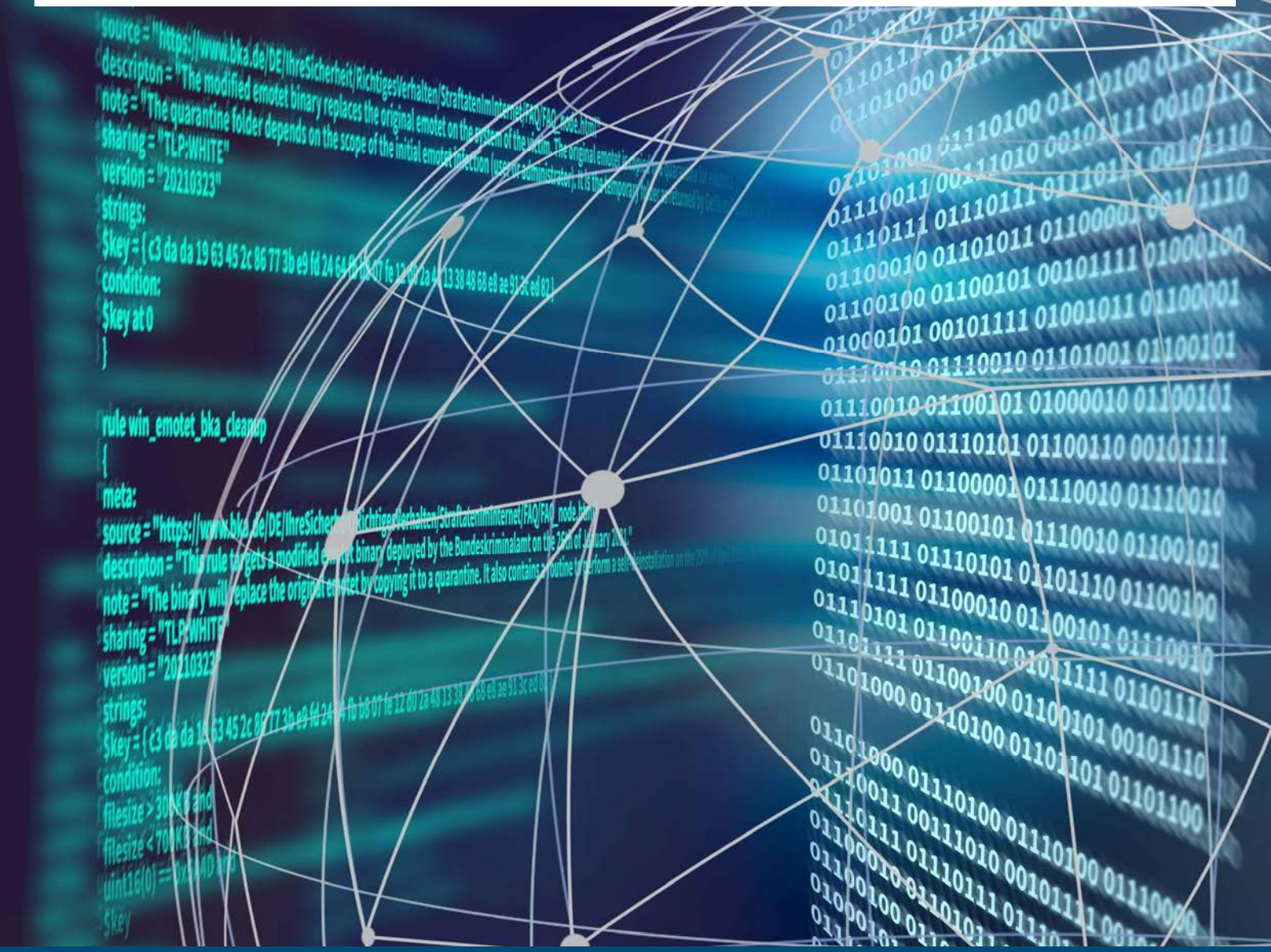
Bundeskriminalamt

BKA



Cybercrime

Bundeslagebild 2022

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 die diesbezüglichen Ergebnisse polizeilicher Strafverfolgungsaktivitäten ab.

Schwerpunkt des Bundeslagebild 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 (sogenannte Cybercrime im weiteren Sinne, CCiwS), werden 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). Hier 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 Cybercrime 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 2022 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

Rückgang der erfassten Cyberstraftaten um 6,5% (Inlands-PKS). Auslandstaten steigen an.

Die Aufklärungsquote für Cybercrime bewegt sich mit ca. 29% auf dem Niveau des Vorjahres.

Der russische Angriffskrieg auf die Ukraine birgt auch im Cyberraum massives Eskalationspotential.

Ransomware bleibt primäre Bedrohung für Unternehmen und öffentliche Einrichtungen.

Phishing ist Haupteintrittsvektor für Schadsoftware und passt sich aktuellen gesellschaftlich relevanten Themen an.

DDoS-Angriffe werden effizienter.

Zum Jahresende 2022 erfolgten vermehrt Angriffe auf das Bildungswesen.

Die vom Bitkom e.V. bezifferten Schäden u.a. durch Cyberangriffe belaufen sich auf 202,7 Mrd. Euro.

Weniger Unternehmen gehen auf Erpressungsforderungen von Cybertätern ein.

1.1 FOKUS 2022 – AUSWIRKUNGEN DES RUSSISCHEN ANGRIFFSKRIEGES AUF DEN CYBERRAUM

Der russische Angriffskrieg

Am 24.02.2022 begann Russland einen groß angelegten militärischen Angriff auf die Ukraine. Diese Auseinandersetzung findet auch im Cyberraum statt.

Cyberangriffe im Kontext des Krieges sind auf eine Vielzahl unterschiedlicher Akteure zurückzuführen. Neben staatlichen Gruppierungen spielen auch politisch und ideologisch motivierte Cyber-Akteure, sogenannte Hacktivisten, eine zentrale Rolle.

DDoS

DDoS-Angriffe nehmen einen hohen Stellenwert als Mittel der Cyberkriegsführung ein: Seit Kriegsbeginn führen Akteure beider Kriegsparteien zahlreiche Überlastungsangriffe gegen strategische Ziele durch.

Malware

Im Vorfeld und während des Russland-Ukraine-Kriegs fanden mehrere gezielte Kampagnen russischer Cyber-Akteure statt. Diese verfolgten das Ziel, ukrainische Regierungs- und Militär- Systeme sowie Kritische Infrastrukturen (KRITIS) mittels Malware anzugreifen und zu stören.

Hacktivismus

Im Zuge des Russland-Ukraine-Kriegs nehmen hacktivistische Akteure auf beiden Seiten eine zentrale Rolle ein und setzen bei Angriffen unterschiedliche Modi Operandi ein, darunter DDoS-Angriffe, Hack & Leak, Defacements, u.v.m.

Bedrohungsszenarien

Seit Beginn des Russland-Ukraine-Kriegs besteht für Kritische Infrastrukturen in der Ukraine sowie in deren Unterstützerstaaten (auch Deutschland) eine erhöhte Gefährdung, Ziel russischer Cyberangriffe zu werden.

Der Cyberangriff auf das amerikanische Unternehmen ViaSat, Betreiber des Satellitennetzwerks KA-SAT, steht exemplarisch für die Gefahr von Kollateralschäden bei Cyberangriffen mit Auswirkungen auf Kritische (EU-) Infrastrukturen.

Begleitet werden der Angriffskrieg Russlands und die maliziösen Aktivitäten im Cyberraum darüber hinaus durch umfangreiche Desinformationsaktivitäten.

1.2 BEDEUTENDE SACHVERHALTE 2022 IN DEUTSCHLAND

Januar

Am 13.01.2022 wurde der Großteil der Server des Medizin Campus Bodensee bei einem Ransomware-Angriff verschlüsselt. Infolgedessen konnten keine neuen Notfälle aufgenommen werden und eine ambulante Patientenversorgung war auch Tage später nicht möglich.

März

Am 11.03.2022 erfolgte durch Anonymous Deutschland der erste gezielte Cyberangriff auf ein deutsches KRITIS-Unternehmen im Zusammenhang mit dem Russland-Ukraine-Krieg. Die Gruppierung wollte mit dem Diebstahl und der Zerstörung von Daten bei der deutschen Tochter des russischen Mineralölkonzerns Rosneft verhindern, dass das russische Mutterunternehmen über ihre Tochtergesellschaft Sanktionen der EU umgeht.

April

Die pro-russische Gruppierung Killnet führte seit Frühjahr 2022 fortlaufende DDoS-Kampagnen gegen die Ukraine und Unterstützerstaaten durch, darunter auch Deutschland. Anlass hierfür waren u.a. Sanktionen und Waffenlieferungen an die Ukraine.

April

Der größte und umsatzstärkste illegale Darknet-Marktplatz „Hydra Market“ wurde in Folge einer international koordinierten Operation durch das BKA abgeschaltet. Über 50 Server, 1,8 Petabyte Daten und 543 Bitcoin (ca. 23 Mio. Euro) wurden sichergestellt.

Juli

Im Juli 2022 erlangte die Gruppierung LockBit Zugang zu den Systemen des Unternehmens Continental und exfiltrierte Daten in einer Gesamtmenge von ca. 40 TB, die für 50 Mio. US-Dollar im Darknet angeboten wurden. Die geleakten Daten enthielten vertrauliche Informationen wie Strategiepläne, Korrespondenz und Kundendaten.

September

Die von der Bundesregierung beschlossene Energiepauschale wurde im September in einer Phishing-Kampagne aufgegriffen. Hierbei versendeten die Täter Phishing-Nachrichten, in denen sie sich als ein Finanzinstitut bzw. das Bundesministerium für Finanzen ausgaben.

September

Nachdem die Infrastruktur der Malware Emotet Anfang 2021 zerschlagen wurde, kehrte diese 2022 mit neuen Eigenschaften zurück. Im Herbst 2022 lag das Volumen täglich versendeter E-Mails bei rund 100.000. Dies entspricht dem Durchschnitt vor dem Takedown.

November

Im November 2022 wurde die Universität Duisburg-Essen Ziel eines Ransomware-Angriffs der Gruppierung ViceSociety. Zusätzlich kam es zu DDoS-Angriffen auf die Webseite der Universität.

Dezember

Im Zuge der international koordinierten „Operation Power Off“ wurden unter Beteiligung des BKA im Dezember ca. 50 „DDoS-as-a-Service-Dienste“ abgeschaltet.

2. Polizeiliche Kriminalstatistik

Die Polizeiliche Kriminalstatistik (PKS) ist die bundesweit geführte und qualitätsgesicherte Ausgangsstatistik nach Abschluss polizeilicher Ermittlungen. Aufgrund des erheblichen Dunkelfeldes im Bereich Cybercrime (CC), das in Studien auf bis zu 91,5% geschätzt wird,[1] hat die PKS allerdings lediglich eine begrenzte Aussagekraft hinsichtlich der tatsächlich in Deutschland verübten Cyber-Straftaten. Sie ist insofern eine Datenbasis, auf der vor allem Trendaussagen zur Entwicklung der Cyberkriminalität getroffen werden können.

Innerhalb der PKS sind die relevanten Cybercrime-Delikte im sogenannten Summenschlüssel Cybercrime zusammengefasst. Nachdem für das Jahr 2021 ein Rückgang bei den registrierten Straftaten insgesamt und ein Anstieg bei den Cybercrime-Delikten festgestellt werden konnte, kehrt sich diese Entwicklung im Jahr 2022 um: Die Gesamtanzahl der in der PKS erfassten Straftaten steigt im Vergleich zum Vorjahr in 2022 um 11,5% an; bei den Cyber-Straftaten ist ein Rückgang um 6,5% festzustellen.
Der Anteil von Cybercrime-Delikten an den Straftaten insgesamt beläuft sich im Jahr 2022 auf 2,4% (vgl. 2021: 2,9%).

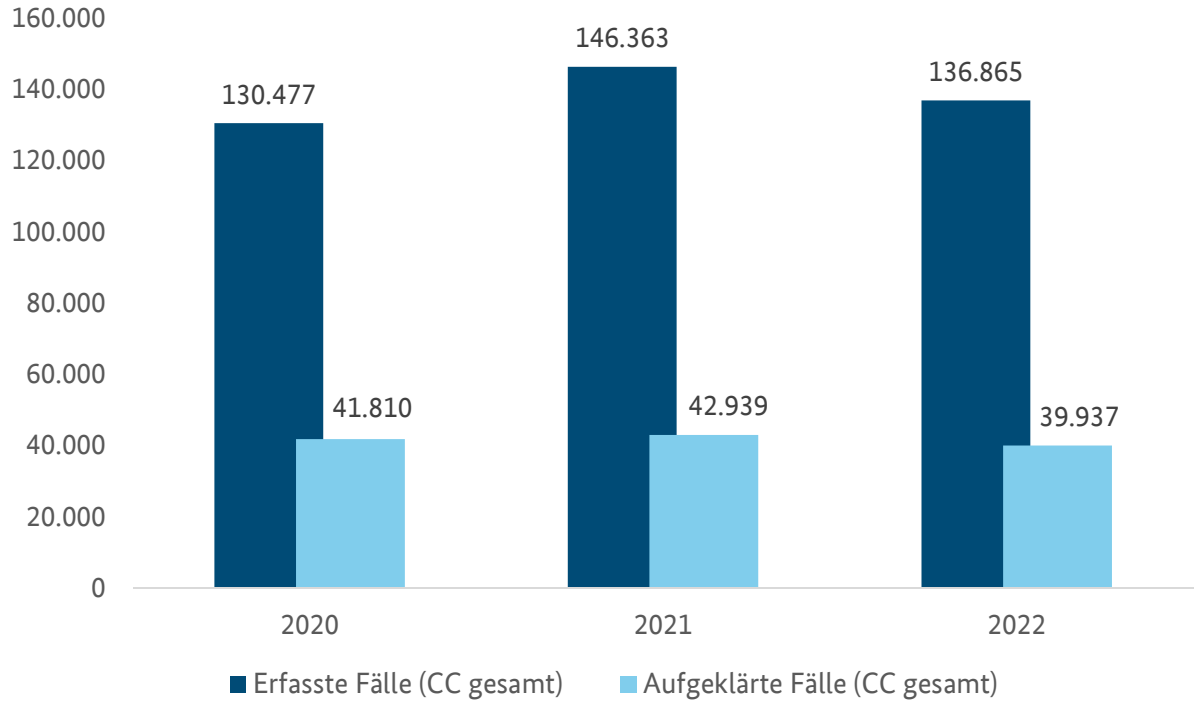


Abbildung 1: Erfasste und aufgeklärte Cybercrime-Fälle in Deutschland von 2020 bis 2022

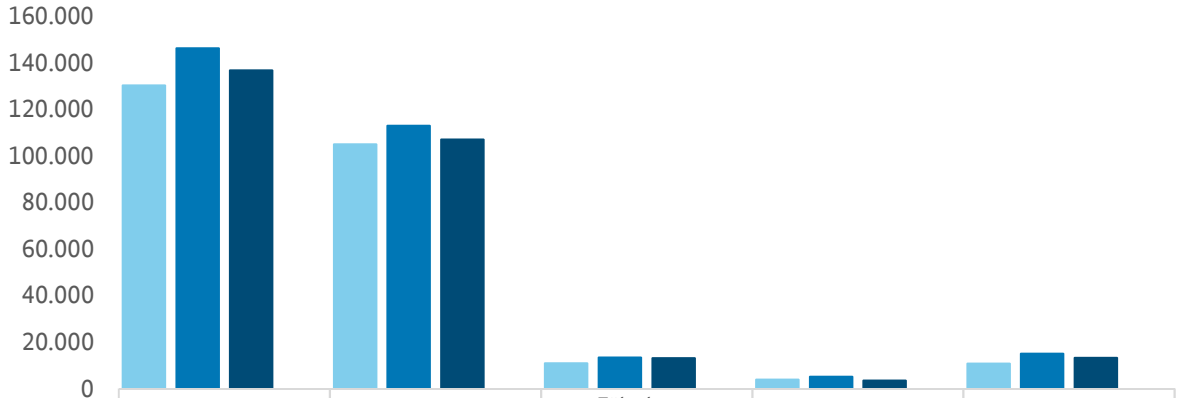
Nach Einführung des neuen Straftatbestands des §127 StGB (Betreiben krimineller Handelsplattformen im Internet) wird dieser seit dem 01.01.2022 in der PKS separat erfasst, ohne dass bis zum jetzigen Zeitpunkt eine Zuordnung zum Summenschlüssel Cybercrime erfolgte. Bemerkenswert an den unten aufgeführten Daten zu diesem Deliktsfeld ist, dass zehn der 13 registrierten Fälle aufgeklärt werden konnten, was einer Aufklärungsquote von 76,9% entspricht.

[1] Dreißigacker, A., von Skarczinski, B. & Wollinger, G. R. (2021). Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer Folgebefragung 2020, KFN-Forschungsberichte No. 162. Hannover: KFN.; online abrufbar unter: **https://kfn.de/publikationen/kfn-forschungsberichte/**

	Anzahl erfasster Fälle (absolut)	Differenz erfasster Fälle zum Vorjahr	Prozentuale Differenz erfasster Fälle zum Vorjahr	Aufgeklärte Fälle (absolut)	Differenz aufgeklärter Fälle zum Vorjahr	Aufgeklärte Fälle in %, Aufklärungs-Quote (AQ)	Veränderung AQ (Prozent-punkte)
Summenschlüssel Cybercrime							
2020	130.477	7.677	6,3%	41.810	2.731	32%	0,2
2021	146.363	15.886	12,2%	42.939	1.129	29,3%	-2,7
2022	136.865	-9.498	-6,5%	39.937	-3.002	29,2%	-0,1
Betreiben krimineller Handelsplattformen im Internet § 127 StGB							
2022	13	-	-	10	-	76,9%	-

Abbildung 2: Relation erfasster und aufgeklärter Fälle in Deutschland von 2020 bis 2022

Generell weisen nicht nur der Summenschlüssel Cybercrime als Ganzes, sondern auch alle dort enthaltenen cyberspezifischen Delikte (Computerbetrug, Fälschung beweiserheblicher Daten, Datenveränderung/Computersabotage, Ausspähen von Daten/Datenhehlerei) im Vergleich zum Vorjahr Rückgänge auf.



	CC gesamt	Computerbetrug	Fälschung beweiserheblicher Daten, Täuschungen im Rechtsverkehr bei Datenverarbeitung	Datenveränderung, Computersabotage	Ausspähen von Daten einschl. Vorbereitungs-handlungen und Datenhelerei
2020	130.477	105.049	10.895	3.770	10.763
2021	146.363	113.002	13.390	5.053	14.918
2022	136.865	107.165	13.043	3.451	13.206
Diff. zu 2021	-6,5%	-5,2%	-2,6%	-31,7%	-11,5%

Abbildung 3: Fallaufkommen der Cyberstraftaten nach Deliktsbereich seit 2020

Die PKS weist auf den ersten Blick auf einen (scheinbaren) Rückgang der registrierten Cyberstraftaten (-6,5%) bei nahezu gleichbleibender Aufklärungsquote im Inland hin. Dies spiegelt jedoch nicht realitätsgetreu die tatsächliche Entwicklung im Deliktsbereich Cybercrime wider. In der Inlands-PKS werden Fälle, bei denen zwar Schäden in Deutschland verursacht werden, aber der Aufenthaltsort des Täters im Ausland liegt oder unbekannt ist (sogenannte Auslandstaten), nicht berücksichtigt.
Daher wurde zum 01.01.2020 die separate Erfassung dieser Auslandstaten in der PKS eingeführt. Aufgrund etwaiger Ungenauigkeiten bei der Erfassung insbesondere zu Beginn dieser Erhebungsphase wurde auf die Abbildung absoluter Fallzahlen verzichtet. Die gewählte indexbasierte Darstellung (siehe Abbildung 4) ermöglicht dennoch Trendaussagen:

- Auslandstaten steigen seit 2020 – dem Jahr der erstmaligen Erfassung – stetig an. Im Vergleich zum letzten Jahr ist hier ein Anstieg von über 8% festzustellen, während die Inlands-PKS einen Rückgang der Fallzahlen ausweist.

- Die in 2022 festgestellten Auslandstaten übersteigen die im letzten Jahr registrierten Fälle der Inlandstaten.

- Innerhalb der Auslandstaten ist der Deliktsbereich Cybercrime überproportional stark vertreten. So wird bei den Cyberstraftaten mit festgestelltem Täterhandeln in Deutschland ein Anteil von 2,4% an den Gesamtstraftaten registriert, während dieser Anteil bei den Auslandstaten ca. zehnmal so hoch ist. Fast ein Viertel aller registrierten Auslandstaten betreffen den Bereich Cybercrime.

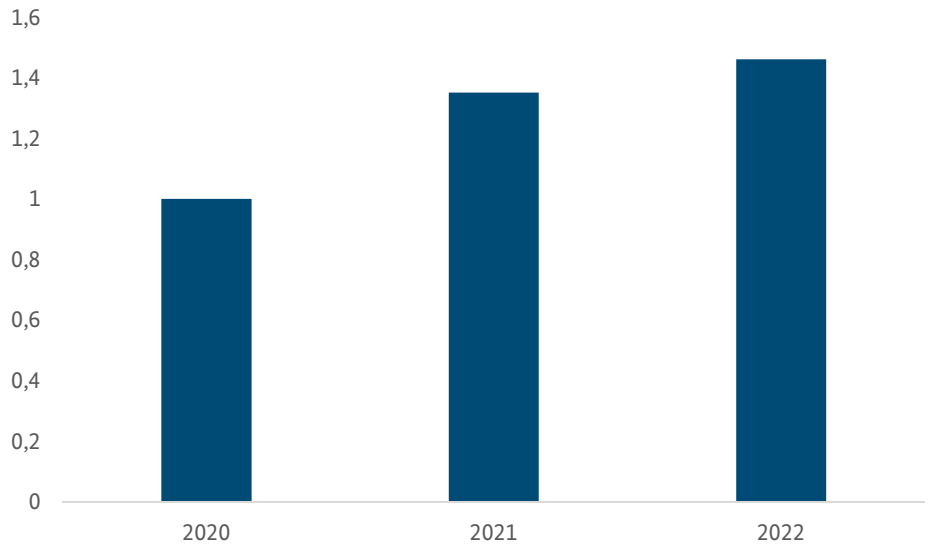


Abbildung 4: Erfasste Auslandstaten Cybercrime (Der Indexwert zeigt die Veränderung der erfassten Auslandstaten. Dabei wird das Jahr 2020 als Basiswert auf 1 festgelegt. Die Werte der Folgejahre stehen in Relation zu diesem Basiswert und zeigen damit den Trend der steigenden Auslandstaten.)

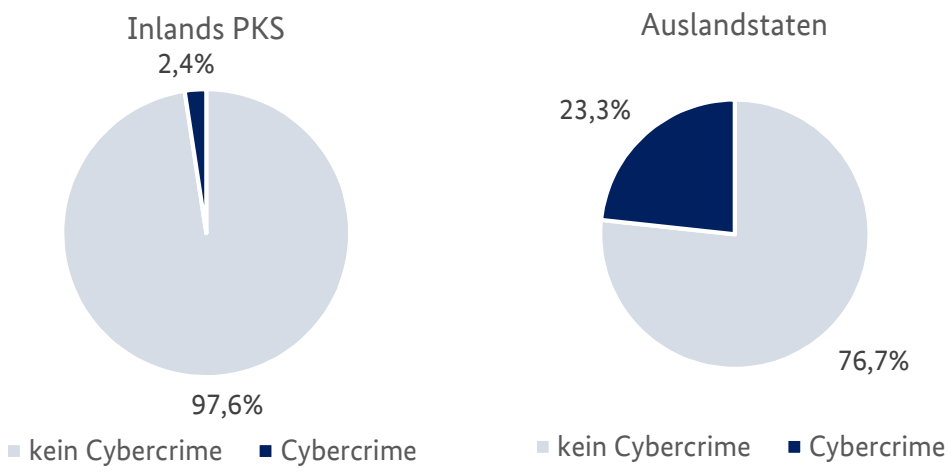


Abbildung 5: Anteil Cybercrime-Delikte an den Gesamtstraftaten

Die rückläufige Entwicklung der Cybercrime-Fallzahlen der Inlands-PKS kann mit der Lockerung der Corona-Schutzmaßnahmen begründet werden. Während die starke Zunahme des Onlinehandels und des mobilen Arbeitens in den Vorjahren zusätzliche Angriffsmöglichkeiten für Cybertäter boten, verlagerten sich 2022 Teile des Kriminalitätsgeschehens wieder zunehmend zurück in die analoge Welt. Ohne Aufhebung der Corona-Schutzmaßnahmen wäre von einem erneuten Anstieg der Fallzahlen der Inlands-PKS sowie von einem stärkerem Anstieg der Auslandstaten auszugehen. Faktisch verbleiben die Fallzahlen des Phänomenbereichs 2022 auf einem hohen Niveau und liegen weiterhin über dem festgestellten Fallaufkommen von 2020.

Der hohe Anteil an Auslandstaten stellt die im Phänomenbereich ermittelnden Polizeibehörden vor große Herausforderungen. Dies drückt sich unter anderem in der niedrigen Aufklärungsquote aus, die sich im Bereich der Auslandstaten im unteren einstelligen Bereich bewegt. So fehlen in der digitalen Welt häufig geeignete Ermittlungsansätze zur Täteridentifizierung, wodurch der Aufenthaltsort der Täter vielfach ungeklärt bleibt. Selbst bei vorliegenden Ermittlungsansätzen können juristische Hürden und mangelnde Kooperationsbereitschaft im Ausland die Strafverfolgung erschweren oder sogar gänzlich verhindern. Dies kann Cybertätern einen Rückzugsraum („safe haven“) bieten.

Knapp ein Viertel aller Auslandstaten der PKS sind der Cyberkriminalität zuzuordnen. Deren Aufklärung stellt höhere Anforderungen an die Strafverfolgungsbehörden.

3. Relevante Phänomenbereiche

3.1 UNDERGROUND ECONOMY

Die Underground Economy (UE) ist primärer Umschlagplatz für illegale Waren und unrechtmäßig erlangte Daten, wie kompromittierte Zahlungs- und Zugangsdaten, sowie für verschiedenste Cybercrime-as-a-Service-Angebote (Zergliederung und Spezialisierung einzelner „Teiltatbeiträge“ des Phänomenbereichs Cybercrime).

Die Angebote der UE besitzen auch weiterhin eine hohe Bedeutung für den Cyber-Bereich, da sie vielfach Ausgangspunkt für die Begehung weiterer Cybercrime-Delikte sind. Auch der Ausbau des arbeitsteiligen Cybercrime-as-a-Service-Modells setzte sich 2022 weiter fort. Exemplarisch können folgende Angebote der UE im Kontext CCieS aufgeführt werden:

Service	Preis in US $ (gesamt oder pro Nutzungszeitraum / pro Einheit)	
BankingTrojaner *(Malware, die Bankdaten abgreift)*		
▪ **Desktop-Version**	1.000 - 10.000 $	bei Kauf
▪ **Mobile-Version**	1.000 - 10.000 $	bei Kauf
Bulletproof Hosting *(Siehe QR-Code)*		
▪ **Shared**	5 - 50 $	pro Monat bei Miete
▪ **Dedicated**	12,50 – 3.300 $	pro Monat bei Miete
Counter-AV-Service *(Siehe QR-Code)*	0,15 - 85 $	pro Monat und 300 Scans
Crypting *(Siehe QR-Code)*	0 - 200 $ 30 – 2.900 $	bei Kauf von einem Crypt Wochen-Abo mit 50 Crypts pro Tag
DDoS-as-a-Service *(Services zum Durchführen von DDoS-Angriffen)*	50 – 2.600 $	pro Monat bei Miete
Infection-on-Demand *(Phishing-Services o.ä.)*	100 – 600 $	pro Monat
Mining Bots *(Malware, die auf infizierten Endgeräten Kryptowährung „schürft“)*	50 – 300 $ 500 – 3.500 $	pro Monat bei Miete bei Kauf
RAT (Remote Administration Tool) *(Programm, dass Fernzugriffe auf ein Zielsystem ermöglicht)*	3 - 530 $ 40 - 8.000 $	pro Monat bei Miete bei Kauf
Stealer Logs *(Protokolldateien ausgespähter Daten eines infizierten Systems, z.B. Zugangsdaten)*	0,01 - 40 $ 400 – 3.000 $	pro Stück pro Monat für Abonnement

Abbildung 6: Übersicht krimineller Services der Underground Economy

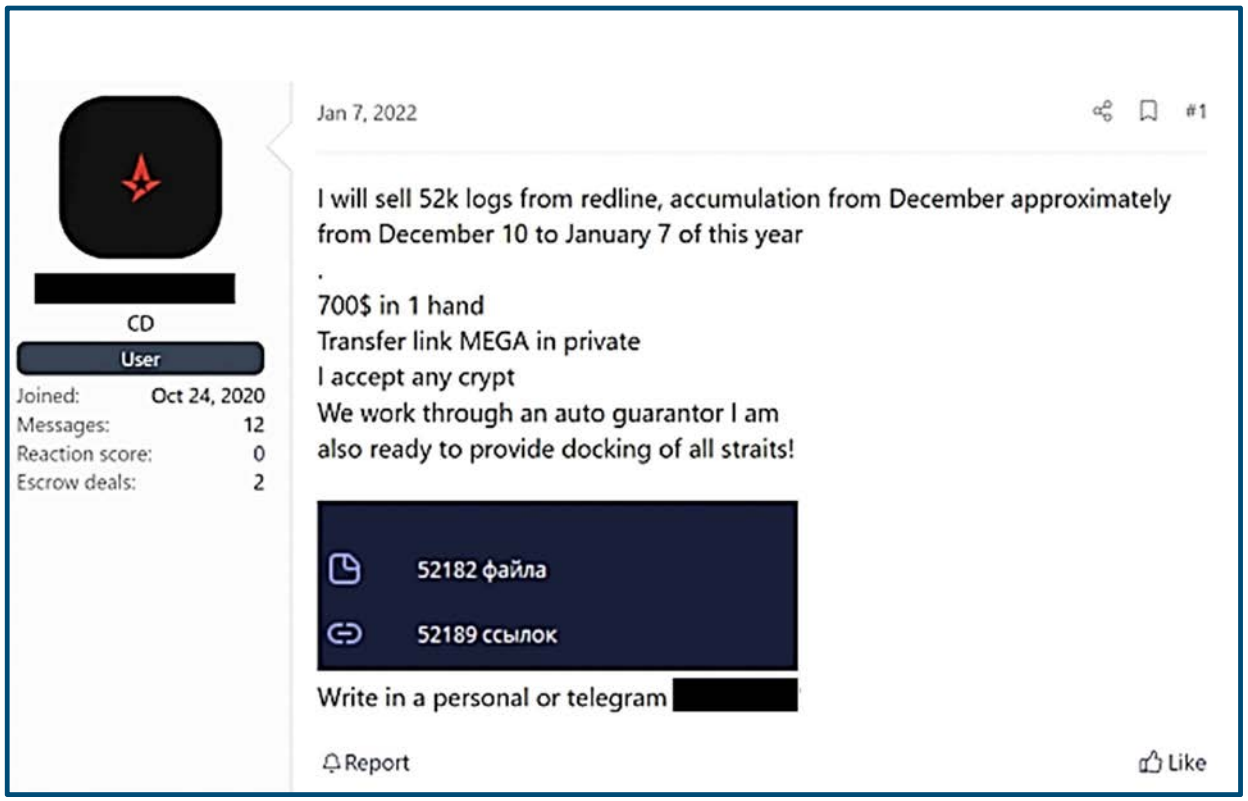


Abbildung 7: Beispielhaftes Angebot für Stealer-Logs

Laut Erkenntnissen des Blockchain-Analyse-Unternehmens Chainalysis betrug der Gesamtumsatz auf allen unternehmensseitig ausgewerteten Darknet-Marktplätzen im Jahr 2022 1,5 Mrd. US-Dollar und war damit im Vergleich zum Vorjahr rückläufig (2021: 3,1 Mrd. US-Dollar Umsatz).[2] Dies ist unter anderem auf den Takedown des Darknet-Marktplatzes Hydra Market zurückzuführen. Diese Plattform war der umsatzstärkste Marktplatz in 2022 trotz des Ermittlungserfolgs im April vergangenen Jahres. Nach dessen Schließung sanken die täglichen Umsätze illegaler Marktplätze insgesamt erheblich und näherten sich erst im Verlauf der zweiten Jahreshälfte wieder dem vorherigen Niveau an.

[2] Chainalysis (2023). The 2023 Crypto Crime Report

Takedown Hydra Market

Das Ermittlungsverfahren:

Bei Hydra Market handelte es sich um den weltweit größten und umsatzstärksten illegalen Darknet-Marktplatz, welcher seit mindestens 2015 bestand. Auf dem Marktplatz waren über 17 Mio. User und 21.000 Händler-Accounts registriert. Der Schwerpunkt der russischsprachigen kriminellen Verkaufsplattform lag auf dem Handel mit illegalen Betäubungsmitteln, deren An- und Verkauf ausschließlich in Russland und einigen Staaten der ehemaligen Sowjetunion erfolgte. Zudem wurden über den Marktplatz ausgespähte Daten, gefälschte Dokumente sowie digitale Dienstleistungen und Möglichkeiten zur Verschleierung illegaler Gewinne angeboten. Im Zuge der Ermittlungen wurde festgestellt, dass sich die technische Infrastruktur des Markplatzes ausschließlich in Deutschland befand.

Das Ermittlungsverfahren des BKA war in erster Linie von der Umsetzung innovativer und technisch hochkomplexer Maßnahmen geprägt, welche die Identifizierung und Aufklärung der technischen Infrastruktur des Hydra Market sowie die Gewinnung beweiserheblicher Daten und kriminalistisch relevanter Erkenntnisse ermöglichten und in der erfolgreichen und nachhaltigen Abschaltung des Darknet-Marktplatzes mündeten.

Die Auswirkungen:

Im Zuge des Takedowns am 05.04.2022 ist die Beschlagnahme von über 50 Servern und ca. 1,8 Petabyte Daten, die der Infrastruktur des Marktplatzes zugeordnet wurden, sowie die Sicherstellung der finanziellen Mittel des Marktplatzes (mehr als 543 BTC, umgerechnet ca. 23 Mio. Euro zum Zeitpunkt der Sicherstellung) gelungen. Neben dem Reputationsverlust für die Betreiber und Administratoren des Marktplatzes führten die Maßnahmen zu einem enormen finanziellen Verlust. Wie die Reaktionen der Underground Economy zeigen, hat die Szene die Abschaltung des langjährigen Marktplatzes durch Strafverfolgungsbehörden überwiegend für unmöglich gehalten. Eine Neueröffnung des Marktplatzes wurde bislang nicht festgestellt.

Abbildung 8: Seizure Banner Hydra Market

3.2 PHISHING

Das in der Underground Economy etablierte Cybercrime-as-a-Service-Modell beinhaltet auch Angebote für Eintrittsvektoren in Zielsysteme, darunter Phishing. Dieser Modus Operandi ist trotz seiner verhältnismäßig einfachen Funktionsweise weiterhin eine ernstzunehmende Bedrohung für Unternehmen und Privatpersonen hinsichtlich des Abgreifens von Zugangsdaten sowie des Einschleusens von Schadsoftware. Phishing-Mails waren 2022 beispielsweise der häufigste Eintrittsvektor für Ransomware.[3]

Phishing unterliegt einer besonders hohen Dynamik in Bezug auf Modi Operandi und greift hierbei besonders schnell aktuelle gesellschaftliche Narrative auf. Festgestellt wurde unter anderem, dass vermehrt Archiv-Dateien und maliziöse QR-Codes via Phishing-Mails distribuiert werden. Phishing-as-a-Service-Tools bieten zudem die Möglichkeit, dass Multi-Faktor-Authentifizierungen auch von Cyberkriminellen mit wenig technischem Know-How umgangen werden können und somit auch Logindaten auf Webseiten weniger gut geschützt sind. Inhaltlich nahmen Phishing-Mails auch im Jahr 2022 häufig auf aktuelle gesellschaftliche Entwicklungen Bezug, z.B. den russischen Angriffskrieg oder die Energiepauschale.

Die weltweit am häufigsten für Phishing genutzte Branche war laut der Anti-Phishing-Working-Group (APWG)[4], wie bereits 2021, das Finanzwesen.[5] In Deutschland warnte die Verbraucherzentrale ebenfalls am häufigsten vor Phishing-Mails, die Unternehmen des Finanzsektors nachahmen.[6] Dahingegen zählten zu den weltweit am häufigsten für Phishing imitierten Absendern DHL, LinkedIn, Microsoft, Google und Netflix.[7]

Folgende Grafik zeigt Entwicklungen im globalen Phishing-Aufkommen:

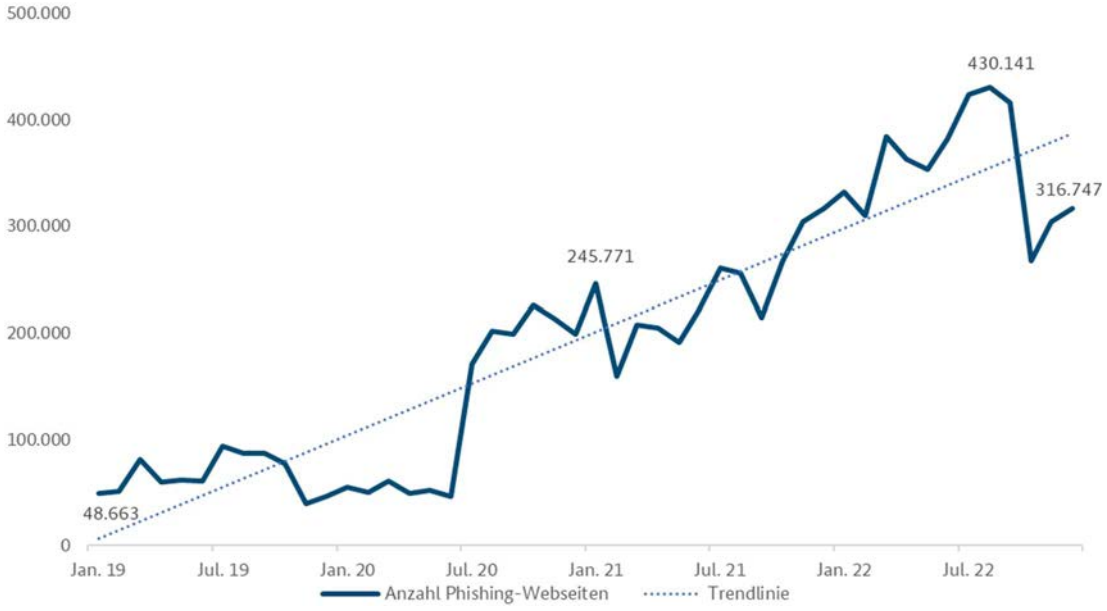


Abbildung 9: Anzahl der durch die Anti-Phishing-Working-Group festgestellten Phishing-Seiten seit 2019

[3] Vgl. Coveware. Quartalsberichte 2022; online abrufbar unter **https://www.coveware.com/blog**
[4] Internationale Arbeitsgruppe mit mehr als 3.000 Mitgliedern weltweit zur Bekämpfung von Phishing und Betrugsdelikten
[5] Anti-Phishing-Working-Group. Quartalsberichte 2022; online abrufbar unter **https://apwg.org/trendsreports/**
[6] Vgl. Phishing-Radar der Verbraucherzentrale; online abrufbar unter **https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/phishingradar-aktuelle-warnungen-6059**
[7] Vgl. Checkpoint. Brand Phishing Reports. Quartalsberichte 2022; online abrufbar unter **https://blog.checkpoint.com**

In der Gesamtbetrachtung zeigen die weltweiten Daten der APWG einen kontinuierlichen und starken Anstieg an Phishing-Webseiten seit Mitte 2020. Von Februar auf März 2022 gab es einen besonders starken Anstieg um ca. 22%, der mit dem Beginn des russischen Angriffskriegs auf die Ukraine korreliert.

Darüber hinaus erfasst das Bundesamt für Sicherheit in der Informationstechnik Spam-Mails und abgewehrte Malware-Angriffe per Mail auf die Netze des Bundes sowie die Anzahl an präventiven Sperrungen maliziöser Webseiten. Der Jahresverlauf 2022 stellt sich wie folgt dar:

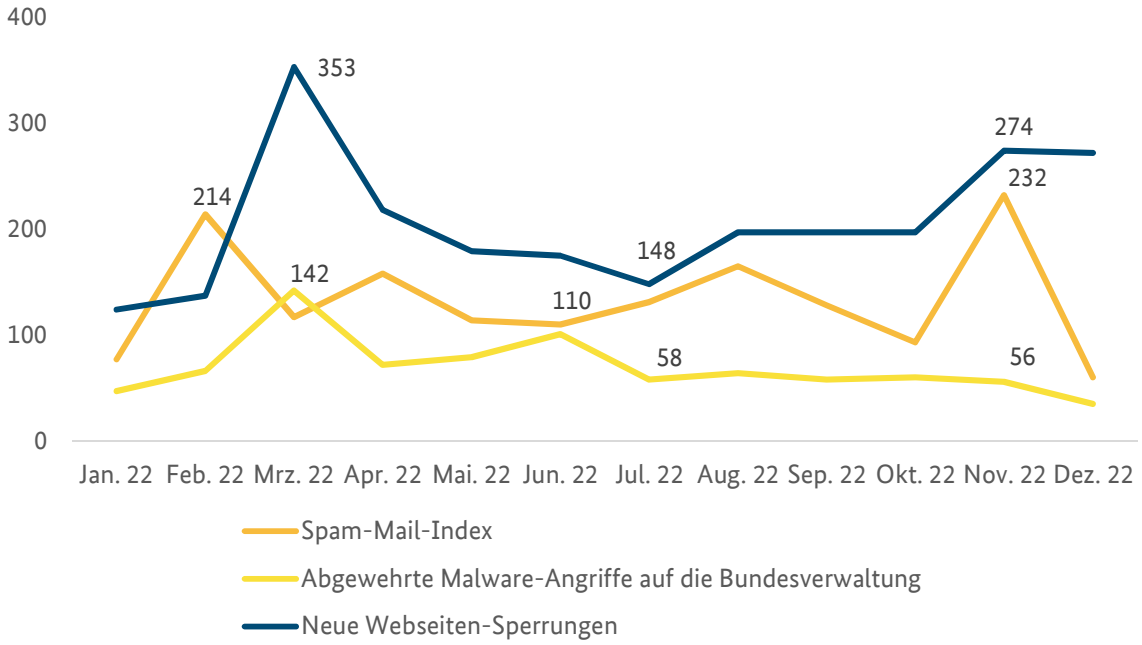


Abbildung 10: Spam-Mail-Index und Abwehr-Indizes des Bundesamtes für Sicherheit in der Informationstechnik für 2022[8]

Der erste Anstieg des Spam-Mail-Indexes im Februar 2022 kann unter anderem auf eine ausgeprägte, über mehrere Tage andauernde Sextortion-Kampagne (Erpressung mit angeblich kompromittierendem Bildmaterial) zurückgeführt werden. Der Jahreshöhepunkt im November spiegelt das alljährliche Spam-Aufkommen zur Zeit des Vorweihnachtsgeschäfts wider. Der starke Ausschlag im März 2022 bei neuen Webseitensperrungen ist auf eine erhöhte Bedrohungslage zu Beginn des russischen Angriffskriegs auf die Ukraine zurückzuführen, wonach zahlreiche Webseiten als potentiell bedrohlich eingeschätzt wurden. Der Jahreshöchstwert der abgewehrten Malware-Angriffe wurde ebenfalls im März erreicht und begründet sich in der Zunahme an Mails zur Emotet-Distribution. Alle drei Parameter zeigen für 2022 höhere Werte als für das Vorjahr.

Phishing ist und bleibt einer der beliebtesten Eintrittsvektoren zur Distribution von Malware und dem Abgriff von Zugangsdaten.

[8] Basisjahr 2018=100

3.3 MALWARE

Nach erfolgreicher Kompromittierung des Zielsystems folgt oftmals das Nachladen von Malware. Die Vielzahl an im Umlauf befindlichen Malware-Familien stellt eine fortdauernde Bedrohung dar. Ein großes Gefahrenpotential liegt hierbei in der umfangreichen und sich schnell anpassenden Funktionsweise verschiedener Malware-Typen nach erfolgtem Systemzugriff.

Im Berichtszeitraum zeigt sich der bereits seit Jahren anhaltende Trend der vermehrten missbräuchlichen Nutzung legaler kommerzieller Tools: Ob Pen-Testing-Tools[9] wie Cobalt Strike, das als Info-Stealer missbräuchlich nutzbare Directory Tool AdFind oder Krypto-Miner wie XMRig – Cyberkriminelle nutzen verfügbare Tools wie diese, um auf Rechnern oder in Netzwerken hinterlegte Daten auszuspähen oder Zugriff auf sensible IT-Systeme zu verschaffen. Neben der Erlangung von Daten kann auch deren Zerstörung ein zweckdienliches Mittel sein, welches vor allem im Bereich der Sabotage oder Erpressung zu erwarten ist. Der Einsatz sogenannter Wiper[10] spielt im russischen Angriffskrieg gegen die Ukraine eine bedeutende Rolle (siehe Kapitel 4.1).

Die nachfolgenden Malware-Familien stellen eine beispielhafte Auswahl relevanter Schadprogramme mit unterschiedlichsten Funktionsweisen dar:

Emotet

Dropper/Loader

- Primäre Funktion: Unbemerktes Infizieren von Opfersystemen und Nachladen weiterer Schadsoftware
- Distribution: Spam-Mails mit maliziösen Anhängen
- Takedown 01/2021
- Ab 11/2021 erneute Aktivitäten

QBot

Infostealer

- Primäre Funktion: Abgreifen von Anmeldeinformationen bei Online-Banking und Social Media Konten sowie das Nachladen weiterer Malware wie Ransomware
- Distribution: Spam-Mails mit maliziösen Links/Anhängen, OneNote, OneDrive

Anubis

Mobile Malware

- Primäre Funktion: Abgreifen von Anmeldedaten von Finanz- und Trading-Apps
- Distribution: Maliziöse Webseiten, Spam-Mails, Download via Google Play Store
- Erhielt nach dem Takedown von FluBot Mitte 2022 erhöhte Relevanz

Durch Malware-as-a-Service werden Funktionen der eingesetzten Schadsoftware ständig erweitert.

[9] Programme zur unternehmensseitigen Durchführung umfassender Sicherheitstests einzelner Rechner oder Netzwerke.
[10] Malware, die auf die Zerstörung von Daten spezialisiert ist.

3.4 RANSOMWARE

Von allen Malware-Arten hat Ransomware weiterhin das höchste Schadenspotential. Im Jahr 2022 wurde im Durchschnitt täglich mindestens ein deutsches Unternehmen Ziel eines Ransomware-Angriffs. [11] Bei diesen Angriffen wurden insgesamt 42 unterschiedliche Ransomware-Varianten identifiziert. Am häufigsten waren deutsche Geschädigte im vergangenen Jahr von Angriffen mit der Ransomware-Variante LockBit betroffen.

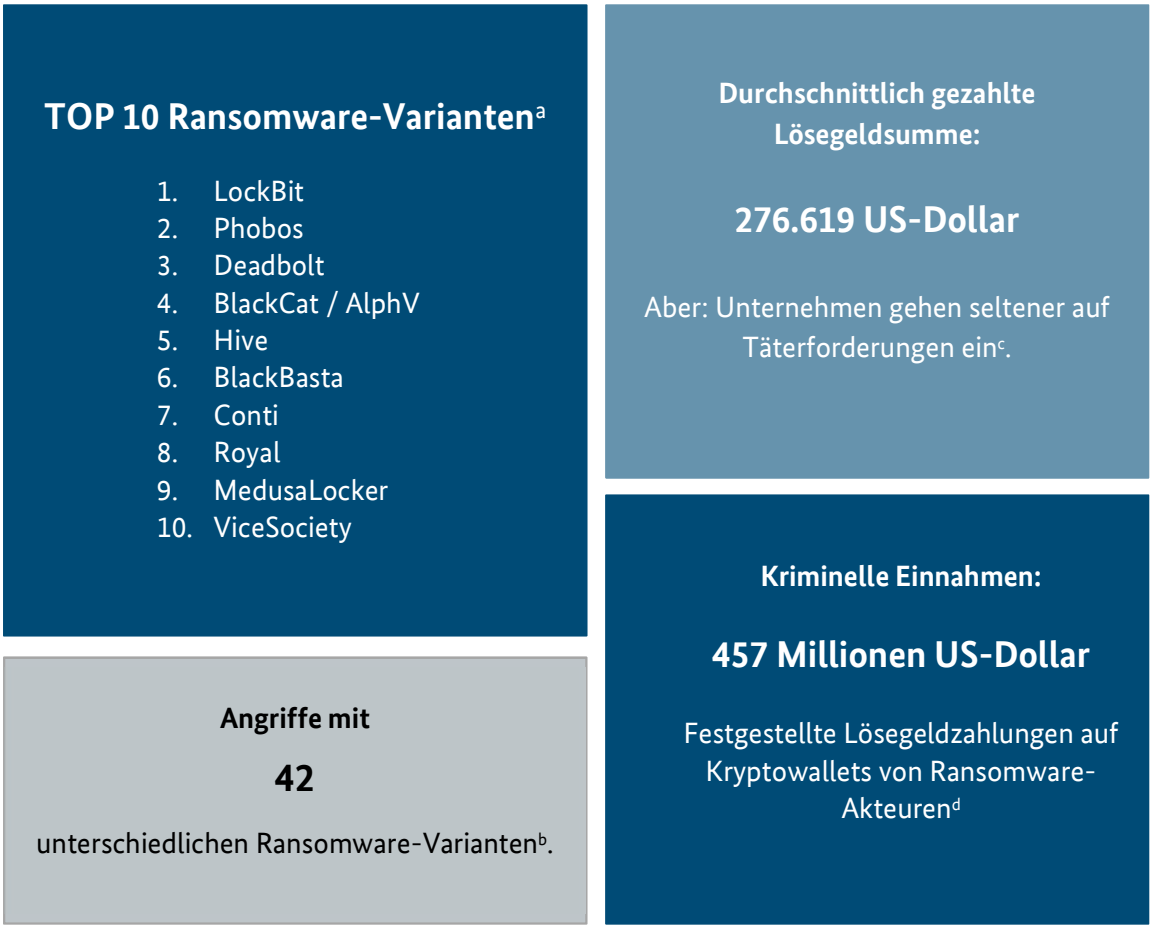


Abbildung 11: Kennzahlen zu Ransomware-Angriffen im Jahr 2022
a = Top 10 der am häufigsten festgestellten Varianten bei Ransomware-Angriffen auf deutsche Unternehmen. Die Auflistung basiert ausschließlich auf einer quantitativen Auswertung der Ransomware-Fallzahlen. Quelle: BKA
b = Quelle: BKA
c = Global durchschnittlich festgestellte Lösegeldsumme. Quelle: Coveware. Quartalsberichte 2022; online abrufbar unter https://www.coveware.com/blog
d = Einnahmen durch Ransomware-Angriffe. Quelle: Chainalysis (2023). The 2023 Crypto Crime Report

Ransomware-Angriffe können schwerwiegende Folgen für betroffene Unternehmen und Einrichtungen haben, denn finanzielle Schäden entstehen dabei nicht nur durch das von Tätern geforderte Lösegeld, sondern zusätzlich durch Ausfälle und Einschränkungen im Geschäftsbetrieb sowie durch entstehende Wiederherstellungskosten als Folge eines Angriffs.

[11] Bundesweite Erhebung polizeilich bekannt gewordener Ransomware-Angriffe. Die abgebildeten Daten umfassen ausschließlich das polizeiliche Hellfeld. Erhebungszeitraum: 01.01.2023-31.03.2023

Das Cybersecurity Unternehmen Coveware [12] stellt einen fortlaufenden Rückgang der Zahlungsbereitschaft von durch Ransomware-Angriffe betroffenen Unternehmen fest (siehe Abbildung 12). Nach Einschätzung von Coveware versuchen Ransomware-Gruppierungen die daraus resultierenden finanziellen Einbußen durch höhere Lösegeld-Forderungen auszugleichen. So stellte das Unternehmen bei der Betrachtung der global gezahlten Lösegeldsummen fest, dass diese 2022 im Mittel bei 276.619 US-Dollar lagen, was im Vergleich zum Vorjahr einen Anstieg von 35% bedeutet.[13] Die Höhe geforderter Lösegeldsummen orientiert sich häufig an der Zahlungsfähigkeit eines betroffenen Unternehmens. Aus dem Anstieg der durchschnittlichen Höhe der Lösegeldforderungen im vergangenen Jahr lässt sich schlussfolgern, dass sich Ransomware-Angriffe vermehrt gegen große, zahlungsfähige Unternehmen richten. Allerdings stehen kleine und mittelständische Unternehmen (KMU) auch weiterhin im Fokus der Ransomware-Akteure. Die Folgen eines solchen Angriffs können für KMU teilweise existenzbedrohend sein.

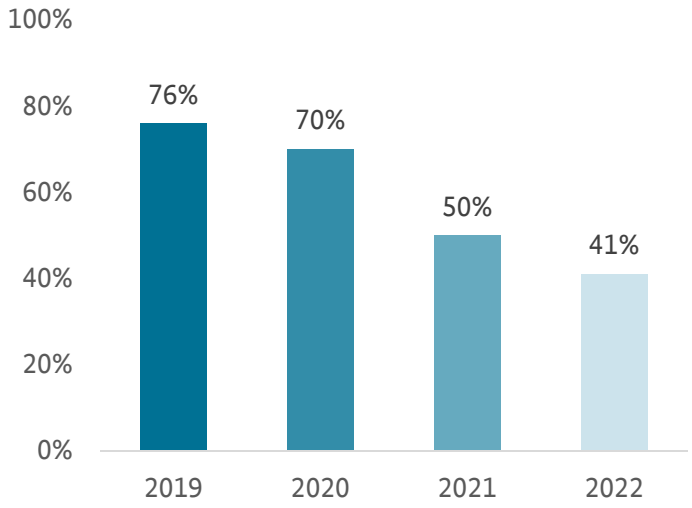


Abbildung 12: Anteil an Unternehmen, die nach einem Ransomware-Angriff Lösegeld gezahlt haben. Anmerkung: Nach Daten von Coveware in Chainalysis (2023). The 2023 Crypto Crime Report

Nach Erkenntnissen von Chainalysis sanken kriminelle Einnahmen durch Lösegeldzahlungen nach Ransomware-Angriffen im Vergleich zu den vergangenen Jahren deutlich.

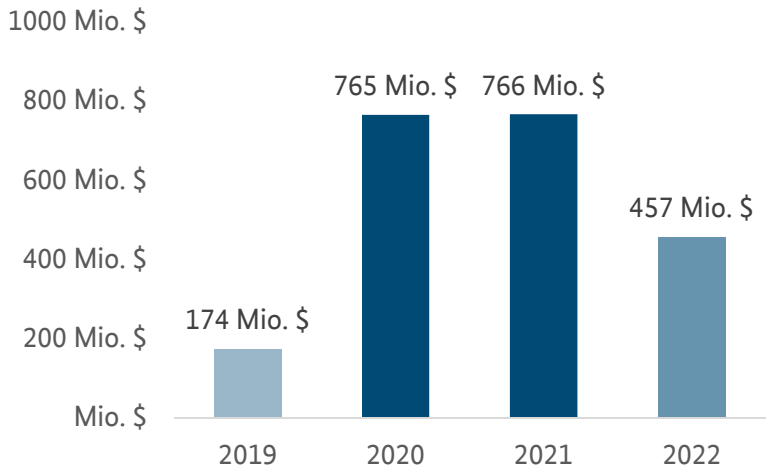


Abbildung 13: Weltweit festgestellte Lösegeldzahlungen auf Kryptowallets von Ransomware-Akteuren im Jahr 2022

[12] Vgl. Coveware. Quartalsberichte 2022; online abrufbar unter **https://www.coveware.com/blog**
[13] 2021: 204.695 US-Dollar

2022 konnten weltweit durch das Unternehmen auf Kryptowallets von Ransomware-Akteuren Lösegeldzahlungen in Höhe von 458,8 Mio. US-Dollar festgestellt werden, knapp 300 Mio. US-Dollar (-40,3%) weniger als 2021 (765,6 Mio.) und 2020 (765 Mio.). Auch hierfür dürfte die sinkende Zahlungsbereitschaft Geschädigter ursächlich sein.[14]

Als finanziell besonders lukratives Modell entwickelte sich im Bereich Ransomware bereits in den vergangenen Jahren das sogenannte „Ransomware-as-a-Service“ (RaaS)-Geschäftsmodell. Hierbei vermieten Ransomware-Entwickler den Einsatz ihrer Schadsoftware an sogenannte „Affiliates“, die Ransomware-Angriffe durchführen und Anteile des erpressten Lösegelds erhalten. Diese Form der „Dienstleistung“ versetzt potenzielle Cyberkriminelle in die Lage, auch ohne eigene umfangreiche technische Fertigkeiten, Ransomware-Angriffe durchzuführen. Innerhalb eines RaaS-Modells agieren die Akteure arbeitsteilig und professionell, deren Organisationsstruktur ist mit der eines Unternehmens vergleichbar. Beleg für eine zunehmende Professionalisierung im Bereich Cybercrime ist auch die steigende Zahl an Ermittlungsverfahren mit Bezügen zur Organisierten Kriminalität. So wurde im Jahr 2022 gegen 17 OK-Gruppierungen im Bereich Cybercrime ermittelt (2021: 15). Von diesen OK-Verfahren wurden die häufigsten (7) im Bereich der digitalen Erpressung durchgeführt.

Nach im BKA vorliegenden Erkenntnissen organisierte sich eine größere RaaS-Gruppierung beispielhaft entsprechend der folgenden Struktur:

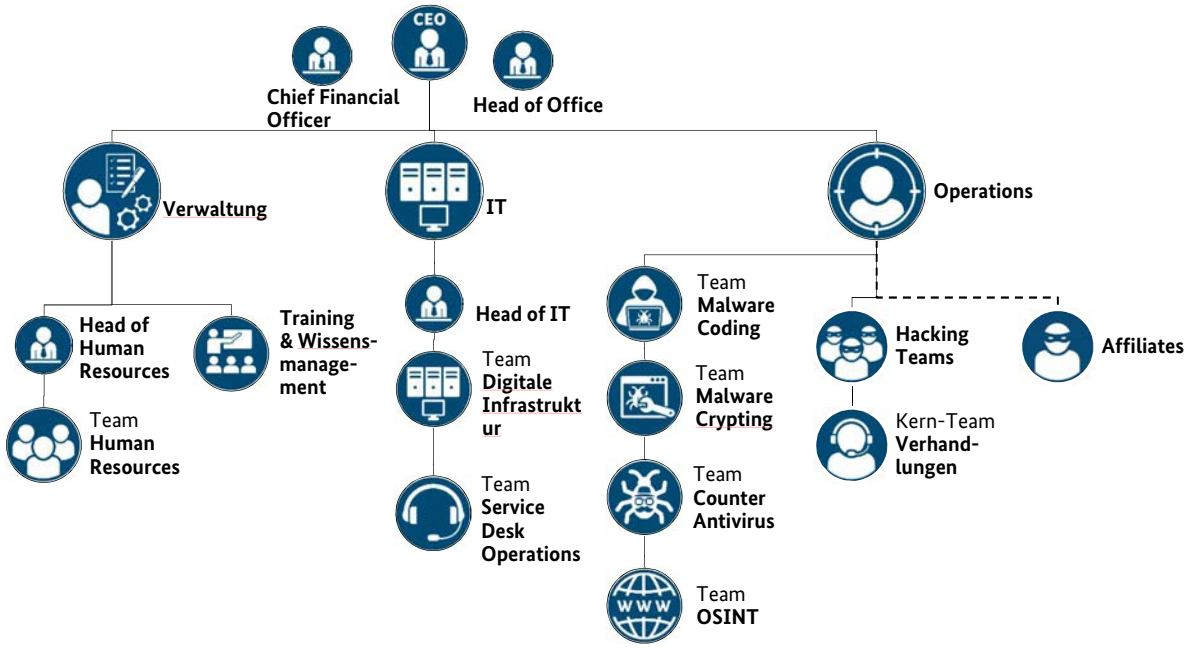


Abbildung 14: Arbeitsteilung innerhalb einer RaaS-Gruppierung analog der Struktur eines mittelständischen Unternehmens mit ca. 30-100 Mitarbeitern

Neben der Verwaltung des RaaS-Modells, stehen spezialisierte Teams zur Verfügung, die IT-Infrastruktur bereitstellen und pflegen, Malware entwickeln und anpassen, über Open Source Intelligence [15] (OSINT) potenzielle Ziele identifizieren sowie nach einem erfolgreichen Angriff Lösegeldsummen verhandeln. Die eigentlichen Angriffe werden sowohl durch eigene Hacking-Teams als auch Affiliates durchgeführt.

[14] Chainalysis (2023). The 2023 Crypto Crime Report. Anmerkung: Die Daten von Chainalysis unterliegen retrograden Anpassungen.
[15] OSINT beschreibt Informationen, welche über frei verfügbare Quellen bezogen werden können.

Häufig betreiben etablierte RaaS-Gruppierungen zusätzlich sogenannte „Dedicated Leak Sites“ (DLS) im Darknet. Die DLS stellen ein weiteres Bedrohungsszenario für Betroffene von Ransomware-Angriffen dar, denn diese werden häufig dazu genutzt, um zuvor ausgeleitete Daten der Geschädigten bei Nichtzahlung zu veröffentlichen („Double Extortion“).

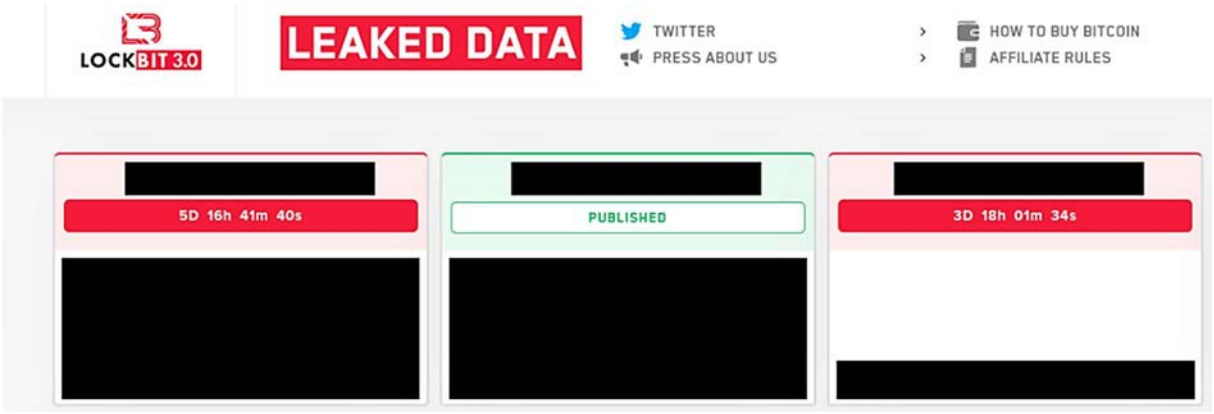


Abbildung 15: Screenshot der DLS der Ransomware-Gruppierung LockBit. Anmerkung: Die rot hinterlegten Felder zeigen die Zahlungsfrist an, nach Ablauf derer die Daten Geschädigter veröffentlicht werden. Im grün hinterlegten Feld stehen Daten Geschädigter nach Ablauf der Zahlungsfrist zum Download zur Verfügung. Alle Geschädigtendaten wurden geschwärzt.

Eine Auswertung der DLS gewährt einen zusätzlichen Einblick in das Ransomware-Aufkommen in Deutschland. Nachfolgende Angaben beziehen sich ausschließlich auf den Modus Operandi Double Extortion und bilden damit lediglich einen Teil des Ransomware-Fallaufkommens in Deutschland ab. Geschädigte, die ausschließlich mit der Verschlüsselung ihrer Systeme erpresst und bei denen keine Daten ausgeleitet und veröffentlicht werden („Single Extortion“), sind bei dieser Auswertung nicht enthalten.

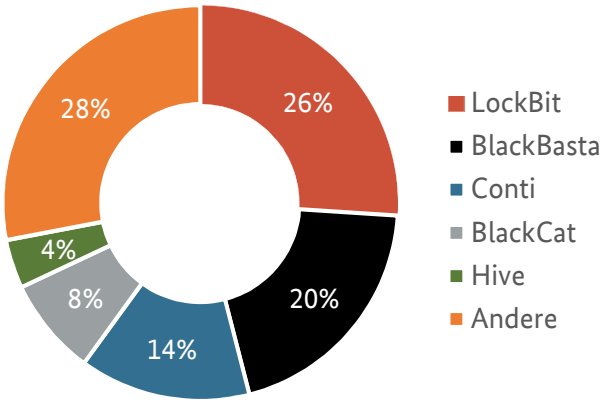


Abbildung 16: Verteilung deutscher Geschädigter auf DLS nach Ransomware-Gruppierung

Im BKA durchgeführte Auswertungen der DLS [16] zeigen, dass 2022 137 Unternehmen mit Sitz in Deutschland auf DLS mit der Veröffentlichung ihrer Daten erpresst wurden. Damit war Deutschland nach den USA und dem Vereinigten Königreich am dritthäufigsten betroffen. Daten deutscher Geschädigter wurden am häufigsten auf den DLS der Ransomware-Gruppierungen LockBit, BlackBasta und Conti veröffentlicht. Diese finden sich auch in der Auflistung der in Deutschland aktivsten Ransomware-Varianten (siehe Abbildung 11).

[16] Eigene Auswertung nach den Daten von eCrime.ch; online abrufbar unter **https://ecrime.ch/**

Weniger Betroffene gehen auf Lösegeldforderungen nach Ransomware-Angriffen ein und beeinträchtigen das RaaS-Geschäftsmodell deutlich.

LockBit

Aktivität: Seit 2019

Zielspektrum: Primär KMU

Relevanz: Eine der aktivsten RaaS-Gruppierungen weltweit.

Besonderheiten: Im Juni 2022 veröffentlichten die Akteure hinter LockBit Version 3.0 ihrer Ransomware sowie eine aktualisierte DLS. Ein Novum stellt dabei unter anderem das angebotene „Bug Bounty Programm“ dar, im Rahmen dessen Hinweise auf Schwachstellen in der Ransomware LockBit 3.0 mit einer Geldprämie entlohnt werden.

Conti

Aktivität: 2020 – 2022

Zielspektrum: Big Game, einschl. Gesundheitswesen

Relevanz: Bis zur Auflösung eine der aktivsten RaaS-Gruppierungen weltweit.

Besonderheiten: Die Akteure hinter der Malware Conti (alias Wizard Spider) werden auch mit der Ransomware Ryuk in Verbindung gebracht. Im Zuge des Russland-Ukraine-Kriegs wurden interne Chats und Teile des Conti-Quellcodes geleakt. Dies hatte die Abschaltung der Conti-Infrastruktur zur Folge. Es ist davon auszugehen, dass die Akteure unter neuem Namen weiterhin aktiv sind.

BlackBasta

Aktivität: Seit 2022

Zielspektrum: Kein spezifischer Zieltypus erkennbar

Relevanz: International ist Deutschland am zweithäufigsten von Angriffen mit BlackBasta betroffen.

Besonderheiten: Trotz des kurzen Aktivitätszeitraums hat sich BlackBasta bereits international und vor allem in Bezug auf Deutschland zu einer der aktivsten RaaS-Gruppierungen entwickelt. Es ist davon auszugehen, dass es sich bei den Akteuren hinter BlackBasta um erfahrene Cyberkriminelle handelt.

Während Ransomware-Aktivitäten in der ersten Jahreshälfte 2022 überwiegend von wenigen „Key Playern“ wie Conti, LockBit und BlackBasta geprägt waren, diversifizierte sich die Ransomware-Szene in der zweiten Jahreshälfte deutlich und zahlreiche neue Akteure gewannen an Relevanz. Die Analyse von Kryptotransaktionen im Zusammenhang mit Lösegeldzahlungen ergab außerdem, dass sich die durchschnittliche „Lebensspanne“[17] von Ransomware-Gruppierungen von 152 Tagen im Jahr 2021 auf nur 70 Tage im Jahr 2022 reduzierte.[18] Hierbei ist es wahrscheinlich, dass es sich in Teilen um sogenannte Rebrandings handelt und etablierte Täter unter neuem Namen agieren. Im vergangenen Jahr waren diese Entwicklungen auch durch den Russland-Ukraine-Krieg beeinflusst, nicht zuletzt strukturierten sich Ransomware-Gruppierungen aufgrund der unterschiedlichen nationalen Identitäten oder Ideologien ihrer Mitglieder um. Insgesamt sind diese Feststellungen Beleg für eine hohe Dynamik des Phänomenbereichs. Russland fungiert bereits seit einigen Jahren als safe haven und somit als beliebter Aufenthaltsort für Ransomware-Akteure, von dem Cyberangriffe gegen Ziele weltweit getätigt werden.

[17] Aktivitätszeitraum einer Ransomware-Variante.
[18] Chainalysis (2023). The 2023 Crypto Crime Report.

3.5 DISTRIBUTED DENIAL-OF-SERVICE

Neben Malware- bzw. Ransomware-Angriffen waren auch Distributed Denial-of-Service (DDoS)-Angriffe 2022 eine relevante und vor allem medial präsente Bedrohung. Im Zuge des russischen Angriffskrieges auf die Ukraine etablierten sich DDoS-Angriffe als beliebtes Instrument von hacktivistischen Cyber-Akteuren, wie der pro-russischen Gruppierung Killnet. Diese führte seither mehrere DDoS-Kampagnen auch gegen Webseiten deutscher Unternehmen und Einrichtungen aus, wie z.B. der Bundeswehr und des Flughafens Köln-Bonn.

Nachfolgende Grafik gibt die Anzahl der DDoS-Angriffe wieder, die seitens der Deutsche Telekom AG (DTAG) registriert wurden.[19] Wie im Berichtszeitraum 2021 zeigen sich auch 2022 starke Schwankungen im Jahresverlauf.

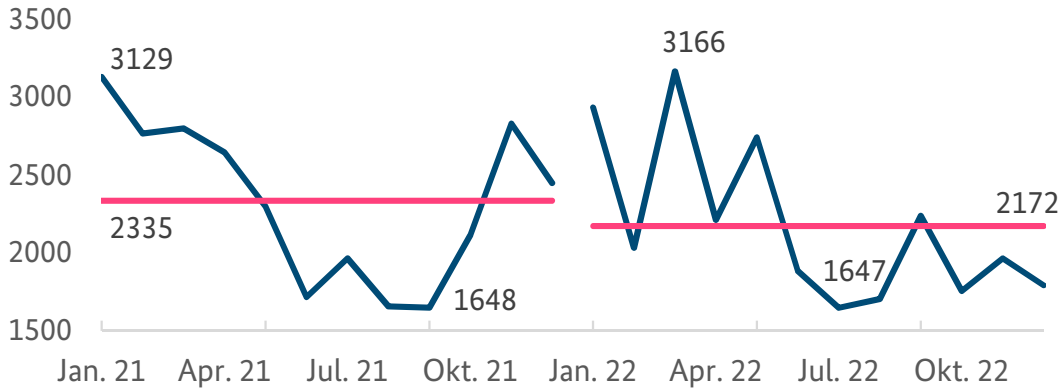


Abbildung 17: Anzahl an DDoS-Angriffen pro Monat im Netz der DTAG für die Jahre 2021 und 2022

Die IT-Dienstleister DTAG und Link11 stellen einen Rückgang an DDoS-Angriffen fest. Link11 begründet diesen Rückgang mit folgenden Aspekten:[20]

- Während der Corona-Pandemie stieg die Anzahl an DDoS-Angriffen an, da Cyberkriminelle die von der weitreichenden Homeoffice-Pflicht verursachte digitale Abhängigkeit ausnutzten. Dies führte vor allem in den Jahren 2020 und 2021 zu erhöhten Fallzahlen im DDoS-Bereich.
- 2022 fokussierten sich Täter eher auf Ziele, die mit dem Russland-Ukraine-Krieg in Verbindung gebracht werden können. Die Angriffe erfolgten somit häufig aus einer politischen oder ideologischen Motivation heraus. Gleichzeitig konzentrierten sich die üblichen Cyber-Akteure auf Ziele, die enger mit dem Krieg in Zusammenhang stehen, als deutsche Unternehmen.
- Die Schließung von Darknet-Marktplätzen wie Hydra Market (siehe Kapitel 3.1) sowie das Abschalten von ca. 50 DDoS-as-a-Service-Diensten (sogenannter Booter- oder Stresser-Dienste) im Rahmen operativer Maßnahmen der seit 2018 durchgeführten Operation Power Off führten im Dezember 2022 zu einem verminderten Angebot an DDoS-Services und infolgedessen zu weniger Angriffen.

[19] Daten der DTAG im Berichtszeitraum Januar 2021 bis Dezember 2022.
[20] Link11 (2023). DDoS-Report 2022; online abrufbar unter: **https://www.link11.com/de/download/ddos-report-2022/**

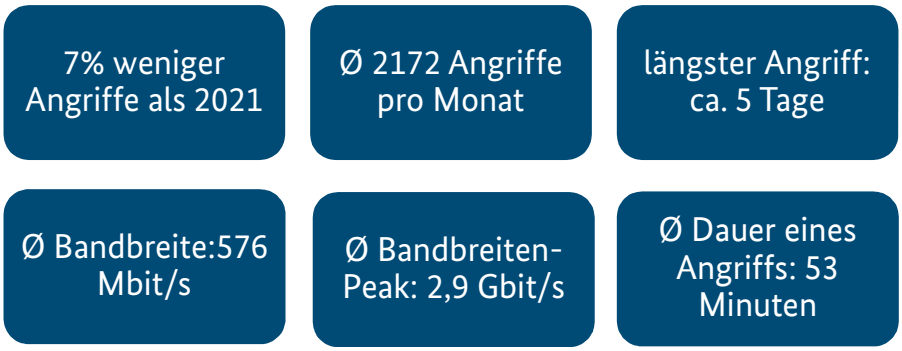


Abbildung 18: Relevante Eckdaten von DDoS-Angriffen 2022. Daten der DTAG

Neben der Anzahl der Angriffe nahmen auch spezielle Angriffsformen wie RDoS[21] und Multivektor-Angriffe[22] ab. Zugleich konnte allerdings bei durchgeführten Multivektor-Angriffen ein Anstieg an verwendeten Vektoren festgestellt werden, womit Angriffe eine höhere Erfolgswahrscheinlichkeit haben und zu einer längeren Störung des angegriffenen Systems führen.[23]

Aus den Daten der DTAG und von Link11 ergibt sich ein eindeutiger Trend: DDoS-Angriffe werden kürzer. Knapp dreiviertel der Angriffe waren kürzer als fünf Minuten. Mit kurzen Angriffen werden IT-Systeme auf Schwachstellen überprüft oder andere Cyberangriffe verschleiert. DDoS-Angriffe erreichen darüber hinaus schneller ein kritisches Volumen, mit dem Systemstörungen herbeigeführt werden können. 2022 konnte ca. dreimal so schnell ein solches kritisches Volumen erreicht werden wie noch 2021, was die Mitigation der Angriffe erschwert.

Aus diesen Entwicklungen lässt sich ableiten, dass die Qualität von DDoS-Angriffen stetig zunimmt. Nach Auswertungen von Link11 entwickelten sich die Charakteristika von DDoS-Angriffen wie folgt:

Kürzere Angriffsdauer	Schneller Aufbau kritischen Volumens	Korrelation zwischen Dauer und Intensität
Die durchschnittliche Angriffsdauer von DDoS-Angriffen ist geringer geworden: 2022 betrug diese 53 Minuten – 2021 ca. 96 Minuten.	Allerdings erreichten DDoS-Angriffe 2022 im Durchschnitt bereits nach 55 Sekunden ein kritisches Niveau. 2021 benötigten DDoS-Angreifer dafür im Durchschnitt noch 184 Sekunden.	Vor allem im ersten Halbjahr 2022 zeigte sich, dass DDoS-Angriffe zwar kürzer, dafür intensiver ausfielen.

DDoS-Angriffe werden kürzer – aber intensiver.
2022 waren sie beliebtes Werkzeug hacktivistischer Akteure.

[21] Ransom-DoS: Erpressung mit Androhung von DDoS-Angriffen.
[22] Angriffe gegen unterschiedliche Schwachstellen und Ebenen des Zielsystems.
[23] Link11 (2023). DDoS-Report 2022; online abrufbar unter: **https://www.link11.com/de/download/ddos-report-2022/**

3.6 DIGITALE ANGRIFFE AUF GELDAUTOMATEN

Im Gegensatz zu vielen anderen europäischen Staaten sind die Fallzahlen der digitalen Angriffe auf Geldautomaten in Deutschland stark zurückgegangen. Grund hierfür ist u.a. das aktive Agieren insbesondere eines dieser deutschen Geldautomatenhersteller, welcher schnell auf Bedrohungsszenarien reagiert und erkannte Sicherheitslücken schließt. Außerdem folgen viele deutsche Finanzinstitute zeitnah den sicherheitstechnischen Empfehlungen von Geldautomatenherstellern sowie Sicherheitsbehörden. Somit verfügen die in Deutschland aufgestellten Geldautomaten größtenteils über aktuelle Firmware, was Jackpotting-Angriffe erschwert oder verhindert. Ein daraus resultierender Verdrängungseffekt kann nicht ausgeschlossen werden.

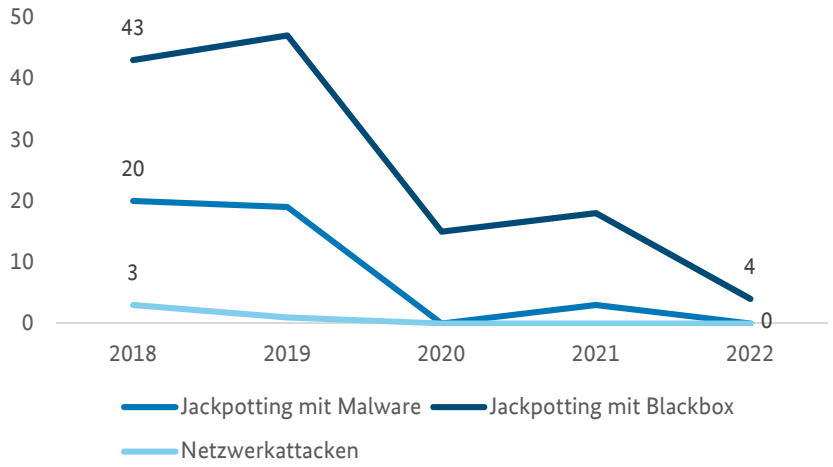


Abbildung 19: Fallzahlen digitaler Angriffe auf Geldautomaten[24]

Das BKA befindet sich sowohl bilateral als auch über internationale Gremien im beständigen engen Austausch mit den beiden weltweit größten Geldautomatenherstellern. Neben technischen Aspekten der verschiedenen Modi Operandi werden mit diesen auch polizeiliche, präventive und repressive Möglichkeiten erörtert.

[24] Jackpotting mit Malware bezeichnet Angriffe auf den Rechner/PC eines Geldautomaten mittels Schadsoftware.
Jackpotting mit Blackbox bezeichnet Angriffe auf das Auszahlungsmodul des Geldautomaten mittels tätereigener Hardware.
Malware-Angriff auf die kartenausgebende Bank oder Processing-Gesellschaft, um Transaktionsprozesse zu manipulieren. Anschließend erfolgt ein sogenannter kartengebundener „Cash Out“ oder Malware-Angriff auf die Geldautomaten betreibende Bank, um einen direkten Zugriff auf die im Netzwerk verbundenen Geldautomaten zu erhalten und einen sogenannten kartenungebundenen Cash Out durchzuführen.
Quelle: BKA

4. Relevante Entwicklungen

4.1 DER RUSSISCHE ANGRIFFSKRIEG AUF DIE UKRAINE

Seit dem 24.02.2022 führt Russland einen Angriffskrieg gegen die Ukraine, der von einer gestiegenen Anzahl destruktiver Cyberaktivitäten begleitet wird. Diese Entwicklung führte seither auch in Deutschland zu einer erhöhten Cyber-Bedrohungslage. Die Aktivitäten sowohl staatlich-gelenkter und -geduldeter, als auch bislang politisch unabhängig eingeschätzter Cyber-Akteure führten im Kontext des Kriegs zu einem erhöhten Fallaufkommen, das auch über die unmittelbaren Kriegsparteien hinaus Wirkung entfaltete. Neben Desinformationskampagnen und der Verbreitung von Propaganda konnten vor allem DDoS-Angriffe, das Eindringen in IT-Systeme mit nachgelagerter Datenexfiltration und -veröffentlichung („Hack & Leak"), Defacements[25] sowie der Einsatz von Wipern festgestellt werden.

Gezielte Kampagnen russischer Cyber-Akteure gegen strategische Ziele in der Ukraine:

Eine massive Cyber-Offensive Russlands gegen den Westen blieb bislang aus. Allerdings fanden bereits im Vorfeld und während des Russland-Ukraine-Kriegs mehrere gezielte Kampagnen russischer Cyber-Akteure statt. Ziel war die Zerstörung strategischer Ziele in der Ukraine mittels Wiper. Von russischer Seite wurden unter anderem folgende Wiper-Familien eingesetzt: WhisperGate, HermeticWiper (FoxBlade), CaddyWiper, DesertBlade, IsaacWiper und Acid Rain.

Hacktivismus-Kampagnen:

Hacktivismus vereint die Konzepte des Hackings und des Aktivismus und beschreibt ideologisch, sozial und/oder politisch motivierte Aktionen unter Nutzung von Hackingtools. Im Zuge des Russland-Ukraine-Kriegs solidarisierten sich Hacktivisten öffentlich mit den jeweiligen Kriegsparteien. Auf pro-ukrainischer Seite sind vor allem die sogenannte IT Army of Ukraine und Anonymous aktiv. Als pro-russische hacktivistische Gruppierung erlangte vor allem Killnet Aufmerksamkeit.

Dem Russland-Ukraine-Krieg ist ein fortwährendes Eskalationspotential auch im Cyberraum immanent. Es besteht die andauernde Gefahr, dass sich Cyberangriffe gezielt gegen Kritische Infrastrukturen in der Ukraine als auch in deren Unterstützerstaaten richten. Im bis heute andauernden Krieg konnten auch Angriffe festgestellt werden, die nicht explizit auf KRITIS-Einrichtungen abzielten, jedoch Kollateralschäden in diesem Bereich verursachten.

Nachfolgende Sachverhalte skizzieren die mittelbare und unmittelbare Betroffenheit deutscher, (west-)europäischer und ukrainischer KRITIS-Einrichtungen im Bereich der Energieversorgung im Kontext des Russland-Ukraine-Kriegs:

[25] Unberechtigtes Verändern des Erscheinungsbildes einer Webseite.

Cyberangriffe auf ViaSat

Angriff via AcidRain:

Am 24.02.2022 erfolgte ein Cyberangriff auf das Unternehmen ViaSat, Betreiber des Satellitennetzwerks KA-SAT, bei dem ein Angreifer den internen Updateserver der Firma kompromittierte. In diesem Zusammenhang wurde ein maliziöses Update auf Endkundengeräte ausgebracht, der Wiper AcidRain auf die betroffenen Geräte aufgespielt und die betroffenen Kundenmodems unbrauchbar gemacht. Der Ausfall der Endgeräte und auch der flächendeckende Ausfall des Satellitennetzwerkes KA-SAT, primär in der Ukraine aber auch in Europa, waren die Folge.

Auswirkungen auf Deutschland:

Zu den Endkunden ViaSats zählen unter anderem das US-amerikanische und ukrainische Militär.
Das Satellitennetzwerk KA-SAT wird in Deutschland und weiten Teilen Europas für die satellitenbasierte Breitbandversorgung genutzt und bedient unter anderem die industriellen Steuerungsanlagen von Offshore-Windparks. In Deutschland fielen durch den Ausfall von KA-SAT die Modems an ca. 5.800 Windkraftanlagen des Herstellers Enercon aus, weshalb eine Fernwartung an den betroffenen Windkraftanlagen zunächst nicht mehr möglich war.

Während der Cyberangriff vermeintlich auf die Ukraine abzielte und den kriegerischen Angriff Russlands auf diesem Wege auch im Cyberraum vorbereiten sollte, hatte der Ausfall KA-SATs auch Auswirkungen auf zahlreiche europäische Windkraftanlagen. Die wurmartige Verbreitung von Schadsoftware über Lieferketten illustriert das Gefährdungspotential von Kollateralschäden bei Cyberangriffen.

Erster Cyberangriff auf deutschen KRITIS-Betreiber im Kontext des Kriegs

Rosneft Deutschland GmbH:

Am 11.03.2022 erfolgte ein Cyberangriff auf die Rosneft Deutschland GmbH, Tochtergesellschaft des russischen Mineralölunternehmens Rosneft und nach eigenen Angaben das drittgrößte Unternehmen für Mineralölverarbeitung in Deutschland. Das Unternehmen ist mit Anlagen für Distribution von und Handel mit Mineralöl als KRITIS-Betreiber registriert.

Angriff und Auswirkungen auf Deutschland:

Zu dem Angriff bekannte sich das Internetkollektiv Anonymous Deutschland und gab an, 20 TB Daten von Rosneft Deutschland entwendet zu haben. Die Gefährdung des KRITIS-Bereichs im Kontext des Russland-Ukraine-Krieges hat sich durch den Angriff auf Rosneft Deutschland erstmalig konkretisiert. Der Angriff ist als hacktivistisch einzuordnen, da Anonymous Deutschland nach eigener Aussage verhindern wollte, dass Rosneft über die deutsche Tochtergesellschaft Sanktionen der EU umgehen könne.

DDoS-Kampagne gegen deutsche Webseiten

Ankündigung via Telegram:

Seit April 2022 erfolgten mehrere DDoS-Angriffe durch pro-russische hacktivistische Kollektive wie Killnet oder Anonymous Russia auf Webseiten deutscher Behörden und Unternehmen. Auch 2023 setzten sich diese Angriffe fort. Am Abend des 24.01.2023 kündigte Killnet auf dessen Telegram-Kanal eine großangelegte DDoS-Kampagne gegen Ziele in Deutschland an. Als Grund für die Durchführung eines Cyberangriffs auf Deutschland wurde die angekündigte Lieferung von Leopard-2-Kampfpanzern an die Ukraine genannt. Mittels des Hashtags „#GermanyRIP“ bekannten sich 16 weitere Hacktivismus-Gruppierungen zu der Angriffswelle auf deutsche Einrichtungen.

Die Angriffe:

Der „kollektive Cyberangriff auf die BRD“ (Zitat Killnet) wurde am Morgen des 25.01.2023 mit der Verkündung von mehr als 40 deutschen Ziele gestartet. Unter den von Killnet benannten Zielen befanden sich unter anderem die Webseiten deutscher Flughäfen, Ziele im Energie- und Finanzsektor sowie Webseiten von Bundesbehörden, unter anderem die des BKA. Bereits in der Nacht vom 24.01. auf den 25.01.2023 kam es zu ersten DDoS-Angriffen auf ausgewählte Ziele. Diese Angriffe waren auf eine niedrige bis mittlere Bandbreite beschränkt. Das Bundesamt für Sicherheit in der Informationstechnik gab in diesem Zusammenhang eine schriftliche Warnmeldung heraus. Es liegen keine Hinweise vor, dass es bei den betroffenen Institutionen zu einem Schaden durch die Angriffe gekommen ist.

Bereits zuvor waren deutsche Webseiten Ziel von mehreren DDoS-Angriffskampagnen geworden. Von den Tätern begründet wurden diese häufig mit Waffenlieferungen der Bundesregierung an die Ukraine und Sanktionen gegen Russland. Das reaktionäre Angriffsmuster der Akteure hinter Killnet unterstreicht den politisch-hacktivistischen Charakter, denn die Angriffe sollen vor allem der Demoralisierung der westlichen Unterstützung der Ukraine dienen. Daher ist erwartbar, dass auch weiterhin DDoS-Angriffe gegen Staaten und Unternehmen, die an der militärischen Unterstützung für die Ukraine beteiligt sind, stattfinden werden. Insgesamt wird das Bedrohungspotential durch DDoS-Angriffe vor allem seitens Killnet für Deutschland als eher gering eingeschätzt.

Beispiele im Jahr 2022 involvierter Akteure[26]

Killnet

Killnet ist ein pro-russischer Akteur, der zahlreiche DDoS-Angriffe gegen Ziele in der Ukraine sowie deren Unterstützerstaaten durchgeführt hat, darunter auch Deutschland.

Das Zielspektrum umfasst primär öffentlichkeitswirksame Ziele. Killnet führt anlassbezogene DDoS-Kampagnen je nach geopolitischem Interesse durch. Vergangene Angriffe zielten unter anderem auf Internetpräsenzen von Regierungsstellen, Behörden sowie Unternehmen ab.

Bei Sandworm handelt es sich um eine Gruppierung, die unter anderem auch unter den Aliassen Vodoo Bear, Iridium, Telebots und Iron Viking bekannt ist.

Bekannt ist die Gruppierung vor allem für den Einsatz destruktiver Malware (Wiper) und Angriffe gegen die Energieversorgung, war in der Vergangenheit aber auch im Rahmen staatlicher Cyberspionage oder der Einmischung in ausländische Wahlen tätig. 2022 soll Sandworm Angriffe gegen ukrainische Umspannwerke durchgeführt haben.

In einer Anklageschrift aus dem Jahr 2020 ordnet das US-Justizministerium Sandworm der Hauptverwaltung für Aufklärung (GRU) des russischen Militärnachrichtendienstes zu.

Sandworm

Anonymous

Das Hackerkollektiv Anonymous stellt einen losen, dezentral organisierten Zusammenschluss von Internetnutzern dar, der über die kollektive Kraft seiner Mitglieder Protest- und Hacktivismus-Aktionen koordiniert. Mit Beginn des russischen Angriffskriegs auf die Ukraine hat sich Anonymous umgehend mit der Ukraine solidarisiert und erklärte am 24.02.2022 Russland offiziell den Cyberkrieg. Anonymous etablierte sich als zentraler Akteur in der russisch-ukrainischen Auseinandersetzung im Cyberraum, dem sich zahlreiche pro-ukrainische Cyber-Akteure anschlossen. Anonymous setzt vor allem DDoS-Angriffe, Hack & Leak-Operationen, Defacements, Live-Streams von Kriegsmaterial sowie öffentliches Shaming von Unternehmen mit Russlandgeschäft als Mittel gegen Russland ein.

Die sogenannte IT Army of Ukraine gründete sich am 26.02.2022 aufgrund eines Aufrufs des ukrainischen Ministers für digitale Transformation, Mykhailo Fedorov. IT-Experten, Hacker und weitere Freiwillige wurden in einem öffentlichen Aufruf des Ministers dazu aufgefordert, die Ukraine im Cyberkrieg gegen Russland zu verteidigen. Bereits einen Tag später zählte der Telegram-Kanal der IT-Army 175.000 Follower. Zu den Aufgaben der Gruppe zählen die Verteidigung der ukrainischen IT sowie Angriffe auf russische Ziele, vorwiegend in Form von DDoS-Angriffen. Potentielle Angriffsziele in Russland und Belarus werden dabei von der ukrainischen Regierung an die Mitglieder der IT Army kommuniziert. Der Einsatz einer solch großen Anzahl freiwilliger Hacktivisten im Rahmen staatlicher Auseinandersetzungen stellt eine bislang nicht beobachtete Entwicklung im Cyberraum dar.

IT Army of Ukraine

[26] Bildquellen: Killnet: @killnet Telegram-Kanal (Stand: 12.04.2023); Sandworm: Mandiant; Anonymous: offizielles Logo (hier entnommen **https://de.wikipedia.org/wiki/Anonymous_(Kollektiv)**); IT Army of Ukraine: **https://itarmy.com.ua**

4.2 ANGRIFFE AUF BILDUNGSEINRICHTUNGEN

Im Verlauf des letzten Jahres zeichnete sich ein verstärktes Angriffsaufkommen gegen Ziele im nationalen und internationalen Forschungs- und Bildungssektor ab.

Auf Darknet-Leakseiten bekannter Ransomware-Gruppierungen konnten im gesamten Jahr 2022 weltweit insgesamt 125 Geschädigte aus dem Bildungssektor festgestellt werden. Einer Auswertung des IT-Dienstleisters Checkpoint[27] zufolge war der Bildungssektor zum Ende des Jahres der weltweit am häufigsten von Malware-Angriffen betroffene Sektor.

Erhöhtes Angriffsaufkommen

Spätestens seit Oktober 2022 kommt es zu vermehrten Angriffen auf Forschungseinrichtungen und Universitäten. Dieser Trend ist sowohl auf nationaler, als auch auf internationaler Ebene feststellbar.

Ransomware

Im Zuge der meisten Angriffe wurde Ransomware eingesetzt. Die verwendeten Ransomware-Familien deuten darauf hin, dass verschiedene Gruppen, darunter ViceSociety, HIVE, Royal und BlackCat, den Sektor als lukratives Ziel betrachteten.

Attraktive Ziele

Sensible Forschungsdaten, öffentlicher Charakter, vielfältige Eintrittsvektoren bedingt durch die Anzahl von Lehrenden und Studierenden.

Bei Angriffen auf Bildungseinrichtungen kamen unterschiedliche Modi Operandi zum Einsatz, am häufigsten konnten dabei Ransomware-Angriffe festgestellt werden.

An den jeweils betroffenen Hochschulen fielen die Auswirkungen der Angriffe sehr unterschiedlich aus: Der kurzzeitige Verzug von Vorlesungen oder Immatrikulationen, das Ausleiten von personenbezogenen Daten und anhaltende Störungen der entsprechenden Hochschul-Webseiten waren feststellbar.

Es ist davon auszugehen, dass das vorrangige Ziel der Täter bei den Angriffen auf die Forschungseinrichtungen das illegale Ausleiten und Erlangen sensibler Daten ist. Insbesondere zum Teil langjährig erarbeitete Forschungserkenntnisse versprechen den Ransomware-Gruppierungen bei der weiteren Verwertung einen hohen finanziellen Gewinn.

Die mutmaßliche Täterschaft befindet sich dabei unter den bekannten und etablierten Akteuren der Ransomware-as-a-Service-Szene.

Obwohl nicht davon ausgegangen werden kann, dass das vermehrte Angriffsaufkommen das Resultat von fokussierten Kampagnen ist, waren Bildungseinrichtungen 2022 äußerst attraktive Ziele von Cyber-Gruppierungen. Derartige Angriffe zeigen erneut den gewinnmaximierenden und opportunistischen Charakter der Ransomware-Szene: Jeder kann ein potentielles Ziel werden – vor allem jene Einrichtungen, die mit sensiblen Daten agieren und auf deren Verfügbarkeit angewiesen sind.

[27] Vgl. Checkpoint. Most wanted Malware. Monatsberichte 2022; online abrufbar unter **https://blog.checkpoint.com**

5. Schäden und Betroffenheit

Der Bitkom e.V. als enger Kooperationspartner des BKA veröffentlicht in seinem Wirtschaftsschutzbericht[28] regelmäßig Erkenntnisse über Schäden und Betroffenheit von Wirtschaftsunternehmen durch Cybercrime. Der aktuellste Bericht wurde im August 2022 veröffentlicht und deckt inhaltlich die vorangegangenen zwölf Monate ab dem Befragungszeitraum (Januar bis März 2022) ab. Im Betrachtungszeitraum waren Unternehmen folgendermaßen betroffen bzw. vermutlich betroffen:

- Diebstahl von sensiblen digitalen Daten bzw. Informationen: 63% (+3 Prozentpunkte zum Vorjahr)
- Ausspähen von digitaler Kommunikation: 57% (+5 Prozentpunkte im Vergleich zum Vorjahr)
- Digitale Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen: 55% (+3 Prozentpunkte im Vergleich zum Vorjahr)

Bei den entstandenen Schadenssummen stellt der Bitkom e.V. eine rückläufige Entwicklung fest. Während in dem 2021 veröffentlichten Bericht ein Rekordwert von 223 Mrd. Euro verzeichnet wurde, weist die in 2022 durchgeführte Befragung einen Wert von 203 Mrd. Euro aus. Die festgestellte Schadenssumme stellt trotzdem eine Verdopplung im Vergleich zum 2019 veröffentlichten Bericht dar und stabilisiert sich somit nach einem starken Anstieg auf einem hohen Niveau. Besonders hervorzuheben ist, dass die Schadenssumme durch "Erpressung mit gestohlenen Daten oder verschlüsselten Daten“ von ca. 24 Mrd. Euro auf ca. 11 Mrd. Euro gesunken ist. Eine mögliche Erklärung hierfür liegt in der gesunkenen Zahlungsbereitschaft betroffener Unternehmen. Dennoch sind die Schadensummen weiterhin erheblich und können in Folge für Unternehmen existenzbedrohend sein.

Schaden durch:	Schadens-summen in Mrd. Euro (2022)	Schadens-summen in Mrd. Euro (2021)	Schadens-summen in Mrd. Euro (2019)	Schadens-summen in Mrd. Euro (2017)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	41,5	61,9	13,5	5,3
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	**10,7**	**24,3**	**5,3**	**0,7**
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	18,3	17,1	4,4	3,2
Patentrechtsverletzungen (auch schon vor der Anmeldung)	18,8	30,5	14,3	7,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	41,5	29,0	11,1	8,6
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	21,1	22,7	11,1	3,5
Imageschaden bei Kunden oder Lieferanten/Negative Medienberichterstattung	23,6	12,3	9,3	7,7
Kosten für Ermittlungen und Ersatzmaßnahmen	10,1	13,3	18,3	10,6
Kosten für Rechtsstreitigkeiten	16,2	12,4	15,6	5,5
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	-	-	-	2,2
Sonstige Schäden	0,9	0	< 0,1	< 0,1
Gesamtschaden pro Jahr	**202,7**	**223,5**	**102,9**	**54,8**

Abbildung 20: Verursachte Schäden u.a. durch Cybercrime laut Bitkom e.V. Wirtschaftsschutzbericht 2021 und 2022. Anmerkung: Die in Klammern angegebenen Jahreszahlen beziehen sich auf das Veröffentlichungsdatum des Berichts.

[28] Bitkom e.V. (2022). Wirtschaftsschutz 2022. Online abrufbar unter: **www.bitkom.org/presse/presseinformation/Wirtschaftsschutz-2022**

Ransomware verursachte einen Schaden von 10,7 Mrd. Euro in Deutschland. Die Schadenssumme bleibt für viele Unternehmen existenzbedrohend.

In einer weiteren repräsentativen Umfrage erhob der Bitkom e.V. die Betroffenheit von Privatpersonen durch Cybercrime.[29] Auch diese hält sich mit 75% auf dem hohen Niveau des Vorjahres (siehe Abbildung 21). In 2022 gaben außerdem 27% der Befragten an, dass ihr Computer mit Malware infiziert wurde – 17% bemerkten Schadsoftware auf dem Smartphone. Von Ransomware-Angriffen auf dem Smartphone waren lediglich 2% betroffen – von Ransomware-Angriffen auf dem Computer sogar nur 1%. Weitere 13% der Befragten gaben an, dass sie Schäden bei Geldgeschäften wie Online-Banking oder dem Missbrauch eigener Kontodaten erlitten.

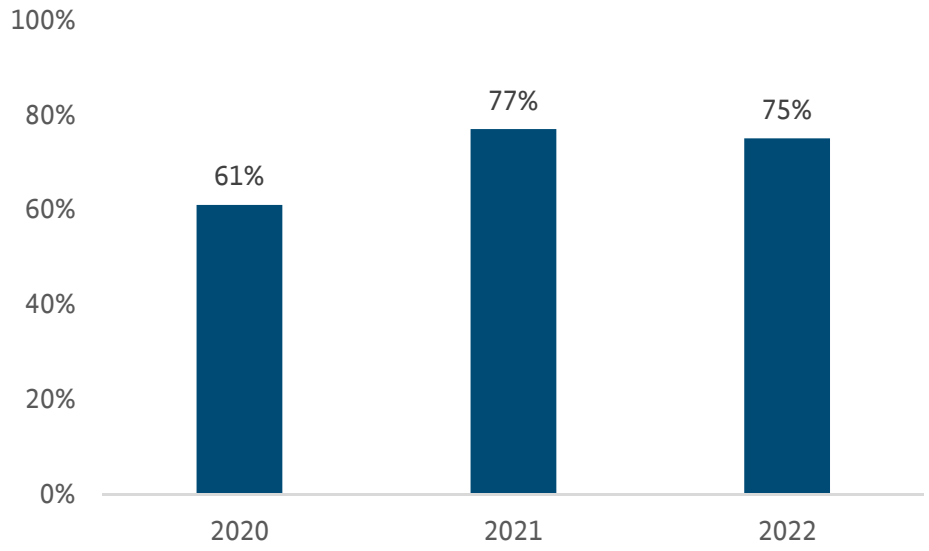


Abbildung 21: Betroffenheit von Privatpersonen durch Cybercrime laut Bitkom e.V. Anmerkung: Die angegebenen Jahreszahlen beziehen sich auf das Jahr der Datenerhebung.

Nur 18% der durch Cybercrime betroffenen Privatpersonen haben die Straftat angezeigt.

[29] Bitkom e.V. (2022). Drei Viertel von Cyberkriminalität betroffen. Online abrufbar unter: **https://bitkom.org/Presse/Presseinformation/Drei-Viertel-Cyberkriminalitaet-betroffen**
Anmerkung: Alle Angaben beziehen sich auf die vergangenen zwölf Monate ab Befragungszeitpunkt (KW37 bis KW40 2022).

6. Quo vadis, Cybercrime?

Der russische Angriffskrieg gegen die Ukraine förderte die Formierung hacktivistischer Gruppierungen und Kampagnen. Die Grenzen zwischen finanziell und staatlich motivierten Akteuren verschwimmen zunehmend.

Der russische Angriffskrieg auf die Ukraine hat die Verhältnisse der internationalen Geopolitik nachhaltig verändert. Der Krieg, welcher das Bedrohungspotenzial im Cyberraum spürbar erhöht hat, ist Katalysator für ein Verschwimmen von staatlicher und finanziell motivierter Cyberkriminalität. Zuvor primär finanziell motivierte Cyber-Akteure beziehen mit Ausbruch des Krieges vermehrt politisch Stellung und weiten ihren Fokus auf ideologische Gegner aus. Dabei kann nicht ausgeschlossen werden, dass finanziell motivierte Täter den Krieg und entsprechende ideologische Positionierungen als „Vorwand“ nutzen, um sich selbst zu etablieren.

Trotz der bereits bei Kriegsbeginn errichteten Drohkulissen konnten in der Folge bisher keine schwerwiegenden Angriffe gegen deutsche Einrichtungen und Organisationen festgestellt werden. Angesichts der Aufrechterhaltung auch medial vermittelter Drohungen der russischen Regierung gegen Unterstützerstaaten der Ukraine besteht aber weiterhin ein hohes Eskalationspotential mit Blick auf die Sicherheitslage im Cyberraum. Insbesondere eine mögliche Ausweitung des Konfliktes auf weitere Staaten sowie die Realisierung einer Cyber-Offensive, einschließlich Angriffe auf Kritische Infrastrukturen und öffentliche Einrichtungen, bergen ein hohes Gefährdungspotential.

Maßnahmen der Gefahrenabwehr - durch Cyberangriffe entstehende Schäden könnten verhindert bzw. minimiert werden.

Cybertäter agieren länderübergreifend und global, weshalb ihrem Handeln mit einer international koordinierten Zusammenarbeit der Strafverfolgungsbehörden begegnet werden muss. Im Rahmen eines „Cybercrimefighting-as-a-Service“ Ansatzes gilt es, entsprechende Kooperationen zwischen Behörden nicht nur auf nationaler, sondern auch auf internationaler Ebene auszubauen. Auch die Reduzierung virtueller und örtlicher Rückzugsräume von Cybertätern sollte hierbei im Fokus stehen.

Generell gilt für die Zusammenarbeit: Spuren im Netz sind flüchtig. Zudem stellen sich Cybertäter dank eines hochdiversifizierten, netzwerkartigen und nutzerfreundlichen Cybercrime-as-a-Service-Modells schnell auf IT-Sicherheitsmaßnahmen ein. In der Konsequenz sollte die Kooperation zwischen der IT-Sicherheitswirtschaft, den von Cybercrime bedrohten und betroffenen Unternehmen sowie den Strafverfolgungsbehörden frühzeitiger erfolgen und weiter intensiviert werden. Eine frühe Einbindung der Polizei erhöht die Wahrscheinlichkeit deutlich, strafprozessuale und gefahrenabwehrende Maßnahmen schneller und effektiver umsetzen zu können. Gerade der Gefahrenabwehr im Bereich Cybercrime kommt eine immer höhere Bedeutung zu. Aufgrund der Alltäglichkeit von Cyberangriffen wird neben dem Eigenschutz der potentiell Betroffenen selbst insbesondere die behördenseitige Gefahrenabwehr im Cyberraum als relevant eingestuft. Um die regelmäßig internationalen und zeitkritischen Cyber-Gefahren effektiv und effizient abwehren zu können, sind eine schnelle und bundesweit koordinierte Reaktionsfähigkeit sowie entsprechende internationale Abstimmungen unabdingbar. Die Systeme Geschädigter könnten dann zu größeren Teilen verfügbar bleiben, vorhandene Einschränkungen schneller behoben und digitale Spuren rechtzeitig gesichert werden.

Künstliche Intelligenz kann Cyberstraftaten erleichtern - eine weitergehende kriminelle Ausnutzung ist zu erwarten.

Der Einsatz Künstlicher Intelligenz (KI) gewinnt zunehmend an Bedeutung. Mit der Vorstellung des frei verfügbaren Chatbots „ChatGPT“ Ende 2022 ist die arbeitsalltägliche Nutzung von Tools, die auf KI basieren, auf eine neue Ebene auch der öffentlichen Diskussion gehoben worden. Neben der legalen Nutzung solcher Anwendungen bieten diese auch Potential für cyberkriminelle Zwecke. KI wurde bereits zur automatisierten Erstellung von Phishing-Nachrichten, für Desinformationskampagnen oder zur Entwicklung von Malware ausgenutzt. Eine weitergehende kriminelle Ausnutzung von KI-Methoden, beispielsweise zur (Weiter-) Entwicklung eingesetzter Werkzeuge und Angriffsvektoren, ist zu erwarten.

Um den täterseitigen Anpassungs- und Entwicklungsmöglichkeiten wirksam entgegen wirken zu können, bedarf es auf Seiten der Strafverfolgung außerdem einer leistungs- und zukunftsfähigen, technischen und personellen Ausstattung sowie einer agilen, arbeitsteiligen und flexiblen Weiterentwicklung von Ermittlungs- und Analysewerkzeugen.

Schaden in Deutschland – Täter im Ausland.
Der internationale Aspekt der Cyberkriminalität tritt weiter in den Vordergrund.

Insgesamt weisen im Phänomenbereich Cybercrime in 2022 sowohl die polizeilichen Daten als auch die Erkenntnisse von IT-Sicherheitsdienstleistern darauf hin, dass Fallaufkommen und Schäden im Phänomenbereich Cybercrime nach einem starken Anstieg in den vergangenen Jahren auf einem hohen Niveau verbleiben. Insbesondere im Jahr 2021 wurden durch den coronabedingten Digitalisierungsschub überproportional viele neue Tatgelegenheiten geschaffen, die sich aufgrund der Aufhebung der Corona-Schutzmaßnahmen im Folgejahr zumindest teilweise wieder reduziert haben.

Da im Bereich der Cyberkriminalität weiterhin von einem überdurchschnittlich hohen Dunkelfeld ausgegangen werden muss, bleibt für die realitätsnahe Beschreibung der Cyberbedrohungslage – neben der Weiterentwicklung der polizeilichen Datenbasis (Hellfeld) – eine Ergänzung z.B. durch Erkenntnisse von IT-Sicherheitsdienstleistern unerlässlich. Die Tendenz einer weitergehenden Öffnung betroffener Unternehmen und ihrer Sicherheitsdienstleister in Richtung Strafverfolgungsbehörden ist zur erfolgreichen Bekämpfung der Cyberkriminalität zu begrüßen.

Bei der Interpretation der polizeilichen Fallzahlen muss die Internationalität der Täterschaft zukünftig noch stärker reflektiert werden. Cyberstraftaten, die nachweislich aus dem Ausland heraus begangen werden, fließen in die bisherigen Betrachtungen der polizeilichen (Inlands-)Kriminalstatistik PKS nicht ein (siehe hierzu auch Punkt 2.1). Den gesunkenen Zahlen der Inlands-PKS müssen konsequenterweise die steigenden Fallzahlen der Auslandstaten hinzugestellt werden und in die Gesamtbewertung einfließen. Entsprechende Maßnahmen zur Erhebung und Auswertung der Auslandstaten sind bereits eingeleitet und werden künftig ein umfassenderes und realitätsgetreueres Abbild des Phänomenbereichs Cybercrime liefern.

Kriminelle Infrastrukturen zerschlagen und Aktivitäten von Cybertätern nachhaltig eindämmen.

Die bisherigen Erfahrungen im Bereich Cybercrime zeigen: Personelle Ermittlungen alleine sind nicht dazu geeignet, die cyberkriminelle Szene langfristig zu schädigen. Die Ermittlung der Hintermänner cyberkrimineller Aktivitäten ist langwierig und ressourcenintensiv. Gelingt die Ermittlung, wird eine Festnahme oft dadurch erschwert, dass betreffende Personen sich in sog. safe havens wie Russland aufhalten. Dies führt dazu, dass cyberkriminelle Handlungen aus dem Ausland rechtlich oft nicht geahndet und Täter nicht an einer weiteren Tatausführung gehindert werden können. Eine sinnvolle Ergänzung personeller Ermittlungen ist insofern die bewusste Zerschlagung (sog. Disruption) von kriminellen IT-Infrastrukturen. Die bisherigen Erfolge der deutschen Polizeibehörden wie z.B. der Takedown der illegalen Verkaufsplattform Hydra Market, das Abschalten von DDoS-Booter-Diensten durch die Operation Power Off und die Zerschlagung der Emotet-Infrastruktur zeigen, dass eine Wiederinbetriebnahme vieler Infrastrukturen in der Regel kurzfristig nicht möglich und für die Täter sehr „teuer“ ist.

Insbesondere das Beispiel Emotet macht das Potential des Infrastrukturansatzes sehr deutlich: Es dauerte insgesamt zehn Monate, bis die dahinterliegende Infrastruktur wieder soweit aufgebaut war, dass Schadsoftware erneut festgestellt werden konnte. Ein – für den Cyber-Bereich – verhältnismäßig langer Zeitraum, in dem Emotet nicht für Angriffe auf Opfer genutzt werden konnte. Ergänzt wird das technische Vorgehen gegen kriminelle Infrastrukturen durch den Zugriff auf illegale Gewinne der Tätergruppierungen. Ein Verfahren, das beide Elemente vereint, ist hierbei der erfolgreiche Zugriff auf die Serverinfrastruktur des Bitcoin-Mixers Chipmixer im März 2023. Neben der Zerschlagung der Infrastruktur gelang es, inkriminierte Bitcoin im Wert von ca. 90 Mio. Euro zu sichern und so dem kriminellen Wirtschaftskreislauf zu entziehen.

Der Infrastrukturansatz ermöglicht es, kriminelle IT-Infrastrukturen zu zerschlagen und den Tätergruppierungen kriminelle Erträge zu entziehen. In Ergänzung zu personenbezogenen Ermittlungen können damit die Aktivitäten von Cybertätern für einen relevanten Zeitraum gestört und künftige Angriffe zumindest temporär eingeschränkt bzw. unterbunden werden. Zur umfassenden Bekämpfung von Cyberkriminalität zielt das BKA daher künftig verstärkt auf die Zerschlagung krimineller Infrastrukturen ab.

Impressum

Herausgeber
Bundeskriminalamt, 65173 Wiesbaden

Stand
Mai 2023

Gestaltung
Bundeskriminalamt, 65173 Wiesbaden

Bildnachweis
Bundeskriminalamt

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