Bundeskriminalamt

BKA

Cybercrime

Bundeslagebild 2023

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 Strafverfolgungsaktivitäten ab.

Schwerpunkt des Bundeslagebildes Cybercrime sind die Delikte, die sich gegen das Internet und informationstechnische Systeme richten die 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 werden daher nicht der CCieS zugeordnet und bleiben bei den Betrachtungen im Bundeslagebild Cybercrime weitestgehend unberücksichtigt.

Grundlage für den statistischen Teil des Lagebildes sind die Daten der Polizeilichen Kriminalstatistik (PKS) Da ein Großteil der Straftaten der CCieS aus dem Ausland heraus ausgeführt wird oder der Aufenthaltsort der Täter unbekannt ist, benötigt es zur ganzheitlicheren Beschreibung des Phänomens der Darstellung der sogenannten Auslandstaten, die bislang in der PKS nicht berücksichtigt wurden Seit dem 01 01 2020 erfolgt im Rahmen eines Pilotverfahrens eine separate Erfassung dieser Auslandstaten, ab 2025 ist eine Veröffentlichung im Rahmen der PKS vorgesehen Davon umfasst sind Straftaten, bei denen zwar Schäden in Deutschland verursacht werden, aber der Aufenthaltsort des Täters im Ausland liegt oder 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 werden, können aus den statistischen Grunddaten der PKS nicht abgeleitet werden. Im Bereich der Cyberkriminalität ist das Dunkelfeld weit überdurchschnittlich ausgeprägt, so dass es für eine quantitativ und qualitativ zutreffende Lagebeschreibung von besonderer Bedeutung ist, polizeiexterne Erkenntnisse in die Lagebilderstellung 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 2023 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.

Inhaltsverzeichnis

1. Cybercrime

Polizeiliche Maßnahmen schwächen zunehmend die globale Infrastruktur der Cybertäter.

Die Aufklärungsquote ist bei den Cybercrime Delikten mit 32% leicht angestiegen.

Den leicht rückläufigen Cyberstraftaten in der Inlands PKS steht ein stärkerer Anstieg der Auslandstaten* gegenüber

Über 800 Unternehmen und Institutionen haben Ransomware-Angriffe zur Anzeige gebracht.

Die weltweiten Ransomware-Zahlungen steigen auf über 1 Mrd. US-Dollar.

DDoS Angriffe sind das "Mittel der Wahl" hacktivistischer Gruppierungen

Einzelne Software-Schwachstellen wurden für massive Angriffskampagnen ausgenutzt.

Die vom Bitkom e.V. bezifferten Schäden in Deutschland belaufen sich auf 205,9 Mrd. Euro - 72% davon entstanden direkt durch Cyberangriffe.

** Dabei handelt es sich um Taten, bei denen der Aufenthaltsort des Täters im Ausland liegt oder unbekannt ist, aber der Schadenseintritt in Deutschland erfolgte.*

1.1 BEDROHUNGSLAGE

Die Ziele von cyberkriminellen Akteuren sind äußerst vielfältig. Neben finanzstarken Unternehmen standen auch Einrichtungen und Institutionen mit hoher Öffentlichkeitswirksamkeit im Fokus. Aber auch leicht verwundbare kleine und mittelständische Unternehmen waren aufgrund des opportunistischen Vorgehens der Täter stark betroffen

Die täterseitigen Aktivitäten konzentrierten sich 2023 auf Frühjahr und Herbst, während sie in den Sommermonaten abflachten und dem jährlichen Trend einer „Sommerpause“ folgten Insgesamt war die hohe Bedrohungslage für das Jahr 2023 geprägt von hacktivistischen[1] DDoS-Kampagnen und einer Vielzahl an Ransomware-Angriffen, die teils weitreichende Auswirkungen auf IT-Supply-Chains (dt. IT-Lieferketten) hatten Dabei konnten sowohl Aktivitäten etablierter Täter als auch neue Gruppierungen und Rebrandings festgestellt werden

Der Underground Economy als Gesamtheit krimineller Plattformen und Marktplätze kommt eine besondere Bedeutung zu. Detaillierte Informationen hierzu können über den abgebildeten QR-Code abgerufen werden.

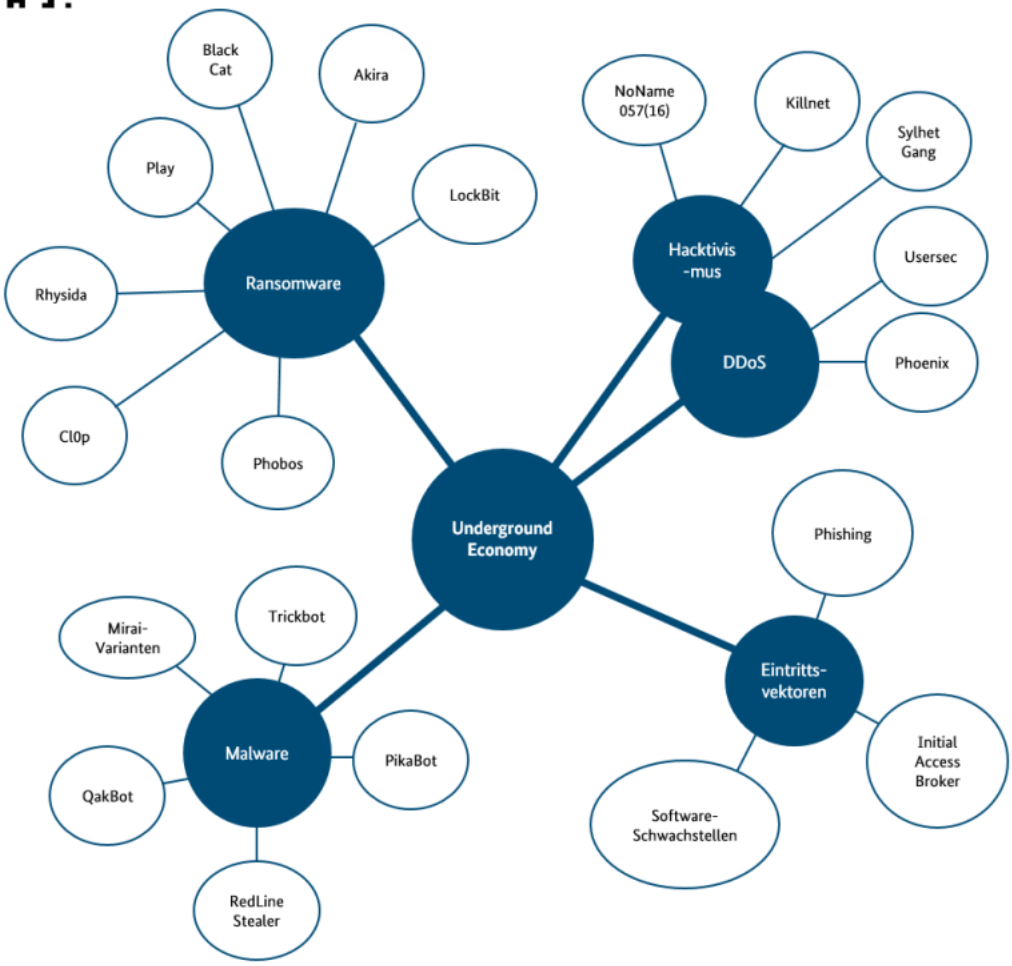

Abbildung 1: Relevante Bedrohungen der Cyberkriminalität 2023

[1]Hacktivismus vereint die Konzepte des Hackings und des Aktivismus und beschreibt ideologisch, sozial und/oder politisch motivierte Aktionen unter Nutzung von Hackingtools. Insbesondere im Zuge des russischen Angriffskrieges auf die Ukraine etablierten sich DDoS Angriffe als beliebtes Instrument von hacktivistischen Cyber Akteuren.

1.2 BRANCHEN IM FOKUS

Der Vorjahrestrend zu vermehrten Angriffen auf **Bildungseinrichtungen** setzte sich auch 2023 fort.

> *Bei einem Angriff auf eine Hochschule im September kam es durch die Verschlüsselung von Daten zu starken Einschränkungen der IT-Systeme. Die Hochschule war zeitweise weder per E-Mail noch über die Homepage erreichbar. Beim Angriff entwendete Daten wurden später im Darknet veröffentlicht. Einige verschlüsselte Daten konnten nicht wiederhergestellt werden.*

Das **Finanzwesen** stand verstärkt im Fokus pro russischer Hacktivisten, wodurch es zu einer Vielzahl an DDoS Angriffen auf Webseiten von Banken kam Zudem blieben Zugangsdaten zu Online-Banking weiterhin ein beliebtes Ziel von Phishing.

> *Über einen Link in einer Phishing-SMS, die augenscheinlich von einer seriösen Bank stammte, gelangten Privatpersonen auf eine der Bank nachgeahmten Webseite. Nach dem Eintragen ihrer Zugangsdaten zum Online-Banking und einer weiteren SMS, mit der TANs abgegriffen wurden, kam es zu unrechtmäßigen Überweisungen von den betroffenen Bankkonten und zur Aufladung fremder PayPal-Accounts.*

Einrichtungen des **Gesundheitswesens** waren häufige Ziele von Angriffen und stets mit einem großen Schadenspotenzial verbunden.

> *Infolge eines im Dezember stattgefundenen Ransomware Angriffs auf eine Hospitalvereinigung waren in mehreren Krankenhäusern die Arbeiten auf den Intensivstationen und Radiologie Abteilungen eingeschränkt. Außerdem war die Kommunikation per Telefon und E Mail zeitweise nicht möglich*

Cyberangriffe auf **IT-Dienstleister** führten zu weitreichenden Folgen bei einer Vielzahl von Unternehmen und Verwaltungen, die mit den angegriffenen Dienstleistern durch eine **IT-Supply-Chain** verbunden sind.

> *Durch eine Schwachstellenausnutzung in der Software eines IT Dienstleisters kam es Mitte des Jahres zu einer Vielzahl von nachgelagerten Angriffen auf große deutsche Banken und Versicherungen. U.a. wurden bei den betroffenen Banken vertrauliche Kundendaten entwendet, darunter Namen und Kontodaten, welche später im Darknet veröffentlicht wurden.*

Öffentliche Verwaltungen und Behörden standen zunehmend im Fokus von DDoS- und/oder Ransomware Angriffen Einige waren infolge von Angriffen auf IT Dienstleister mittelbar betroffen.

> *Infolge eines Ransomware-Angriffs auf einen IT-Dienstleister im Oktober kam es zu Beeinträchtigungen bei über 72 Kommunen. Die Folgen waren in vielen Bereichen zu spüren. So fiel u.a. die Telefon- und E-Mail-Kommunikation aus, die Koordination von Rettungskräften wurde erschwert, Standesämter und das Wohnungswesen waren teilweise nur eingeschränkt arbeitsfähig und es kam zu Verzögerungen bei Fahrerlaubnisbehörden.*

Das **verarbeitende Gewerbe** war die mit am stärksten von Ransomware- bzw. Double Extortion-Angriffen betroffene Branche.

> *Durch einen Ransomware-Angriff auf eine Molkerei im Juni kam es zur Verschlüsselung des Warenwirtschaftssystems. Die Produktion war eingeschränkt möglich, die Produkte konnten allerdings nicht ausgeliefert werden. Zudem wurden unternehmensinterne Daten im Darknet veröffentlicht.*

2023 kam es zu einem vermehrten Aufkommen von DDoS-Angriffen auf **Verkehrsverbünde und Flughäfen**. Zudem gab es mehrere Ransomware-Angriffe.

> *Bei einem Angriff auf einen Verkehrsverbund im März kam es zu Verschlüsselungen der Systeme und Einschränkungen im Betriebsablauf U a. waren Verzögerungen beim Verkauf des 49 Euro Tickets feststellbar Später wurden entwendete unternehmensinterne Daten im Darknet veröffentlicht*

1.3 HERAUSRAGENDE SACHVERHALTE

Januar
Durch die Zusammenarbeit internationaler Strafverfolgungsbehörden kann die Serverinfrastruktur der Ransomware-Gruppierung **HIVE** erfolgreich vom Netz genommen werden. An der **Operation Dawnbreaker** sind Behörden aus insgesamt 13 Staaten beteiligt, darunter das Bundeskriminalamt und die Polizeidirektion Reutlingen aus Deutschland.

Januar
Die hacktivistische Gruppierung Killnet beginnt die DDoS-Kampagne **#GermanyRIP** gegen deutsche Ziele. Darunter befinden sich die Webseiten deutscher Flughäfen, Ziele im Energie- und Finanzsektor sowie Webseiten von Bundesbehörden, unter anderem die des BND und des BKA.

Februar
In Zusammenarbeit mit internationalen Strafverfolgungsbehörden vollzieht das LKA Nordrhein-Westfalen Exekutivmaßnahmen gegen mutmaßliche Beteiligte hinter der Ransomware **DoppelPaymer**. Die Drahtzieher hinter der Ransomware werden öffentlich zur Fahndung ausgeschrieben.

März
Das BKA beschlagnahmt unter Sachleitung der Generalstaatsanwaltschaft Frankfurt am Main – Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) – die Serverinfrastruktur des Krypto-Mixers **ChipMixer** und stellt umgerechnet ca. 90 Mio. Euro sicher.

April
Internationale Strafverfolgungsbehörden beschlagnahmen die Infrastruktur des Underground Economy Marktplatzes **Genesis Market** und nehmen über einhundert Tatverdächtige fest.

April
Zwei kritische Schwachstellen in der Druckmanagement-Software **PaperCut** werden aktiv durch Cyberkriminelle ausgenutzt.

Mai bis Juli
Über die massenhaft ausgenutzte Schwachstelle in der Datenübertragungssoftware **MOVEit** wird u.a. ein Dienstleister des Finanzwesens sowie dessen Kunden kompromittiert.

August
Die technische Infrastruktur des Trojaners **Qakbot** wird mithilfe des BKA übernommen und damit die Kompromittierung weiterer Endgeräte verhindert.

August
Die hacktivistische Gruppierung **NoName057(16)** beginnt ihre DDoS-Kampagne gegen deutsche Ziele und greift regelmäßig Behörden, Verkehrsbetriebe sowie das Finanzwesen an.

September
Unter Mitwirken des BKA wird der Tor-Marktplatz **Piilopuoti** im Rahmen eines internationalen Action Days beschlagnahmt, ein Beschuldigter in Finnland festgenommen und die täterseitig genutzten Server in Deutschland abgeschaltet.

Oktober
Die technische Infrastruktur des Ransomware-Akteurs **RagnarLocker** in Deutschland, Schweden und den Niederlanden wird zerschlagen.
Ein mutmaßlicher Entwickler der Ransomware wird festgenommen.

Oktober
Ein IT-Dienstleister in Nordrhein-Westfalen wird mittels der Ransomware **Akira** verschlüsselt. Infolgedessen sind über 70 Kommunen und öffentliche Verwaltungen kaum arbeitsfähig.

November
Im Zuge der **Operation Dawnbreaker** wird eine durch Europol und Eurojust koordinierte Razzia durchgeführt. Dabei werden mehrere Verdächtige festgenommen.

Dezember
Im Rahmen einer international koordinierten Aktion unter Leitung des BKA wird der Darknet-Marktplatz **Kingdom Market** abgeschaltet.

2. Polizeiliche Kriminalstatistik

Vor dem Hintergrund eines immer noch sehr hohen Dunkelfeldes im Bereich Cybercrime kommt der PKS vor allem als Datenbasis für Trendaussagen und für die Beschreibung der Entwicklung des Phänomenbereichs eine hohe Bedeutung zu.

Nachdem im Jahr 2021 ein Höhepunkt bei den registrierten Inlands Straftaten im Bereich der Cybercrime-Delikte festgestellt wurde, ist die Entwicklung seit 2022 rückläufig. Im Jahr 2023 konnte mit 1,8% ein weiterer leichter Rückgang an Cyber-Straftaten bei der (Inlands-)PKS verzeichnet werden. Die Aufklärungsquote bei diesen Delikten ist angestiegen (32,2%), liegt damit aber auf dem Niveau der letzten vier Jahre. Der Anteil von Cybercrime-Delikten an den registrierten Straftaten insgesamt nimmt leicht ab und lag für das Jahr 2023 bei 2,2% (vgl. 2021: 2,9%; 2022: 2,4%).

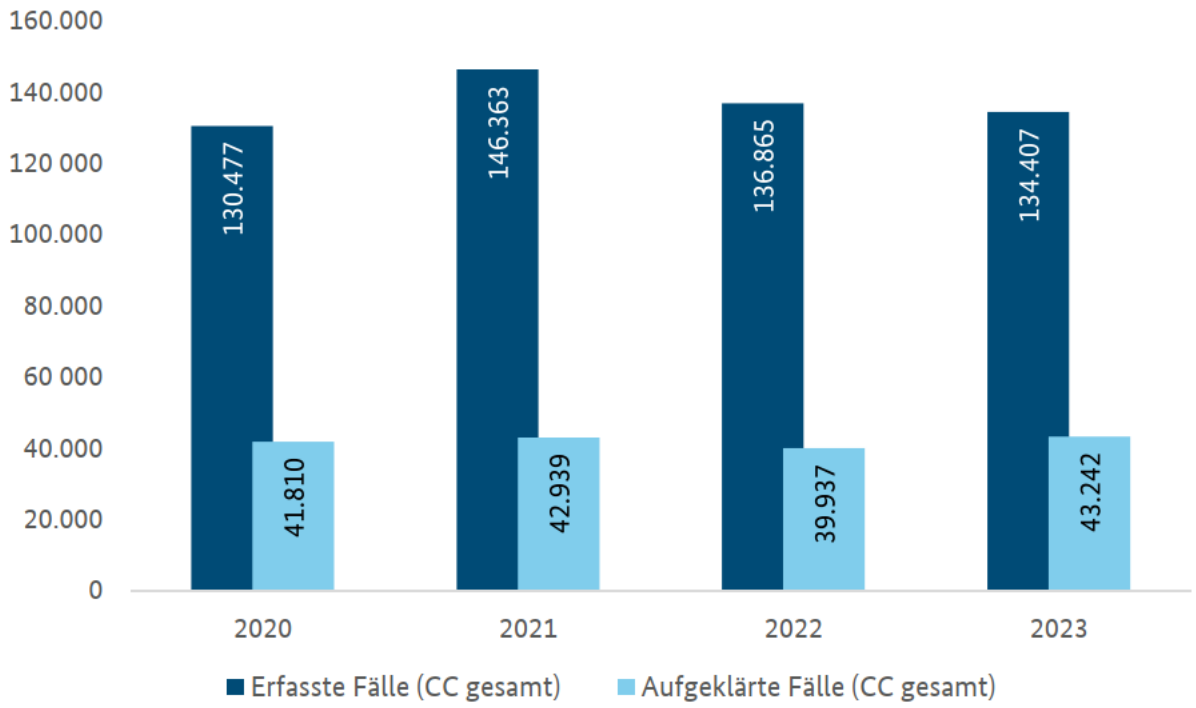

Abbildung 2: Erfasste und aufgeklärte Cybercrime-Fälle in Deutschland 2020 bis 2023

In der PKS werden die cyberspezifischen Delikte in einem Summenschlüssel Cybercrime zusammengefasst. Einzeldelikte wie die Fälschung beweiserheblicher Daten, die Datenveränderung/Computersabotage oder das Ausspähen von Daten/Datenhehlerei weisen einen Rückgang im Vergleich zum Vorjahr auf. Beim Computerbetrug, der den größten Anteil an den cyberspezifischen Delikten im Summenschlüssel Cybercrime ausmacht, ist jedoch ein leichter Anstieg zu verzeichnen.

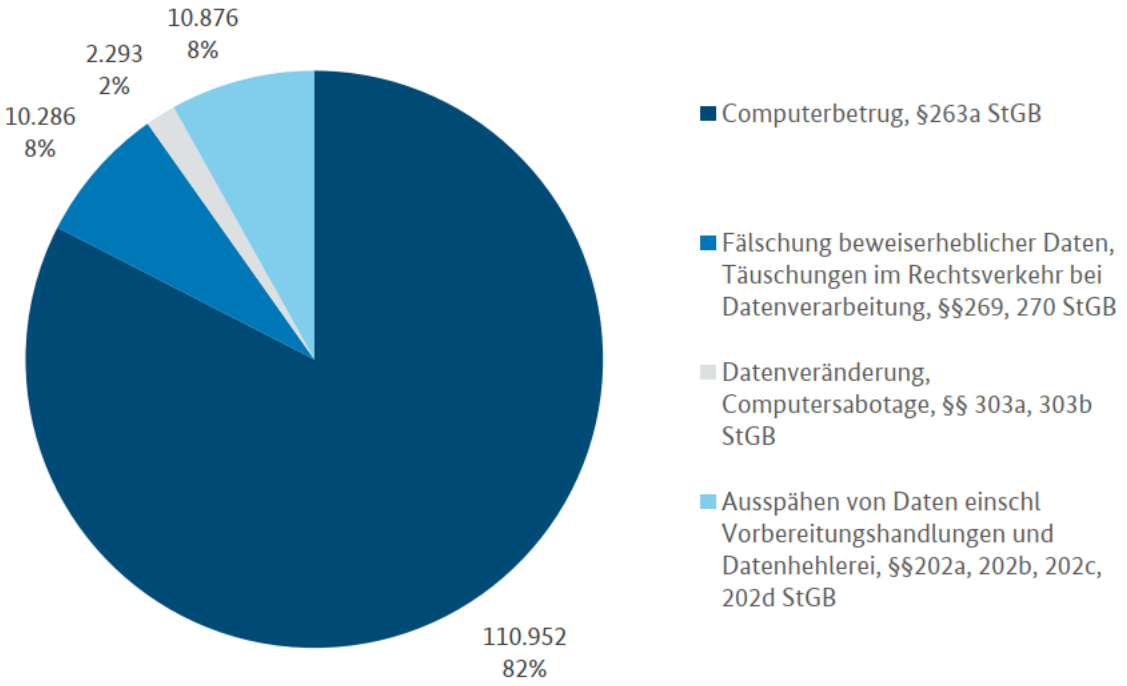

Abbildung 3: Fallaufkommen der Cyberstraftaten nach Deliktsbereich für das Jahr 2023

Im Gegensatz zur Inlands-PKS sind die erfassten Cybercrime-Delikte bei Auslandstaten im Jahr 2023 um ca. 28% angestiegen. Dabei handelt es sich um Sachverhalte, bei denen zwar Schäden in Deutschland verursacht werden, aber der Aufenthaltsort des Täters im Ausland liegt oder unbekannt ist.[2] Seit Beginn der separaten Erfassung dieser Auslandstaten zeigt sich hier ein fortlaufender Anstieg.

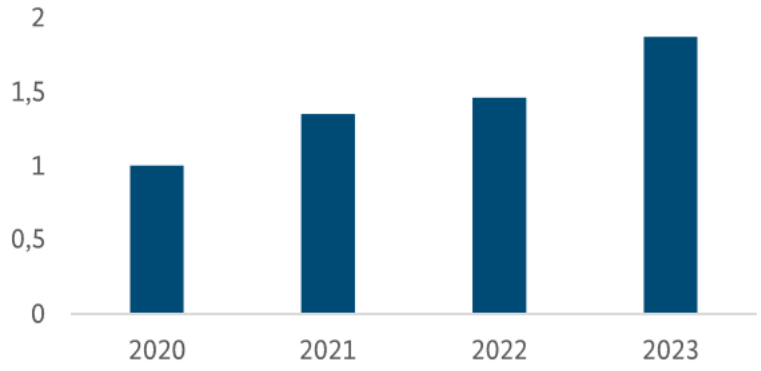

Abbildung 4: Erfasste Auslandstaten Cybercrime. (Anm.: Der Indexwert zeigt die Veränderung der erfassten Auslandstaten, dabei wird das Jahr 2020 als Basiswert auf 1 festgelegt. Die Werte der Folgejahre stehen in Relation zu diesem Basiswert und zeigen damit den Trend der steigenden Auslandstaten.)

[2] Die separate Erfassung von Auslandstaten in der PKS wurde zum 01.01.2020 eingeführt. Nach gemeinsamer Evaluation und Abstimmung mit den Ländern ist eine erstmalige Ausweisung der absoluten Zahlen im Berichtsjahr 2024 vorgesehen.

Die Auslandstaten haben besonders im Bereich Cyberkriminalität eine hohe Relevanz:

- Die Anzahl an Auslandstaten Cybercrime übersteigt die der Inlandstaten des Jahres 2023, ebenso wie bereits im Vorjahr.
- Während Cybercrime nur 2,2% an allen Straftaten der Inlands-PKS ausmachen, sind über ein Viertel aller Auslandstaten der Cybercrime zuzurechnen (26,5%).

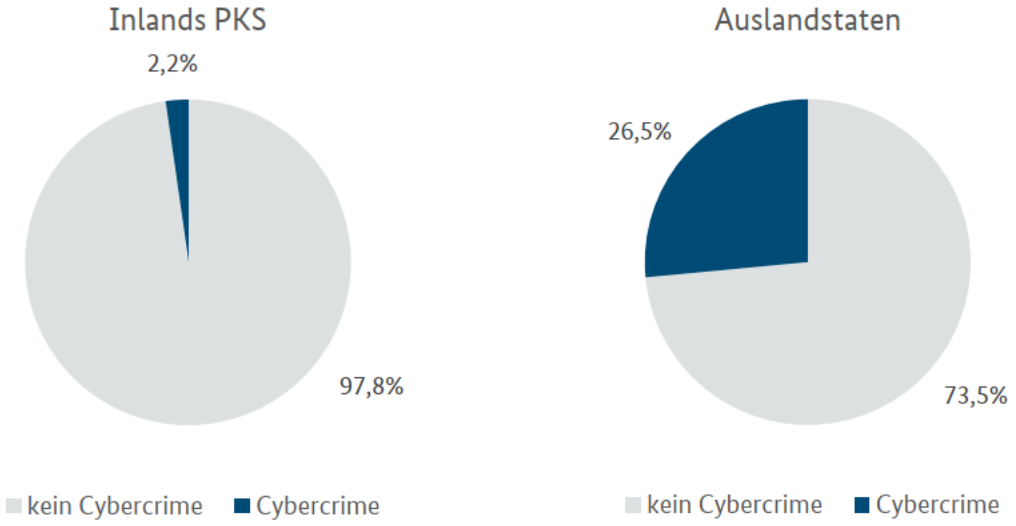

Abbildung 5: Anteil von Cybercrime-Delikten an den Gesamtstraftaten 2023

Auch wenn die Fallzahlen der (Inlands-)PKS für das Jahr 2023 leicht rückläufig sind, ist dies kein Indiz für einen generellen Rückgang der 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. Die Auslandstaten, bei denen sich die Täter nicht in Deutschland aufhalten oder deren Aufenthaltsort unbekannt ist, geben hier ein realistischeres Bild wieder. Diese Fallzahlen steigen weiter an.
Der hohe Anteil an Auslandstaten stellt die im Phänomenbereich ermittelnden Polizeibehörden vor große Herausforderungen, was sich auch weiterhin in einer Aufklärungsquote der Auslandstaten im niedrigen einstelligen Bereich widerspiegelt. Es fehlen in der digitalen Welt häufig geeignete Ermittlungsansätze zur Täteridentifizierung; aber auch bei vorliegenden Ermittlungsansätzen können juristische Hürden und mangelnde Kooperationsbereitschaft im Ausland eine Täteridentifizierung und die Strafverfolgung erschweren oder sogar gänzlich verhindern.

Die Fallzahlen zum Straftatbestand §127 StGB „Betreiben krimineller Handelsplattformen im Internet“ sind nicht vom Summenschlüssel Cybercrime erfasst. Nachdem 2022 bei der erstmaligen Erfassung insgesamt 13 Fälle in der PKS registriert wurden, stieg die Fallzahl 2023 auf 27 Fälle an – mehr als eine Verdoppelung. 15 von diesen erfassten Fällen konnten aufgeklärt werden, was eine Aufklärungsquote von 55,6% bedeutet Es muss hierbei aber berücksichtigt werden, dass es aufgrund der niedrigen Fallzahlen schnell zu einem bedeutenden Anstieg bzw. Rückgang dieser Quote kommen kann (Vgl. 2022: 10 aufgeklärte Fälle von insgesamt 13 entsprechen einer Quote von 76,9%).

In der gesamtheitlichen Betrachtung steigen die polizeilich bekannt gewordenen Fälle an.

3. Relevante Phänomenbereiche

3.1 EINTRITTSVEKTOREN

Phishing war auch 2023 ein von Kriminellen häufig genutzter Eintrittsvektor für Cyberangriffe, wobei sowohl Mails mit maliziösen Anhängen oder Links, als auch maliziöse Webseiten selbst eine Rolle spielen. Die besondere Relevanz dieses Eintrittsvektors und die tendenziell stetig wachsende Anzahl an Phishing-Seiten besteht seit Jahren und wird anhand der nachfolgenden Darstellung mit Zahlen der Anti Phishing-Working-Group (APWG)[3] deutlich:

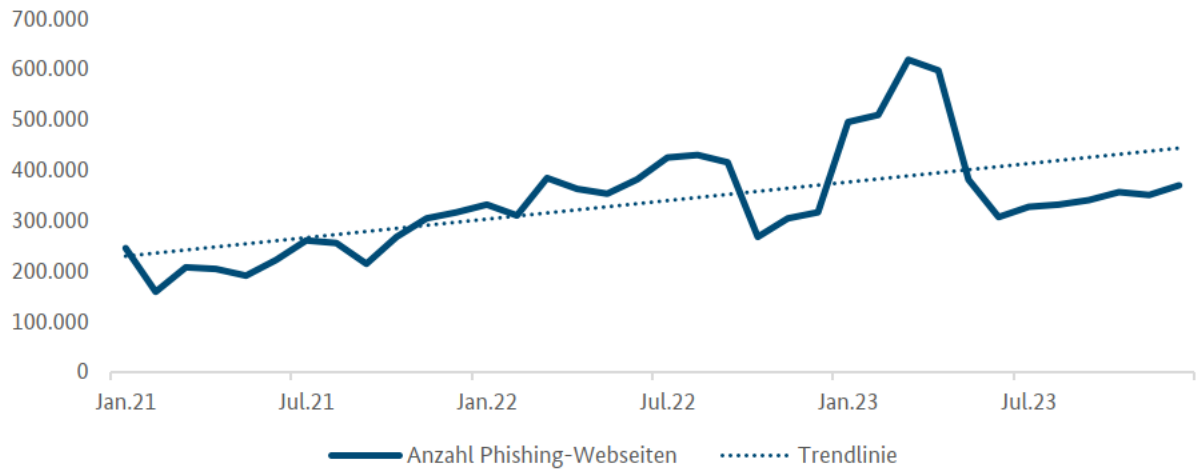

Abbildung 6: Anzahl der durch die Anti-Phishing-Working-Group festgestellten Phishing-Seiten seit 2021

Von den Cyberkriminellen wurden auch 2023 zeitkritische oder emotionalisierende Inhalte beim Verfassen der Mails verwendet, um Druck auf die Empfänger auszuüben und diese zu weiteren Handlungen, wie z B dem Herunterladen von Anhängen[4], zu verleiten Nachgeahmt werden u a bekannte und weit verbreitete Marken und Unternehmen aus der Finanz und Logistikbranche wie auch Streaming-Dienstleister. Spear-Phishing-Mails verwenden zum Teil reale, unternehmensinterne Vorgänge als Narrativ, wobei solch exklusive Informationen in zuvor erfolgten Ausspähmaßnahmen erlangt werden.

Die Relevanz von Phishing spiegelt sich auch in diversen Angeboten für Phishing Kits in der Underground Economy wider. Solche Kits erlauben es den Tätern, Phishing-Kampagnen zu gestalten und zu initiieren. Dabei wird seit 2023 häufig auch der Messenger-Dienst Telegram in diverse Phishing-Tools einbezogen. Durch Telegram-Bots wie Telekopye können Cyberakteure Social Engineering[5] einfacher und effektiver gestalten.

[3] Internationale Arbeitsgruppe mit mehr als 3.000 Mitgliedern weltweit zur Bekämpfung von Phishing und Betrugsdelikten.
[4] Zu den beliebtesten maliziösen E Mail Anhängen in Phishing- und Spam Mails gehören weiterhin MS Office Dateien, PDFs, LNK Dateien sowie HTML Redirect-Anhänge.
[5] Beim Social Engineering nutzt der Angreifer die Schwachstelle Mensch aus. Das Vorgehen der Straftäter ist dadurch gekennzeichnet, dass ein direkter Kontakt zu dem potenziellen Geschädigten hergestellt wird. Dabei werden Eigenschaften wie Angst, Hilfsbereitschaft oder auch Vertrauen ausgenutzt, um die angegriffene Person zur Herausgabe vertraulicher Informationen zu bewegen oder Schadsoftware zu installieren.

Phishing as a Service Angebote: Telegram Bot Telekopye

Tools wie Telekopye ermöglichen Cyberkriminellen, großflächige Phishing-Kampagnen auch ohne tiefergehende technische Kenntnisse durchzuführen.

Durch Telekopye können Nutzer über ein vereinfachtes Interface via Telegram auf zahlreiche Funktionen zur Durchführung einer Phishing-Kampagne zugreifen Zu den Funktionen zählen die Erstellung von Phishing Webseiten, der Versand von Phishing Mails und SMS sowie die Generierung von gefälschten Proof-Screenshots und QR-Codes. Das Toolkit bietet verschiedene HTML-Vorlagen für Phishing-Webseiten in unterschiedlichen Ländern an, darunter auch Deutschland. Die nutzerfreundliche HTML-Vorlage stellt hierbei das Hauptmerkmal von Telekopye dar Die auf diesem Weg erstellten Phishing-Webseiten imitieren Zahlungsseiten verschiedener Webseiten, Login Webseiten zu Zahlungsdienstleistungen oder anderweitigen Zahlungsgateways.

Über den Phishing-Link werden Nutzer, die beispielsweise im Glauben sind, einen Online-Kauf zu tätigen, aufgefordert, ihre Zahlungsdaten einzugeben, die von den Tätern abgegriffen werden können. Einige Versionen von Telekopye sind darüber hinaus in der Lage, erbeutete (Zahlungs-)Daten der Geschädigten auf dem Server des Bots zu speichern. Die im Rahmen der Phishing-Kampagne erbeuteten Gewinne gelangen an die Telekopye-Administratoren, die die Herkunft der Gelder über einen Mixing-Dienst verschleiern und einen eigenen Anteil abschöpfen Diese Provision ist abhängig von der Telekopye Version und Rolle des Nutzers und beträgt 5 40%. Telekopye erleichtert die Ausführung von Phishing-Angriffen über das Interface erheblich. Allerdings enthält das Tool keine Chatbot-KI-Funktionen und führt die Kampagnen somit nicht autonom aus.

Die Nutzung eines Bots wie Telekopye stellt ein Novum dar Die zunehmende Automatisierung erreicht mit Telekopye im Bereich Phishing eine neue Stufe, da so zur Durchführung größerer Kampagnen nicht einmal das Verlassen der Telegram-Anwendung erforderlich ist. Ebenfalls wird durch die Vermarktung von Telekopye via Telegram die Relevanz des Messengers als Underground Economy Plattform deutlich

Für den Bereich der Eintrittsvektoren gewinnen große Sprachmodelle wie der Chatbot ChatGPT und entsprechende kriminelle Nachbildungen zunehmend an Bedeutung Beginnend mit dem Zeitpunkt der Veröffentlichung von ChatGPT und dem damit ausgelösten Hype um Künstliche Intelligenz (KI) Ende 2022 verzeichnen verschiedene IT Dienstleister einen enormen Anstieg an neuartigen Phishing Mails. Von generativer KI verfasste Texte können im Vergleich zu herkömmlichen Phishing Mails stärker personalisiert sein und kaum bis keine sprachlichen oder formalen Fehler aufweisen, die generell Anhaltspunkte für Zweifel liefern Hinzu kommt, dass Phishing Kampagnen durch KI Tools automatisiert erstellt und verbreitet werden können

Cyberkriminelle verschaffen sich besonders häufig über Phishing, Social Engineering oder kompromittierte Zugangsdaten Zutritt in ihre jeweiligen Zielsysteme. Die Vermittlung solcher kriminell erlangten Zugänge an andere Cyberakteure erfolgt durch sogenannte Initial Access Broker (IAB) Diese bieten ihre Dienstleitung in der Regel mehreren Akteuren an Infektionen können über mehrere Monate unbemerkt bleiben und in diesem Zeitraum verkauft werden Auch bekannte Cyber Akteure nehmen vermehrt die Angebote von IABs in Anspruch Nur in Einzelfällen konnten hochprofessionalisierte Gruppierungen festgestellt werden, die über eigene Fähigkeiten im Bereich Initial Access verfügen Insgesamt sind diese Fähigkeiten vergleichsweise rar, sodass eine hohe Nachfrage für die Angebote von IABs besteht.

Neben kompromittierten Zugangsdaten umfassen die Angebote von IABs auch die Kenntnisse über (Zero Day)Schwachstellen Dieses Wissen stellte im Jahr 2023 eine besonders relevante Bedrohung dar, wobei vor allem die erste Jahreshälfte von der Ausnutzung mehrerer kritischer Schwachstellen geprägt war. Schwachstellen in Software stellten in diesem Zeitraum besonders häufig den Eintrittsvektor in Unternehmensnetzwerke dar und zogen eine Vielzahl an kompromittierten Systemen mit sich Die US Bundesbehörde Cybersecurity & Infrastructure Security Agency (CISA) erhebt im sogenannten "Known Exploited Vulnerabilities Catalog" die Anzahl der identifizierten Software-Schwachstellen, welche aktiv durch Cyberkriminelle ausgenutzt werden Für 2023 registrierte die CISA 187 derartiger Schwachstellen Einige Schwachstellen waren von besonderer Bedeutung:

ESXi

Anfang Februar sind nach der Ausnutzung einer Schwachstelle in ESXi Servern von VMware weltweit tausende Systeme Ziel einer Ransomware Kampagne geworden.

GoAnywhere

Im März 2023 fand weltweit ein starker Anstieg der Angriffe durch Cl0p statt. IT-Sicherheitsforscher konnten feststellen, dass diese Kampagne wahrscheinlich unter Ausnutzung der Schwachstelle CVE 2023 0669 in Fortra GoAnywhere MFT erfolgt war Bei GoAnywhere MFT (Managed File Transfer) handelt es sich um eine Softwarelösung, die die Übertragung und Verwaltung von Dateien und Daten über verschiedene Netzwerke und Protokolle ermöglicht. Die Schwachstelle erlaubte den unberechtigten Fernzugriff auf die betroffenen Systeme.

Papercut

Mitte März wurden zwei Schwachstellen (CVE2023 27350 und CVE 2023 27351) in PaperCut MF/NG, einer Druckmanagement Software, entdeckt. Nach Angaben des Herstellers wird die Software von über 139 Millionen Nutzern in über 195 Ländern genutzt. Die Schwachstellen sollen seit dem 14. April 2023 aktiv durch cyberkriminelle Akteure ausgenutzt worden sein, u.a. durch Ransomware-Gruppierungen.

MOVEit

Am 31.05.2023 gab der Applikations- und Software-Anbieter Progress Software bekannt, dass eine Sicherheitslücke in der Datentransfer-Software MOVEit sowie der MOVEit Cloud identifiziert wurde Die Software erlaubt den sicheren Transfer von Daten innerhalb eines Unternehmens sowie an Kunden und Dritte.
Die Schwachstelle mit der Bezeichnung CVE-2023-34362 ermöglicht Angreifern eine Erweiterung der Rechte (Privilegieneskalation) sowie den unautorisierten Zugriff auf Dateisysteme
Die Ausnutzung erfolgt unter anderem über eine sogenannte SQL Injection Dabei kann ein Angreifer über spezielle Befehle Informationen über Struktur und Inhalt einer angegriffenen SQL-Datenbank ableiten und eigene Befehle ausführen lassen. Auf diesem Weg können Datenbankelemente abgefragt, geändert oder sogar gelöscht werden.
Im Juni wurde bekannt, dass unter anderem Affiliates der Gruppierung Cl0p, ebenfalls bekannt als TA505, diese Schwachstelle ausnutzen, um Systeme zu kompromittieren und Daten auszuleiten. In einem auf der eigenen Dedicated Leak Site (DLS) veröffentlichten Statement gibt Cl0p an, über die MOVEit-Schwachstelle diverse Systeme infiziert und Daten ausgeleitet zu haben.
Weltweit sollen tausende Systeme gegen die Schwachstelle ungeschützt gewesen sein, darunter in Deutschland im dreistelligen Bereich.

Im Bereich der Eintrittsvektoren zeigt sich die hohe Anpassungsfähigkeit krimineller Akteure.

3.2 MALWARE

Auch im Jahr 2023 bleibt die Bedrohung durch Malware bestehen Malware jeder Art, insbesondere sogenannte Loader bzw. Dropper und Info-Stealer, werden zunehmend mit einer Vielzahl an Funktionalitäten programmiert und nicht mehr nur für einen spezifischen Zweck eingesetzt. Ein Trend in Richtung Multifunktionalität von Malware Familien ist erkennbar. So weisen dezidierte Loader wie Qakbot oder Pikabot auch Fähigkeiten zur Sammlung und Exfiltration von Daten auf, während Info-Stealer wie Truebot ebenfalls als Remote Access Tool dienen und Fernzugriff auf die befallenen Systeme etablieren können

Loadern bzw Droppern, die im Vorfeld von Ransomware Angriffen eingesetzt werden, kommt eine besondere Bedeutung im Bereich Cyberkriminalität zu. Ihre Fähigkeit zum Nachladen weiterer Schadsoftware macht sie zu einer wichtigen Komponente bei besonders schwerwiegenden Angriffen mit anschließenden Verschlüsselungen

Takedown der Qakbot Infrastruktur

Der Trojaner Qakbot, der bereits seit 2007 im Umlauf ist und weltweit Schäden in Millionenhöhe verursacht hat, wurde am 26.08.2023 in Zusammenarbeit mehrerer internationaler Partner unter der Leitung US-amerikanischer Behörden erfolgreich vom Netz genommen Die technische Infrastruktur konnte mithilfe des BKA übernommen und damit die Kompromittierung weiterer Endgeräte verhindert werden Im Rahmen dieses Takedowns wurden nach Auskunft des US-Department of Justice zudem 8,6 Millionen US-Dollar in Kryptowährung, die im Rahmen von Ransomware-Angriffen als Lösegelder erpresst wurden, beschlagnahmt.

Qakbot, auch als Qbot oder Pinkslipbot bekannt, fungierte für Cyberkriminelle primär als sogenannter Dropper oder Loader und gilt nicht nur in Deutschland, sondern auch weltweit als eine der gefährlichsten Schadsoftware-Varianten. Die mit Qakbot infizierten Systeme wurden mittels einer Command-and-Control-Infrastruktur zu einem Botnetz zusammengeschlossen, welches allein im letzten Jahr über 700.000 Systeme umfasste. Diese Anzahl verdeutlicht die Relevanz und das vorhandene Schadenspotenzial dieser Malware Variante.

Qakbot wurde bevorzugt für Angriffe gegen die Finanzbranche und/oder gegen kritische Infrastrukturen genutzt. Der primäre Fokus lag hierbei auf dem Diebstahl digitaler Daten. Darüber hinaus wurde Qakbot in der Vergangenheit auch häufig dafür eingesetzt, Ransomware nachzuladen In der Folge wurden die betroffenen Systeme oder darauf befindliche Daten verschlüsselt, um so Lösegelder zu erpressen.

Qakbot gilt als Nachfolger der Schadsoftware Emotet, dessen Infrastruktur bereits 2021 durch das BKA und andere internationale Partner zerschlagen werden konnte.

Auch wenn die Bedeutung von Malware für die Kriminalitätsentwicklung im Phänomenbereich Cybercrime weiterhin als hoch eingeschätzt wird, ist dies in Deutschland für den speziellen Bereich der digitalen Angriffe auf Geldautomaten anders zu bewerten. 2023 konnten keine derartigen Angriffe mehr festgestellt werden.

Für die Entwicklung und Verbesserung von Malware gewinnt KI ebenfalls zunehmend an Bedeutung. So können die Fähigkeiten generativer KI-Tools für verschiedene Cybercrime-as-a-Service-Angebote missbraucht werden. KI-Modelle sind dabei prinzipiell in der Lage, Schadsoftware zu programmieren, auf Fehler zu prüfen und ggf. auszubessern.

3.3 RANSOMWARE & DATA EXTORTION

Ransomware Angriffe stellen bereits seit Jahren die primäre Bedrohung im Bereich der Cyberkriminalität dar. Ein besonders hohes Schadenspotenzial haben dabei Angriffe mittels Verschlüsselungstrojanern, die sich primär gegen Unternehmen, Institutionen oder die öffentliche Verwaltung richten und in den betroffenen Systemen teilweise ganze Server verschlüsseln. Gemäß einer für das Jahr 2023 bei den Landeskriminalämtern und dem Bundeskriminalamt durchgeführten Fallerhebung haben bundesweit über 800 Unternehmen und Institutionen Ransomware Fälle zur Anzeige gebracht [6] Bei diesen Angriffen wurden über 70 unterschiedliche Ransomware-Varianten identifiziert. Am häufigsten waren deutsche Geschädigte im vergangenen Jahr von Angriffen mit der Ransomware-Variante LockBit betroffen.

Abbildung 7: Kennzahlen zu Ransomware-Angriffen im Jahr 2023
a = Top 10 der relevantesten in Deutschland 2023 aktiven Ransomware-Varianten. Die Auflistung basiert auf einer Erhebung des BKA in den Bundesländern.
b = Quelle: BKA
c = Durchschnittlich festgestellte Lösegeldzahlung weltweit. Quelle: Coveware (2023). Quartalsberichte 2023. Online abrufbar unter https://www.coveware.com/blog
d = Einnahmen durch weltweite Ransomware-Angriffe. Quelle: Chainalysis (2024). The 2024 Crypto Crime Report

Ransomware-Angriffe sind nach wie vor sehr lukrativ für die Täterschaft. Das Blockchain-Analyse Unternehmen Chainalysis wertet jährlich die Summe aller Lösegeldtransaktionen auf Kryptowallets von Ransomware-Akteuren aus und konnte 2023 nahezu eine Verdopplung gegenüber dem Vorjahr

[6] Bundesweite Erhebung polizeilich bekannt gewordener Ransomware Angriffe. Erhebungszeitraum: 01.01.2024 31.03.2024. Die abgebildeten Daten umfassen ausschließlich das polizeiliche Hellfeld.

feststellen Die Gesamtsumme der durch Chainalysis festgestellten Lösegeldzahlungen überstieg 2023 somit erstmalig eine Milliarde US Dollar.[7] Insgesamt lagen kriminelle Einnahmen durch Ransomware Angriffe jedoch bereits in den vergangenen Jahren auf einem hohen Niveau. Der starke Zahlungsrückgang im Jahr 2022 wird seitens Chainalysis als Anomalie gewertet, welcher vor allem mit dem Beginn des russischen Angriffskrieges gegen die Ukraine begründet wird. Die in diesem Zusammenhang neu verhängten Sanktionen gegen Russland dürften besonders in der Anfangsphase der kriegerischen Auseinandersetzung Auswirkungen auf die Zahlungsbereitschaft von Geschädigten gehabt haben.

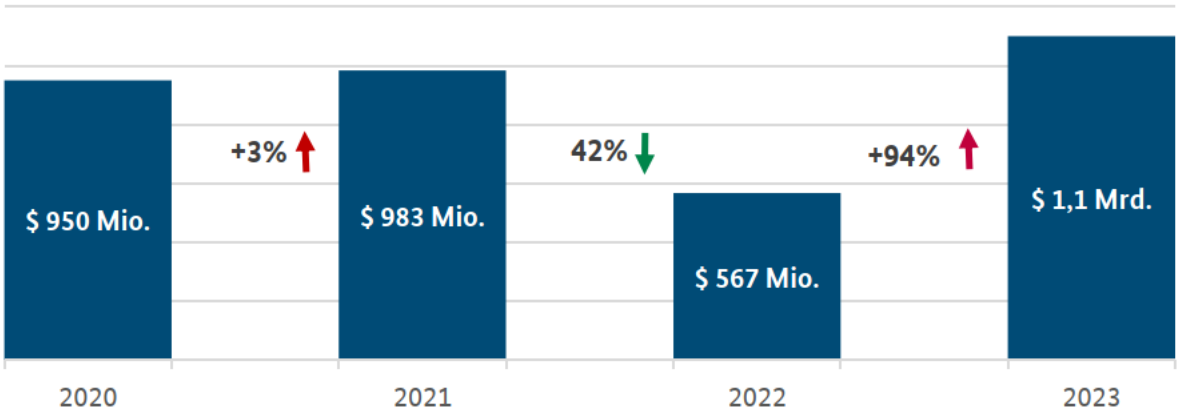

Abbildung 8: Weltweit festgestellte Lösegeldzahlungen auf Kryptowallets von Ransomware-Akteuren 2020 bis 2023. Quelle: Chainalysis (2024). The 2024 Crypto Crime Report

Auch Analysen des IT-Sicherheitsunternehmens Coveware bestätigen, dass Lösegeldzahlungen weltweit stark angestiegen sind. Die 2023 durchschnittlich gezahlte Lösegeldsumme lag nach Coveware bei 621 858 US Dollar dies stellt einen Anstieg von 125% dar [8]
Unabhängig vom verzeichneten Anstieg der Lösegeldzahlungen ist die Zahlungsbereitschaft der von Ransomware betroffenen Unternehmen 2023 weiterhin rückläufig. Um die geringe Zahlungsbereitschaft geschädigter Unternehmen zu kompensieren, stellten Täter durchschnittlich höhere Lösegeldforderungen. Seit 2022 steigt der Anteil an Lösegeldzahlungen mit Beträgen über einer Million US-Dollar an und erreichte Ende 2023 einen vorläufigen Höhepunkt.[9] Um höhere Lösegelder zu erpressen, richten Ransomware Akteure ihren Fokus daher verstärkt auf große und zahlungskräftige Unternehmen (Big Game Hunting).

Kriminelle Einnahmen durch Ransomware stiegen 2023 wieder stark an.

[7] Chainalysis (2024). The 2024 Crypto Crime Report. Die Daten von Chainalysis unterliegen retrograden Anpassungen.
[8] Coveware (2023). Quartalsberichte 2023. Online abrufbar unter **https://www.coveware.com/blog**
[9] Chainalysis (2024). The 2024 Crypto Crime Report.

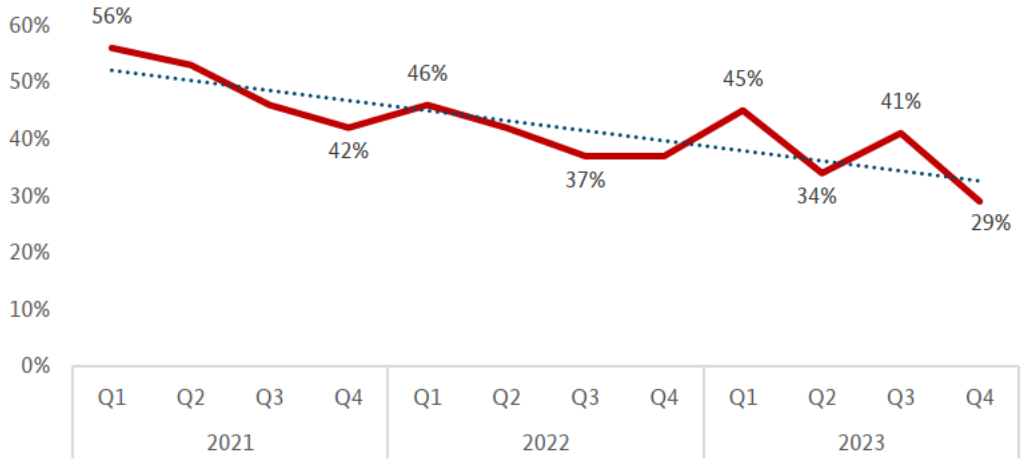

Abbildung 9: Anteil an Unternehmen, die nach einem Ransomware-Angriff Lösegeld gezahlt haben. Quelle: Coveware (2023). Quartalsberichte 2023

Das Ransomware-Ökosystem war 2023 von einer hohen Dynamik geprägt. Exemplarisch hierfür ist das Ransomware-as-a-Service (RaaS)-Geschäftsmodell, das nach wie vor die Aktivitäten der Underground Economy im Bereich Ransomware dominiert. Entwickler einzelner Ransomware-Varianten vermieten den Einsatz ihrer Schadsoftware an Affiliates, die damit Ransomware Angriffe durchführen und Anteile des erpressten Lösegelds erhalten Affiliates sind häufig nicht Teil klar abgegrenzter Gruppierungsstrukturen, sondern setzen auch unterschiedliche Ransomware Varianten für Angriffe ein. Diese Arbeitsteilung innerhalb der RaaS-Economy erschwert es, genaue Zusammenhänge zwischen einzelnen Akteuren nachzuvollziehen. Chainalysis konnte beispielsweise im vergangenen Jahr über die Analyse von Kryptotransaktionen Zusammenhänge zwischen dem Administrator der Dropper-Malware Trickbot sowie den Ransomware Varianten Royal und der seit 2023 aktiven Ransomware Variante 3AM feststellen [10]

Darüber hinaus führen etablierte Täter neben dem Wechsel der verwendeten Schadsoftware mitunter Rebrandings durch, um zumindest für einen gewissen Zeitraum unentdeckt unter neuen Namen zu agieren. 2023 kam es beispielsweise zu einem Rebranding der Gruppierung Vice Society, die inzwischen unter dem Namen Rhysida agiert Durch Feststellung derartiger Rebrandings ist davon auszugehen, dass die Anzahl etablierter Ransomware Akteure deutlich geringer ist, als die Vielzahl an verschiedenen Ransomware-Varianten vermuten lässt.

Aus dem Zusammenspiel der aufgezeigten Entwicklungen ergibt sich die hohe Bedeutung des Phänomenbereichs Ransomware: Die Fallzahlen in Deutschland steigen kontinuierlich an, Ransomware Akteure nehmen zunehmend mehr Lösegeldzahlungen ein und verursachen entsprechend hohe Schäden bei den Betroffenen. Laufende Weiterentwicklungen der Akteure und ihrer Malware sowie schnelle Entwicklungen im Bereich RaaS erschweren zudem die strafrechtliche Verfolgung.
Die hohe Dynamik im Cyberbereich ist auch ein Grund dafür, dass personen- bzw. täterbezogene Ermittlungen alleine nicht ausreichend sind, das Wirken der cyberkriminellen Szene langfristig einzudämmen Ein Fokus operativer Maßnahmen liegt demzufolge auch im Phänomenbereich Ransomware auf der Zerschlagung krimineller Infrastrukturen. Für 2023 können beispielhaft Maßnahmen gegen RagnarLocker und die Operation Dawnbreaker angeführt werden.

[10] Chainalysis (2024). The 2024 Crypto Crime Report.

Operation Dawnbreaker

Die Ransomware HIVE galt seit Mitte 2021 als eine der weltweit aktivsten Ransomware-Varianten. Sie wurde als RaaS vertrieben und barg ein enormes Schadenspotenzial. Laut Europol wurden seit Juni 2021 mehr als 1.500 Unternehmen aus mehr als 80 Ländern Ziele dieser Ransomware. Insgesamt konnten die Angreifer Lösegelder in Höhe von ca. 100 Mio. Euro erlangen.

Ende Januar 2023 konnte im Zuge der Operation Dawnbreaker die Serverinfrastruktur der Ransomware-Gruppierung HIVE inkl. ihrer Dedicated Leak Site (DLS) beschlagnahmt und abgeschaltet werden. Daran waren neben Europol auch Behörden aus insgesamt dreizehn Ländern beteiligt, darunter das Bundeskriminalamt und die Polizeidirektion Reutlingen. Im Rahmen der Ermittlungen wurden Server beschlagnahmt sowie Daten und Accounts des Netzwerks und seiner Nutzer gesichert. Den Ermittlern gelang es außerdem, Entschlüsselungstools festzustellen und diese betroffenen Unternehmen zur Verfügung zu stellen.

Die Analyse der beschlagnahmten Daten führte im November zu Folgemaßnahmen und Festnahmen mehrerer Verdächtiger in der Ukraine. Einer der Tatverdächtigen soll eine führende Position innerhalb der HIVE-Gruppierung innegehabt haben. Neben den Festnahmen kam es zur Sicherstellung weiterer Datenmengen sowie eines sechsstelligen Betrags in Kryptowährung, der möglicherweise aus Lösegelderpressungen stammt.

Cybertäter passen ihre Vorgehensweisen stetig an so auch Ransomware Akteure Während Double Extortion bereits seit Jahren als vielfach eingesetzter Modus Operandi fungiert, konnte 2023 festgestellt werden, dass einige Ransomware Akteure ihren Schwerpunkt auf die Erpressung mittels der Veröffentlichung zuvor ausgespähter Daten legen, ohne dass eine Verschlüsselung oder Sperrung des

Systems erfolgt. Die Data Extortion gewinnt demnach zunehmend an Bedeutung. Begründung hierfür könnte sein, dass Unternehmen ihre Daten vermehrt über Backups sichern und daher über eine Verschlüsselung allein weniger erpressbar sind. Außerdem können Angriffe ohne Verschlüsselung schneller durchgeführt werden, wodurch die Wahrscheinlichkeit sinkt, dass sie von Betroffenen bemerkt und gestoppt werden Eine täterseitige Annahme, dass Strafverfolgungsbehörden sie weniger in den Fokus nehmen, wenn die Schäden bei den Betroffenen geringer ausfallen, kann nicht ausgeschlossen werden. Im Bereich Data Extortion waren im vergangenen Jahr die Akteure hinter Cl0p besonders aktiv.

Cl0p

Von 2019 bis 2021 galt Cl0p als eine der aktivsten Ransomware Varianten weltweit, deren Aktivität 2022 zwar spürbar rückläufig war, Anfang 2023 aber weltweit wieder schlagartig zunahmen. Hierzu nutzten die Angreifer breitflächig IT-Schwachstellen aus, vor allem in Softwarelösungen zur Übertragung und Verwaltung von Dateien. Mit der Ausnutzung von Zero-Day-Schwachstellen fand seitens der Täter hinter Cl0p zunehmend eine Verlagerung zu reiner Data Extortion statt. Die Geschädigtendaten wurden auf der Dedicated Leak Site von Cl0p veröffentlicht

Dedicated Leak Sites (DLS) im Darknet dienen sowohl für Ransomware Angriffe mit Double Extortion als auch für reine Data Extortion Angriffe häufig als Medium zur öffentlichen Erpressung Auf DLS werden bei ausbleibender Lösegeldzahlung zuvor von betroffenen Unternehmen exfiltrierte Daten veröffentlicht Dies fungiert als zusätzliches Druckmittel und nutzt vor allem die Angst vor Reputationsschäden seitens der Geschädigten aus Im BKA durchgeführte Auswertungen der DLS zeigen, dass im Jahr 2023 insgesamt 191 deutsche Unternehmen öffentlich auf DLS erpresst wurden Dies stellt einen Anstieg um 39% im Vergleich zum Vorjahr dar Somit war Deutschland 2023 nach den USA, dem Vereinigten Königreich und Kanada am vierthäufigsten betroffen [11]

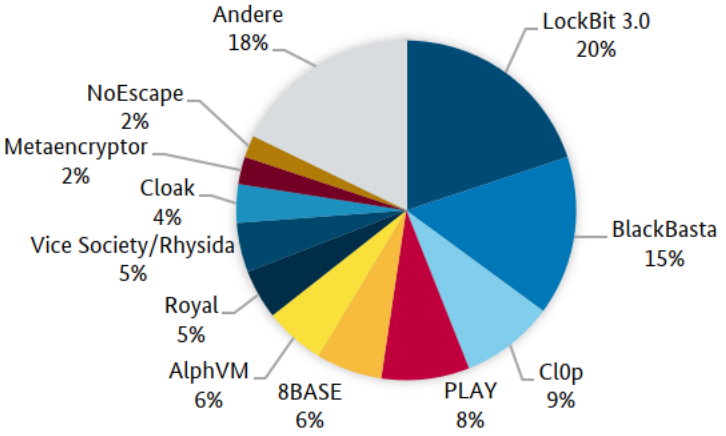

Abbildung 10: Verteilung deutscher Geschädigter auf DLS nach Gruppierung. Hierbei werden Leaks nach Double Extortion und Data Extortion berücksichtigt.

Data Extortion etabliert sich neben Double Extortion als relevanter Modus Operandi von Cyberangriffen.

[11] Eigene Auswertung nach den Daten von eCrime.ch. Online abrufbar unter **https://ecrime.ch/**

3.4 DISTRIBUTED DENIAL OF SERVICE

Die Entwicklungen im Bereich DDoS wurden auch 2023 durch das Agieren hacktivistischer Akteure geprägt. Wie bereits 2022 festgestellt, setzten im Berichtsjahr primär pro-russische Hacktivisten DDoS-Angriffe ein, um gegen die Ukraine und ihre Unterstützerstaaten vorzugehen Auch Ziele in Deutschland standen in diesem Zusammenhang im Fokus der Akteure.

Nach dem Terrorangriff der Hamas am 07.10.2023 und im darauffolgenden andauernden Konflikt Israels mit der Terrororganisation kam es zu DDoS-Attacken von anti-israelischen Hacktivisten gegen deutsche Ziele, da sich die Bundesregierung in diesem Konflikt klar positionierte

Für die konkrete Auswahl der Ziele von DDoS-Attacken und der dadurch betroffenen Webseiten ist eine hohe öffentliche Reichweite entscheidend, sodass ihr Ausfall von einem großen Teil der Bevölkerung wahrgenommen werden kann. Dies gilt vor allem für die oben angesprochenen hacktivistischen Kampagnen, die zu Propagandazwecken genutzt werden.

Abbildung 11: Zahlen und Fakten zur DDoS-Lage 2023 in Deutschland

DDoS Kampagne von NoName057(16)

Der Akteur:
NoName057(16) ist eine hacktivistische Gruppierung, die sich im Zuge des russischen Angriffskrieges auf die Ukraine formierte. Seit Beginn der kriegerischen Auseinandersetzung setzt NoName057(16) primär DDoS-Angriffe ein, um Ziele in der Ukraine, aber auch andere Staaten anzugreifen. Als Begründung für diese DDoS-Angriffe zieht die Gruppierung immer wieder geleistete Unterstützungen, wie u.a Waffenlieferungen an die Ukraine, heran
Um auf ihre Cyberangriffe aufmerksam zu machen und diese öffentlichkeitswirksam darzustellen, nutzt NoName 057(16), wie auch andere hacktivistische Kollektive, intensiv den Messenger Telegram. Über das auf Telegram bereitgestellte Tool DDoSia wird Sympathisanten die Möglichkeit gegeben, an koordinierten DDoS Angriffen mitzuwirken
Für ihre Beteiligung an den erfolgreichen Angriffen können Sympathisanten in der Telegram-eigenen Kryptowährung Toncoin entlohnt werden.

Auswirkungen auf Deutschland:
Im gesamten Berichtszeitraum kündigte NoName057(16) über 140 Angriffe auf deutsche Ziele an Seit August erfolgten dabei regelmäßige Angriffsserien durch den Akteur, wobei die quantitativen Höhepunkte dieser Angriffe in den Monaten September und Oktober festgestellt werden konnten.
Die Angriffe richteten sich primär gegen Webseiten öffentlicher Verwaltungen und Einrichtungen sowie (Strafverfolgungs)Behörden Andere favorisierte Angriffsziele des Akteurs stellten Verkehrsbetriebe und Logistikunternehmen dar
Bereits die ersten Wochen des Jahres 2024 haben gezeigt, dass NoName057(16) seine Aktivitäten gegen deutsche Ziele weiter fortsetzt.

Propaganda durch DDoS:
Die von NoName057(16) beabsichtigten/verursachten Störungen der jeweiligen Webseiten werden immer wieder in der medialen Berichterstattung aufgegriffen. Das Ziel, sich mit diesen Angriffen innerhalb der eigenen Community zu profilieren und hierüber Propaganda zu betreiben, wird von der Gruppierung erreicht .
Generell bleibt aber festzuhalten, dass die meisten der durchgeführten Angriffe keine kritischen Schäden verursachten bzw. mitigiert werden konnten. In einigen Fällen waren die betroffenen Webseiten zeitweise nicht erreichbar.

DDoS Angriffe etablierten sich als Mittel der Wahl für Hacktivisten

Trotz der oben aufgeführten hacktivistischen Aktivitäten im Bereich DDoS ist im kompletten Berichtszeitraum die Anzahl der durch die Deutsche Telekom AG (DTAG) erfassten DDoS-Angriffe erneut gesunken. Insgesamt konnten 22.496 DDoS-Angriffe verzeichnet werden. Dies stellt einen Rückgang von 13,7% im Vergleich zum Vorjahr dar. Während die durchschnittliche Anzahl an Angriffen pro Monat signifikant gesunken ist, stiegen die für die Angriffe verwendeten Bandbreiten und Paketraten an. Gleichzeitig hat aber die durchschnittliche Dauer der registrierten Attacken abgenommen. Die nachfolgende Grafik zeigt die Anzahl der DDoS-Angriffe, die von der Deutschen Telekom AG (DTAG)

registriert wurden.[12] Wie schon in den Jahren 2021 und 2022 zeigte sich auch 2023 ein starker Rückgang an DDoS Angriffen in den Sommermonaten

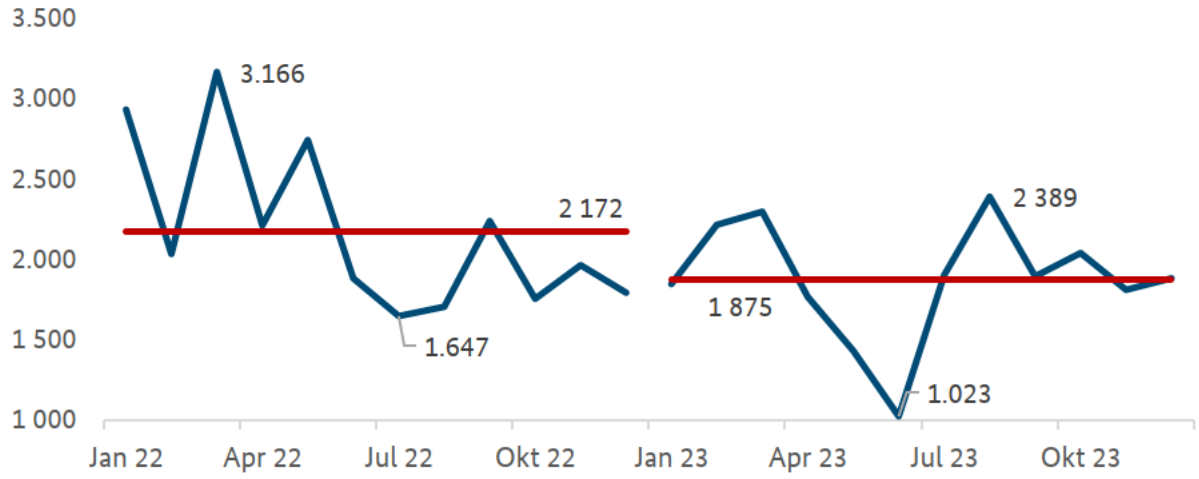

Abbildung 12: Anzahl an DDoS-Angriffen pro Monat in den Netzen der DTAG für die Jahre 2022 und 2023

Im Gegensatz zur DTAG beobachtet der IT-Sicherheitsdienstleister Link11 höhere Fallzahlen, sieht aber gleichzeitig eine Fortsetzung des bereits im letzten Jahr beobachteten Trends: DDoS-Angriffe erreichen innerhalb kürzester Zeit ein kritisches Angriffsniveau. Link11 konnte ebenfalls feststellen, dass DDoS-Akteure bei ausbleibendem Erfolg ihre Angriffe vorzeitig abbrechen, um eigene Ressourcen zu schonen. Gleichzeitig fokussieren sich Cyberkriminelle auf jene Angriffsvektoren, die erfolgsversprechender sind.

DDoS-Angriffe werden zunehmend professioneller ausgeführt.

[12] Daten der DTAG im Berichtszeitraum 01.01.2022 bis 31.12.2023.

4. Quo vadis, Cybercrime?

Die polizeiliche Datenbasis, aber auch die Feststellungen einzelner IT Security-Dienstleister, zeigen für 2023 eine erneut steigende Tendenz bei Cyberangriffen sowohl in quantitativer als auch in qualitativer Hinsicht. Der internationale Aspekt der Cybercrime gewinnt weiter an Bedeutung und hat auch zunehmend Auswirkungen auf nationaler Ebene, was sich in einem weiteren Anstieg der Auslandstaten im Bereich Cybercrime widerspiegelt.

Diese Entwicklung schlägt sich auch in erneut hohen Schadenssummen nieder, die durch Cybercrime verursacht werden. Die vom Bitkom e.V. 2023 erhobenen Gesamtschäden (analoger und digitaler Diebstahl, Industriespionage oder Sabotage) für Unternehmen in Deutschland betragen 205,9 Mrd. Euro.[13] Nach dem bisherigen Spitzenwert von 223,5 Mrd. Euro[14] scheinen sich die Gesamtschäden nunmehr bei über 200 Mrd Euro einzupendeln [15]
Von diesen Gesamtschäden führt Bitkom e.V. fast drei Viertel (72% / 148,2 Mrd. Euro) auf Cyberattacken zurück.[16] Die explizit ausgewiesenen Schäden durch Erpressung mit gestohlenen oder verschlüsselten Daten belaufen sich auf 16,1 Mrd. Euro, was einem Anstieg von 50,5% entspricht.

Der explizit durch Cyberangriffe entstandene Schaden steigt seit 2021 tendenziell an – dies ist auch für die nächsten Jahren zu erwarten.

In 2023 haben gewisse Eintrittsvektoren zu schwerwiegenden Schäden geführt Neben Initial Access Brokern sind in diesem Kontext vor allem Zero Day Schwachstellen sowie spezifische Malware Varianten hervorzuheben. Das Geschäft mit Initial Access in der Underground Economy hat eine besonders hohe Relevanz bei der Schaffung von Tatgelegenheiten Initial Access Broker sind hoch spezialisiert und machen Cyberangriffe für andere Akteure erst möglich. Für eine nachhaltige Strafverfolgung ist die Identifizierung dieser Affiliates umso entscheidender, je arbeitsteiliger Cybertäter agieren

Initial Access Broker sind ein entscheidender Teil der Underground Economy

Das große Gefährdungspotenzial durch Angriffe auf IT-Supply-Chains wird 2023 erneut deutlich. In einer durch IT-Dienstleister digital stark vernetzten Unternehmenslandschaft ergeben sich mehr Gelegenheiten und Angriffspunkte für Täter, die mit einem einzelnen Angriff eine Vielzahl von Unternehmen und Behörden gleichzeitig erreichen und dabei ggf. hohe Schäden verursachen können. Eine Zunahme von IT-Supply-Chains erhöht die Angriffsfläche für Cyberkriminelle, wobei IT-Dienstleister weiterhin im Fokus stehen dürften. Insbesondere durch Ransomware-Angriffe, Data Extortion und das Ausspähen von Daten ergibt sich eine weiterhin ernstzunehmende Gefahr.

[13] Bitkom e.V. (2023). Wirtschaftsschutz 2023. Online abrufbar unter: **https://www.bitkom.org/** Anmerkung: Die im Bericht erhobenen Zahlen beziehen sich primär auf das Jahr 2022
[14] Cybercrime Bundeslagebild, Bundeslagebild 2021
[15] Aufgrund der Aufnahme eines neuen Kostenpunkts in den Wirtschaftsschutzbericht 2023 sollte hier kein direkter Vergleich der Gesamtschadenssummen mit den Vorjahren erfolgen.
[16] Die restlichen Schadenssummen sich nicht explizit auf Schäden durch Cybercrime im engeren Sinne zurückzuführen.

Angriffe auf IT-Supply-Chains bergen ein hohes Gefährdungspotenzial.

Spätestens seit Veröffentlichung von ChatGPT im November 2022 werden KI Tools auch für kriminelle Zwecke missbraucht Bislang stehen dabei vor allem große Sprachmodelle im Fokus, deren einfache Anwendung und enorme Leistung sie zu wertvollen Werkzeugen für verschiedenste Aufgaben macht KI spielt dabei eine grundlegende Rolle für neue, aber auch bestehende Bedrohungsakteure: Einerseits wird die Einstiegshürde für cyberkriminelle Aktivitäten bei Nutzern mit wenig IT Knowhow gesenkt, andererseits vorhandene kriminelle Fähigkeiten verstärkt So beobachtet Microsoft auf Basis der Nutzungsaktivitäten ihrer KI Tools, dass viele cyberkriminelle Akteure ihr bisheriges Repertoire schon heute durch generative KI erweitern [17]

Delikte aus dem Bereich Cybercrime können mit KI Unterstützung nicht nur automatisiert, also wesentlich schneller, sondern auch in größerem Ausmaß durchgeführt werden KI generierte Inhalte werden dabei noch professioneller und authentischer, wodurch z B Phishing Mails noch schwerer von legitimen Mails zu unterscheiden sind Gemäß dem gewinnmaximierenden Antrieb der Underground Economy werden nicht nur entsprechende KI gestützte Dienstleistungen und (kompromittierte) Zugänge zu gängigen KI Tools angeboten, sondern auch „dunkle“ KI Modelle wie WormGPT, die speziell für kriminelle Zwecke entwickelt wurden Langfristig werden sich KI Modelle in ihrer Fähigkeit und Leistung kontinuierlich verbessern und weiterentwickeln Daher könnte KI im Bereich Cybercrime als Katalysator wirken und einen enormen Anstieg der Kriminalität auslösen.

Dieselben Fähigkeiten, die zur Verbesserung von cyberkriminellen Aktivitäten genutzt werden, können jedoch auch zur Stärkung der IT Sicherheit beitragen So kann KI unterstützen, Phishing zu erkennen, Sicherheitslücken zu schließen oder Cyberangriffe frühzeitig zu detektieren.

KI steigert die Qualität und Quantität von Cyberangriffen – kann aber auch eine Chance für die Cybersicherheit sein

In den letzten beiden Jahren übertrugen sich geopolitische Konflikte in die digitale Welt und mündeten in einem starken Aufschwung hacktivistischer Aktivitäten, die sich am offensichtlichsten in DDoS Angriffen niederschlagen. Weitere (geo)politische Konflikte haben das Potenzial, neue ideologisch motivierte hacktivistische Strömungen hervorzubringen, die auch in Deutschland wirtschaftliche und/oder gesellschaftliche Abläufe zumindest temporär in erheblichem Maße betreffen können.

Die Grenze zwischen politisch ideologischer und finanziell motivierter Cyberkriminalität verschwimmt zunehmend. Wie das Beispiel DDoSia zeigt, ermöglicht die monetäre Entlohnung von Sympathisanten gegen Rechenleistung hacktivistische Aktivitäten in dem Ausmaß, wie sie 2023 stattfanden. Es bleibt abzuwarten, wie sich das Zusammenspiel politisch und finanziell motivierter Cyberkriminalität weiterentwickelt und ob ihre ursprüngliche Motivation bestehen bleibt

Mit steigenden Cybercrime as a Service Angeboten und einer Vereinfachung komplexerer Angriffe, u.a. mittels KI, sind perspektivisch auch andere Angriffsformen als verhältnismäßig technisch einfach durchzuführende DDoS-Angriffe erwartbar.

[17] Microsoft Threat Intelligence Blog (14.02.2024). Online abrufbar unter: **https://www.microsoft.com/en us/security/blog/**

Geopolitische Konflikte haben Einfluss auf die digitale Welt und fördern Hacktivismus.

Malware entwickelt sich unablässig weiter. Insbesondere im Bereich der Ransomware Entwicklung wird dabei häufig von vorangegangenen Ransomware-Varianten Gebrauch gemacht. Besonders über eine gewisse Zeit etablierte Varianten wie Babuk Locker, Conti, LockBit oder HIVE bilden häufig die Grundlage für neue Varianten. Die Leaks von Quellcode ermöglichen es auch weniger versierten Akteuren, Ransomware einzusetzen. Die Wiederverwendung bereits existierender Quellcodes, an welchen ggf. einige Anpassungen vorgenommen werden, führt zu neuen und leicht verfügbaren Ransomware Varianten. Von Ransomware Quellcode geht auch nach der Zerschlagung oder Auflösung von Ransomware-Gruppierungen weiterhin eine Gefahr aus.

Ransomware bleibt die primäre Bedrohung Schadsoftware wird immer leichter verfügbar und entwickelt sich permanent weiter.

Das Jahr 2023 war geprägt von einer Vielzahl an Ermittlungserfolgen, die sich primär gegen die Infrastruktur der Täterschaft richteten. Unter anderem wurden ein Krypto-Mixer und mehrere kriminelle Marktplätze abgeschaltet, einer der relevantesten Trojaner in seiner Aktivität stark eingeschränkt sowie die Erpressungsaktivitäten einiger Ransomware-Gruppierungen gestoppt. Infrastrukturmaßnahmen sorgen für eine entscheidende Störung der kriminellen Aktivitäten, verhindern künftige Angriffe, entziehen der Underground Economy finanzielle Mittel und führen durch Analysen sichergestellter Systeme und Daten zu weiteren Ermittlungsansätzen. Daraus können sich wertvolle Informationen zur eingesetzten Malware ergeben, die beispielsweise die Entwicklung von Ransomware-Decryptoren ermöglichen und bereits Geschädigten bei der Wiederherstellung ihrer Systeme helfen.

Wie auch der große Anteil an Auslandstaten im Bereich der Cyberkriminalität zeigt, ist die oftmals nur lose verbundene Täterschaft nicht nur im Bereich Ransomware weltweit verteilt und befindet sich zudem häufig in Staaten, in denen sie geduldet oder sogar geschützt werden (safe haven) Polizeiliche Maßnahmen gegen die von den Tätern genutzte und für Strafverfolgungsbehörden erreichbare Infrastruktur bilden daher neben personellen Ermittlungen eine effektive Strategie, um der Cyberkriminalität nachhaltiger zu begegnen

Die 2023 erzielten Ermittlungserfolge bestätigen die herausgehobene Bedeutung des Infrastrukturansatzes und der internationalen Zusammenarbeit bei der Verfolgung der Cybertäter Auch künftig müssen deutsche Strafverfolgungsbehörden eng mit anderen Ländern zusammenarbeiten, um die Infrastruktur von Cybertätern zu übernehmen und ggf personenbezogene Ermittlungen einleiten zu können

Internationale Kooperation in der Strafverfolgung zahlt sich aus – der Infrastrukturansatz zeigt Wirkung.

Für eine möglichst effektive und nachhaltige Bekämpfung der schwerwiegenden Bedrohungen aus dem Cyberraum ist eine ganzheitlichere Betrachtung und Vorgehensweise erforderlich. Dies bedeutet, neben dem bereits etablierten Handlungsfeld im Bereich der Strafverfolgung auch die (polizeilichen) Handlungsmöglichkeiten zu stärken, um herausragende Cybergefahren für Staat und Gesellschaft besser abwehren zu können.

Impressum

Herausgeber
Bundeskriminalamt, 65173 Wiesbaden

Stand
Mai 2024

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.