: Anteil von Cybercrime-Delikten an Gesamtstraftaten.

Der hohe Anteil an Fällen, bei denen der Handlungsort des Täters nicht im Inland verortet werden kann, stellt die ermittelnden Polizeibehörden vor große Herausforderungen. Dies spiegelt sich weiterhin in einer Aufklärungsquote der in der Auslands-PKS dargestellten Fallzahlen in einem niedrigen einstelligen Bereich wider. Generell gilt innerhalb der PKS ein Fall dann als aufgeklärt, wenn nach dem polizeilichen Ermittlungsergebnis die rechtmäßigen Personalien von mindestens einem Tatverdächtigen bekannt sind. Juristische Hürden und mangelnde Kooperationsbereitschaft im Ausland können gerade diese Täteridentifizierung und Strafverfolgung erschweren oder sogar verhindern, sodass selbst vorliegende Ermittlungsansätze die Aufklärungsquote nicht verbessern.

Die Fallzahlen zum Straftatbestand § 127 StGB „Betreiben krimineller Handelsplattformen im Internet“ werden nicht vom Summenschlüssel Cybercrime umfasst. Nachdem 2023 insgesamt 27 solcher Fälle in der PKS registriert wurden, stieg die Fallzahl 2024 auf 92 an und verdreifachte sich somit innerhalb eines Jahres. Lediglich zwölf Prozent dieser Fälle konnten aufgeklärt werden. Es muss hierbei allerdings berücksichtigt werden, dass eine Zu- bzw. Abnahme aufgeklärter Fälle aufgrund der niedrigen Grundgesamtheit der Fallzahlen stark ins Gewicht fällt und somit zugleich den Anschein eines starken Anstiegs bzw. Rückgangs der Aufklärungsquote wecken kann.

Die Anzahl polizeilich bekannt gewordener Cyberdelikte steigt – maßgeblich hierfür sind vor allem Fälle, bei denen der Handlungsort des Täters unbekannt oder im Ausland ist.

3. Relevante Phänomenbereiche

3.1 ILLEGALE PLATTFORMEN & MARKTPLÄTZE

Gemeinsamer Nenner der meisten Bedrohungen im Cyberraum ist die Underground Economy. Sie ist die Gesamtheit aller kriminellen Plattformen und Marktplätze und nimmt daher eine zentrale Rolle im Phänomenbereich ein.

Dabei beschränken sich Anbieter längst nicht mehr nur auf Darknet-Marktplätze, um ihre jeweiligen Waren zu vertreiben. Auch Messenger-Dienste wie Telegram gehören mittlerweile zu etablierten Verkaufsplattformen. Einige Vendoren nutzen Bots, die Bestellungen automatisiert annehmen, und/oder Abo-Modelle, um Kunden langfristig an sich zu binden.

Sog. Initial Access Broker bleiben weiterhin wichtige Dienstleister bei der Begehung von Cyberstraftaten. Das Wissen um Eintrittsvektoren, Zero-Day-Schwachstellen, Exploits sowie Zugangsdaten zu bereits kompromittierten Systemen stellt nach wie vor eine lukrative Handelsware in der Underground Economy dar, die gleichzeitig Ausgangspunkt vieler schwerwiegender Cyberangriffe ist. Nach Angaben des IT-Sicherheitsdienstleisters Crowdstrike ist die Anzahl der Angebote von Initial Access Brokern 2024 um nahezu 50 % im Vergleich zum Vorjahr gestiegen. Insgesamt zählte Crowdstrike ca. 4.500 derartiger Angebote.[3]

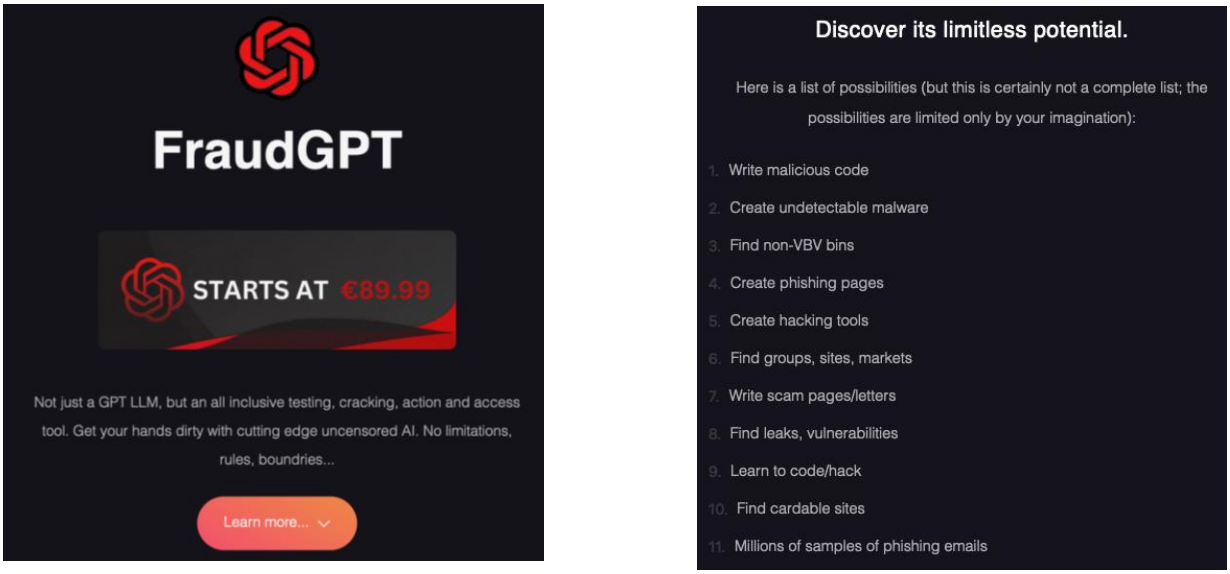


Abbildung 4: Screenshots aus der Underground Economy.

Auch KI-Fähigkeiten werden in der Underground Economy breit diskutiert. Neben einer anfänglich hohen Aufmerksamkeit für Dark AI (eigens für kriminelle Zwecke entwickelte oder angebotene KI-Modelle wie WormGPT und FraudGPT) werden in der Underground Economy auch vermeintliche KI-Tools beworben und vertrieben, die sich nach Kauf als unzureichend und/oder Betrug herausstellen. Im Jahresverlauf 2024 entwickelte sich der Trend zunehmend hin zum Missbrauch herkömmlicher

[3] Crowdstrike (2025). 2025 Global Threat Report.

leistungsstarker KI-Tools, die mittels Jailbreaking [4] oder kompromittierter Nutzeraccounts für cyberkriminelle Aktivitäten eingesetzt werden.

Messenger-Dienste etablieren sich als Vertriebskanal für Cybercrime-as-a-Service-Angebote.

[4] Jailbreaking bezeichnet das nicht-autorisierte Deaktivieren von Nutzungsbeschränkungen, um beispielsweise zusätzliche oder vom Hersteller beschränkte Funktionen freizuschalten.

3.2 EINTRITTSVEKTOREN

Im Jahr 2024 haben neben den verschiedenen Modi Operandi auch die Eintrittsvektoren an Komplexität zugenommen. Die neuesten technologischen Entwicklungen, insbesondere im Bereich der künstlichen Intelligenz, haben auch einen enormen Einfluss auf den Bereich der Eintrittsvektoren und bringen eine veränderte Dynamik zutage. Die Cyber-Akteure werden in ihrer Angriffsplanung kreativer und versuchen, effizientere Methoden zu finden.

3.2.1 Schwachstellen

IT-Schwachstellen bleiben ein relevanter Eintrittsvektor. Die Anzahl der ausgenutzten Schwachstellen bewegt sich im Jahr 2024 auf dem gleichen Niveau wie 2023: Insgesamt wurden 186 IT-Schwachstellen gesichert für cyberkriminelle Handlungen ausgenutzt – durchschnittlich waren dies 15 Schwachstellen im Monat.[5]

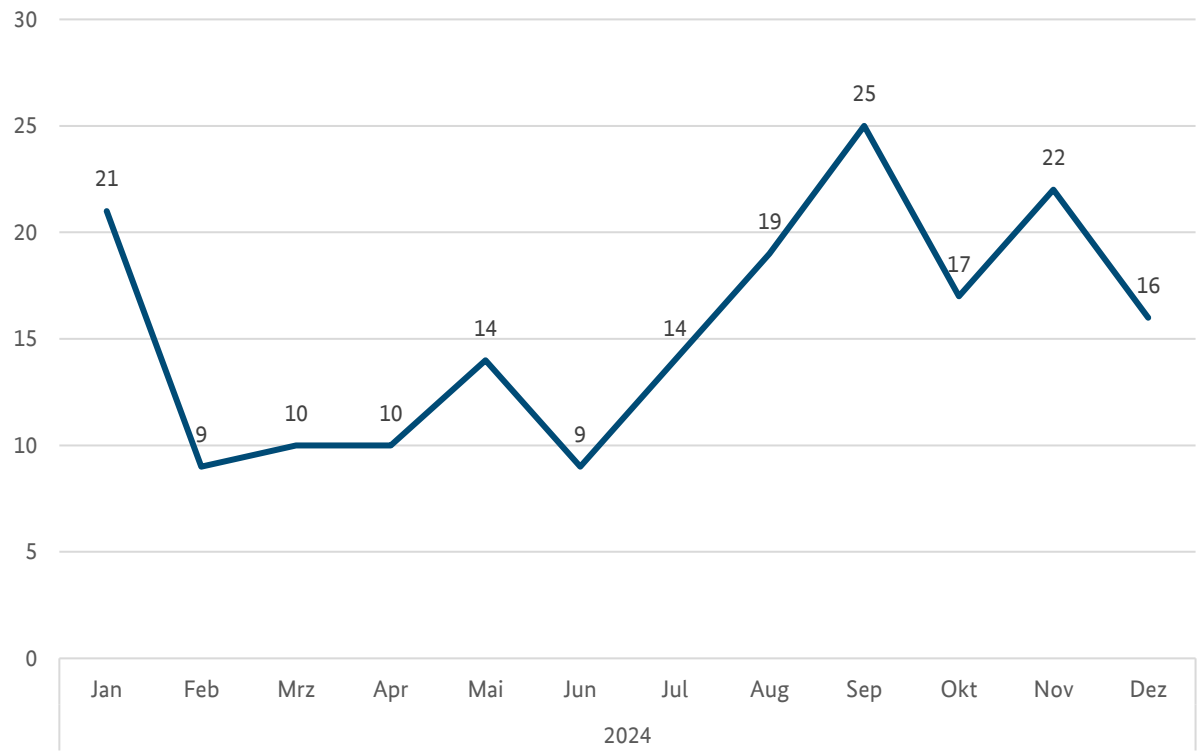


Abbildung 5: Anzahl der ausgenutzten Schwachstellen. Quelle: US-amerikanische CISA.

Die Ausnutzung von Schwachstellen führt in einer Vielzahl der Fälle zur Kompromittierung von IT-Systemen. Wie bereits im Vorjahr waren hierfür insbesondere Zero-Day-Schwachstellen (z. B. im Produkt FortiManager) von großer Bedeutung. Aber auch kritische Sicherheitslücken in anderer, weit verbreiteter Software, nutzten u. a. Ransomware-Akteure dazu, in IT-Systeme einzudringen und Daten zu exfiltrieren.

[5] Known-Exploited-Vulnerabilities-Katalog der US-amerikanischen CISA; Datenbestand von 2024. Online abrufbar unter: **https://www.cisa.gov/known-exploited-vulnerabilities-catalog**

Fortinet FortiManager

Die Schwachstelle CVE-2024-47575 in FortiManager, einer Softwarelösung des Unternehmens Fortinet für die Verwaltung von Sicherheitsgeräten, ermöglichte Angreifern, beliebige Befehle oder Schadsoftware auszuführen. Dadurch war das Risiko hoch, dass Zugangsdaten durch unbefugten Zugriff erlangt werden konnten.

Zyxel Firewall

Sicherheitslücken in der Firewall-Software des Herstellers Zyxel wurden insbesondere von der Ransomwaregruppierung Helldown als Eintrittsvektor benutzt, um IT-Systeme zu infilitrieren und Daten abzugreifen. Anschließend forderte die Gruppierung ein Lösegeld.

Windows 10

Die Schwachstelle CVE-2024-43491 in Windows 10 wurde als sehr kritisch eingestuft, da Angreifer über die Update-Funktion Schadcode ausführen konnten. Betroffen war ausschließlich die Version 1507 aus dem Jahr 2015.

IT-Sicherheitsforscher haben im Dezember 2024 eine höchst kritische Sicherheitslücke bei einem großen deutschen Automobilhersteller aufgedeckt und damit das Risiko unbekannter und somit ungepatchter Schwachstellen deutlich gemacht. Aufgrund unzureichender Sicherheitsvorrichtungen waren Standortdaten und umfassende Bewegungsbilder zu einer Vielzahl von Fahrzeugen öffentlich einsehbar, darunter auch Daten sicherheitsbehördlicher Mitarbeiter. Cyberakteure hätten diese unter anderem für Phishing-Angriffe missbrauchen und/oder in der Underground Economy veröffentlichen können.

Je weiter die jeweilige Software verbreitet ist, desto großflächiger ist der potenzielle Schaden bei Ausnutzung einer entsprechenden Schwachstelle. Das gilt auch für KI-Modelle. 2024 wurden erste Schwachstellen in verschiedenen KI-Umgebungen bekannt. Aber perspektivisch bergen KI-Modelle auch weiteres Gefahrenpotenzial, indem sie Sicherheitslücken, wie beispielsweise Zero-Day-Schwachstellen und Exploits, systematisch aufspüren und ausnutzen.

Schwachstellen können durch KI perspektivisch effizienter ausgenutzt werden.

3.2.2 Phishing

Phishing ist nach wie vor eine effektive und häufig genutzte Methode zur Verbreitung von Malware und/oder zur Erlangung von Zugangsdaten und anderen sensiblen Daten. Phishing-Kampagnen verbreiteten 2024 massenhaft Mails mit schädlichen Links, die mittlerweile automatisiert und ohne IT-

Vorkenntnisse versendet werden können. Sogenannte Phishing-Kits[6] sind in der Underground Economy für wenig Geld erhältlich und ermöglichen eine unkomplizierte und schnelle Erstellung und Versendung von Phishing-Mails.

Die jüngsten Entwicklungen im Bereich künstliche Intelligenz verschärfen das Bedrohungspotenzial von Phishing-Mails weiter. So können diese mithilfe von KI nicht nur authentischer gestaltet (z. B. durch stärker personalisierte Inhalte, fehlerfreie Texte und weltweite Übersetzungen), sondern durch Automatisierung auch schneller und weiter verbreitet werden. IT-Dienstleister verzeichnen bereits eine deutliche qualitative und quantitative Steigerung von KI-unterstützten Phishing-Kampagnen. Auch KI-Entwickler OpenAI bestätigte auf Basis seiner Nutzungsaktivitäten, dass generative KI von cyberkriminellen Akteuren u. a. zur inhaltlichen Erstellung von Phishing-Kampagnen missbraucht wird.

Phishing erfolgt auf verschiedene Arten, ob klassisch per E-Mail, per QR-Code (Quishing), per Telefon (Voice-Phishing oder Vishing) oder per SMS (Smishing). Letzteres war besonders im Jahr 2024 eine von Straftätern beliebte Herangehensweise, um an Zahlungskartendaten zu gelangen. Im Rahmen einzelner Ermittlungsverfahren wurden Smishing-Kampagnen mit bis zu einer halben Million betrügerischer SMS festgestellt. Bei den vermeintlichen Absendern handelte es sich in den häufigsten Fällen um Versanddienstleister und Finanzinstitute. Um diesen Modus Operandi einzudämmen, wurde 2024 von einem Mobilfunkanbieter ein Prozess entwickelt, um Smishing-Nachrichten auf mobilen Endgeräten abzufangen und zu analysieren.
Für bestimmte Endgeräte besteht sogar die Möglichkeit, Spam-SMS direkt an den Provider zu melden, sodass sie neben der Analyse auch zur Prävention genutzt werden können. Im Durchschnitt gehen seit Beginn dieses Prozesses 113.000 Meldungen pro Tag ein, was den Bedarf an solchen Mechanismen verdeutlicht.[7]

Die Verbraucherzentrale Nordrhein-Westfalen führt seit 2010 mit dem Phishing-Radar eine eigene Statistik über das Aufkommen von Phishing-Mails. Verbraucher können hierbei erhaltene Phishing-Mails an ein Postfach der Verbraucherzentrale weiterleiten, wo diese gesammelt und ausgewertet werden. Da diese Statistik u. a. vom Anzeigeverhalten der Verbraucher abhängig ist, bildet sie das tatsächliche Aufkommen von Phishing-Mails lediglich näherungsweise ab. Dennoch gibt diese Auswertung einen Überblick über Trends und Entwicklungen im Bereich Phishing und hilft bei der Identifizierung häufig verwendeter Narrative.

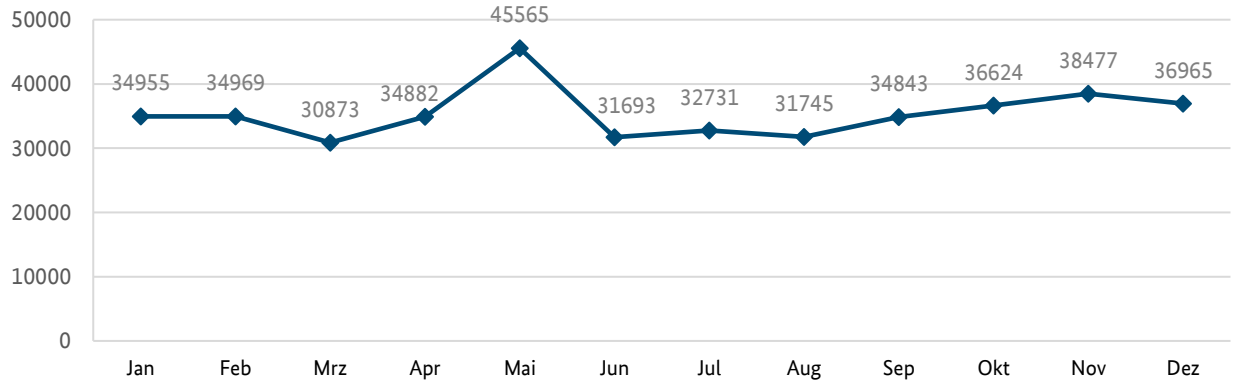
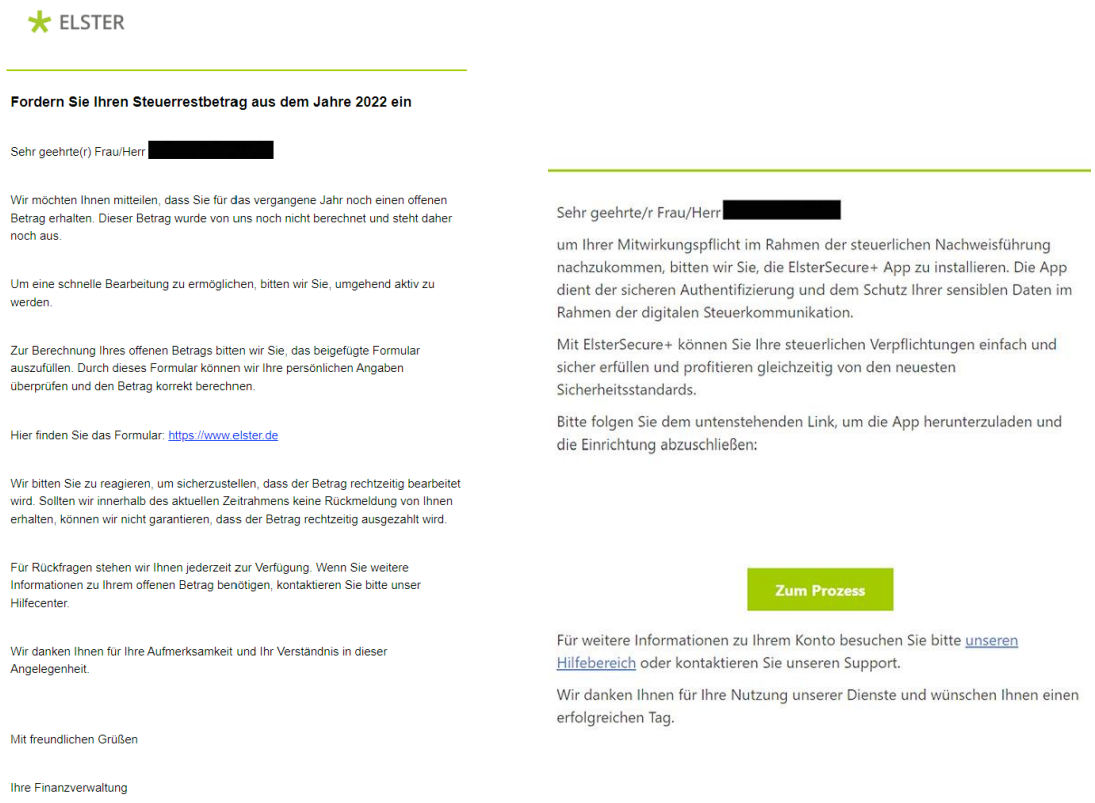


Abbildung 6: Anzahl der weitergeleiteten Phishing-Mails (2024). Quelle: Verbraucherzentrale Nordrhein-Westfalen.

[6] Phishing-Kits sind sogenannte „All-in-One" Pakete von Tools und Ressourcen, die für Phishingangriffe und -kampagnen genutzt werden können und diese effizienter bzw. die Umsetzung leichter machen.
[7] Daten der Deutschen Telekom AG.

Im Jahr 2024 erreichten das Postfach der Verbraucherzentrale Nordrhein-Westfalen über 400.000 E-Mails, die von Verbrauchern als Phishing-Mail gemeldet wurden. Ein Spitzenwert wurde im Mai mit 45.465 weitergeleiteten Mails erreicht, die übrigen Monate blieben darüber hinaus auf einem ähnlichen Niveau. Wie in den Vorjahren beziehen sich die häufigsten Narrative auf den Finanzsektor, der durch seine Bedeutung für Staat und Bevölkerung zu einem attraktiven Ziel der Cyberkriminellen gehört. Die mittlerweile professionell wirkenden Phishing-Mails mit Banken als vermeintlichen Absendern nutzen die Angst der Kunden und üben Druck aus, um diese zum (schnellen) Handeln zu bewegen und so eine Herausgabe von Zugangsdaten und anderen sensiblen Daten zu erreichen.

Andere nachgeahmte Marken und Unternehmen sind bekannte Versanddienstleister, Onlineversandhändler und Streaming-Dienstleister. Auffällig ist 2024 die häufige Nutzung von Bundesbehörden als vermeintliche Absender. Die Analyse der eingegangenen E-Mails im Phishing-Radar belegt zudem eine dynamische Anpassung an die Entwicklungen in der Wirtschaft, beispielsweise die Übernahme neuer, populärer Online-Shops als Absender der Phishing-Mails.



ELSTER

Fordern Sie Ihren Steuerrestbetrag aus dem Jahre 2022 ein

Sehr geehrte(r) Frau/Herr [redacted]

Wir möchten Ihnen mitteilen, dass Sie für das vergangene Jahr noch einen offenen Betrag erhalten. Dieser Betrag wurde von uns noch nicht berechnet und steht daher noch aus.

Um eine schnelle Bearbeitung zu ermöglichen, bitten wir Sie, umgehend aktiv zu werden.

Zur Berechnung Ihres offenen Betrags bitten wir Sie, das beigefügte Formular auszufüllen. Durch dieses Formular können wir Ihre persönlichen Angaben überprüfen und den Betrag korrekt berechnen.

Hier finden Sie das Formular: https://www.elster.de

Wir bitten Sie zu reagieren, um sicherzustellen, dass der Betrag rechtzeitig bearbeitet wird. Sollten wir innerhalb des aktuellen Zeitrahmens keine Rückmeldung von Ihnen erhalten, können wir nicht garantieren, dass der Betrag rechtzeitig ausgezahlt wird.

Für Rückfragen stehen wir Ihnen jederzeit zur Verfügung. Wenn Sie weitere Informationen zu Ihrem offenen Betrag benötigen, kontaktieren Sie bitte unser Hilfecenter.

Wir danken Ihnen für Ihre Aufmerksamkeit und Ihr Verständnis in dieser Angelegenheit.

Mit freundlichen Grüßen

Ihre Finanzverwaltung

Sehr geehrte/r Frau/Herr [redacted]

um Ihrer Mitwirkungspflicht im Rahmen der steuerlichen Nachweisführung nachzukommen, bitten wir Sie, die ElsterSecure+ App zu installieren. Die App dient der sicheren Authentifizierung und dem Schutz Ihrer sensiblen Daten im Rahmen der digitalen Steuerkommunikation.

Mit ElsterSecure+ können Sie Ihre steuerlichen Verpflichtungen einfach und sicher erfüllen und profitieren gleichzeitig von den neuesten Sicherheitsstandards.

Bitte folgen Sie dem untenstehenden Link, um die App herunterzuladen und die Einrichtung abzuschließen:

Zum Prozess

Für weitere Informationen zu Ihrem Konto besuchen Sie bitte unseren Hilfebereich oder kontaktieren Sie unseren Support.

Wir danken Ihnen für Ihre Nutzung unserer Dienste und wünschen Ihnen einen erfolgreichen Tag.

Abbildung 7: Screenshots der Verbraucherzentrale NRW als Beispiel für Phishing-Mails (hier: MeinELSTER+-App für Steuererklärungen).

Phishing ist nach wie vor eine der effektivsten Methoden, um Daten abzugreifen und in Systeme einzudringen.

3.3 MALWARE

Malware wird noch immer zur Begehung einer Vielzahl von Cyberstraftaten genutzt und stellt somit auch 2024 eine anhaltende Bedrohung dar. Über die im vorherigen Kapitel beschriebenen Eintrittsvektoren gelangt Schadsoftware in das angegriffene Zielsystem, um dort ihre maliziösen Funktionen auszuführen.

Die Malware-Szene ist äußerst vielseitig. Die verschiedenen Malware-Varianten werden dabei über Plattformen und Foren in der Underground Economy und via Messenger-Diensten wie Telegram angeboten. Je nach Variante, Funktionsumfang und geplanter Dauer der Nutzung werden auch Abo-Modelle für den Erwerb von Malware angeboten.

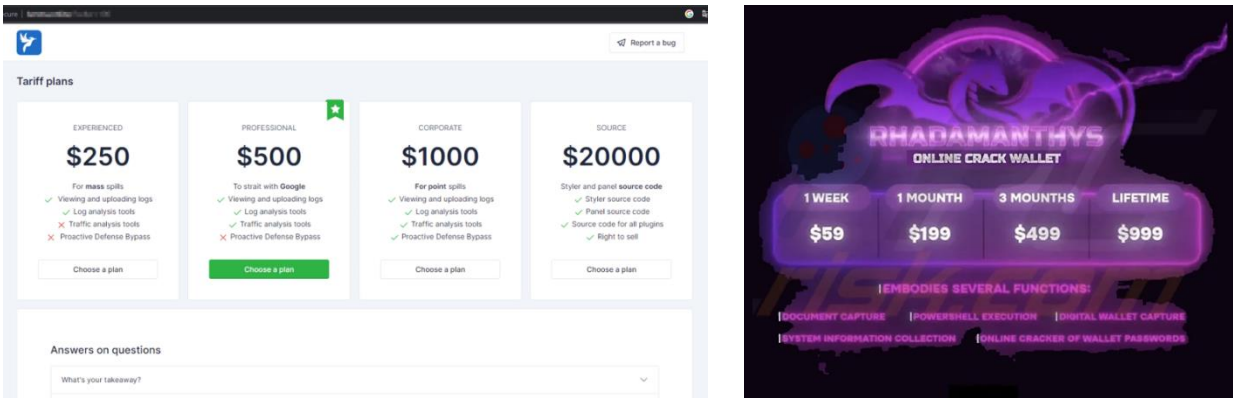


Abbildung 8: Angebote für die Malware-Varianten Lumma und Rhadamanthys.

Die jüngsten Entwicklungen im Bereich künstliche Intelligenz wirken sich auch auf den Bereich Malware aus. Bei einer Angriffskampagne mit vermeintlichen Rechnungen eines deutschen Unternehmens im April 2024 wurde ein vermutlich mittels KI geschriebenes Skript beobachtet, das den Rhadamanthys-Stealer nachlud. Auch OpenAI beobachtete, dass deren generative KI bereits in über 20 Fällen nachweislich zur Entwicklung und Ausbesserung von Malware-Code eingesetzt wurde. Wesentliche Fortschritte bei der Erstellung von Malware konnten bislang jedoch noch nicht verzeichnet werden.

Eine weitere herausragende Bedeutung für den Bereich Malware haben Loader bzw. Dropper. Diese können nach initialer Kompromittierung des Zielsystems weitere Schadsoftware nachladen und werden häufig im Vorfeld von Ransomware-Angriffen eingesetzt. Im Mai 2024 konnten im Ermittlungsverfahren Endgame weitreichende Erfolge bei der Bekämpfung der beschriebenen Loader bzw. Dropper erzielt werden.

KI erhöht das Gefährdungspotenzial von Malware noch weiter.

3.4 RANSOMWARE & DATA EXTORTION

Wie bereits in den Vorjahren blieben Ransomware-Angriffe auch 2024 eine der zentralen Bedrohungen im Bereich der Cyberkriminalität. Obwohl mit 950 Fällen ein Rückgang der angezeigten Fälle mit Verschlüsselungstrojanern im Vergleich zu 2023 (1.018 Fälle) verzeichnet wurde, blieb das Angriffsaufkommen auf einem hohen Niveau.[8]

950 Angriffe

wurden zur Anzeige gebracht.

Häufigste Ransomware-Varianten

1. LockBit
2. Phobos
3. MetaEncrypter
4. Akira
5. Fog
6. Qilin;
   MedusaLocker
8. Helldown
9. RansomHub
10. BlackBasta

Ca. **72 %**

aller Ransomware-Angriffe konnten dem Modus Operandi **Double Extortion** zugeordnet werden.

94 %

der Angriffe richteten sich gegen Unternehmen, Organisationen und Institutionen.

Über **80 %**

der Angriffe richteten sich gegen KMU.

Ca. **50 %**

der Angriffe zielten auf das **verarbeitende Gewerbe**, den **Handel** und das **Gesundheitswesen** ab.

Nur

9 % der Geschädigten zahlten Lösegeld.

Im Mittel wurden umgerechnet ca. **277.000 US-Dollar** gezahlt.

Abbildung 9: Kennzahlen zu Ransomware-Angriffen im Jahr 2024. Die Informationen basieren auf einer Erhebung des BKA in den Bundesländern.
Alle hier berichteten Zahlen der bundesweiten Fallerhebung berücksichtigen nur diejenigen Fälle, bei denen Informationen zu den jeweiligen Kategorien vorlagen. Fälle mit Angaben „unbekannt“ oder ohne Angaben wurden hier nicht berücksichtigt.

[8] Aufgrund geänderter Erfassungsmodalitäten in der bundesweiten Fallerhebung 2024 muss die im Bundeslagebild 2023 abgebildete Zahl auf nunmehr 1.018 Fälle angepasst werden.

Besonders im ersten und vierten Quartal 2024 konnten vermehrt Ransomware-Angriffe festgestellt werden, während um die Jahresmitte weniger Angriffe verzeichnet wurden.

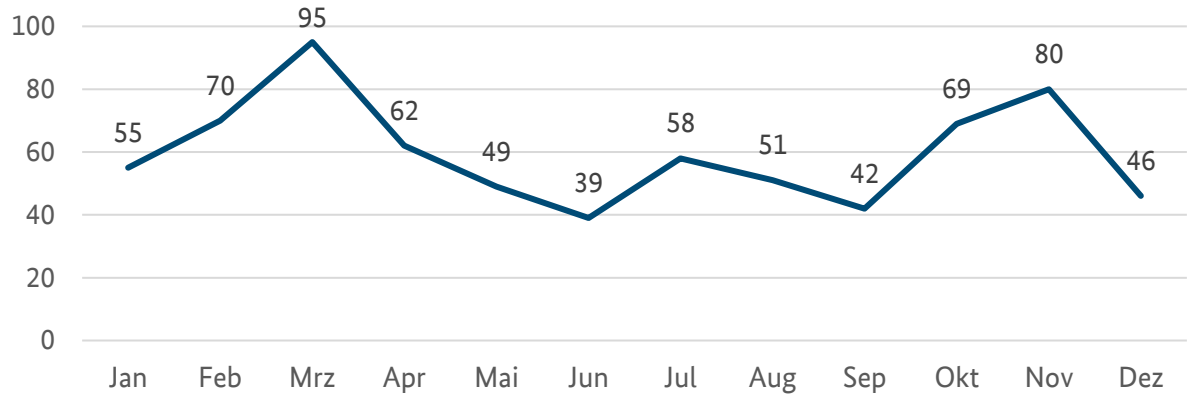


Abbildung 10: Bundesweite Erhebung polizeilich bekannt gewordener Ransomware-Angriffe im Jahr 2024. Die abgebildeten Daten umfassen ausschließlich das polizeiliche Hellfeld.

Eine Vielzahl an Ransomware-Akteuren nutzt sogenannte Dedicated Leak Sites (DLS) im Darknet. Diese Vorgehensweise wird sowohl für Double Extortion als auch für Data Extortion[9] angewandt. Eine für 2024 durchgeführte Analyse dieser Daten ergab 161 öffentlich auf DLS gelistete deutsche geschädigte Unternehmen.[10] Dies stellt im Vergleich zum Vorjahr zwar einen Rückgang dar (-16 %), der Wert liegt aber weiterhin über den Werten von 2021 und 2022.
Eine Analyse von eCrime.ch[11] zeigt, dass der weltweite Anstieg von Geschädigtenzahlen auf DLS unter anderem auch auf eine strategische Nennung von Geschädigten zurückzuführen ist, ohne dass es zu einer (erneuten) Verschlüsselung kam; etwa als Reaktion auf operative Maßnahmen. Das ist insbesondere beim Akteur LockBit der Fall.[12]
Weltweit konnten 56 neue DLS ausfindig gemacht werden. Zudem ist der Anteil an Ransomware-Akteuren, die verhältnismäßig wenig Angriffe durchführen, deutlich gestiegen (+17 %).[13]

Im internationalen Vergleich zeigt sich, dass Deutschland weiterhin das am vierthäufigsten betroffene Land weltweit ist.

[9] Erpressung mit zuvor exfiltrierten Daten ohne Verschlüsselung der Systeme.
[10] Stand 17.01.2025.
[11] Auf der Internetseite eCrime.ch werden Daten zu Unternehmen bereitgestellt, die Ziel von Data Extortion und Double Extortion Angriffen waren und öffentlich auf aktiven DLS erpresst werden.
[12] Chainalysis (2025). The 2025 Crypto Crime Report.
[13] ebd.

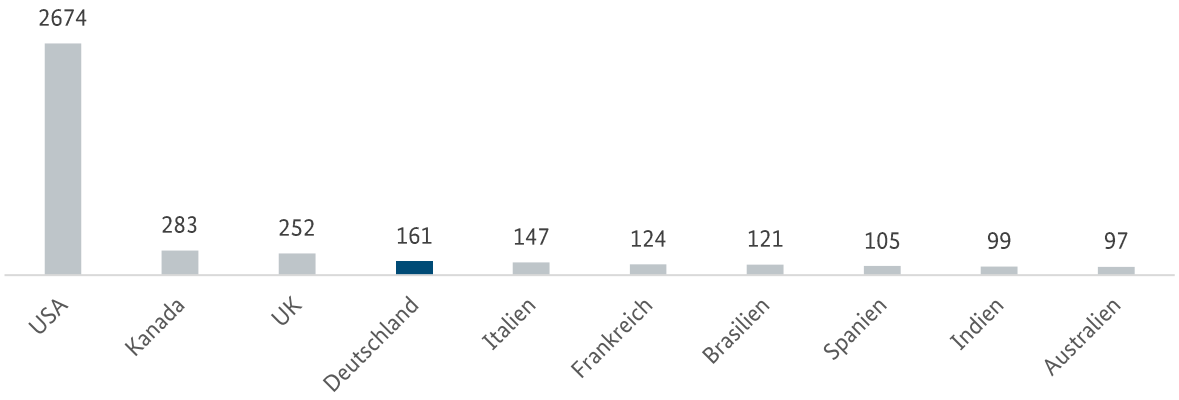


Abbildung 11: Anzahl Geschädigter nach DLS im Ländervergleich. Hierbei werden Leaks nach Double Extortion und Data Extortion berücksichtigt. Daten auf Basis von eCrime.ch (Stand 17.01.2025).

Die Modi Operandi Double Extortion und Data Extortion können mit KI-Unterstützung effizienter durchgeführt werden. So nutzen Ransomware-Akteure KI-Tools für gezielte Erpressungsversuche, indem ausgeleitete Daten aus einem kompromittierten System schneller strukturiert und präziser analysiert werden. Aber auch generative KI-Fähigkeiten werden von Ransomware-Akteuren missbraucht. So setzt beispielsweise die Ende 2024 aktiv gewordene Gruppierung FunkSec bei ihren Kommunikationsinhalten und vermutlich auch beim Coding auf KI-Unterstützung.[14]

Im Jahr 2024 kam Bewegung in die Ransomware-Szene. Zum einen führten polizeiliche Maßnahmen, die sich gezielt gegen Ransomware-Gruppierungen richteten, zu einem spürbaren Rückgang der Angriffe. Zum anderen trugen operative Maßnahmen gegen Cybercrime-as-a-Service-Angebote zu einem allgemeinen Einbruch der Fallzahlen bei und störten die Geschäfte der Ransomware-Akteure und ihr Vertrauensverhältnis untereinander erheblich.
Bislang wurde die Ransomware-Szene von einzelnen herausragenden Akteuren dominiert, aber einige dieser Gruppierungen lösten sich entweder auf oder ihre Aktivitäten wurden durch Takedown-Maßnahmen der Strafverfolgungsbehörden massiv eingeschränkt. Als Beispiele aus den letzten Jahren können hier REvil, DarkSide/BlackMatter oder Conti genannt werden, sowie seit Frühjahr 2024 LockBit. Zudem sorgten die Exit-Scams[15] von NoEscape Ende 2023 und BlackCat Anfang 2024 für weitere Verunsicherung in der Ransomware-Szene. Nachdem etablierte Akteure wie LockBit und BlackCat an Relevanz verloren haben, konnte in Deutschland bislang kein anderer Akteur das entstandene Vakuum füllen. Stattdessen verteilen sich die Angriffe auf verschiedene Akteure, die mit Angriffen gegen kleinere Unternehmen versuchen, weniger Aufmerksamkeit der Strafverfolgungsbehörden auf sich zu ziehen.

Ransomware bleibt die prägende Bedrohung im Cyberraum, jedoch werden bislang dominierende Ransomware-Akteure erfolgreich bekämpft.

[14] Checkpoint (2024). Research-Blog. Online abrufbar unter: **https://blog.checkpoint.com/research/meet-funksec-a-new-surprising-ransomware-group-powered-by-ai/**

[15] Exit-Scams bezeichnen eine Art von Betrug, bei der (Voraus-)Zahlungen für Dienstleistungen oder Waren geleistet werden, aber ohne Gegenleistung bleiben und die Täter mit dem Geld untertauchen.

Durchschnittlich gezahlte Lösegeldsumme: [a]

451.548 US-Dollar

Die Gesamtsumme der Lösegeldzahlungen ist 2024 gesunken.

Kriminelle Einnahmen:

> 800 Mio. US-Dollar

Festgestellte Lösegeldzahlungen auf Kryptowallets von Ransomware-Akteuren.[b]

a = Durchschnittlich festgestellte Lösegeldzahlung weltweit. Quelle: Coveware (2024). Quartalsberichte 2024. Online abrufbar unter https://www.coveware.com/blog
b = Einnahmen durch weltweite Ransomware-Angriffe. Quelle: Chainalysis (2025). The 2025 Crypto Crime Report.

Die veränderten Bedingungen hatten Auswirkungen auf die Einnahmen der Täter. Das Blockchain-Analyse-Unternehmen Chainalysis, welches jährlich die Summe aller Lösegeldtransaktionen auf Kryptowallets von Ransomware-Akteuren auswertet, stellte für 2024 im Vergleich zum Vorjahr einen starken Rückgang von 35 % fest. Die Gesamtsumme der durch Chainalysis festgestellten Lösegeldzahlungen sank wieder unter die Eine-Milliarde-Marke und betrug umgerechnet rund 814 Mio. US-Dollar, obwohl im ersten Halbjahr noch ein Anstieg an Lösegeldzahlungen festgestellt worden war. Maßgeblich beeinflusst wurde diese Entwicklung durch das vollständige Ausbleiben von Angriffen des Akteurs BlackCat sowie die deutlich gesunkenen Fallzahlen durch LockBit.

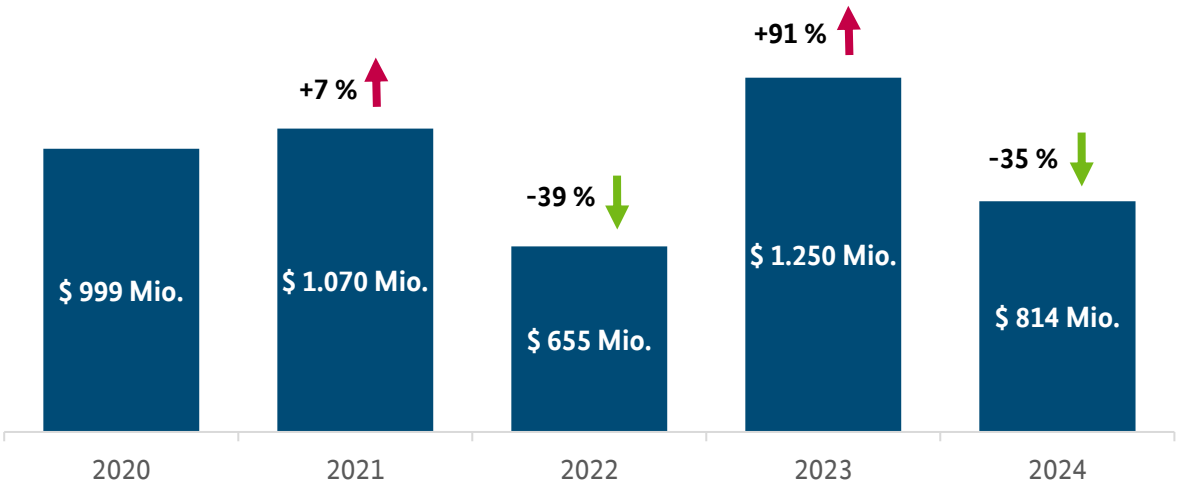


Abbildung 12: Weltweit festgestellte Lösegeldzahlungen auf Kryptowallets von Ransomware-Akteuren 2020 bis 2024. Die Daten unterliegen retrograden Anpassungen. Quelle: Chainalysis (2025). The 2025 Crypto Crime Report.

Die Zahlungsbereitschaft geschädigter Unternehmen sinkt weiter. Während weltweit zwar mehr Ransomware-Angriffe festgestellt werden konnten, wurden dabei weniger Lösegeldzahlungen verzeichnet. Nach Analysen des IT-Dienstleisters Coveware zahlten 2024 weltweit durchschnittlich 30 %

der angegriffenen Unternehmen Lösegelder[16], in der bundesweiten Fallerhebung gaben ca. 90 % der Geschädigten an, kein Lösegeld gezahlt zu haben.[17] Die Lösegeldzahlung bei Verschlüsselung scheint daher von vielen Geschädigten lediglich als letzte Möglichkeit genutzt zu werden, wenn die eigenen Daten nicht mehr anders wiederhergestellt werden können.
Die Zahlungsrate bei Data Extortion, bei denen es zu keiner Verschlüsselung kam, ist dagegen stabil geblieben.[18] Obwohl Ransomware-Angriffe 2024 mengenmäßig noch deutlich vor Data Extortion lagen, scheint sich ein Trend zu entwickeln, dass Verschlüsselungen zunehmend weniger lukrativ für die Täter werden.

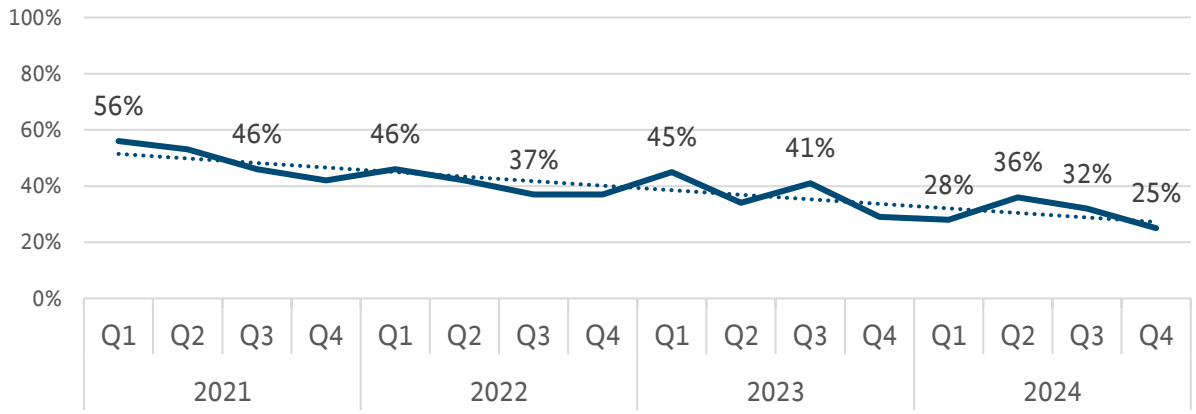


Abbildung 13: Anteil an Unternehmen, die nach einem Ransomware-Angriff Lösegeld gezahlt haben. Quelle: Coveware (2024 u. 2025). Quartalsberichte 2024.

Sowohl der Rückgang der Fallzahlen ab Mai als auch die gesunkenen Ransomware-Zahlungen machen den Erfolg der im Frühjahr stattgefundenen Strafverfolgungsmaßnahmen gegen Ransomware-Akteure sowie Malware-Varianten deutlich.

Die Eindämmung der Aktivitäten von Ransomware-Akteuren hat auch ein Sinken der illegalen Profite zur Folge.

[16] Coveware (2024 und 2025). Quartalsberichte 2024. Online abrufbar unter **https://www.coveware.com/blog**
[17] Angabe für Fälle, in denen eine Angabe zur Lösegeldzahlung gemacht wurde. N = 508.
[18] Chainalysis (2025). The 2025 Crypto Crime Report.

3.5 DISTRIBUTED DENIAL-OF-SERVICE

Auch 2024 ist der Bereich DDoS weiterhin von Kampagnen hacktivistischer Akteure geprägt. Im gesamten Berichtszeitraum konnten über 220 Angriffsankündigungen durch Hacktivisten gegen Ziele in Deutschland verzeichnet werden. 2023 erfolgten lediglich ca. 160 derartiger Ankündigungen. Ein signifikanter Anstieg an mutmaßlichen DDoS-Angriffen erfolgte vor allem gegen Ende des Jahres, als ein Zusammenschluss verschiedener hacktivistischer Akteure eine Kampagne gegen deutsche Ziele ausrief.

Die Täterschaft lässt sich primär in zwei Lager einordnen: pro-russisch oder anti-israelisch. Ihre Motivation begründet sich aus geopolitischen Konflikten, die spätestens seit 2022 vermehrt in den digitalen Raum übertragen werden. Akteure beider Lager referenzieren sich in ihren Telegram-Kanälen und unterstützen sich gegenseitig. Zumindest einen losen Zusammenschluss derartiger Akteure stellen laut IT-Dienstleistern wie Radware und Netscout die Kollektive High Society und 7 October Union dar.[19] Ab Mitte des Jahres proklamieren diese eine gemeinsame Zusammenarbeit unter der Bezeichnung Holy League.

Ziele der im Laufe des Jahres festgestellten Kampagnen waren primär öffentliche Einrichtungen und (Bundes-)Behörden. Ebenso waren Logistikdienstleister und Unternehmen des verarbeitenden Gewerbes unter den Zielen der mutmaßlich ausgeführten DDoS-Angriffe. Begleitet wurden die Angriffsankündigungen szenetypisch mit martialischen Botschaften und Propaganda.

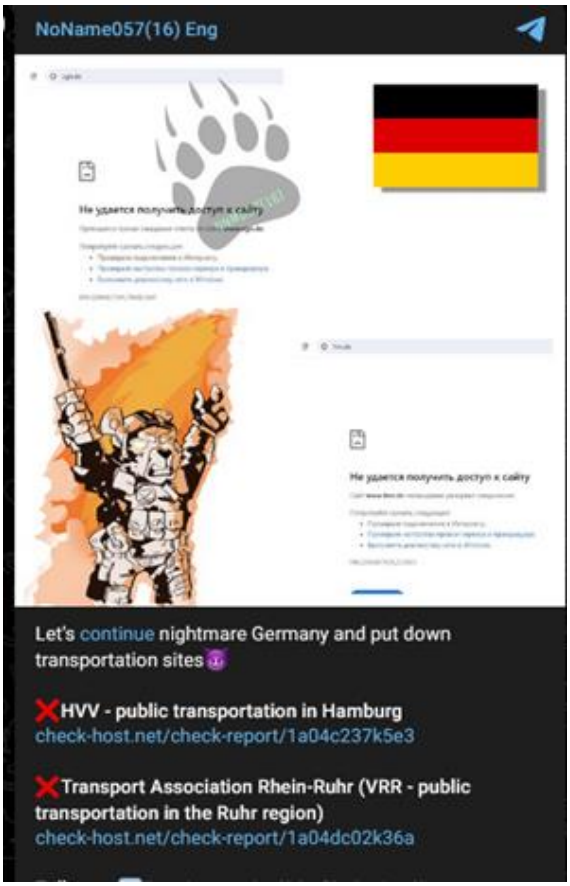


Abbildung 14: Post des pro-russischen Akteurs NoName057(16) auf Telegram.

[19] Radware (2024). Online abrufbar unter: **https://www.radware.com/security/threat-advisories-and-attack-reports/holy-league-a-unified-threat-against-western-nations/;** Netscout (2024). Online abrufbar unter: **https://www.netscout.com/blog/asert/ddos-attacks-spain**

Angriffsparameter 2024[a]

Ø 2.450 Angriffe pro Monat
Ø Bandbreite: 1.201 Mbit/s
Ø Dauer eines Angriffs: 48 Minuten

Häufigste Angriffsziele durch DDoS-Attacken 2024

- Behörden
- Öffentliche Verwaltungen
- Logistikdienstleister
- verarbeitendes Gewerbe

Mehr Hacktivismus

Über 200 Angriffsankündigungen auf Ziele in Deutschland via Telegram in 2024

Vernetzung der Szene

Hacktivistische Gruppierungen kooperieren und bilden neue Kollektive

Abbildung 15: Zahlen und Fakten zur DDoS-Lage 2024 in Deutschland.
a = Daten der Deutschen Telekom AG.

Neben einer gesteigerten Bedrohungslage durch hacktivistische Akteure ist generell ein Anstieg an DDoS-Angriffen zu verzeichnen. Nach Angaben der Deutschen Telekom AG (DTAG) konnten im Berichtsjahr 29.399 DDoS-Angriffe registriert werden. Dies stellt einen Anstieg von 30,7 % zum Vorjahr dar. 2024 wurde somit die bislang größte Anzahl an DDoS-Angriffen seit dem Jahr 2021 verzeichnet. Besonders auffällig ist hierbei das Frühjahr 2024, welches durch einen starken Anstieg der Fallzahlen geprägt ist. Neben den Fallzahlen sind laut DTAG auch die für die Angriffe verwendeten Bandbreiten und Paketraten gestiegen.

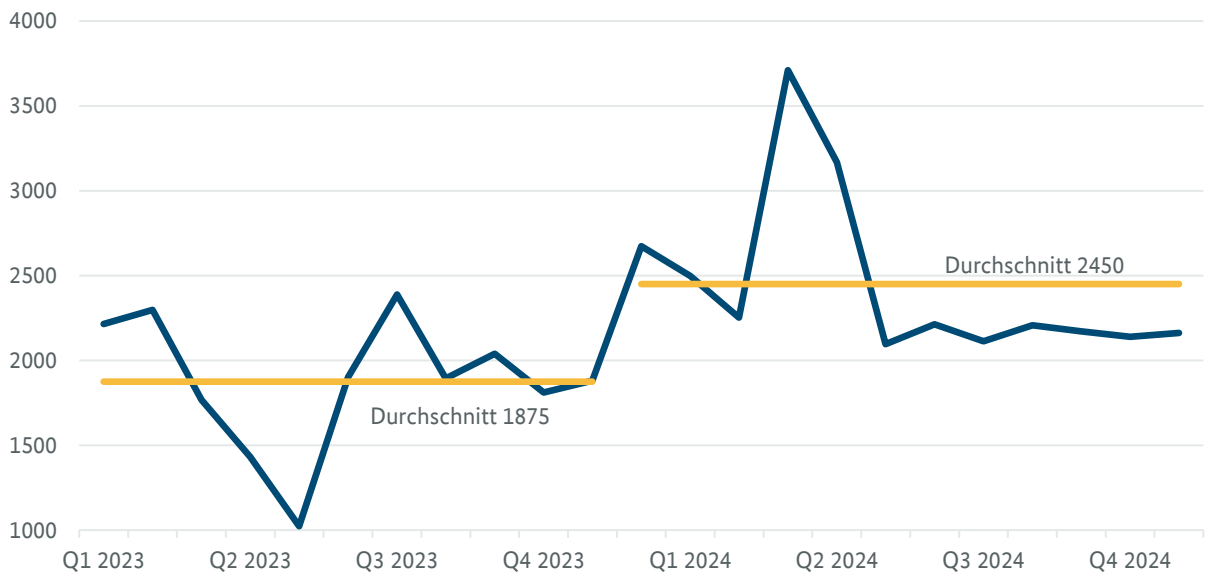


Abbildung 16: Anzahl an DDoS-Angriffen pro Monat in den Netzen der DTAG für die Jahre 2023 und 2024.

Die steigende Anzahl an DDoS-Angriffen spiegelt sich auch im gesamteuropäischen Raum wider. Nach Angaben des DDoS-Mitigationsdienstleisters Link11 ist die Anzahl an DDoS-Angriffen auf Ziele in Europa von 2023 auf 2024 um ca. 137 % gestiegen.[20] Der wachsenden Anzahl an DDoS-Angriffen sowie der erhöhten Bedrohungslage durch Hacktivisten wurden 2024 verschiedene polizeiliche Maßnahmen entgegengestellt.

Aktivitäten hacktivistischer Gruppierungen steigen an.

[20] Link11 (2025). European Cyber Report 2025.

4. Operative Erfolge

Der steigenden Bedrohungslage haben die Strafverfolgungsbehörden 2024 intensive Ermittlungsarbeiten und strafprozessuale Maßnahmen entgegengesetzt. Die Anzahl der operativen Maßnahmen nahm im Vergleich zu den Vorjahren weiter zu und setzte damit einen neuen Maßstab für die Bekämpfung der Cyberkriminalität.

Zielrichtung waren sämtliche Bereiche der Cyberkriminalität wie Marktplätze und Dienstleister der Underground Economy, Krypto-Exchange-Services, Stresser- und Crypting-Services sowie die Infrastruktur mehrerer Ransomware-Akteure. Die Vielzahl an verschiedenen Maßnahmen schränkte die Akteure nicht nur in ihren Mitteln und Tools ein, sondern konnte auch Misstrauen in (etablierten) Arbeits- und Vertrauensverhältnissen der Underground Economy erzeugen.

Auch wenn sich strafprozessuale Maßnahmen gegen Cyberkriminelle im Ausland aufgrund unterschiedlicher rechtlicher Rahmenbedingungen häufig besonderen Herausforderungen stellen müssen, wurde durch die teilweise mit internationaler Beteiligung durchgeführten erfolgreichen Einsätze 2024 deutlich, dass der digitale Raum nicht rechtsfrei ist. Um diese Tatsache auch gegenüber der Täterseite zu verdeutlichen, wurden im Rahmen der OP Endgame Tatverdächtige erstmals gezielt mit Videos im Netz angesprochen. Ziel dabei war es auch, Druck auf die Täter sowie auf mögliche Affiliates auszuüben, indem Informationen zu ihren mutmaßlichen Identitäten und Aufenthaltsorten veröffentlicht wurden.

2024 war das Jahr zahlreicher Ermittlungserfolge.

Durch Abschaltung der größten deutschsprachigen illegalen Marktplätze wurde der Onlinehandel mit inkriminierten Waren und Dienstleistungen erheblich eingegrenzt. Gerade der überwiegend auf Deutsch kommunizierenden Täterschaft fehlt dadurch eine wichtige Grundlage für Folgestraftaten im Bereich CCieS.

Durch Maßnahmen gegen die technische Infrastruktur von cyberkriminellen Dienstleistungen wie Marktplätze, Malware-Varianten oder Exchange-Services, wurden Cybertätern wichtige Bausteine ihrer Aktivitäten entzogen. Der Wiederaufbau dieser Dienstleistungen dauert häufig mehrere Monate und bindet erhebliche Ressourcen. Maßnahmen der Strafverfolgungsbehörden, die sich zusätzlich gegen die entsprechende kriminelle finanzielle Infrastruktur richten, verzögern diesen weiter. Und auch wenn diese Dienstleistungen nach gewisser Zeit wieder angeboten werden, stellen sie häufig nicht mehr dasselbe Bedrohungspotential dar wie vor den Maßnahmen: Wichtige Ressourcen sind nicht mehr zugänglich und Kunden sowie Affiliates verlieren Vertrauen in die Sicherheit und Zuverlässigkeit der angebotenen illegalen Services und dahinterstehender Anbieter. Unter anderem bestehen Zweifel hinsichtlich der Authentizität von Marktplatzbetreibern und die Befürchtung, dass sich hinter den vermeintlichen Dienstleistungsanbietern Strafverfolgungsbehörden verbergen könnten.

Der in Kapitel 3.4 dargestellte Einbruch der Ransomware-Fallzahlen zwischen Mai und September 2024 geht u. a. auf die Kombination aus den Nachwirkungen der Operation Cronos gegen die führende Ransomware-Gruppierung LockBit und der Operation Endgame gegen Dropper zurück. Ransomware-Akteure, die einen oder mehrere der betroffenen Dropper nutzten, mussten teilweise auf mühsame Methoden zur Primärinfektion umsteigen, wodurch das Geschäftsmodell insgesamt weniger lukrativ wurde.

Im Folgenden werden die relevantesten Ermittlungserfolge 2024 dargestellt:

Februar: Takedown Crimemarket

Ende Februar fanden unter der Leitung der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) operative Maßnahmen des PP Düsseldorf gegen die zu diesem Zeitpunkt größte deutschsprachige kriminelle Handelsplattform im Internet, Crimemarket, statt. Im Zuge der Maßnahmen wurden bundesweit mehr als 100 Durchsuchungen durchgeführt und mehrere Personen festgenommen. Es konnten u. a. Rauschgift und Vermögen in Höhe von 600.000 Euro beschlagnahmt werden. Zudem wurde auf der Plattform ein Seizure Banner geschaltet.

Die Plattform war über das Clear Web mittels gängiger Suchmaschinen zu erreichen. Es wurden neben Betäubungsmitteln und Waffen auch digitale Güter gehandelt sowie Cybercrime-as-a-Service-Angebote vermarktet, darunter auch Informationen und Tutorials zu einem einfachen Einstieg in die Cyberkriminalität, z. B. in Form von Anleitungen zur Verschlüsselung von IT-Systemen. Crimemarket zählte zuletzt rund 180.000 Nutzer.

Februar: Operation Cronos

Mitte Februar 2024 beschlagnahmten Strafverfolgungs- und Justizbehörden aus zehn Ländern sowie Europol und Eurojust unter Federführung der britischen National Crime Agency (NCA) im Rahmen einer international koordinierten Aktion einen Teil der technischen Infrastruktur der Ransomware-Gruppierung LockBit.

Der Fokus der operativen Maßnahmen lag auf der Beschlagnahme von 34 Servern in den Niederlanden, Deutschland, Finnland, Frankreich, der Schweiz, Australien, den USA sowie Großbritannien. Bei einem der Server handelte es sich um den Hosting-Server der Dedicated Leak Site der Gruppierung. Später wurde die DLS mit einem Seizure Banner versehen. Ebenfalls konnten das Admin-Panel sowie die für die Weiterleitung der exfiltrierten Geschädigtendaten genutzte

Infrastruktur übernommen, über 200 Accounts bei Kryptowährungsdienstleistern eingefroren und 14.000 Accounts, die im Zusammenhang mit der Exfiltration der Daten stehen, gelöscht werden.

Auf der übernommenen Leak Site wurden anschließend polizeiliche Erkenntnisse zur Auswertung der Server und gesicherten Accounts, Informationen zur Identität einer führenden Person hinter der Ransomware sowie die Anzahl erfolgreich dekryptierter Unternehmen und Maßnahmen veröffentlicht.

In der Folge war ein enormer Rückgang der Aktivitäten feststellbar, was auf ein massiv geschädigtes Vertrauen der Szene in die Gruppierung schließen lässt.

März: Takedown Nemesis Market

Im März stellte das BKA unter Sachleitung der Generalstaatsanwaltschaft (GenStA) Frankfurt am Main die in Litauen und Deutschland befindliche Server-Infrastruktur des weltweit agierenden kriminellen Darknet-Marktplatzes Nemesis Market sicher und schaltete die Plattform damit ab.

Auf der 2021 gegründeten Plattform, bei der es sich um den weltweit drittgrößten Darknet-Marktplatz handelte, waren zuletzt über 150.000 Nutzer- und über 1.100 Verkäuferkonten registriert, davon eine sehr große Anzahl aus Deutschland. Das Angebot auf Nemesis Market umfasste Betäubungsmittel, betrügerisch erlangte Daten und Waren sowie eine Auswahl an Dienstleistungen der Cybercrime wie Ransomware, Phishing oder DDoS-Services. Neben der Abschaltung der Infrastruktur beschlagnahmte das BKA Vermögenswerte in Höhe von über 94.000 Euro in Form von Kryptowährungen. Den Maßnahmen sind Ermittlungen des BKA sowie des FBI und weiteren internationalen Behörden vorausgegangen, sie fanden in enger Abstimmung zwischen deutschen, amerikanischen und litauischen Strafverfolgungsbehörden statt.

April: Takedown AegisTools.pw

Im April 2024 schalteten die Landeszentralstelle Cybercrime (LZC) Rheinland-Pfalz und das BKA unter Sachleitung der GenStA Koblenz den illegalen Online-Dienst AegisTools.pw ab und führten operative Maßnahmen gegen einen Verdächtigen in Rheinland-Pfalz durch.

AegisTools.pw war eine seit 2020 bekannte Plattform der Underground-Economy, die unter anderem Software zur illegalen Beschaffung von Benutzerpasswörtern sowie Crypting- und Counter-Anti-Virus-Services und damit zwei entscheidende Elemente des Cybercrime-as-a-Service-Modells anbot.

Eine Registrierung war für die Nutzung von AegisTools.pw nicht erforderlich, was eine nahezu anonyme Verwendung ermöglichte. Die Auswertung der täterseitigen Infrastruktur ergab, dass die Plattform global von über 1.000 Nutzern für cyberkriminelle Zwecke genutzt wurde, wobei alle Transaktionen in Kryptowährungen abgewickelt wurden.

Mai: Operation Endgame

Ende Mai initiierte und koordinierte das BKA mit der Operation Endgame unter Sachleitung der GenStA Frankfurt am Main – Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) die bislang größte weltweite internationale Polizeioperation gegenCCieS.

Im Rahmen einer internationalen Action-Week nahm das BKA zusammen mit Strafverfolgungsbehörden aus den Niederlanden, Frankreich, Dänemark, Großbritannien sowie den USA, Europol und Eurojust die sechs einflussreichsten Loader und Dropper (IcedID, SystemBC, Bumblebee, Smokeloader, Pikabot, Trickbot) vom Netz. Die Schadsoftware-Varianten wurden als Tools zur Erstinfektion genutzt und dienten Cyberkriminellen als Türöffner, um unbemerkt Opfersysteme zu infizieren. Unter anderem standen sie in Verbindung mit über 15 Ransomware-Varianten.

Die Maßnahmen richteten sich hierbei nicht nur gegen die technische Infrastruktur, sondern auch gegen kriminelle Akteure und in Teilen gegen die täterseitige finanzielle Infrastruktur.

So wurden im Verlauf der personenbezogenen Maßnahmen zehn Haftbefehle erlassen sowie vier vorläufige Festnahmen und 16 Durchsuchungen im europäischen Ausland durchgeführt. Außerdem wurden ein Vermögensarrest in Höhe von 69 Mio. Euro erwirkt und mehr als 70 Mio. Euro Kryptovermögen gesperrt.

Juni: Operation Morpheus

Ende Juni wurde die bei Europol seit 2021 geführte OP Morpheus in die offene Phase überführt. Ziel war es, den kriminellen Einsatz der Pentesting-Software Cobalt Strike zu verhindern/zu erschweren. Durch die Zusammenarbeit mit diversen privaten Unternehmen und Behörden konnten 690 illegal

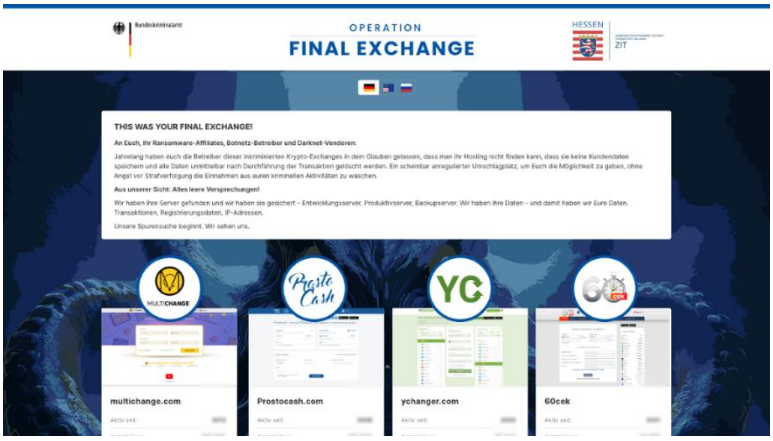
genutzte Server aus 27 Ländern identifiziert und 600 abgeschaltet werden, fünf der Server wurden in Deutschland lokalisiert und gesichert.

August: Takedown Radar/Dispossessor

Mitte August führte das Bayerische LKA unter Sachleitung der GenStA Bamberg im Rahmen einer international abgestimmten Aktion mit dem FBI Maßnahmen gegen die Ransomware-Gruppierung Radar/Dispossessor durch.

Zwölf Tatverdächtige der seit 2023 bestehenden Gruppierung wurden identifiziert, 17 Server in Deutschland, drei in Großbritannien und fünf in den USA sowie acht kriminell genutzte Domains beschlagnahmt und vom Netz genommen. Durch die Ermittlungen konnten weltweit 43 weitere geschädigte Unternehmen identifiziert werden.

September: Operation Final Exchange



Ende September schaltete das BKA unter Sachleitung der GenStA Frankfurt am Main im Rahmen der Operation Final Exchange 47 Handelsplattformen für Kryptowährungen ab. Im Zuge der Maßnahmen wurde sowohl die Infrastruktur der Plattformen beschlagnahmt - mehr als 140 Server - sowie dazugehörige Domains gesperrt.

Gegen die Betreiber der Exchange Services besteht der Verdacht, durch mangelhafte Umsetzung von gesetzlichen Vorgaben zur Geldwäschebekämpfung die Herkunft kriminell erlangter Gelder bewusst verschleiert und sich der Geldwäsche und dem Betreiben krimineller Handelsplattformen strafbar gemacht zu haben. Die zugrundeliegenden Plattformen waren insbesondere für Cyberkriminelle aus Ransomware-Gruppierungen oder Botnetzbetreiber attraktiv, um Lösegelder oder andere Taterträge durch anonyme Finanztransaktionen zu waschen.

November: Operation Magnus

Anfang November wurde im Rahmen einer von Eurojust koordinierten internationalen Polizeioperation die Infrastruktur der Infostealer Redline und Meta Stealer vom Netz genommen. Der von den niederländischen Strafverfolgungsbehörden initiierte Takedown von 17 Servern in Deutschland wurde vom BKA koordiniert. Im Rahmen des Verfahrens wurden eine Person in Belgien festgenommen und weitere Personen in den USA angeklagt. Die Telegramgruppen von Redline und Meta wurden von den Strafverfolgungsbehörden übernommen und mit entsprechenden Posts belegt, die an die Betreiber und Affiliates der Stealer adressiert waren.

November: Operation PowerOff

Von Oktober bis Dezember erfolgten im Rahmen der international koordinierten Operation „Power Off“ operative Maßnahmen durch das hessische LKA (HLKA) sowie das BKA unter Sachleitung der GenStA Frankfurt am Main gegen mehrere DDoS-Plattformen der Underground Economy.

Im Zuge der Maßnahmen wurden sieben Objekte in Deutschland durchsucht. Dabei wurden im Rahmen des vom HLKA geführten Verfahrens zwei Administratoren der Plattformen in Deutschland festgenommen. Weiterhin wurden umfangreiche IT-Infrastrukturen sichergestellt. Den Beschuldigten wird vorgeworfen, mehrere Plattformen bereitgestellt zu haben, die sowohl zur Computersabotage mittels DDoS-Angriffen als auch zum Handel mit Betäubungsmitteln genutzt wurden.

Dstat.CC

Bei Dstat.CC handelte es sich um eine in der Underground Economy zentrale Plattform, die mittels einer umfassenden Auflistung und Bewertung von Stresser-Diensten das einfache Ausführen von DDoS-Angriffen ermöglichte. Kunden der Plattform benötigten kein tiefergehendes technischen Wissen, um DDoS-Angriffe auf Webpräsenzen ihrer Wahl auszuführen. Durch die einfache Nutzung stellte Dstat.CC seine Dienste einem breiten Nutzerkreis zur Verfügung.

Die durchgeführten Maßnahmen gegen Stresser-Dienste und Dstat.CC sind Teil der bereits seit 2018 andauernden internationalen Operation „Power Off“, an der verschiedene Strafverfolgungsbehörden aus den USA und Europa beteiligt sind. Unter anderem erfolgten 2019 Maßnahmen gegen die Plattform webstresser.org und 2022 gegen 50 weitere DDoS-Dienste.

Relevanz Stresser-Dienste

DDoS-Angriffe und Stresser-Dienste gewinnen seit Jahren zunehmend an Relevanz. Spätestens ab dem Beginn des russischen Angriffskrieges auf die Ukraine und den Aktivitäten pro-russischer Hacktivisten sind DDoS-Angriffe eine ständige Bedrohung im Cyberraum.

Dezember: Takedown von Crimenetwork

Anfang Dezember erfolgten polizeiliche Maßnahmen gegen die kriminelle Plattform Crimenetwork und deren technischen Administrator durch das BKA unter Sachleitung der GenStA Frankfurt am Main – Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT). Dabei konnten der Beschuldigte

festgenommen, die Serverinfrastruktur der Plattform abgeschaltet und Vermögenswerte in Höhe von mehr als einer Million Euro sichergestellt werden. Crimenetwork war zu diesem Zeitpunkt mit ca. 100.000 Nutzern und über 180 Verkäufern der größte deutschsprachige Marktplatz für illegale Dienstleistungen und Waren.

Im Rahmen der Presse- und Öffentlichkeitsarbeit wurde die Plattform auf die eigens gestaltete Landingpage (https://bustedcrime.network/) umgeleitet. Die Maßnahmen wurden außerdem mit einem Video flankiert, welches sich an die Betreiber und Nutzer der Plattform richtet und auf fortlaufende Auswertungen verweist. Auf der Onion-Domain von Crimenetwork erschien nach der erfolgreichen Übernahme ein Seizure Banner als Hinweismeldung.

Dezember: Durchsuchung bei einem Anonymous-Mitglied

Anfang Dezember führten die Staatsanwaltschaft Berlin und das BKA Durchsuchungsmaßnahmen bei einem 29-jährigen deutschen Staatsangehörigen in NRW durch. Der Beschuldigte soll über mehrere Jahre hinweg Cyber-Straftaten im Namen des Anonymous-Kollektivs verübt und u. a. einen Betreiber kritischer Infrastruktur angegriffen haben. Die Straftaten des Beschuldigten führten in mehreren Fällen zu großer medialer Resonanz.

Die Taten wurden durch das Anonymous-Kollektiv auf der Webseite anonleaks.net veröffentlicht, um eine hohe öffentliche Aufmerksamkeit zu generieren. Die Seite soll durch den Beschuldigten sowie zwei weitere Personen betrieben worden sein. Bereits Ende 2022 und Anfang 2024 war bei diesen Beschuldigten durchsucht worden. Sie hatten die Straftaten des Kollektivs über die Webseite anonleaks.net und andere Social-Media-Kanäle öffentlichkeitswirksam vermarktet.

5. Quo vadis, Cybercrime?

Seit Jahren ist eine zunehmende Dynamik im Phänomenbereich Cybercrime festzustellen: Die Tatgelegenheiten steigen in Folge von zunehmend digitaler Vernetzung, die Eintrittsschwellen sinken über Cybercrime-as-a-Service-Angebote in der Underground Economy, neue KI-Möglichkeiten und nicht zuletzt die geopolitischen Entwicklungen der letzten Jahre haben sich als erheblicher Treiber für Cyberdelikte erwiesen. Insbesondere die nicht aufzuhaltende Entwicklung nahezu aller Lebensbereiche hin „zum Digitalen“ bedeutet aber nicht nur mehr Tatgelegenheiten, sondern vor allem auch eine deutlich höhere Verwundbarkeit wesentlicher Elemente des öffentlichen bzw. gesellschaftliche Lebens. All das führt zu einer quantitativ wie qualitativ gestiegenen Bedrohungslage im Cyberraum, die sich mit Blick auf die teils hohe Professionalität der Tätergruppierungen nur teilweise im Hellfeld der PKS abbildet.

Aufgrund seiner Rolle als NATO-Mitglied, EU-Schlüsselstaat sowie maßgeblicher finanzieller und materieller Unterstützer der Ukraine steht Deutschland zunehmend im Zielspektrum aggressiver, hybrider Angriffskampagnen, die u. a. die Schwächung und Destabilisierung von Staat, Gesellschaft und Wirtschaft zum Ziel haben. Im Cyberraum äußert sich die hybride Bedrohung[21] z. B. in häufigen DDoS-Kampagnen von Hacktivisten, Phishing-Kampagnen durch mutmaßlich staatliche Akteure sowie andauernden Angriffen einschlägiger Ransomware-Akteure. Hierbei verschwimmen die Grenzen zwischen finanzieller und politischer Motivation zusehends. Unabhängig von den zugrundeliegenden Motivationen nutzen Cyberakteure für ihre Angriffe oftmals dieselben technischen Werkzeuge und z. T. auch dieselben Infrastrukturen.

Die Bedeutung von Cybersicherheit in Deutschland ist spätestens mit Beginn des Angriffskrieges gegen die Ukraine noch viel mehr in den Fokus der Öffentlichkeit gerückt. Die ordnungsgemäße Funktion technischer Einrichtungen in der Wirtschaft, bei kritischen Infrastrukturen und der öffentlichen Verwaltung sind essentiell für das Funktionieren unseres Gemeinwesens. Cybersicherheit erschöpft sich hierbei allerdings nicht allein in einer möglichst umfassenden technischen Sicherung eigener IT-Systeme, sondern erfordert bei bereits bestehenden Bedrohungslagen konkrete Maßnahmen der polizeilichen Gefahrenabwehr sowie im Falle bereits erfolgter Cyberangriffe auch Maßnahmen der Strafverfolgung, um technische und finanzielle Ressourcen zur Begehung dieser Straftaten nachhaltig zu stören und zur Verunsicherung der Täterseite beizutragen.

Aktive Cybersicherheit - Technische Sicherungsmaßnahmen zum Schutz der Systeme müssen durch gefahrenabwehrende und strafverfolgende Maßnahmen ergänzt werden.

Da insbesondere professionelle Tätergruppierungen häufig aus sog. Safe Havens heraus agieren, also Staaten, die nicht oder nur sehr schlecht mit westlichen Strafverfolgungsbehörden zusammenarbeiten, läuft der klassisch personenbezogene Bekämpfungsansatz alleine vielfach ins Leere. Die personenbezogenen Ermittlungen müssen daher zwingend mit einem koordinierten Vorgehen gegen kriminelle technische Infrastrukturen (sog. Infrastrukturansatz) und dem Entzug finanzieller Mittel (sog. Finanzansatz) kombiniert werden. Ergänzt werden diese Maßnahmen durch die öffentliche Benennung,

[21] Der Begriff hybride Bedrohungen beschreibt eine Mischung konventioneller und nicht-konventioneller Mittel im gesamten zivilen und militärischen Spektrum, um (meist) unter Verschleierung der eigenen Urheberschaft das gesamtgesellschaftliche und politische Gefüge eines anderen Staates nachhaltig zu stören. Quelle: Bundesamt für Verfassungsschutz.

und „szenetypische“ Ansprache sowie öffentlichkeitswirksame Fahndung oder Sanktionierung identifizierter Cyberkrimineller (sog. Disruptive Kommunikation). In Kombination all dieser Werkzeuge kann den Angriffskampagnen von Tätern ein darauf abgestimmter, hybrider Bekämpfungsansatz als Mittel der aktiven Cybersicherheit entgegengestellt werden.

Ein derartiges Vorgehen ist allerdings nur mit vereinten (internationalen) Kräften permanent zu gewährleisten. Die Täterschaft agiert international und ihre inkriminierte Infrastruktur ist oftmals weltweit verteilt. Aus diesem Grund ist gerade die internationale Zusammenarbeit bei der Bekämpfung der Cybercrime unverzichtbar.

Die dargestellten Bedrohungen und steigenden Kennzahlen verdeutlichen die Notwendigkeit dieses hybriden Bekämpfungsansatzes, der mit einer hohen Taktung und großen Bandbreite unterschiedlicher internationaler polizeilicher Maßnahmen die Handlungsfähigkeiten von Cyberkriminellen einschränkt. Die dargestellten operativen Erfolge gegen die Underground Economy verdeutlichen die Effektivität des Ansatzes und seinen Einfluss auf die Täterseite.

Operative Maßnahmen müssen der steigenden Anzahl von Angriffen und der zunehmenden Vernetzung der Cyberakteure in hoher Frequenz entgegengesetzt werden.

Für die nachhaltige Bekämpfung der internationalen cyberkriminellen Szene ist auch die Kooperation zwischen Privatwirtschaft und Strafverfolgungsbehörden weiterhin von besonderer Bedeutung. Die Ergebnisse der Operation Endgame zeigen eindrucksvoll, dass durch die Bündelung der Erkenntnisse und Fähigkeiten von Sicherheitsbehörden und Privatwirtschaft selbst große Bedrohungen effektiv bekämpft werden können. Diese Synergieeffekte müssen auch zukünftig erhalten und weiter ausgebaut werden.

Die stetigen Fortentwicklungen im Bereich der künstlichen Intelligenz kamen 2024 besonders zum Tragen. Seit Veröffentlichung des ersten ChatGPT-Modells im November 2023 wurden inzwischen zahlreiche generative KI-Modelle (weiter-)entwickelt, die nicht nur Wort und Schrift, sondern auch Bild, Ton und Video generieren und verarbeiten können. Auch viele kriminelle Akteure ergänzen bereits ihr bisheriges Repertoire durch generative KI. Im Bereich Cybercrime sind davon vorwiegend die Phänomene Phishing und Malwareentwicklung betroffen. Da KI-Modelle für jegliche Bedarfe kontinuierlich weiterentwickelt werden, ist für das Jahr 2025 eine weitere Verschärfung KI-unterstützer Straftaten zu erwarten. Dabei gilt gerade für den Bereich CCieS: Auch wenn KI bestehende Modi Operandi bislang nicht revolutioniert hat, kann sie Cyberangriffe nicht nur professioneller gestalten, sondern durch Automatisierung auch schneller ein breiteres Ausmaß und folglich eine höhere Kritikalität von Cyberdelikten erreichen.

Zunehmende geopolitische Spannungen und kriminelle Nutzung von KI: Die Bedrohungslage wird 2025 weiter ansteigen.

Wesentlich für die Entwicklungen der Cybercrime in den nächsten Jahren wird auch die geopolitische Lage sein, die sich seit Beginn des Angriffskrieges gegen die Ukraine massiv verändert hat. Insbesondere der Bereich der politisch motivierten Cybercrime ist aufgrund der dahinterstehenden Professionalität dazu geeignet, als gefahrenverstärkender Katalysator im Bereich Cybercrime zu wirken. Auf der

Bekämpfung dieser Phänomenausprägung muss auch in Deutschland künftig ein wesentlich stärkerer Fokus liegen.

Mit Blick auf die gestiegene Bedrohungslage gilt es zur Gewährleistung der Cybersicherheit in Deutschland, dem Agieren der Tätergruppierungen neben der Stärkung der passiven Sicherheit von Systemen auch ein noch proaktiveres Vorgehen der Polizeibehörden als Maßnahme der aktiven Cybersicherheit entgegenzustellen.

Hierfür ist es erforderlich, die bestehenden Fähigkeiten dieser Behörden weiter zu entwickeln und sie so dabei zu unterstützen, ihre Maßnahmen zur erfolgreichen Bekämpfung von Cybercrime fortsetzen und insbesondere intensivieren zu können.

Impressum

Herausgeber
Bundeskriminalamt, 65173 Wiesbaden

Stand
Mai 2025

Gestaltung
Bundeskriminalamt, 65173 Wiesbaden

Bildnachweis
Bundeskriminalamt

Weitere Lagebilder des Bundeskriminalamtes zum Herunterladen finden Sie ebenfalls unter:
www.bka.de/Lagebilder

Diese Publikation wird vom Bundeskriminalamt im Rahmen der Öffentlichkeitsarbeit herausgegeben.
Die Publikation wird kostenlos zur Verfügung gestellt und ist nicht zum Verkauf bestimmt.