Bundeskriminalamt

BKA

Cybercrime

Bundeslagebild 2021

Allgemeine Informationen

Das Bundeslagebild Cybercrime 2021 wird durch das Bundeskriminalamt in Erfüllung seiner Zentralstellenfunktion erstellt. Es enthält die aktuellen Erkenntnisse und Entwicklungen im Bereich der Cybercrime 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 sog. Cybercrime im engeren Sinne (CCieS). Die einzelnen Delikte dieses Phänomenbereichs werden in Kapitel 2 „Die Polizeiliche Kriminalstatistik (PKS)“ genauer beschrieben.

Delikte, die lediglich unter Nutzung von Informationstechnik begangen werden (sog. Cybercrime im weiteren Sinne, CCiwS) und nicht der CCieS zugeordnet werden können, bleiben bei den Betrachtungen in diesem Bundeslagebild weitestgehend außen vor.

Grundlage für den statistischen Teil des Lagebildes sind die Daten der Polizeilichen Kriminalstatistik (PKS). Hier wird das sog. 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 zutreffende Lagebeschreibung von Bedeutung ist, die qualitative Aussagekraft des polizeilichen Hellfeldes zu erhöhen, indem verstärkt auch polizeiexterne Erkenntnisse in die Lagebilderstellung einbezogen werden.

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 2021 finden Sie QR-Codes, über die Sie sich bei Bedarf ergänzende Informationen und Definitionen erschließen können.

Inhaltsverzeichnis

1 Cybercrime 2021

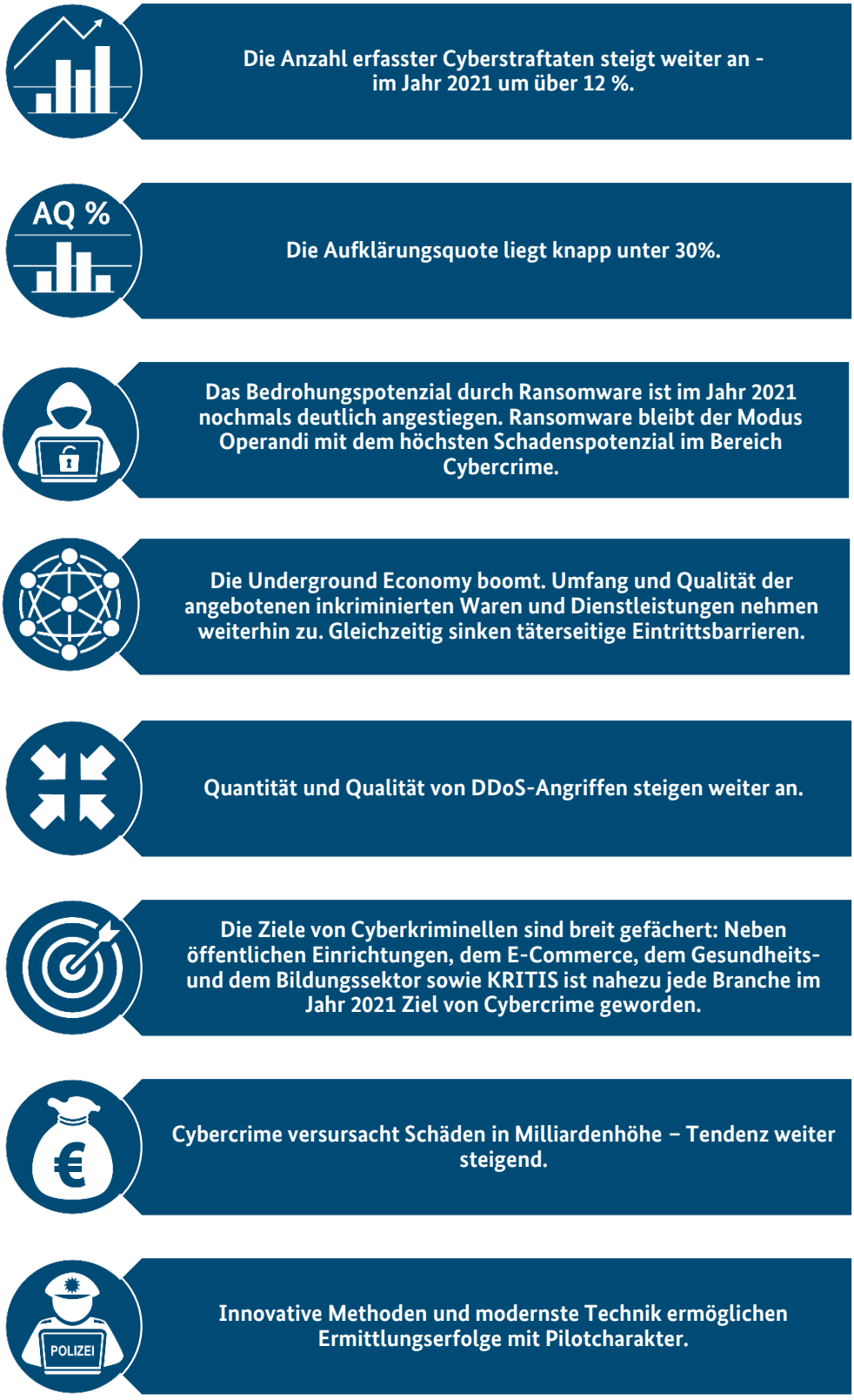


Abbildung 1: Die wesentlichen Aspekte der Cybercrime in Deutschland 2021

1.1 FOKUS 2021 – RANSOMWARE

2021 – Das Jahr der Ransomware

Ransomware war erneut die primäre, gesamtgesellschaftliche Bedrohung im Bereich der Cybercrime. Das Bedrohungs- und Schadenspotenzial ist im Jahr 2021 nochmals spürbar angestiegen.

2021 war geprägt von Angriffen auf Kritische Infrastrukturen, die öffentliche Verwaltung oder internationale Lieferketten. Neben monetären Schäden beeinträchtigen derartige Angriffe auch die Funktionsfähigkeit des Gemeinwesens.

Schadensdimension und Profit

Ø-Ransom 2021:
204.695 US-Dollar.

Ø-Ransom 2020:
169.446 US-Dollar [a]

Anstieg um 21%

Jährlicher Schaden durch Ransomware

2021: ca. 24,3 Mrd. Euro.

2019: ca. 5,3 Mrd. Euro [b]

Das Schadenspotenzial von Ransomware nimmt rasant zu.

Profit durch Ransomware-Gruppierungen 2021:

602 Millionen US-Dollar [c].

Modi Operandi

Double Extortion:
Der Standard-Modus-Operandi (Datenverschlüsselung und -veröffentlichung).

Triple Extortion:
Zusätzlich zur Datenverschlüsselung und -veröffentlichung erfolgen DDoS-Attacken beim Opfer.

Second-Stage-Extortion:
Auch Kunden der eigentlichen Opfer werden damit erpresst, dass Ihre Daten veröffentlicht werden, sollte keine Zahlung erfolgen.

Ransomware: Die Top-Bedrohung

- Alle Unternehmen, Organisation und Einrichtungen können zum Ziel werden – egal ob KMU, KRITIS oder öffentliche Einrichtungen.
- Durch Ransomware-as-a-Service steigt die Professionalisierung stetig an.
- Ransomware kann ganze Lieferketten und Geschäftsprozesse lahmlegen.
- Die Akteure passen sich schnell den internationalen Entwicklungen an und machen sich Rebrandings zunutze (siehe Kapitel 5).
- Wirksames Mittel gegen Ransomware:
  Eine vertrauensvolle Zusammenarbeit von Wirtschaft und Polizei als Fundament erfolgreicher polizeilicher Prävention und Strafverfolgung.

Abbildung 2: Wesentliche Aspekte des Modus Operandi Ransomware und seine Relevanz für das Jahr 2021
a = Aggregierte Daten des Incident-Response-Dienstleisters Coveware, abrufbar unter: https://www.coveware.com/blog
b = Bitkom e.V, Wirtschaftsschutzbericht 2021, 05.08.2021, abrufbar unter: https://www.bitkom.org/sites/default/files/2021-08/bitkom-slides-wirtschaftsschutz-cybercrime-05-08-2021.pdf
c = Chainalysis, Crypto Crime Report 2022, 10.02.2022, Exzerpt abrufbar unter: https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/

1.2 HERAUSRAGENDE SACHVERHALTE 2021

- Die Webseite eines Impfzentrums sowie die Homepage des zugehörigen Landkreises wurden ab dem 05.03.2021 Ziele von DDoS-Attacken. Beide Internetseiten waren für einige Tage nicht erreichbar.

DDoS

- Am 08.05.2021 kam es zu einem Ransomware-Angriff auf die US-Firma Colonial Pipeline. Aufgrund des Angriffs musste eine der größten Ölpipelines der USA vom Netz genommen werden. Es kam zu Versorgungsengpässen und Lieferausfällen. Das FBI ordnete den Angriff der Ransomware bzw. Gruppierung DarkSide (CarbonSpider) zu.

Ransomware

- Ein deutscher IT-Dienstleister für Banken, wurde zwischen dem 03.06 und dem 14.06.2021 Ziel anhaltender DDoS-Angriffe. Teilweise waren Webseiten, Online-Banking und weitere Services nicht erreichbar oder nur eingeschränkt möglich.

DDoS

- Am 02.07.2021 gab der amerikanische IT-Dienstleister Kaseya Ltd. einen Ransomwares-Angriff auf eine von ihm angebotene Remote-Lösung bekannt. In der Folge kam es zu einem Supply-Chain-Angriff - das Unternehmen wurde als Distributor für die Ransomware REvil missbraucht. Über mehrere IT-Systemhäuser gelangte sie anschließend an eine Vielzahl, auch deutscher, Endkunden.

Ransomware

- Nach einem Ransomware-Angriff auf die Landkreisverwaltung Anhalt-Bitterfeld am 05.07.2021 wurde erstmals der Cyber- Katastrophenfall in Deutschland festgestellt. Die Bereitstellung öffentlicher Dienstleistungen war nachhaltig eingeschränkt. Zwar war zwei Wochen nach dem Angrif eine Notinfrastruktur einsatzbereit. Allerdings war auch Monate nach dem Angriff noch kein normaler Regelbetrieb möglich.

Ransomware

- In einem Hacker-Forum wurde im August 2021 eine Datenbank mit Daten von angeblich 30 Mio. Nutzern eines US-amerikanischen Mobilfunkanbieters angeboten. Der geforderte Preis belief sich auf 6 Bitcoin, damals etwa 240.000 Euro. Der Anbieter gab an, dass die Daten aus einem Angriff auf den Mobilfunkanbieter stammten.

Data-Leak

- Am 30.09.2021 wurde ein Cyber-Sicherheitsvorfall durch ein städtisches Klinikum in Sachsen-Anhalt gemeldet. Im Netzwerk des Klinikums wurde das unrechtmäßig eingesetzte Penetration-Testing-Tool Cobalt Strike entdeckt. Die Kommunikationssysteme sowie die Nutzung der IT waren nur eingeschränkt möglich. Zudem wurden täterseitig Daten ausgeleitet. Die medizinische Versorgung konnte durchgehend gewährleistet werden.

Malware

- Ein Softwareunternehmen, dessen Softwarelösungen in etwa einem Viertel der deutschen Arztpraxen eingesetzt wird, stellte am 04.11.2021 die Verschlüsselung ihrer Server- und Netzwerkinfrastruktur fest und war ab diesem Zeitpunkt nicht mehr arbeitsfähig. Bei der eingesetzten Ransomware handelte es sich um Conti.

Ransomware

- Am 09.12.2021 wurde eine Zero-Day-Schwachstelle in der weitverbreiteten Protokollierungsbibliothek Log4j bekannt, die Bestandteil zahlreicher Open-Source- sowie kommerzieller Softwareprodukte ist. Die Schwachstelle ermöglicht die Installation von Schadsoftware und führt so zur Verwundbarkeit zahlreicher Unternehmen. Die langfristigen Folgen sind noch nicht absehbar.

Exploit/ Schwachstelle

Abbildung 3: Beispiele für relevante Cyberangriffe in Deutschland 2021

2 Die Polizeiliche Kriminalstatistik (PKS)

Das Bundeslagebild Cybercrime bildete in den vorherigen Jahren die Fallzahlen der Cybercrime im engeren Sinne nach einem BKA-eigenen Summenschlüssel („CCieS“) ab (siehe hierzu Abb. Nr. 5). Die Fachlichkeit Cybercrime und PKS haben sich im Jahr 2020 auf die Einführung eines neuen PKS-Summenschlüssels „Cybercrime“ zur bundesweit einheitlichen Beschreibung der Cybercrime verständigt, der erstmalig in der PKS 2021 ausgewiesen wird. Dieser Summenschlüssel ersetzt den bis 2020 in der PKS ausgewiesenen Summenschlüssel „Computerkriminalität“.

Aus Gründen der Vergleichbarkeit wurden die Fallzahlen dieses Summenschlüssels auch für die Jahre 2019 und 2020 anhand der neuen Erfassungsmodalitäten manuell berechnet (siehe hierzu Abbildung Nr. 6). Darüber hinaus erfolgt aus dem gleichen Grund für das Jahr 2021 letztmalig die Darstellung des BKA-eigenen Summenschlüssels „CCieS“. Es ist vorgesehen, Aussagen zur Fallentwicklung cyberrelevanter Straftaten anhand der PKS-Zahlen künftig mittels des neu eingeführten Summenschlüssels „Cybercrime“ zu treffen.

Bei der Polizeilichen Kriminalstatistik handelt es sich um die einzige bundesweit geführte und qualitätsgesicherte Statistik auf der Grundlage polizeilicher Ermittlungen. Aufgrund des phänomenbedingt erheblichen Dunkelfeldes im Bereich Cybercrime, das in Studien auf bis zu 91,5% geschätzt wird [1], ist der PKS allerdings lediglich eine begrenzte Aussagekraft hinsichtlich der Gesamtheit der in Deutschland verübten Cyber-Straftaten zuzuschreiben. Sie ist insofern eine Datenbasis, auf der vor allem Trendaussagen zur Entwicklung der Cybercrime getroffen werden können.

Auch im Berichtsjahr 2021 sind in der PKS signifikante Steigerungen bei den Fallzahlen der dort aufgeführten Cyber-Straftaten feststellbar. So bildet der cyberspezifische Summenschlüssel „Cybercrime“ einen Anstieg von über 12% ab. Die Aufklärungsquote liegt mit knapp unter 30% weiterhin deutlich unter dem PKS-Durchschnitt.

Mögliche Erklärungsansätze für diese Entwicklung sind u.a.:

- Die Zahl der tatsächlichen Cybercrime-Vorfälle ist angestiegen und Täter bedienen sich der vielfältigen Tatgelegenheiten, die ihnen die Underground Economy bietet.
- Die Corona-Pandemie ist mit ihrem Schub an Digitalisierung ein „Beschleuniger“ für Cybercrime gewesen, wodurch zusätzliche Tatgelegenheiten geschaffen und täterseitig ausgenutzt wurden.
- Straftaten verlagern sich vom analogen zunehmend in den digitalen Raum.
- Über eine erhöhte Akzeptanz zur Anzeigeerstattung sind trotz erheblichem Dunkelfeld mehr Fälle in das polizeiliche Hellfeld gelangt.

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

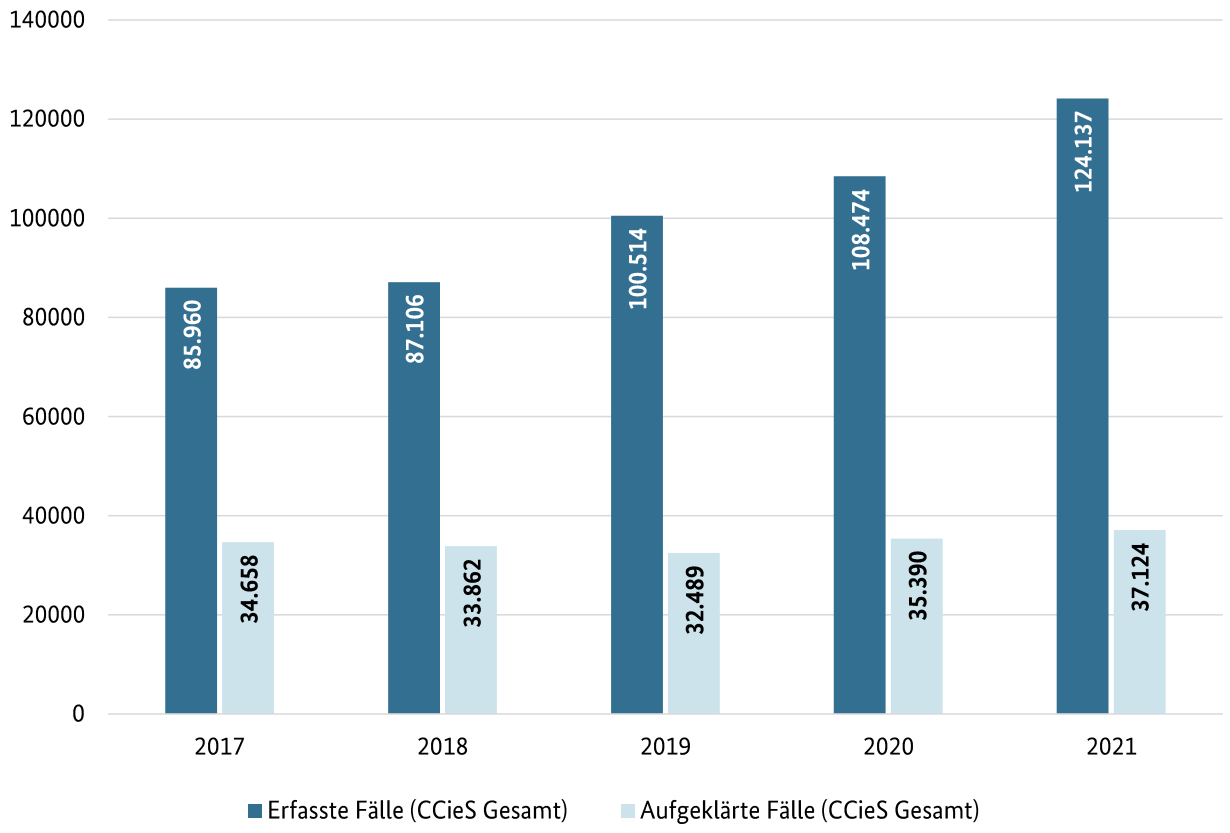


Abbildung 4: Relation zwischen erfassten und aufgeklärten Cybercrime-Fällen in Deutschland von 2017 bis 2021 vor Änderung der Erfassungsmodalitäten

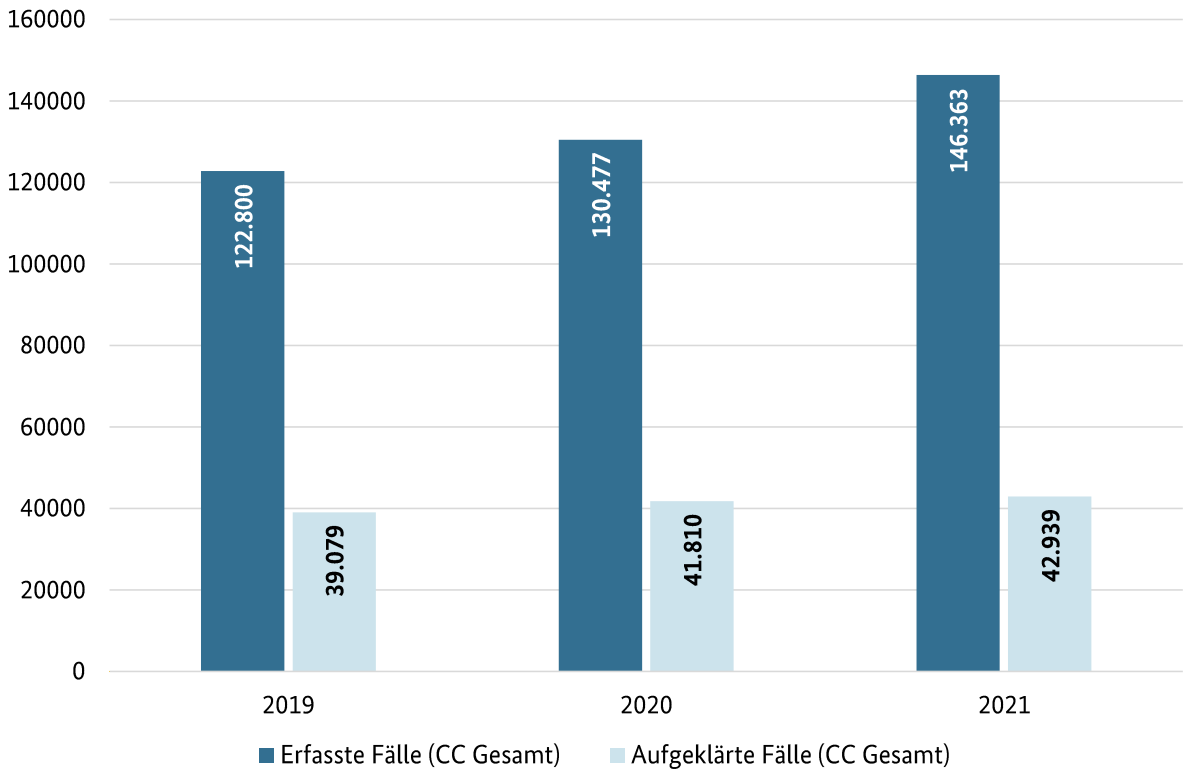
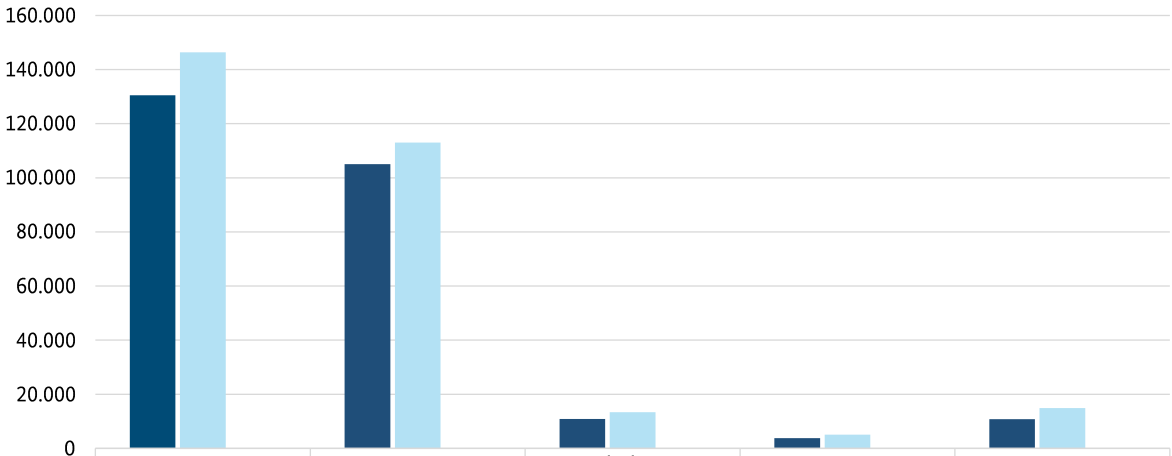


Abbildung 5: Relation zwischen erfassten und aufgeklärten Cybercrime-Fällen in Deutschland von 2019 bis 2021 unter Berücksichtigung der geänderten Erfassungsmodalitäten

	Anzahl erfasster Fälle (absolut)	Absolute Differenz erfasster Fälle	Prozentuale Differenz erfasster Fälle	Aufgeklärte Fälle (absolut)	Aufgeklärte Fälle Differenz (absolut)	Aufgeklärte Fälle in %, Aufklärungs-Quote (AQ)	Veränderung AQ (Prozent-punkte)
2017	85.960			34.658		40,3%	
2018	87.106	1.146	1,3%	33.862	-796	38,9%	-1,4
2019	100.514	13.408	15,4%	32.489	-1.373	32,3%	-6,6
2020	108.474	7.960	7,9%	35.390	2.901	32,6%	0,3
2021	124.137	15.663	14,4%	37.124	1.734	29,9%	-2,7
Fallzahlen 2019- 2021 nach modifizierten Erfassungsmodalitäten							
2019	122.800			39.079		31,8%	
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

Abbildung 6: Erfasste und aufgeklärte Fälle (absolute und prozentuale Angaben inkl. der jeweiligen Aufklärungsquote) in Deutschland von 2017 bis 2021 – Tabellenübersicht mit alten und neuen Erfassungsmodalitäten

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 Anstiege auf (siehe hierzu Abbildung 7).



	CC gesamt	Computerbetrug	Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	Datenveränderung, Computersabotage	Ausspähen von Daten einschl. Vorbereitungshand-lungen und Datenhehlerei
2020	130.477	105.049	10.895	3.770	10.763
2021	146.363	113.002	13.390	5.053	14.918
Veränderungsrate	12,2%	7,6%	22,9%	34%	38,6%

Abbildung 7: Fallaufkommen von Straftaten der Cybercrime 2020 und 2021

Während bei der Gesamtzahl der in der PKS erfassten Straftaten im Jahr 2021 im Vergleich zum Vorjahr ein Rückgang von 4,9% verzeichnet wurde, ist bei den Cyber-Straftaten mit einem Anstieg von 12,2% ein stark gegenläufiger Trend auszumachen (siehe oben). Die bereits in den letzten Jahren festgestellte Entwicklung, wonach Cyber-Straftaten zunehmend an Bedeutung gewinnen, setzt sich damit weiterhin fort.

Demgegenüber steht eine umgekehrte Entwicklung im Bereich der Aufklärungsquote: Während die Aufklärungsquote im PKS-Durchschnitt leicht angestiegen ist (2021 Gesamt: 58,7%, + 0,3%) ist bei allen Cyberdelikten ein gegenläufiger Trend feststellbar (2021 Gesamt: 29,3%, - 2,7%).

Dieser Trend ist unter anderem durch die zunehmende Digitalisierung der Gesellschaft, die verstärkte Anonymisierung im Netz und die komplexe Ermittlung und Attribuierung von vielfach im Ausland befindlichen Tätern bedingt und stellt eine besondere Herausforderung für alle mit Cybercrime befassten Dienststellen dar.

3 Relevante Phänomenbereiche der Cybercrime

3.1 DIE UNDERGROUND ECONOMY

Die Underground Economy (UE) bezeichnet die Gesamtheit der Plattformen und Services, welche von (Cyber-)Kriminellen genutzt wird, um Daten, Tools, Jobs und relevantes Täter-Know-How anzubieten oder in Anspruch zu nehmen. Dieses Angebot bildet die Grundlage vieler Straftaten im Cyber-Bereich.

Exemplarisch können folgende Services und Angebote der UE im Kontext Cybercrime aufgeführt werden:

Service	Preis in US $ (gesamt oder pro Nutzungszeitraum / pro Einheit)	
BankingTrojaner		
▪ **Desktop-Version**	1.000 - 10.000 $	bei Kauf
▪ **Mobile-Version**	1.000 - 10.000 $	bei Kauf
RAT (Remote Administration Tool)	60 - 530 $ ca. 3.000 $	pro Monat bei Miete bei Kauf
Mining Bots	50 – 150 $	pro Monat bei Miete
Crypting	0 - 100 $ 30 - 500 $	bei Kauf von einem Crypt bei einem Wochen-Abo mit 50 Crypts pro Tag
DDoS-as-a-Service	80 - 1.500 $	pro Monat bei Miete
Bulletproof Hosting		
▪ **Shared**	5 - 50 $	pro Monat bei Miete
▪ **Dedicated**	50 - 700 $	pro Monat bei Miete
Counter-AV-Service	10 $	pro Monat und 300 Scans
Infection-on-Demand (Phishing-Services o.ä.)	Ab 100 $	pro Monat
Stealer Logs	5 -15 $ 400 – 900 $	pro Stück pro Monat für Abonnement

Abbildung 8: Übersicht krimineller Services der Underground Economy/ im Darknet

Neben diesen und weiteren Services, waren es im Jahr 2021 vor allem die sog. Initial Access Broker (IAB) und im Netz angebotene gefälschte Impfzertifikate, die an Relevanz innerhalb der Underground Economy und des „Crime-as-a-Service-Modells“ gewonnen haben.

Initial Access Broker handeln mit unrechtmäßig erlangten Zugängen zu Netzwerken, vielfach für Unternehmens- oder Behördennetzwerke. Meist handelt es sich dabei um RDP-, VPN-, Citrix-, Webshell- und Control-Panel-Zugänge. Diese sind feste Bestandteile der UE und haben wesentlichen Anteil an der Begehung von Cyber-Straftaten. Abnehmer der erbeuteten Zugangsdaten sind u.a. Ransomware-Gruppierungen. Durch die steigende Verbreitung von Remote-Zugängen für Home-Office-Arbeitsplätze steigt bei unverändertem Entdeckungsrisiko das Potenzial für einen wirtschaftlichen Gewinn beim Einsatz

von Ransomware. Entsprechend steigert sich auch die Attraktivität der Tätigkeiten von IAB im Gesamtkontext der Services der UE.

Die Preise der IAB sind abhängig von der Art des Zugangs, insbesondere aber auch von Unternehmensparametern wie der Branche, dem jährlichen Umsatz, der Mitarbeiteranzahl, der Anzahl an dort eingesetzten PC, ebenso aber auch von dem gesellschaftlichen Prestige, der Nationalität und der Reputation des jeweiligen Brokers. Sie schwanken daher zwischen wenigen Hundert und mehreren Zehntausend Euro.

Seit Beginn der Corona-Impfungen konnte auf unterschiedlichen Foren der Verkauf von unrechtmäßig ausgestellten QR-Codes als Impfnachweis festgestellt werden. Die Verkäufer bieten neben den QR-Codes meist auch die „klassischen" gelben Impfpässe mit dem Nachweis einer Corona-Impfung, sowie Chargen-Aufkleber von Corona-Impfungen an. Der Preis für einen digitalen QR-Code lag entsprechend der hohen Nachfrage 2021 zeitweise bei ca. 350 Euro.

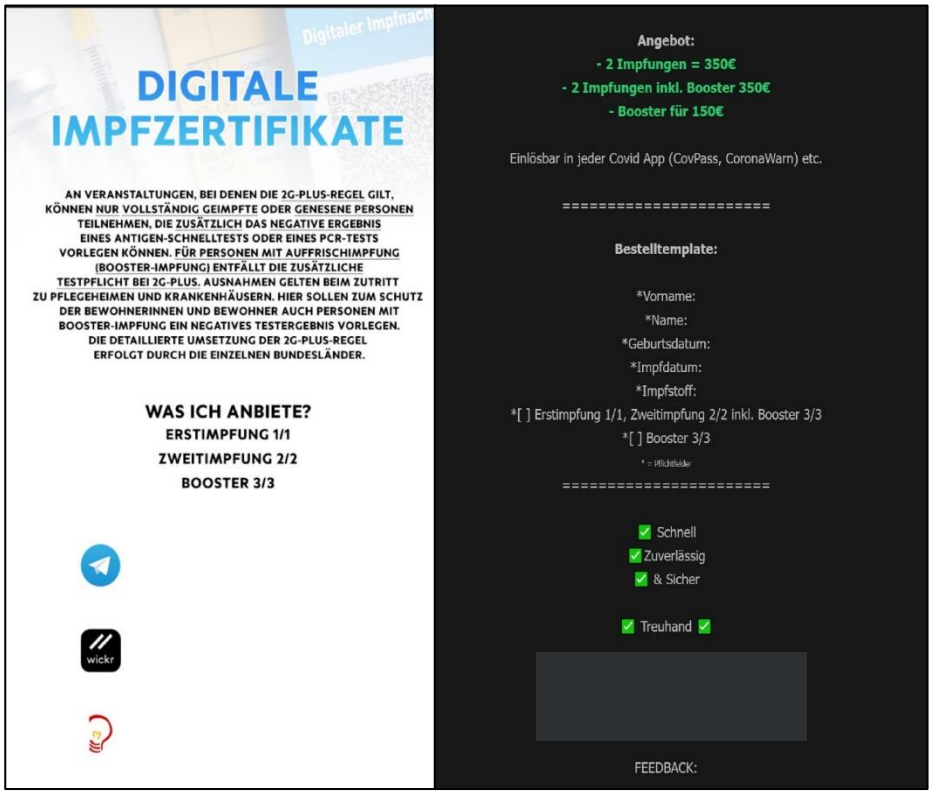


Abbildung 9: Krimineller Service für den Erwerb von gefälschten digitalen Impfzertifikaten (Screenshot)

Die Underground Economy boomt: 2021 haben sich besonders Angebote für Ransomware-as-a-Service, Initial Access Broker und gefälschte Impfzertifikate hervorgetan.

Bei der Beobachtung der Marktplätze lässt sich im Verlauf der Jahre eine zunehmende Selbstregulierung über sog. „Ethik-Codes" festzustellen. Anfänglich betraf dies nur Verbote zum Handel mit Schusswaffen oder Kinderpornografie, mittlerweile werden u.a. auch Impfstoffangebote verboten. Ein entscheidender Einschnitt innerhalb der Community war in diesem Zusammenhang auch das Verbot von Ransomware auf

den größten UE-Foren Mitte 2021 (siehe Kapitel 3.4.2 Ransomware). In den letzten Jahren ist zudem feststellbar, dass die Lebensdauer von neuen Darknet-Marktplätzen immer kürzer wird. Teilweise sind diese nur wenige Monate aktiv.

Von besonderer Bedeutung im Kampf gegen die Betreiber krimineller IT-Infrastrukturen war das Verfahren gegen die Hoster des sogenannten „Cyberbunkers“. Die Landeszentralstelle Cybercrime (LZC) der Generalstaatsanwaltschaft Koblenz und das Landeskriminalamt Rheinland-Pfalz führten seit 2015 ein umfangreiches Ermittlungsverfahren gegen die Betreiber des als "Bulletproof-Hoster" bezeichneten Rechenzentrums.

Gegen die Beschuldigten bestand der dringende Verdacht, in einem ehemaligen NATO-Bunker in Traben-Trarbach unter dem Szenenamen "Cyberbunker" ein Rechenzentrum betrieben zu haben, dessen einziger Zweck es war, Webseiten krimineller Täter zu speichern und diesen einen Schutz vor Strafverfolgung „anzubieten“. In dem Bunker wurden zahlreiche Webseiten gehostet, über die international agierende Kriminelle verbotene Waren wie Drogen und gefälschte Dokumente sowie gestohlene Daten vertrieben und groß angelegte Cyberangriffe durchführten.

Nach umfangreichen Ermittlungsmaßnahmen der Landespolizei Rheinland-Pfalz, zeitweise unterstützt durch Kräfte der Polizei Hessen sowie der Bundespolizei, wurde der Hauptangeklagte am 13.02.2021 vor dem Landgericht Trier zu fünf Jahren und neun Monaten Haft verurteilt. Gegen weitere Mitglieder der kriminellen Vereinigung sprach das Gericht Haftstrafen zwischen drei sowie vier Jahren und drei Monaten aus. Die Verurteilung erfolgte hierbei wegen der Bildung einer kriminellen Vereinigung gemäß § 129 StGB und unterstreicht den Unrechtscharakter der Bereitstellung von IT-Infrastrukturen für kriminelle Plattformen.

Zukünftig kann das im Cyberbunker-Verfahren festgestellte „Bereitstellen von Infrastruktur“ als Beihilfehandlung zum neuen § 127 StGB (Betreiben krimineller Handelsplattformen) erfasst sein.

Cyber-Straftaten haben durch ihre hohe Reichweite ein enormes Schadenspotenzial. Strafnormen und Eingriffsbefugnisse müssen hierbei mit der technischen Entwicklung der Täterseite Schritt halten.

Die „GermanRefundCrew“

Verfahrenshintergrund

Das BKA hat im Jahr 2020 erstmals gegen mehrere Betreiber illegaler Handelsplattformen auf dem Messengerdienst „Telegram“ ermittelt und bei operativen Maßnahmen im Oktober 2020 neun Telegram-Gruppen geschlossen.
Durch die Auswertung der Beweismittel konnten im Nachgang sieben Mitglieder der sog. „GermanRefundCrew“ identifiziert werden, die im Verdacht stehen über Telegram die gewerbs- und bandenmäßige Durchführung von „Refund“-Betrügereien angeboten und gemeinsam begangen zu haben.

Die Telegram-Gruppe / Modus Operandi

Die Täter nutzten die Telegram-Gruppe „GermanRefundCrew“, um ihren „Kunden“ die Durchführung von sog. Rückerstattungsbetrugstaten für eine bestimmte Provision anzubieten. Hierbei war es ihnen durch eine dynamische Anpassung der Tatbegehungsweise möglich, Betrugserkennungssysteme der Versandhäuser zu überlisten und Rückerstattungen für die Waren ihrer „Kunden“ zu erlangen, die faktisch nie zurückgesendet wurden.
In dem vorliegenden Fall wurden insbesondere die Rücksendeetiketten, welche durch die Versandhäuser an ihre Kunden verschickt wurden, von der Gruppe „GermanRefundCrew“ manipuliert bzw. teilweise durch den Kundensupport der Versandhäuser die Rückerstattung des Kaufpreises veranlasst. Insgesamt führten die Täter über 600 Betrugstaten durch. Es entstand bei den Versandhändlern hierbei ein Gesamtschaden von über 500.000 Euro.

Operative Maßnahmen:

Bei einer konzertierten Aktion der Generalstaatsanwaltschaft Bamberg – ZCB, des BKA und weiterer Strafverfolgungsbehörden wurden am 18.05.2021 gegen sieben Tatverdächtige Durchsuchungsbeschlüsse vollstreckt. Im Rahmen dieser Durchsuchungen stellten die Ermittler Smartphones, Laptops und andere Datenträger sicher. Weiterhin konnten aus den Taten erlangte Waren, Bargeld sowie Kryptowährungen aufgefunden und sichergestellt werden. Darüber hinaus gelang die technische Sicherung und Übernahme von sechs Telegram-Accounts.

3.2 DATA LEAKS

Auf einschlägigen Foren und Marktplätzen der Underground Economy werden Daten, die zuvor durch einen unberechtigten Zugriff erlangt wurden, zum Kauf angeboten. Dieses Angebot umfasst Anmeldedaten, Zahlungsdaten, personenbezogene Daten etc., welche dann für weitere kriminelle Taten genutzt werden; entweder für Phishing-Kampagnen oder zur Übernahme der entwendeten Konten und Identitäten. Solche personenbezogenen Daten bilden einen elementaren Bestandteil des Cybercrime-as-a-Service-Angebots (CaaS). Die Daten werden in Form von Datensätzen angeboten und können bereits für geringe Summen erworben werden; teilweise mit einer Garantie auf Ersatz, sollten die Zahlungs- und Login-Daten kurz nach Erwerb nicht mehr gültig sein. Ebenfalls finden vermehrt Verkäufe von Zugangs- und Zahlungsdaten über Telegram statt.

Das Hasso-Plattner-Institut (HPI) erfasst jeden Monat Millionen von Data Leaks kompromittierter Konten.[2] Im Jahr 2021 zeichneten sich dabei quartalsweise Schwankungen ab mit einem besonders starken Anstieg im November 2021. Insgesamt erfasste das HPI im Jahr 2021 mit Stand 14.01.2022 ca. 184,65 Mio. kompromittierte Nutzerkonten.

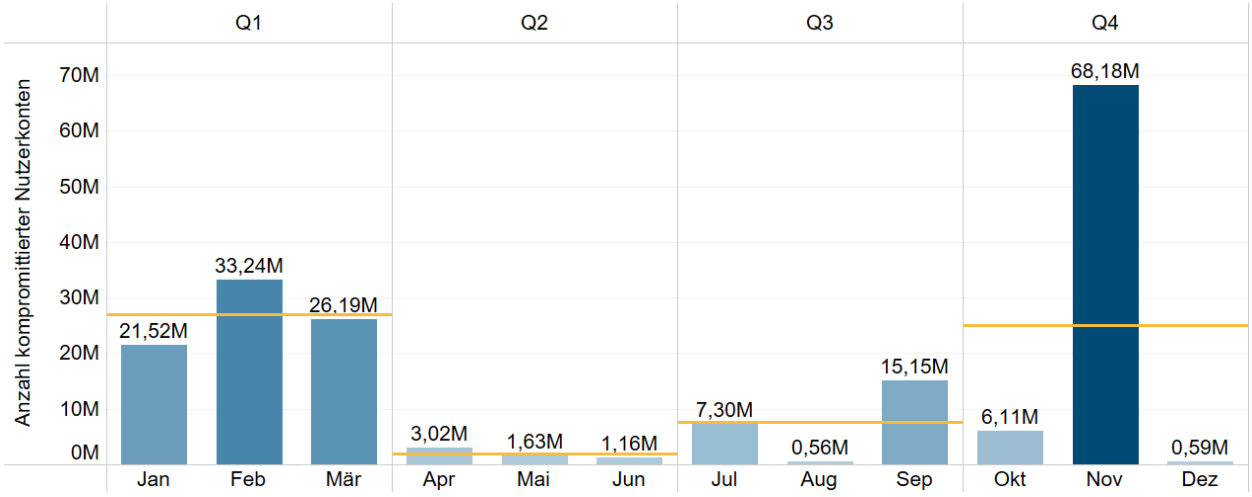


Abbildung 10: Anzahl der durch das Hasso-Plattner-Institut verzeichneten Data Leaks nach Quartal und Monat. Die orangene Linie gibt die jeweiligen Quartalsdurchschnitte an.

(Zugangs-)Daten jeder Art werden innerhalb der Underground Economy als „Rohstoff" gehandelt und dienen als Ausgangspunkt für weitere kriminelle Handlungen.

[2] Hasso-Plattner-Institut (HPI), Identity Leak Checker, online einsehbar unter: **https://sec.hpi.de/ilc/statistics**

3.3 EINTRITTSVEKTOREN

Für das Eindringen in ausgewählte Systeme bedienen sich Cyberkriminelle verschiedener Methoden. Hier reicht das Angebot von illegal erlangten Zugangsdaten (siehe Kapitel 3.2), dem Wissen um vorhandene Zero-Day-Exploits und nicht gepatchte Schwachstellen bis hin zu Bots, welche automatisiert Spam-Mails versenden.

3.3.1 Phishing

Klassisches Phishing gehörte auch 2021 zu den Haupteintrittsvektoren für Schadsoftware und war ursächlich für den massenhaften Abgriff sensibler personenbezogener Daten, wie beispielsweise Bankdaten. Schadsoftware wird hierbei häufig über maliziöse Dokumente als E-Mail-Anlage verteilt. Phishing betrifft Unternehmen wie auch Privatpersonen gleichermaßen, denn die abgegriffen personenbezogenen Daten werden auf Darknet-Marktplätzen gehandelt und dienen als „Rohstoff“ für weitere Straftaten.

Für betroffene Unternehmen kann erfolgreiches Phishing zu Datenverlust, kompromittierten Nutzerkonten und – bei erfolgreichem Einschleusen von Malware – zu hohen finanziellen Schäden führen. Die Anzahl an Phishing-Versuchen nimmt stetig zu. Der Microsoft Defense Report 2021[3] zeigt seit der Corona-Pandemie einen nahezu linearen Anstieg hinsichtlich der Anzahl festgestellter Phishing-Mails. Eine Entspannung dieser Zahlen ist aufgrund der Attraktivität von Spam-Mails und Phishing-Mails nicht zu erwarten.

Gemäß Erkenntnissen der Anti-Phishing-Working-Group (APWG)[4], war der Finanzsektor 2021 weltweit am stärksten von Phishing betroffen.[5] Ein starker Anstieg der Phishing-Zahlen konnte seit Beginn der Corona-Pandemie auch bei Verwaltungen, Wirtschaftsdienstleistern und im Gesundheitswesen verzeichnet werden. Die APWG stellt bezogen auf die Anzahl monatlich neu identifizierter Phishing-Webseiten seit der Hochphase der Corona-Pandemie 2020 einen massiven Anstieg fest. Deren Anzahl verweilt auch für das Jahr 2021 auf einem signifikant höheren Niveau als noch vor Beginn der Corona-Krise.

Phishing ist damit nicht nur einer der beliebtesten Eintrittsvektoren und Angriffsarten von Cyberkriminellen – die Zahl an Phishing-Vorfällen stieg in den letzten Jahren auch stark an.

[3] Microsoft, Microsoft Digital Defense Report 2021, 02.11.2021, online einsehbar unter: **https://www.microsoft.com/de-de/techwiese/news/microsoft-digital-defense-report-2021-die-aktuelle-lage-im-bereich-cybercrime.aspx**

[4] Internationale Arbeitsgruppe mit mehr als 3000 Mitgliedern weltweit zur Bekämpfung von Phishing und Betrugsdelikten

[5] Anti-Phishing-Working-Group, Trendberichte, quartalsweise Publikation, online einsehbar unter: **https://apwg.org/trendsreports/**

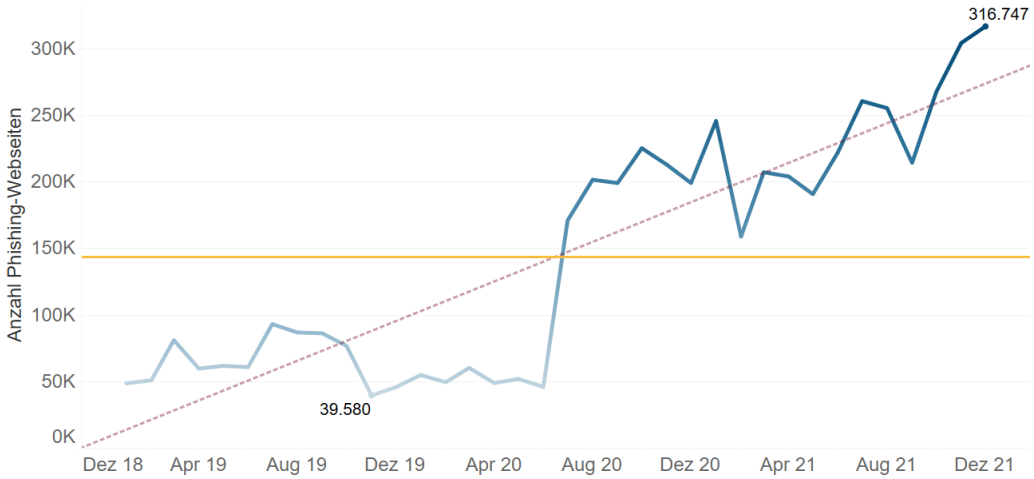


Abbildung 11: Anzahl der durch die Anti-Phishing-Working-Group festgestellten Phishing-Seiten seit 2019. Die orangene Linie zeigt den Durchschnitt im betrachteten Zeitraum, die rote Linie gibt den Tendenzverlauf an.

Phishing-Nachrichten nehmen auch im Jahr 2021 häufig auf aktuelle gesellschaftliche Entwicklungen Bezug. Sie versuchen Unsicherheiten der Empfänger auszunutzen oder eine Angstkulisse aufzubauen, etwa durch knappe Zeitfristen oder Androhung von Geldstrafen. Im Vergleich zum Vorjahr haben Phishing-Nachrichten mit Covid-19-Bezug deutlich abgenommen.[6] Die am häufigsten für Phishing imitierten Absender waren 2021 Microsoft, DHL, Amazon, Google und WhatsApp.[7] Im Spätsommer 2021 erfolgten in Deutschland zusätzlich Phishing-Kampagnen mit Narrativen im Kontext von Banking-Daten der Sparkassen und Volksbanken. Die 2021 genutzten Phishing-Methoden waren vielfältig. Neben E-Mails wird sich Fake-Webseiten, SMS, Telefonie und Sozialer Medien bedient. Dabei können Phishing-Nachrichten auch als Antworten auf tatsächlich getätigte Konversation, etwa via Mail, erscheinen und damit täuschend echt wirken.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erhebt fortlaufend die sog. Abwehr-Indizes, die das Aufkommen und die Entwicklung von Malware-Angriffen per E-Mail auf die Netze des Bundes sowie die Menge präventiver Sperrungen von maliziösen Webseiten messen.

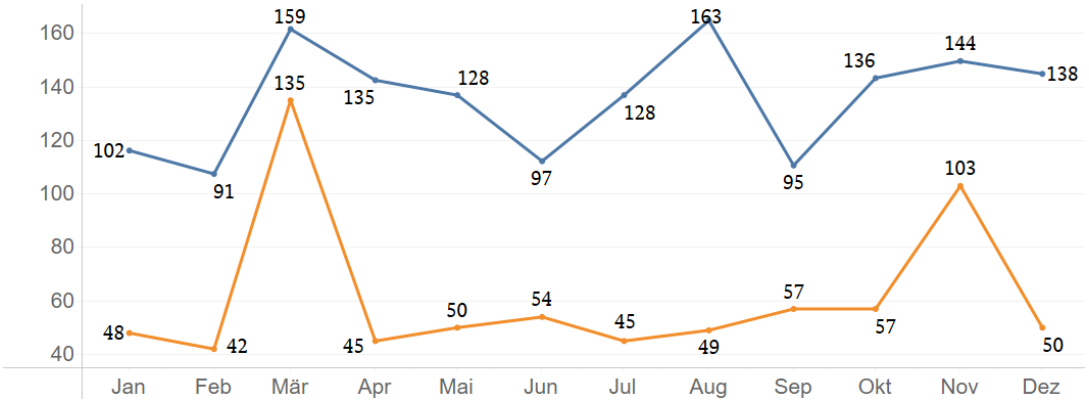


Abbildung 12: Abwehr-Indizes 2021 des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die blaue Linie zeigt neue Webseiten-Sperrungen, die orangene Linie gibt abgewehrte Schadprogramm-Angriffe auf die Bundesverwaltung an.

[6] Vgl. Trend Micro, Attack from All Angles – 2021 Midyear Cyber Security Report, online abrufbar unter **https://documents.trendmicro.com/assets/rpt/rpt-attacks-from-all-angles.pdf**

[7] Vgl. Quartalsberichte 2021 „Brand Phishing Report" von Checkpoint; online abrufbar unter: **blog.checkpoint.com**

Der Index für abgewehrte Malware-Angriffe auf die Bundesverwaltung verlief 2021 stark unterdurchschnittlich mit jeweiligen Peaks im März und November. Insgesamt wurden im Vergleich zum Jahr 2020 40% weniger abgewehrte Malware-Angriffe auf die Netze der Bundesverwaltung verzeichnet. In Bezug auf die Sperrung neuer Webseiten lassen sich Peaks im März und im August identifizieren sowie ein gradueller Anstieg gegen Ende des Jahres. Im Berichtsjahr wurden etwa 12% weniger Webseiten durch das BSI gesperrt als im Vorjahr.

Auch die in den Netzen des Bundes festgestellte Anzahl der Spam-Mails ist Gegenstand regelmäßiger Auswertungen des BSI (sog. Spam-Mail-Index). Anhand der nachfolgenden Grafik, die auf Daten des BSI beruht, ist ein hohes Spam-Niveau bis zur Mitte des Jahres 2021 zu beobachten. In den Sommer- und Herbstmonaten hat das Spam-Aufkommen dann abgenommen und ist erst gegen Ende des Jahres wieder graduell angestiegen.

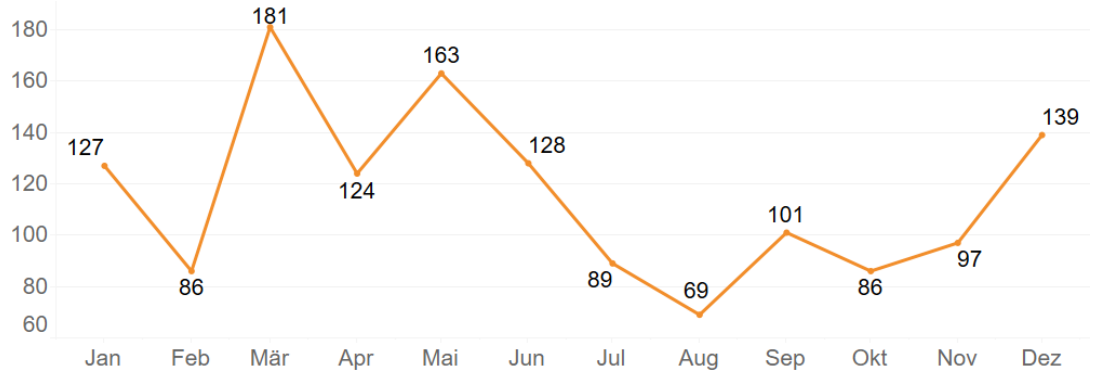


Abbildung 13: Spam-Mail-Index 2021 des BSI

Phishing ist und bleibt einer der beliebtesten Eintrittsvektoren. Die verwendeten Narrative sind mannigfaltig und passen sich dem aktuellen politischen wie gesellschaftlichen Geschehen an.

3.3.2 IT-Schwachstellen

Bei einer IT-Schwachstelle [8] oder Sicherheitslücke handelt es sich um einen Fehler im Softwarecode, der sicherheitskritisch sein kann, da über diesen z.B. ein Zugang zum Zielsystem hergestellt werden kann. Die zum Ausnutzen einer IT-Schwachstelle eingesetzten Techniken oder Taktiken werden als Exploits bezeichnet.

Laut IT-Security-Dienstleister Trend Micro hat sich Access-as-a-Service (AaaS) zu einem lukrativen Angebot innerhalb der Underground Economy entwickelt. Angreifer können auf diesem Wege Schwachstellen in IT-Systemen auffinden und ausnutzen. Der Wert der angebotenen Exploits richtet sich unter anderem danach, wie lange diese schon bekannt sind. Zero-Day-Exploits haben beispielsweise einen

[8] Die Kritikalität einer IT-Schwachstelle wird mit dem Common Vulnerability Scoring System (CVSS) bewertet. Die CVSS-Skala reicht von 0,0 – 10,0; ein Wert zwischen 9,0 – 10,0 gilt dabei als kritische Schwachstelle. Kritische Schwachstellen zeichnen sich z.B. durch eine hohe Verbreitung und eine hohe Bandbreite an Ausnutzungsmöglichkeiten aus.

höheren Wert und werden daher für durchschnittlich 10.000 US-Dollar gehandelt. Bei N-Day-Exploits belaufen sich handelsübliche Preise auf etwa 2.000 US-Dollar.[9]
Nach Angaben von Trend Micro wurden 54% der in der Underground Economy verkauften Exploits innerhalb der vergangenen zwei Jahre veröffentlicht. Betrachtet man die Anzahl entdeckter IT-Schwachstellen, ist eine immense Steigerung seit 2017 zu erkennen.

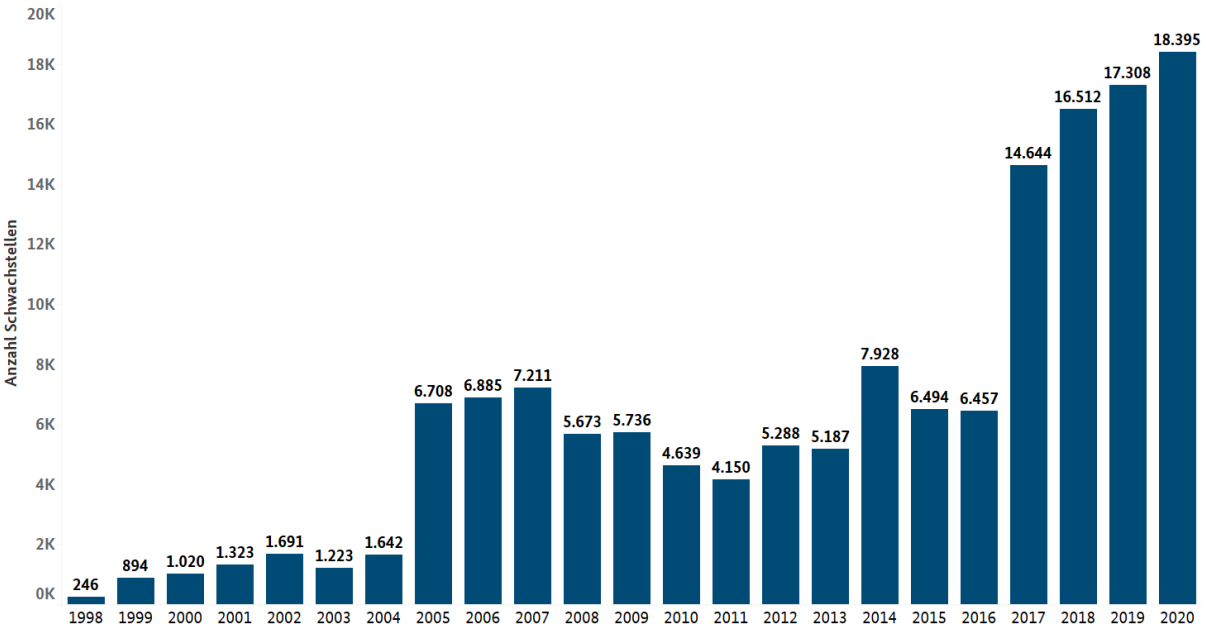


Abbildung 14: Anzahl an veröffentlichten Software-Schwachstellen basierend auf zugewiesenen CVE-Nummern (Common Vulnerabilities and Exposures; Standard zur Benennung von Sicherheitslücken in Computersystemen; Quelle der Grafik siehe Fußnote 8)

Auch öffentliche Datenbanken wie 0Day „In The Wild“ [10], ein Projekt, welches Zero-Day-Exploits auflistet, lassen erkennen, dass die Anzahl entdeckter kritischer Schwachstellen vor allem im letzten Jahr zugenommen hat. Im Vergleich zum Vorjahr hat sich dort die Zahl der entdeckten Zero-Day-Exploits in 2021 von 25 auf 57 mehr als verdoppelt. Trotz oder gerade wegen der sich ständig weiter entwickelnden Verteidigungsmaßnahmen und der Identifizierung derartiger Schwachstellen, hat die „Exploit-Industrie“ der Underground Economy im Jahr 2021 stark an Bedeutung gewonnen.

Eine schwerwiegende Schwachstelle konnte im Jahr 2021 mit „Log4Shell“ (CVE-2021-44228) festgestellt werden. Es handelt sich dabei um eine Schwachstelle in der populären Java-Programmier-Bibliothek Log4j mit potentiell erheblichen Folgen für die Betroffenen.

2021 wurden mehrere kritische IT-Schwachstellen für schwere Cyberangriffe ausgenutzt. Teilweise werden Schwachstellen jahrelang nicht gepatcht und sind somit für Angreifer jederzeit ausnutzbar.

[9] Vgl. Trend Micro, The Rise and Imminent Fall of the N-Day Exploit Market in the Cybercriminal Underground, 2021, online abrufbar unter: **https://documents.trendmicro.com/assets/white_papers/wp-the-rise-and-imminent-fall-of-the-n-day-exploit-market-in-the-cybercriminal-underground.pdf**

[10] Team Project Zero, 0day "In the Wild", aufrufbar unter: **https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/view#gid=0**

Was ist Log4j?

Log4j ist eine Protokollierungsbibliothek für Java-Anwendungen und Bestandteil zahlreicher Open-Source- sowie kommerzieller Softwareprodukte. Sie gilt als Standard unter bestehenden Logging-Frameworks.

Zero-Day-Schwachstelle Log4shell

Am 09.12.2021 wurde eine Zero-Day-Schwachstelle in Log4j bekannt: Ein Mitarbeiter der Alibaba Cloud Security in China hatte Informationen zur Schwachstelle in der Log4j-Bibliothek auf Twitter veröffentlicht und verwies darüber hinaus auf ein auf GitHub veröffentlichtes Proof-of-Concept (PoC) der Schwachstelle. Die Ausnutzung der unter „Log4Shell“ oder CVE-2021-44228 bekannten Schwachstelle wurde kurz darauf auf den Servern des Online-Spiels „Minecraft“ entdeckt. Nachdem daraufhin massenhaft Scans nach Log4Shell festgestellt werden konnten, erklärte das BSI am 12.12.2021 die Warnstufe Rot für die Schwachstelle.

Ausnutzung der Schwachstelle

Über die Schwachstelle ist es Angreifern möglich, auf dem Logging-Server Remote Code einzubringen und in der Folge Schadcode auf das Zielsystem zu laden und auszuführen. Die Kompromittierung erfolgte primär, um Krypto-Miner und Bot-Netze aufzubauen, aber auch um das Einbringen weiterer Malware zu ermöglichen.

Es wurden einzelne Vorfälle bekannt, in denen die Schwachstelle bereits zur Installation von Ransomware ausgenutzt wurde. IT-Dienstleister gehen mittlerweile davon aus, mindestens zehn Schadsoftware-Familien die Schwachstelle ausnutzen, darunter die Ransomware Conti, die Malware Dridex und das Mirai-Botnetz. Auch das Ausnutzen der Schwachstelle durch „Würmer“ konnte festgestellt werden, in deren Verlauf sich Schadsoftware automatisch weiterverbreitete.
Darüber hinaus kann die Schwachstelle auch zur Offenlegung von vertraulichen Daten, wie zum Beispiel API-Keys, missbraucht werden.

Platzierte Malware muss nicht zwangsläufig sofort, sondern kann auch erst Wochen oder Monate nach der Kompromittierung des Systems aktiviert werden. Demnach ist erwartbar, dass sich das Ausmaß der Schwachstelle Log4Shell erst im Laufe der Zeit vollständig zeigt.

Betroffenheiten in Deutschland

Es ist von einer weit verbreiteten Verwundbarkeit innerhalb der Wirtschaft, aber auch in der Verwaltung auszugehen. Die auf GitHub veröffentlichte Liste betroffener Produkte zählte am 15.12.2021 insgesamt 140 Hersteller. Auch gelten einige Hersteller für Produkte im Bereich KRITIS als betroffen.

Bewertung

Die Kritikalität der Schwachstelle begründete sich vor allem durch die scheinbare Omnipräsenz der Java-Bibliothek Log4j und damit der massiven Anzahl verwundbarer Systeme. Damit einhergehend zeigte sich ein vielseitiges Spektrum an Angriffsszenarien – vor allem aber durch die Distribution von Schadsoftware. Die Automatisierung derartiger Verbreitung durch Würmer ist nicht neu, zeigt aber auch in diesem Fall, welche Ausmaße derartige Angriffsvektoren annehmen können.

Grundsätzlich zeigt die Ausnutzung von Log4j, wie gefährlich ungepatchte Systeme sein können.

Am 12.01.2022 verringerte das BSI seine Risiko-Einschätzung zur Schwachstelle auf Stufe Gelb. Voraus gingen diverse Apelle und Sensibilisierungsaufrufe sowie die Arbeit von IT-Sicherheitsforschern und -dienstleistern, welche sich um das schnelle Patchen der Schwachstelle bemühten.

3.4 SCHADPROGRAMME

Über die verschiedenen Eintrittsvektoren ist es Angreifern möglich, Schadsoftware auf Zielsysteme zu installieren. Schadsoftware ist ein elementarer Bestandteil der Cybercrime. Sie besitzt dutzende Facetten und Funktionen und hat immense Bedeutung für mehrere Säulen der Cybercrime.

3.4.1 Malware

Relevanz	Ransomware	RAT und Info-Stealer
• Primäre Werkzeuge zur Begehung von Cyberstraftaten • Malware nimmt drei Säulen des CaaS-Modells in Anspruch (siehe QR-Code auf Seite 8)	• Weiterhin Malware-Typus mit medial höchster Relevanz • Besitzt immenses Schadenspotenzial	• Hohe Relevanz für die Persistenz im System und zur Ausleitung von Daten

Abbildung 15: Wesentliche Aspekte von Malware

Auch im Jahr 2021 bilden Remote Access-Tools (RAT), Info-Stealer und Ransomware die bedeutendsten Malware-Varianten. Erstere dienen vor allem dazu, dauerhaft Zugriff zum kompromittierten System zu erhalten und Informationen auszuleiten. Trotz ihrer weniger offensiven Natur als Ransomware oder DDoS-Angriffe, sind es auch derartige, „subtilere“ Malware-Varianten, die einen beträchtlichen finanziellen Schaden verursachen können. Schließlich werden durch sie Daten erbeutet, die dann in der Underground Economy weiterverwertet werden und für nachgelagerte Angriffe von Bedeutung sein könnten (siehe Kapitel 3.2).

Die Relevanz von Malware bleibt ungebrochen – sie ist eines der primären Werkzeuge von Cyberkriminellen.

Auch bei logischen/digitalen Angriffen auf Geldautomaten kommt oftmals Schadsoftware zum Einsatz. Generell unterscheidet dieser Phänomenbereich drei Modi Operandi:

Jackpotting mit Malware

- Angriff auf den Rechner/PC eines Geldautomaten mittels Schadsoftware.

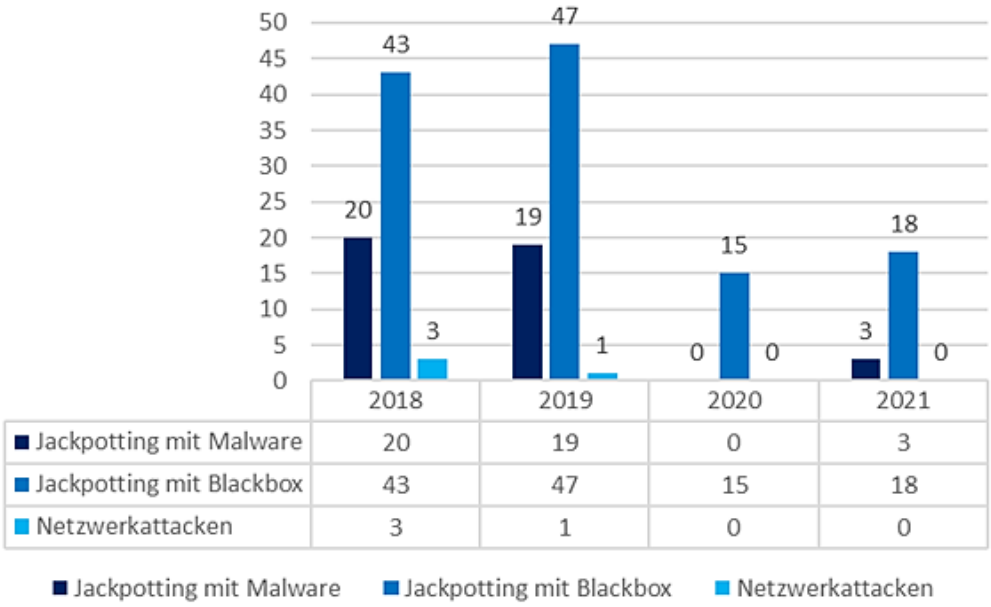
Jackpotting mit Blackbox

- Angriff auf das Auszahlungsmodul des Geldautomaten mittels tätereigener Hardware.

Netzwerkattacke

- Malware-Angriff auf die kartenausgebende Bank oder Processing-Gesellschaft, um Transaktionsprozesse zu manipulieren. Anschließend erfolgt ein sog. 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 sog. kartenungebundenen „Cash Out“ durchzuführen.

Abbildung 16: Modi Operandi bei logischen/digitalen Angriffen auf Geldautomaten



	2018	2019	2020	2021
Jackpotting mit Malware	20	19	0	3
Jackpotting mit Blackbox	43	47	15	18
Netzwerkattacken	3	1	0	0

Abbildung 17: Fallzahlen logische Angriffe auf Geldautomaten in Deutschland

Alle 18 Fälle des Jackpotting mit Blackbox gehörten zu einer im Mai 2021 in Deutschland begonnenen Tatserie. Die geringe Erfolgsquote lässt sich mit der schnellen Bereitstellung eines Sicherheitsupdates durch den Automatenhersteller erklären. In Abstimmung mit verschiedenen betroffenen Europol-Mitgliedsstaaten wurde festgestellt, dass die Serie in Deutschland in Verbindung zu weiteren Attacken im europäischen Ausland steht. Die Auswertung von sichergestellten Blackboxen ergab, dass die Angriffe remote aus dem osteuropäischen Raum durchgeführt wurden.

Durch technische Sicherheitsvorkehrungen, wie die Verschlüsselung der Festplatte (Jackpotting) oder Verschlüsselung der Kommunikation zwischen dem Geldautomaten-PC und Auszahlungsmodul (Blackboxing) werden die meisten logischen Angriffe auf Geldautomaten abgewehrt. Aufgrund der erwartbar hohen Beute ist die Bedrohungslage durch logische Geldautomatenangriffe trotz des derzeit geringen Fallaufkommens weiterhin hoch.

3.4.2 Ransomware

Ransomware ist die Malware-Variante, welche aufgrund ihres hohen Schadenspotentials nicht nur in Fachkreisen, sondern auch medial die höchste Aufmerksamkeit genießt. Der Einsatz von Ransomware kann Produktionsprozesse erheblich beeinträchtigen und damit für Unternehmen existenzschädigend sein. Ebenso stellt sie eine Bedrohung für die Funktionsfähigkeiten kritischer Infrastrukturen (KRITIS) und staatlicher Einrichtungen dar.

Abbildung 18: Finanzielle Dimensionen von Ransomware-Angriffen

Neben dem enormen Schadenspotenzial gewinnt Ransomware auch durch konstant steigende Fallzahlen an Relevanz im Bereich Cybercrime.[11] Im internationalen Vergleich ist Deutschland überdurchschnittlich häufig von Ransomware-Angriffen betroffen und gilt als eines der häufigsten Angriffsziele für Ransomware-Akteure.[12] [13]

Die sog. Double Extortion hat sich inzwischen als Standard-Modus-Operandi etabliert. Hierbei erfolgt die Erpressung durch Verschlüsselung der Systeme bei gleichzeitiger Drohung mit Veröffentlichung abgeflossener, sensibler Daten. Dieser Modus Operandi machte im Jahr 2021 laut dem IT-Security-Dienstleister Coveware 81% der Ransomware-Angriffe aus. Im vierten Quartal 2021 waren es sogar 84%. Gleichzeitig unterlag die durchschnittlich gezahlte Ransom starken Schwankungen im vergangenen Jahr. Während die durchschnittlich von Coveware verzeichneten Ransom-Summen im Q1 2021 noch bei 220.298 US-Dollar lagen, sank dieser Wert im zweiten Quartal um 38%. Erst im vierten Quartal 2021 stiegen die Ransom-Summen auf einen Höchstwert von 322.168 US-Dollar.

Das Bedrohungspotenzial von Ransomware ist immens und steigt weiter an.

[11] Microsoft, Microsoft Digital Defense Report 2021, Oktober 2021, online abrufbar unter: **https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report**
[12] Vgl. Sonicwall, Cyber Threat Report 2021 – Mid Year Update, online abrufbar unter: **https://www.sonicwall.com/de-de/resources/infographics/2021-mid-year-update-sonicwall-cyber-threat-report/**
[13] Vgl. Sophos, Ransomware-Report 2021, online abrufbar unter: **https://www.sophos.com/de-de/content/state-of-ransomware**

Der erste Cyber-Katastrophenfall: Angriff auf die Landkreisverwaltung von Anhalt-Bitterfeld

Die Verschlüsselung

Die Landkreisverwaltung von Anhalt-Bitterfeld in Sachsen-Anhalt wurde am 05. Juli 2021 Opfer eines Ransomware-Angriffs. Das Netzwerk der Verwaltung war sowohl im Hauptsitz in Köthen wie auch in den Außenstellen in Bitterfeld und Zerbst von der Datenverschlüsselung betroffen. Alle IT-Systeme des Landkreises wurden vorsorglich heruntergefahren. In der Folge kam es zu erheblichen Beeinträchtigungen der kommunalen Verwaltungsprozesse.

Die Täter

Zu dem Angriff bekannte sich die Tätergruppierung „Grief“. Sie nutzte die sog. Double Extortion und forderte ein Lösegeld in der Kryptowährung Monero. Ihrer Forderung verliehen die Täter durch die Veröffentlichung von 200 MB der entwendeten Daten auf einer Dedicated-Leak-Website im Darknet Nachdruck.

Um umfassendere Reaktionsmöglichkeiten zur Abwehr bzw. Eindämmung des Ausmaßes zu erhalten, wurde mit Wirkung zum 09.07.21 der erste, durch einen Cyberangriff verursachte Katastrophenfall ausgerufen, welcher erst über ein halbes Jahr später wieder aufgehoben werden konnte.

Die Folgen

Trotz des Hinzuziehens mehrerer Behörden sowie externer Dienstleister konnten die betroffenen IT-Systeme auch ein halbes Jahr später noch nicht vollständig wiederhergestellt werden. Am 31.01.2022 wurde der Katastrophenfall für beendet erklärt - der Wiederherstellungsprozess wird sich jedoch auch 2022 noch fortsetzen. Die geschätzten Kosten für die Wiederherstellung der Infrastruktur belaufen sich auf ca. zwei Millionen Euro.

Im Frühjahr 2021 erfolgten mehrere öffentlichkeitswirksame Ransomware-Vorfälle. Zum einen die Verschlüsselung des US-Pipelinebetreibers Colonial Pipeline durch die Ransomware-Gruppierung DarkSide, zum anderen der Angriff auf das Washington Police Department durch die BabukLocker-Gruppierung. Nach letzterem wurden am 14.05.2021 nach gescheiterten Verhandlungen 250GB Daten durch die Täter veröffentlicht.

Am 15.05.2021 wurde durch die Administratoren der beiden größten russischsprachigen Foren der Underground Economy, Exploit.in und xss.is, zeitgleich ein umfassendes Verbot für den Verkauf oder die Vermietung von Ransomware sowie aller Arten von Affiliate-Programmen zu diesen erlassen. Als Grund wurde angegeben, dass Ransomware-as-a-Service (RaaS) zu viel unerwünschte Aufmerksamkeit auf die Foren ziehen würde. Außerdem habe das schnelle Geld zu viele unprofessionelle und unseriöse RaaS-Anbieter angezogen.

Die Veränderung wurde durch die Mitglieder des Forums negativ aufgefasst. Der Entscheidung wird im Allgemeinen nicht zugestimmt. Besonders durch die RaaS-Anbieter, z.B. REvil und DarkSide, wurden Beschwerden eingelegt.

Trotz des Verbotes der RaaS auf den dargestellten Plattformen bleiben Ransomware und damit einhergehende Affiliate-Programme weiterhin äußerst attraktiv – wie auch die Reaktion der Foren-Mitglieder unter Beweis stellte.

Operation Nova

Das Ermittlungsverfahren

Im Rahmen einer Kooperation mit zahlreichen internationalen Sicherheitsbehörden sind am 21.12.2020 insgesamt ca. 50 Server eines weltweit agierenden Netzwerks von Cyberkriminellen außer Betrieb gesetzt und teilweise beschlagnahmt worden. Die ehemalige Homepage des früher unter dem Namen „insorg“ und aktuell unter „Safe-Inet“ firmierenden Netzwerks wurde gesperrt und mit einem Seizure Banner versehen.
Die Verantwortlichen des Netzwerks haben ihre mit technischen Anonymisierungsmöglichkeiten ausgestattete IT-Struktur unterschiedlichsten Nutzern gegen Bezahlung zur Verfügung gestellt. Die kriminellen Kunden haben auf den von den Netzwerkbetreibern versprochenen Schutz vor dem Zugriff der Ermittlungsbehörden vertraut und die Infrastruktur zur Begehung schwerer Cyberstraftaten und zur Abwicklung sonstiger illegaler Geschäfte genutzt.

Die Ermittlungen

Bei der sukzessiven Auswertung des gesicherten Datenmaterials wurden diverse, bereits länger andauernde Cyberangriffe zum Nachteil einer Vielzahl von Unternehmen festgestellt. Bei etlichen der angegriffenen Firmen stand eine Verschlüsselung ihrer Daten und damit ein kompletter Ausfall ihrer IT-Systeme unmittelbar bevor. In einzelnen Fällen, in denen die Verschlüsselung der Daten bereits im Gange war, konnten die Unternehmen Schutzmaßnahmen ergreifen, wodurch der Angriff gestoppt und der Schaden so zumindest begrenzt werden konnte.
Insgesamt konnten weltweit rund 250 von den Tätern bereits ausgespähte Unternehmen identifiziert, meist rechtzeitig vor einer Verschlüsselung gewarnt und so vor einem Verlust ihrer Daten und der danach üblicherweise folgenden Erpressung bewahrt werden.

Internationale Zusammenarbeit

Den zuständigen Cyberspezialisten der Kriminalpolizeidirektion Esslingen und einer dort eingerichteten Ermittlungsgruppe war es im Verlauf der Ermittlungen gelungen, in die kriminelle IT-Infrastruktur einzudringen und die Spur bis zu den beschlagnahmten Servern zurückzuverfolgen. Ein wesentlicher Baustein dieses Erfolgs war die hervorragende internationale Zusammenarbeit der Sicherheitsbehörden - insbesondere mit dem FBI, der Kantonspolizei Aargau, dem Schweizerischen Bundesamt für Polizei fedpol, der Polizei der Niederlande, der französischen Police Nationale, EUROPOL und den jeweiligen Justizbehörden.

3.5 DISTRIBUTED DENIAL OF SERVICE (DDOS)-ANGRIFFE

Auch im Jahr 2021 setzte sich im Phänomenbereich DDoS, die allgemeine Entwicklung einer qualitativen und quantitativen Steigerung fort. DDoS zielt darauf ab Webpräsenzen, Server und Netzwerke von Personen und/oder Organisationen zu überlasten und so eine Nichterreichbarkeit der Dienste herbeizuführen. Von dieser Art von Cyberangriffen waren eine Vielzahl verschiedener Branchen betroffen. Neben Finanzdienstleistern, Hosting-Anbietern, Lern- und Impfportalen standen im letzten Jahr auch öffentliche Einrichtungen und – primär in der Vorweihnachtszeit – der E-Commerce im Fokus von DDoS-Angriffen.

3.5.1 Quantitative Entwicklungen der DDoS-Angriffe

Die Anzahl an DDoS-Angriffen ist nicht konstant über das Jahr verteilt, sondern weist zum Teil starke, saisonale Schwankungen auf. Nachfolgende Grafik basiert auf Daten der Deutsche Telekom AG (DTAG) und gibt wieder, wie viele DDoS-Angriffe pro Monat im dortigen Netz registriert wurden.[14]

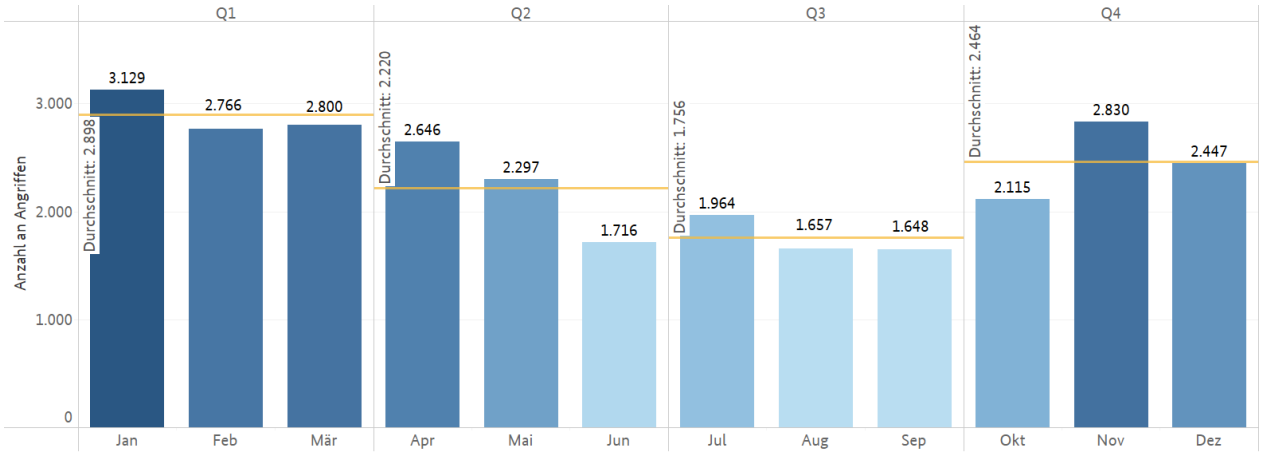


Abbildung 20: Anzahl an DDoS-Angriffen pro Monat im Netz der DTAG für das Jahr 2021. Die orangene Linie zeigt den jeweiligen Quartalsdurchschnitt an.

Das erste und das letzte Quartal 2021 wiesen im Durchschnitt die größte Zahl an Angriffen auf. Das erste Quartal 2021 sticht hierbei als jenes mit der signifikant höchsten durchschnittlichen Anzahl an DDoS-Angriffen hervor. Erklärungsansätze hierfür finden sich bereits im Jahr 2020, als DDoS-Angriffe laut dem DDoS-Mitigationsdienstleister Link11 einen regelrechten „Boom“ erhielten und sich diese Entwicklung vor allem Ende des Jahres 2020 herauskristallisierte: Das erste Quartal 2021 kann daher noch als „Nachbeben“ der durch die Corona-Pandemie katalysierten Anstiege an DDoS-Angriffen gewertet werden. Im zweiten und dritten Quartal 2021 ist ein Rückgang der Angriffszahlen festzustellen. Nach dieser Art „Sommerpause“ folgte erwartungsgemäß im vierten Quartal ein erneuter Anstieg festgestellter Angriffe. Ursachen hierfür dürften in der erhöhten Relevanz von E-Commerce Plattformen in der Zeit um den „Black Friday“ und rund um das Weihnachtsgeschäft zu finden sein.

[14] Daten der DTAG für den Berichtszeitraum 2021.

3.5.2 Qualitative Veränderungen der DDoS-Angriffe

Neben der quantitativen Veränderung ist im Jahr 2021 auch eine deutliche Steigerung in der Qualität von DDoS-Angriffen feststellbar.

Gegen Jahresende konnte gemäß Datenlage der DTAG ein Anstieg der durchschnittlichen sowie maximalen Bandbreite der Angriffe verzeichnet werden. Die jeweiligen Höchstwerte wurden jedoch im Januar 2021 erzielt. Die Fokussierung von DDoS-Akteuren auf das erste und letzte Quartal 2021 ist ebenfalls in den durchschnittlichen Angriffsbandbreiten (Avg Mbps), den durchschnittlichen Maximalangriffsbandbreiten (Max Mbps) sowie der durchschnittlichen maximalen Paketrate (Pps) erkennbar.

Link11 stellt vor allem im November 2021 eine besonders starke Zunahme an hochvolumigen Angriffen fest. Insgesamt identifizierte Link11 für das Jahr 2021 einen signifikanten Anstieg derartiger Angriffe im Vergleich zum Vorjahr.

Der Anstieg aller Parameter gegen Jahresende korreliert erwartungsgemäß mit der Relevanz des E-Commerce um die Zeit zwischen dem Black-Friday- und dem Weihnachtsgeschäft.

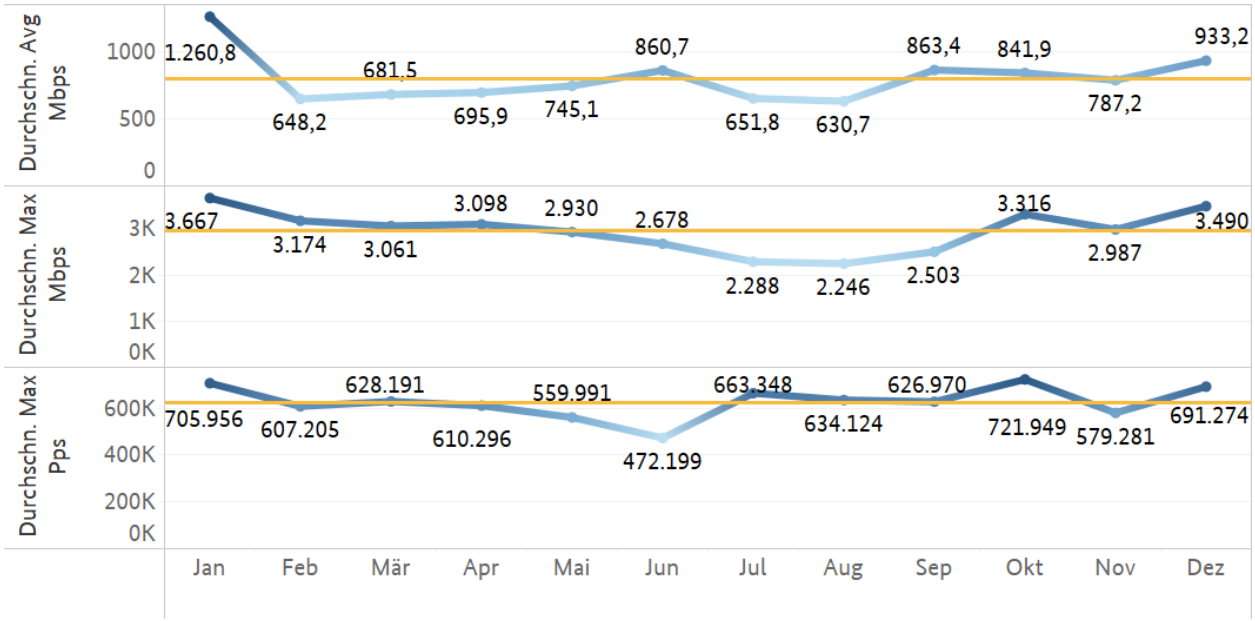


Abbildung 21: Jahresverlauf zu durchschnittlicher Bandbreite (oben), durchschnittlichen Bandbreiten-Peaks (Mitte) und durchschnittlicher Maximalpaketrate (unten), basierend auf Daten der DTAG. Die orangene Linie zeigt den jeweiligen Jahresdurchschnitt.

DDoS-Trends

Im Jahr 2021 konnten verstärkt Multivektor-Angriffe, sog. Carpet-Bombing [15] und eine Kombination von DDoS- und Ransomware-Angriffen festgestellt werden. Die feststellbare Durchführung nachgelagerter DDoS-Angriffe nach einer Infektion mit einer Ransomware verleiht den DDoS-Angriffen eine noch höhere Relevanz als im Vorjahr. Insbesondere in den ersten beiden Quartalen 2021 stellte Link11 eine DDoS-Erpressungswelle mit hohen Angriffszahlen fest. Die Komplexität, mit der DDoS-Angriffe ausgeführt werden, nimmt damit weiter zu.

Multivektor-Angriffe	Carpet Bombing	DDoS-Erpressungen
• Komplexe Angriffe, die auf verschiedene Ebenen, wie Protokolle, Applikationen oder Transport zielen. • Der Anteil von Multivektor-Angriffen stieg von 59% im Jahr 2020 auf 71% im Jahr 2021. [a]	• Angriffe, mit niedrigem Datenverkehr pro IP-Adresse, die auf ganze Netzwerkblöcke abzielen. • Werden aufgrund des niedrigen Volumens von Schutzprogrammen häufig nicht als Angriff erkannt.	• Erpressungen mit DDoS-Angriffen werden häufiger. • Auch im Zusammenhang mit Ransomware-Angriffen (Triple Extortion).

Abbildung 22: Relevante qualitative Entwicklungen von DDoS-Angriffen in 2021 | a = Daten von Link11

3.5.3 DDoS in Zahlen

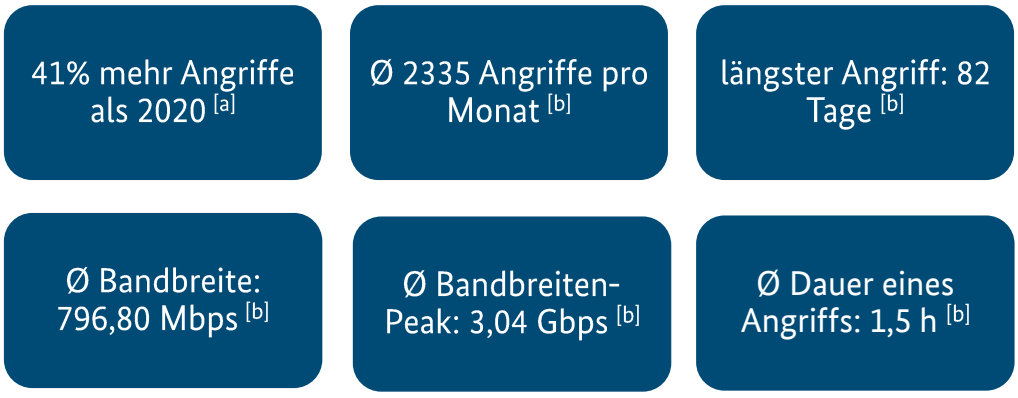


Abbildung 23: Relevante Eckdaten von DDoS-Angriffen 2021 | a = Daten von Link11; b = Daten der DTAG

[15] Angriffe mit niedrigem Datenverkehr auf ganze Netzwerkblöcke.

DDoS-Angriffe nehmen in ihrer Intensität und Komplexität weiter zu.

DDoS-Angriff auf Server der Universität Mainz

Der DDoS-Angriff

Im Januar 2021 kam es zu mehreren DDoS-Angriffen auf Systeme der Universität Mainz. Ziel der Attacken waren Server, die die Universität im Zuge der pandemischen Lage dem Bildungsministerium zwecks Durchführung des Fernunterrichts an rheinland-pfälzischen Schulen zur Verfügung gestellt hatte. Ein erster Angriff begann am 04.01.2021, dem ersten Schultag nach den Weihnachtsferien, und setzte sich bis zum Morgen des folgenden Tages fort. Ein weiterer davon unabhängiger Angriff erfolgte ab dem 19. Januar und hielt bis zum 21. Januar 2021 an. Ausgehend von elf Servern wurden während des zweiten DDoS-Angriffs 13 Mio. HTTP-Anfragen ausgeführt.

Auswirkungen

Auf dem Höhepunkt der DDoS-Attacke gingen 500.000 Anfragen pro Sekunde bei den angegriffenen Servern ein. Dadurch entstanden Schwierigkeiten bei der Erreichbarkeit der Lernplattform moodle@RLP, auf der Lernmaterialen für Schüler zur Verfügung gestellt wurden, und des Web-Konferenzsystems BigBlueButton. Von den Einschränkungen waren rund 900 Schulen in Rheinland-Pfalz betroffen.

Ermittlungen

Der Vorfall fand ein großes Medienecho und wurde mit Bezug auf die Notwendigkeit der Digitalisierung des Bildungssystems im Landtagswahlkampf 2021 aufgegriffen. Die Landeszentralstelle Cybercrime der Generalstaatsanwaltschaft Koblenz und das Dezernat Cybercrime des Landeskriminalamtes Rheinland-Pfalz nahmen Ermittlungen in diesem Fall auf. Für den zweiten Angriff konnte im Verlauf dieser Ermittlungen ein 14-jähriger Schüler als Tatverdächtiger identifiziert werden.

4 Ziele

Branchen	Unternehmensgröße	KRITIS und öffentliche Verwaltung
• Grundsätzlich kann jeder Ziel von Cyberkriminellen werden. • Ransomware-Angriffe zielten im Berichtsjahr vor allem auf das verarbeitende Gewerbe, den Finanzsektor, den Einzelhandel sowie öffentliche Einrichtungen.	• Wie im Jahr 2020 sind größere Unternehmen tendentiell eher Ziele von Cyberangriffen. • Grundsätzlich ist allerdings die Prävalenzrate für alle Unternehmensgrößen angestiegen.	• 2021 war geprägt von Angriffen auf KRITIS und Ziele in der öffentlichen Verwaltung. • Die Anzahl solcher Angriffe ist generell steigend.

Abbildung 24: Wesentliche Fakten zu Zielen von Cyberangriffen

Laut einer repräsentativen Umfrage des Bitkom e.V. gaben 88% der befragten Wirtschaftsunternehmen im zwölfmonatigen Befragungszeitraum an, durch Cybercrime, Spionage oder Sabotage betroffen gewesen zu sein. 2019 lag diese Zahl noch bei 75%. Insgesamt 89% der Befragten, sowohl KRITIS- als auch Nicht-KRITIS-Unternehmen, gaben ferner an, dass sich die Anzahl der Angriffe seit der letzten Bitkom-Untersuchung im Jahr 2019 erhöht habe.

4.1 ANGRIFFE AUF DIE ÖFFENTLICHE VERWALTUNG

Da ab Mitte 2021 insbesondere auch öffentliche Verwaltungen Geschädigte von Cyberkriminellen wurden, gibt die nachfolgende Auflistung einen Überblick über Angriffe, die zusätzlich zu dem Angriff auf die Landkreisverwaltung Anhalt-Bitterfeld (siehe Kapitel 3.4.2 Ransomware) erfolgten.

Stadtverwaltung Geisenheim

Am 14.07.2021 wurde die Stadtverwaltung Geisenheim Opfer eines Cyberangriffs. Die eingeschleuste Malware wurde frühzeitig erkannt und konnte keinen Schaden anrichten. Vorsorglich gingen die Stadtwerke, die Verwaltung und weitere kommunale Einrichtungen offline und waren nicht mehr per E-Mail zu erreichen. Die Stadtverwaltung war mehrere Tage vollständig arbeitsunfähig und konnte für 14 Tage ihre Dienste für die Bürger der Stadt nur eingeschränkt anbieten.

Stadtwerke Wismar

Am Morgen des 28.09.2021 wurden die IT-Systeme der Stadtwerke Wismar und die Strom- und Gasnetz Wismar GmbH Ziel eines Ransomware-Angriffs. Dabei wurde die Serverstruktur verschlüsselt und die betroffenen Systeme vorsorglich abgeschaltet.

IT-Dienstleister Schwerin

Zwischen dem 13.10.2021 und 15.10.2021 wurden die Serverstrukturen zwei kommunaler IT-Dienstleistungsunternehmen in Schwerin angegriffen und teilweise verschlüsselt. Infolge dessen waren große Teile des Bürgerservices in den Kommunalverwaltungen der Stadt Schwerin und des Landkreises Ludwigslust-Parchim für längere Zeit nicht bzw. nur im Notbetriebsmodus verfügbar. Eine Wiederherstellung der beeinträchtigten Systeme erfolgte auf Basis vorhandener Backups.

Stadtverwaltung Witten
Teile der Informations- und Kommunikationstechnik der Stadt Witten wurden in der Nacht zum 17.10.2021 mittels einer Ransomware verschlüsselt. Vor der Verschlüsselung wurden Daten durch die Täter heruntergeladen und Backups gelöscht. Alle Bereiche der öffentlichen Verwaltung der Stadt Witten waren von der Verschlüsselung betroffen. Der Vorfall hatte den beinahe gänzlichen Ausfall der Stadtverwaltung zur Folge. Die Tätergruppierung drohte in einer Ransom-Note mit der Veröffentlichung der extrahierten Daten, was anschließend in der Zeit vom 11.11.2021 bis 15.11.2021 auf dem Leak-Blog der Gruppierung erfolgte.
Stadtwerke Sassnitz
Unbekannte Täter übernahmen am 10.11.2021 den Mailserver der Stadt Sassnitz und verschickten im Namen der dortigen Mitarbeiter E-Mails mit maliziösen Inhalten an einzelne Bürger. Daraufhin wurde der E-Mail-Verkehr der Stadt für mehrere Tage lahmgelegt.
Stadtverwaltung Schmalkalden
Am 16.12.2021 wurden vom Mail-Server der Stadt Schmalkalden unberechtigt E-Mails im Namen der Stadtverwaltung an externe Geschäftspartner, Bürger sowie Behörden versendet. Der kompromittierte Mail-Server wurde daraufhin vom Netzwerk getrennt. Über drei Tage bestand keine Möglichkeit, per E-Mail-Kontakt zur Stadtverwaltung Schmalkalden aufzunehmen.

Abbildung 25: Cyberangriffe auf öffentliche Verwaltungen 2021

Jeder kann Opfer von Cyberkriminellen werden – die Wahrscheinlichkeit für eine Betroffenheit steigt.

4.2 LIEFERKETTEN

Seit 2020 ist die Anzahl an sog. Supply-Chain-Angriffen merklich angestiegen.[16] Supply-Chain-Angriffe, wie jene auf Kaseya Ltd. (siehe unten), sind höchst komplex und haben sowohl nationale als auch internationale Auswirkungen.

Supply-Chain-Angriffe besitzen aufgrund zweier Faktoren ein enormes Bedrohungspotenzial:

1. Sie zeichnen sich häufig durch eine hohe Reichweite und ungezielte Weiterverbreitung aus. Die Zahl der Betroffenen ist deutlich höher als bei einem gezielten Angriff und häufig werden auch IT-Systeme betroffen, die nicht im Fokus der Angreifer standen.
2. Derartige Angriffe können IT-Standards und Cyber-Security-Maßnahmen unterlaufen. Ein hinsichtlich IT-Standards gut aufgestelltes Unternehmen kann, z.B. über den Erwerb einer kompromittierten Software von einem vertrauenswürdigen Geschäftspartner, trotz aller eigener Sicherheitsmaßnahmen kritischen Schaden erleiden.

[16] Vgl. Ausführungen ENISA, Threat Landscape for Supply Chain Attacks, 29.07.2021, online abrufbar unter:

Besonderes Bedrohungspotenzial besteht bei einer Verbindung des Supply-Chain-Angriffs mit einer Ransomware-Infektion. Ein solches Vorgehen könnte die Verschlüsselung aller Unternehmen und Akteure innerhalb dieser Lieferkette nach sich ziehen – das Schadensausmaß wäre damit immens.
Aber auch für das Ziel der Datenspionage eignen sich Supply-Chain-Angriffe. Durch sie kann in besser gesicherte Ziele eingedrungen und eine große Anzahl an Unternehmen und Behörden gleichzeitig angegriffen werden.

Angriff über Kaseya Ltd.

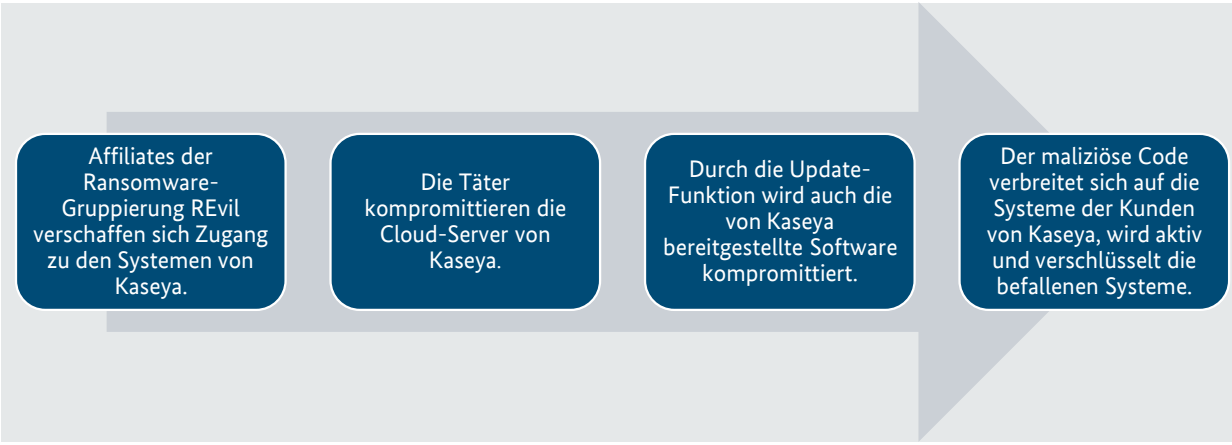
Kaseya Ltd.

Das Unternehmen Kaseya Ltd. bietet Software zur Netzwerkverwaltung sowie Fernwartungssoftware an und betreibt eigene Cloud Server. Direkte Kunden sind IT-Dienstleister, die aus der Ferne die Systeme ihrer jeweiligen Kunden warten. Am 02.07.2021 meldete Kaseya Ltd. einen Ransomware-Angriff auf seine Cloud-Server der Virtual System Administrator (VSA). VSA wird im Regelfall von Dienstleistern genutzt um Software-Updates auf den von ihnen betreuten Systemen durchzuführen. Im Fall des Angriffs wurde diese Funktion von den Tätern ausgenutzt, um über die Server Updates mit Schadsoftware zu verteilen. Auf diese Weise wurden zuerst die IT-Dienstleister und anschließend auch deren Kunden durch die Schadsoftware angegriffen.

Ausmaß des Angriffes

Als indirekter Kunde von Kaseya Ltd. musste unter anderem die schwedische Supermarktkette Coop ihre 800 Filialen wegen ausgefallener Kassensysteme zeitweise schließen. Eine genaue Anzahl an Betroffenen lässt sich nur schwer feststellen, da etlichen Endkunden nicht bekannt war, dass ihre Netzwerke durch Software von Kaseya Ltd. gewartet werden. Medial wird von 1.000 bis 1.500 betroffenen Unternehmen weltweit ausgegangen. Nach Angaben von Kaseya Ltd. ist der Anteil von direkten Kunden an allen Betroffenen prozentual gering.

Ablauf des Angriffes



Entschlüsselung

Für die betroffenen Unternehmen folgte auf den Angriff eine ressourcenintensive Wiederherstellung der IT-Infrastruktur und der verschlüsselten Daten durch Einspielung von Backups. Knappe sechs Wochen nach Beginn des Angriffs wurde der Master Key zur Entschlüsselung der durch die Ransomware verschlüsselten Daten veröffentlicht.

5 Täter

Das Jahr 2021 zeigte erneut, dass ein wesentliches Charakteristikum von Akteuren der Cybercrime, ob finanziell oder politisch motiviert, ihre Anpassungsfähigkeit darstellt. Nicht nur, dass APT [17] und andere Akteure äußerst schnell neue Schwachstellen ausnutzen oder gesamtgesellschaftliche Notlagen als Phishing-Narrativ verwenden, auch sog. Rebrandings[18] zeigen, dass Cyberkriminelle schnell auf äußeren Druck reagieren können. Nachfolgendes Diagramm zeigt einige prominente Rebrandings.

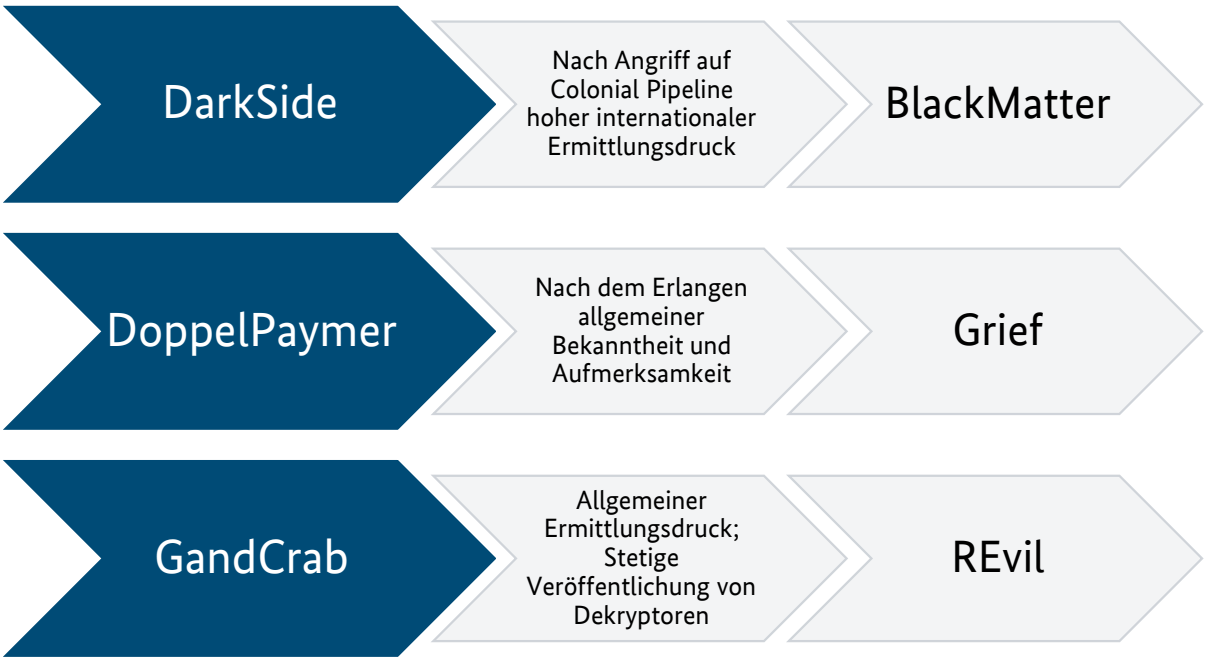


Abbildung 26: Beispiele für das Rebranding von Cybercrime-Akteuren

Ebenfalls setzte 2021 den Trend der Vorjahre fort, wonach sich die Tätergruppierungen, von organisierten Cyberkriminellen bis hin zu staatlichen APT, hinsichtlich ihrer Professionalität, eingesetzter Malware und Vorgehensweisen kaum noch trennscharf unterscheiden lassen – einzig die Motivationslage ist hier eine andere. Beide Arten von Gruppierungen nutzen opportunistisch u.a. die neusten Schwachstellen, komplexe Angriffsmethoden und besonders bedrohliche Phishing-Narrative, um Daten zu erlangen. Sie bedienen sich Ransomware- und DDoS-Angriffen und zielen primär auf Elemente der Gesellschaft ab, deren Funktionsausfall eklatante Schäden erzeugen könnte, wie zum Beispiel schlecht gesicherte Lieferketten. Hybride Bedrohungen, wie Desinformationskampagnen, finden sich vorwiegend bei staatlichen Akteuren.

[17] Als Advanced Persistent Threat (APT) wird der Modus Operandi eines zielgerichteten Cyber-Angriffs mit sehr hohem Ressourceneinsatz und erheblichen technischen Fähigkeiten bezeichnet, durch den ein dauerhafter Zugriff auf das Zielsystem erlangt wird. Zudem bezeichnet APT staatliche Akteure oder Akteure, die sich der organisierten Kriminalität zuordnen lassen.

[18] Namenswechsel des Akteurs. Wird häufig begleitet von einem Infrastrukturwechsel mit dem Ziel, sich von vormals verwendeter Malware (v.a. Ransomware) zu distanzieren.

5.1 TÄTER-TYPEN

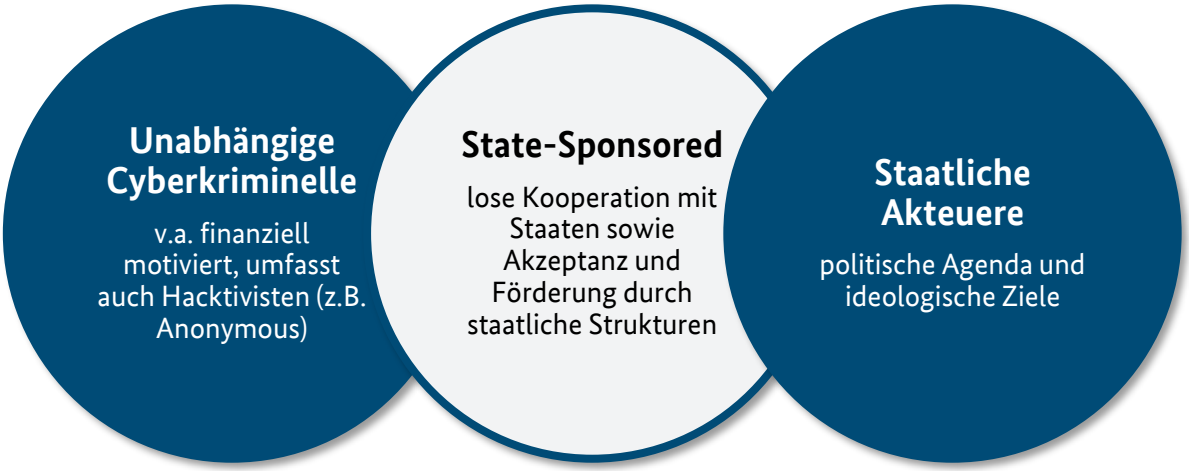


Abbildung 27: Einteilung cyberkrimineller Gruppierungen

Zwischen unabhängigen Cybercrime-Gruppierungen und solchen, die staatlich gesteuert sind, finden sich Gruppierungen, die als „state-sponsored" eingeordnet werden können. Sie arbeiten lose mit Staaten zusammen, nehmen entsprechende Aufträge an und werden mehr oder minder stark durch staatliche Strukturen gefördert oder zumindest unbehelligt geduldet.

Aufgrund der zunehmenden Professionalisierung aller Akteure, welche besonders durch CaaS-Modelle vorangetrieben wird, ist davon auszugehen, dass alle Arten der o.g. Gruppierungen über annähernd dasselbe Gefährdungspotenzial, Know-How und Ressourcen verfügen.

Insbesondere Russland galt lange als „Safe Haven" für Cyberkriminelle. Medial aufgegriffene Ransomware-Angriffe, wie Angriffe auf das US-Energie-Unternehmen Colonial Pipeline und auf den Fleischproduzent JBS, sorgten 2021 für politische Spannungen. Forderungen der US-Regierung an Russland zogen mutmaßlich im Januar 2022 Verhaftungen von Mitgliedern der Ransomware-Gruppierung REvil durch russische Sicherheitsbehörden nach sich und stellten Russland als sichere Operationsbasis für andere Gruppierungen zumindest in Frage. Inwieweit dieser Effekt sich bewahrheitet und welche Auswirkungen der Krieg in der Ukraine auf die Rolle Russlands in diesem Zusammenhang hat, lässt sich zum jetzigen Zeitpunkt noch nicht valide prognostizieren.

Ausblick 2022

- Im Zuge des Russland-Ukraine-Konflikts tritt die Bedeutung staatlich gelenkter sowie geduldeter Cybercrime-Akteure besonders zutage.
- Beide involvierte Staaten machen sich Cybercrime-Gruppierungen für ihre geo-politischen Interessen zu Nutze.
- Bisher politisch unabhängig geglaubte Gruppierungen treten mit ihren Ressourcen dem Konflikt bei.

Der Übergang zwischen finanziell und politisch motivierten Cybercrime-Gruppierungen ist hinsichtlich ihrer gestiegenen Professionalisierung und Anpassungsfähigkeit fließend – einzig die Motivationslage ist eine andere.

5.2 RELEVANTE CYBER-GRUPPIERUNGEN

Nachfolgende Übersicht stellt einen Ausschnitt der Cyber-Akteure dar, die im Jahr 2021 in Deutschland aktiv waren.

LockBit-Gang	
Eingesetzte Software und Tools	**Zieltypen**
Schadsoftware: LockBit, Lockbit 2.0 Tools: CrackMapExec, EmpireProject	Ziele der Gruppierung sind weltweit Unternehmen und Organisationen jeglicher Art. Explizit ausgenommen sind Gesundheits- und Bildungseinrichtungen sowie soziale Dienste und Wohltätigkeitsorganisationen.
Die Gruppierung ist seit mindesten 2019 aktiv, bietet Ransomware-as-a-Service (RaaS) an und warb in der Vergangenheit öffentlich und aggressiv um Affiliates sowie Insider in großen Unternehmen und Organisationen. Die Gruppierung ist medienaffin und hat ein finanzielles Motiv. LockBit 2.0 gilt derzeit als eine der am schnellsten verschlüsselnde Ransomware.	

Wizard Spider (Grim Spider, TEMP, MixMaster, Gold Blackburn, Gold Ulrick, FIN12)	
Eingesetzte Software und Tools	**Zieltypen**
Schadsoftware: Anchor, BazarBackdoor, Conti, Diavol, Dyre, Gophe, LightBot, PowerTrick, Ryuk, TrickBot, TrickMo, Upatre Tools: AdFind, BloodHound, Cobalt Strike, Invoke-SMBAutoBrute, LaZanga, PowerSploit, PsExec, SessionGopher	Ziele der Gruppierung sind weltweit Unternehmen und Organisationen jeglicher Art. Der Fokus der Gruppierung liegt dabei auf dem Big Game Hunting. Ferner werden in der Regel keine russischsprachigen Systeme attackiert.
Wizard Spider ist eine seit mindestens 2014 aktive russische Gruppierung, die finanziell motiviert ist und RaaS anbietet. Die Gruppierung geht seit 2018 zunehmend professionalisiert vor. Ihre Schadsoftware wird nicht öffentlich auf inkriminierten Foren beworben, sondern mutmaßlich nur vertrauenswürdigen Partnern bereitgestellt. Bei Angriffen auf den Gesundheitssektor geht die Gruppierung häufig saisonal vor, sodass ein größtmöglicher Schaden erzielt wird.	

Gold Southfield (Pinchy Spider, Gold Garden, REvil)	
Eingesetzte Software und Tools	**Zieltypen**
Schadsoftware: GrandCrab, REvil / Sodinokibi, VIDAR Tools: Cerbutil, Cobalt Strike, Mimikatz	Fokus der Gruppierung ist Big Game Hunting. Ferner werden in der Regel keine russischsprachigen Systeme attackiert.
Gold Southfield ist seit mindestens 2018 aktiv, finanziell motiviert und mutmaßlich russischen Cyberkriminellen zuzuordnen. Die Gruppierung operiert als RaaS und setzt eine höchst professionelle technische Infrastruktur ein und nutzt die Verschlüsselung vorwiegend an Wochenenden, um einer Entdeckung möglichst lange zu entgehen. Die Gruppierung war u.a. verantwortlich für den Angriff auf Kaseya Ltd. Ende 2021. Anfang 2022 kam es zu mehreren Festnahmen und der Zerschlagung der Infrastruktur.	

APT29/Cozy Bear/Nobelium	
Eingesetzte Software und Tools	**Zieltypen**
Dropper: Ceeloader, OnionDuke InfoStealer und Backdoor: CosmicDuke, WellMail Remote Access Trojaner: WellMess	Vorwiegend Behörden, Einrichtungen des Gesundheitssektors und Energieversorger

APT 29 wird quellenübergreifend dem russischen Auslandsgeheimdienst SWR zugeordnet. Zu ihren Zielen gehören vornehmlich Behörden, das Gesundheitswesen sowie Energieversorger. Auch Spionagetätigkeiten im Zusammenhang mit der Covid-19-Impfstoff-Forschung und -Entwicklung gehörten zu ihren Aktivitäten. Bevorzugte Methoden sind hochvolumige Angriffe, wie Phishing-Kampagnen, um viele Ziele auf einmal angreifen zu können.

AlphV / BlackCat Gang (Noberus)	
Eingesetzte Software und Tools	**Zieltypen**
Schadsoftware: AlphV / BlackCat Tools: GO Simple Tunnel, LaZagne, MEGAsync, Mimikatz, PSExec, WebBrowserPassView	Die Ziele der Gruppierung sind weltweit Unternehmen und Organisationen jeglicher Art.
Bei AlphV / der BlackCat-Gang handelt es sich um eine seit 2021 aktive und finanziell motivierte Gruppierung, die RaaS anbietet. Affiliates der Gruppierungen werden über russischsprachige Foren rekrutiert. Bei der verwendeten Schadsoftware AlphV / BlackCat handelt es sich um die erste in der Programmiersprache Rust geschriebene Ransomware.	

Abbildung 28: Kurzprofile in Deutschland relevanter Cyber-Akteure

Takedown des VPN-Dienstleisters vpnlab.net

Das Ermittlungsverfahren

Die Polizeidirektion Hannover führt seit Ende 2019 unter der Sachleitung der Zentralstelle Cybercrime der Staatsanwaltschaft Verden (Aller) Ermittlungen gegen die verantwortlichen Personen hinter der Ransomware Ryuk. Diese Ransomware wird von den Tätern hauptsächlich für das sog. Big Game Hunting, also Angriffen auf wirtschaftlich starke Unternehmen, verwendet.
Im Rahmen der Ermittlungen wurde festgestellt, dass einige der Ryuk-Akteure den VPN-Dienstleister vpnlab.net genutzt haben, um ihr Vorgehen bei z.B. Cyberangriffen auf Unternehmen und Verwaltungen sowie auf kritische Infrastrukturen wie Krankenhäusern zu verschleiern. Da sich vpnlab.net als ein vielfältig und umfangreich genutztes Werkzeug von Cyber-Straftätern herausstellte, beschlagnahmten die zuständigen Behörden vpnlab.net.

Der Takedown

Durch Beschlagnahme und Auswertung von Knotenservern konnten die Standorte des Netzwerkes im Rahmen einer internationalen Kooperation mit Strafverfolgungsbehörden aus zehn beteiligten Ländern sowie mit der Unterstützung von Europol und Eurojust aufgeklärt und dessen Abschaltung gewährleistet werden.

Der Takedown erfolgte am 17.01.2022 bei insgesamt 15 Servern weltweit (u. a. in Russland) simultan. Nach der Abschaltung des Netzwerks konnte ein täterseitiges Ausweichen auf andere Infrastrukturen festgestellt werden. Die im Rahmen des Takedowns erlangten Daten werden in Zusammenarbeit mit Europol weiter untersucht. Sie enthalten auch Zufallsfunde, welche für andere Cybercrime-Ermittlungsverfahren relevant sind.

6 Schäden durch Cybercrime

Cybercrime stellt einen Phänomenbereich mit hohem Schadenspotenzial dar. Modi Operandi wie DDoS- und Ransomware-Angriffe können existenzschädigende Auswirkungen auf Behörden und Unternehmen haben sowie die Bereitstellung kritischer Dienstleistungen einschränken. Angriffe wie auf den Erdöllieferanten Colonial Pipeline oder den Landkreis Anhalt-Bitterfeld zeigen, dass Cyberangriffe in unterschiedlichsten Bereichen realweltliche Folgen für das Wohl der Bevölkerung nach sich ziehen können.

Auf Basis der Polizeilichen Kriminalstatistik lassen sich keine validen Aussagen zu von Cybercrime verursachten (Gesamt-)Schäden treffen, da lediglich der dem Phänomenbereich zugeordnete Computerbetrug explizit auch Schadenssummen ausweist. Folgeschäden können ebenfalls nicht beziffert werden. Für eine Gesamtbetrachtung des Schadens durch Cybercrime muss daher auf andere Quellen zurückgegriffen werden.

Die durch den Branchenverband Bitkom e.V. errechneten Cybercrime-Schäden in Deutschland beliefen sich im Berichtszeitraum 2020/2021 auf 223,5 Mrd. Euro und sind damit mehr als doppelt so hoch wie noch 2018/2019. Alleine im Bereich Ransomware („Erpressung mit gestohlenen Daten oder verschlüsselten Daten“), hat sich der Schaden unter den Befragten mit 24,3 Mrd. EUR seit dem letzten Wirtschaftsschutzbericht 2019 fast verfünffacht.

Betrachtet man die durch den Bitkom e.V. erhobenen Schadensquantifizierungen, so ist ein kontinuierliches und teils drastisches Wachstum ersichtlich: Seit 2017 errechnet der Bitkom e.V. in jedem Untersuchungszeitraum annähernd eine Verdopplung der durch Cybercrime verursachten Schäden zum Vorjahr.

Schaden durch:	Schadens-summen in Mrd. Euro (2021)	Schadens-summen in Mrd. Euro (2019)	Schadens-summen in Mrd. Euro (2017)	Schadens-summen in Mrd. Euro (2015)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	61,9	13,5	5,3	7,2
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	**24,3**	**5,3**	**0,7**	**1,5**
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	17,1	4,4	3,2	2,0
Patentrechtsverletzungen (auch schon vor der Anmeldung)	30,5	14,3	7,7	9,4
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	29,0	11,1	8,6	6,4
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	22,7	11,1	3,5	11,5
Imageschaden bei Kunden oder Lieferanten/Negative Medienberichterstattung	12,3	9,3	7,7	5,9
Kosten für Ermittlungen und Ersatzmaßnahmen	13,3	18,3	10,6	-
Kosten für Rechtsstreitigkeiten	12,4	15,6	5,5	6,5
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	-	-	2,2	0,9
Sonstige Schäden	0	< 0,1	< 0,1	0,1
Gesamtschaden pro Jahr	**223,5**	**102,9**	**54,8**	**51,2**

Abbildung 29: Verursachte Schäden durch Cybercrime. Quelle: Die Einzelzahlen sowie Summenwerte wurden in dieser Form von Bitkom e.V. aus dem Wirtschaftsschutzbericht 2021 (veröffentlicht am 05.08.2021) übernommen.

Schäden, die im Zuge von Ransomware-Angriffen entstehen, nehmen stetig zu und machen mittlerweile einen bedeutenden Anteil an den Gesamtschäden aus. Neben möglichen Lösegeldzahlungen entstehen

durch Ransomware unter anderem auch die Kosten für die Bereinigung und Ausfallzeiten der Systeme sowie Personal-, Hardware- und Netzwerkkosten.
Laut Untersuchungen des IT-Security-Dienstleisters Sophos [19] verursacht ein einzelner Ransomware-Angriff im Durschnitt ca. 1,85 Mio. US-Dollar Schaden. Die Kosten, die von einer reduzierten Betriebsfähigkeit verursacht werden, variieren ja nach Branche beträchtlich. So ermittelte das IT-Security-Unternehmen McAfee [20] hierfür einen Durchschnitt von 590.000 US-Dollar pro Angriff, bei einer Spannweite von 89.000 US-Dollar für Unternehmen im Personalbereich und 965.000 US-Dollar im Bereich von Unternehmen des Ingenieurwesens.

Nicht direkt quantifizierbar sind auch Schäden, die aus Data Leaks entstehen. Obwohl abgeflossene Datensätze zunächst keinen monetären Schaden verursachen, können sie kaskadenartig zu weiteren Angriffen genutzt werden und damit zu kriminellen Missbrauchsszenarien führen, die weitere finanzielle Schäden verursachen.

Die Dimension von durch Cyberangriffe verursachten Schäden zeigt insgesamt deutlich, dass Betroffene hier nicht nur vor einer großen Herausforderung stehen, sondern sich aus Cyberangriffen auch vielfach existenzbedrohende Notlagen, insbesondere für Unternehmen, entwickeln können.

[19] Vgl. Sophos, Ransomware-Report 2021, online abrufbar unter: **https://www.sophos.com/de-de/content/state-of-ransomware**

[20] Smith, Zhanna Malekos und Eugenia Lostri sowie James A. Lewis (Center for Strategic and International Studies (CSIS) in Partnerschaft mit McAfee), The Hidden Costs of Cybercrime, 09.12.2022, online abrufbar unter: **https://www.csis.org/analysis/hidden-costs-cybercrime**

7 Quo vadis, Cybercrime?

Auch im Jahr 2021 stiegen die Fallzahlen der in der Polizeilichen Kriminalstatistik registrierten Cyberstraftaten weiter an. Gleichzeitig sank die Aufklärungsquote auf unter 30% - ein Trend, der sich bereits in den letzten Jahren abgezeichnet hat. Obgleich das vollständige Ausmaß der Cybercrime aufgrund des überdurchschnittlich großen Dunkelfeldes unbestimmt bleibt, werden die schädigenden Effekte in der „analogen Welt“ immer deutlicher sichtbar. Insbesondere die Corona-Pandemie dürfte hierbei als „Beschleuniger“ für weitere Cyberstraftaten einen nicht unerheblichen Beitrag gehabt haben.

Dabei sind auch die Wertigkeit und das Schadenspotenzial von Cyber-Delikten in den letzten Jahren stetig angestiegen: Durch die Verzahnung von (digitalen) internationalen Lieferketten erhöht sich die Anzahl an potenziellen Eintrittsvektoren für Täter und Schadsoftware kann sich schneller über komplette Lieferketten ausbreiten. Ebenso kann die Kompromittierung eines Teilsystems für einen kaskadenartigen Ausfall der gesamten Lieferkette sorgen.

Hinzu kommt die fortschreitende Digitalisierung mit der Verlagerung von Services und Waren in die digitale Welt. Viele Menschen nutzen und schätzen die neuen Möglichkeiten digitaler Behördengänge und die Flexibilität des mobilen Arbeitens – nicht zuletzt während der Corona-Pandemie. Allerdings wird durch diese Innovationen, sofern keine Sicherung der IT-Prozesse und – Kommunikation erfolgt, eine Vielzahl neuer Tatgelegenheiten für die Cyberkriminalität geschaffen. Erfolgreiche Angriffe auf diese „neue Flexibilität“ haben starke Auswirkungen auf die Gesellschaft insgesamt, aber auch auf das subjektive Sicherheitsgefühl jedes Einzelnen.

Diese Befunde werden sich auch auf die künftige Entwicklung von Cyberstraftaten auswirken. Ebenfalls prägenden Einfluss sowohl auf das Phänomen als auch dessen Bekämpfung dürfte der russische Angriffskrieg gegen die Ukraine haben. Es handelt sich um die erste kriegerische Auseinandersetzung, die zu einem erheblichen Teil auch im Cyberraum geführt wird. Auch wenn sich die langfristigen Auswirkungen auf den Phänomenbereich aktuell noch nicht abschließend beurteilen lassen, hat der Krieg das Potential, nach der Corona-Pandemie als weiterer Katalysator für Cybercrime zu wirken.

Denn neben der konventionellen Kriegsführung setzen beide Staaten verschiedenste Arten von Cyberangriffen ein, um die Gegenseite zu sabotieren oder zu demoralisieren. Eindringliche Beispiele sind die Verwendung von sog. Wipern, welche Daten von IT-Systemen überschreiben oder löschen. Neben der Nutzung bzw. Werbung für eigene „IT-Armeen“ ist eine erhebliche Solidarisierung von hacktivistischen oder bisher unabhängigen Gruppierungen mit einer der Kriegsparteien festzustellen. Aktivitäten jener Akteure machen dabei häufig nicht an Ländergrenzen halt und können schnell Auswirkungen auf Unternehmen, kritische Infrastrukturen und auf staatliche Einrichtungen in nicht direkt am Krieg beteiligten Staaten haben. Dabei können Cyberangriffe militärischen Ursprungs, staatlich gesteuert oder auch allgemeinkriminell motiviert sein.

Diesen Entwicklungen muss mit einem ganzheitlichen und flexiblen Bekämpfungsansatz entgegengewirkt werden. Auf polizeilicher Ebene gehört hierzu neben der Prävention sowohl die polizeiliche Abwehr von Gefahren im Cyberraum als auch eine nachhaltige Strafverfolgung und Zerschlagung krimineller Infrastrukturen.

Cybercrime gemeinsam bekämpfen

Strafverfolgung und Unternehmen kennen einander, kooperieren aber nur bedingt - Straftäter hingegen kennen einander nicht, kooperieren aber vertrauensvoll auch über Ländergrenzen hinweg.

Erst durch die Erstattung einer Strafanzeige ist es den Strafverfolgungsbehörden überhaupt möglich, hinreichend aktiv zu werden. Ohne eine solche Aufhellung des Dunkelfeldes bleiben die meisten Cyberdelikte straffrei, fördern weiter die Underground Economy und bilden die Grundlage für weitergehende Straftaten. Auch Zusammenhänge zwischen einzelnen Taten können ohne ein entsprechendes Anzeigeverhalten nicht erkannt werden.

Die Bekämpfung der Cybercrime ist daher weiterhin als gesamtgesellschaftliche Aufgabe zu verstehen: Repressive Maßnahmen, präventive IT-Sicherheitsvorkehrungen und eine ausreichende Awareness bei Bürgern und Unternehmen sollten einen ausgewogenen Dreiklang in diesem Deliktsfeld bilden. Eine enge und vertrauenswürdige Kooperation zwischen staatlichen Behörden und privaten Unternehmen ist hierbei Grundvoraussetzung für die Implementierung effektiver Maßnahmen zur Eindämmung der Cybercrime.

Die polizeilichen Erfahrungen zeigen, dass sich bei wirksamer Zusammenarbeit aller relevanten Akteure – national wie international, öffentlich wie privat – trotz Professionalisierung der Täterseite auch im Bereich Cybercrime signifikante Ermittlungserfolge erzielen lassen. International stellen u.a. die Takedowns der Emotet-Infrastruktur, des VPN-Dienstleisters vpnlab.net oder auch des bedeutenden Darknet Marktplatzes Hydra Market maßgebliche Erfolge der Sicherheitsbehörden gegen die organisierte Cyberkriminalität dar. National sind insbesondere der sog. „Cyberbunkerprozess“ mit einer erstmaligen Verurteilung nach § 129 StGB im Bereich Cybercrime, wie auch die ersten Ermittlungen gegen kriminelle Gruppierungen, welche sich über den Messenger-Dienst Telegram organisierten, hervorzuheben.

Insbesondere die Ermittlungen gegen das Emotet-Netzwerk zeigt Wege auf, auch zukünftig erfolgversprechend gegen Malware-Infrastrukturen vorgehen zu können.

Emotet

Nachhaltiger Erfolg durch international koordiniertes Vorgehen

Im Januar 2021 wurden in enger Abstimmung mit internationalen Partnerbehörden Exekutivmaßnahmen gegen die Emotet-Infrastruktur umgesetzt, welche zu deren Zerschlagung führten. Maßgeblich für den erfolgreichen Takedown war vor allem die hervorragende Zusammenarbeit auf nationaler und internationaler Ebene zwischen Strafverfolgungsbehörden, IT-Sicherheitsbehörden sowie dem Privatsektor.

Für einen substanziellen Zeitraum wurde eine der weltweit gefährlichsten Schadsoftware-Familien komplett unschädlich gemacht, was auch Auswirkungen auf andere Schadsoftwarefamilien, wie insbesondere Ransomware, hatte.

Erst zum Jahresende 2021 konnte sich wieder eine neue, vergleichsweise weniger wirkungsvolle Emotet-Variante in der Underground Economy etablieren. Hierzu musste die Täterseite einen erheblichen

Aufwand betreiben. Emotet kann insofern als Blaupause auch für künftige Ermittlungsverfahren im Bereich Cybercrime angesehen werden.

Cybercrimefighting-as-a-Service

Cybercrime-as-a-Service fordert entsprechende Entwicklungen auch auf Seiten der Strafverfolgungsbehörden.

Um weiterhin die Deliktsausprägungen der Cybercrime erfolgreich bekämpfen zu können, ist mit Blick auf die zunehmende Professionalisierung durch Cybercrime-as-a-Service auch auf polizeilicher Seite ein besonderes Maß an Spezialisierung erforderlich. Als besonders herausfordernd für die Strafverfolgungsbehörden sind hierbei auch die Bereiche „Verarbeitung von Massendaten“ und die „Auswertung von Schadsoftware“ zu nennen. Hinzu kommt die Notwendigkeit, in sehr kurzen Zeiträumen agil auf technische Innovationen reagieren zu können. Diesem komplexen Anforderungsprofil folgend, bedarf es einer datenbasierten Gesamtausrichtung mit hochspezialisierten Fachkräften auf staatlicher Seite. Über die Implementierung modernster Technik und die agile und flexible Weiterentwicklung bestehender Werkzeuge kann die deutsche Strafverfolgung ihre Position weiter stärken und seine Rolle als aktiver und verlässlicher internationaler Partner ausbauen. Dabei ist nicht erforderlich, dass jede einzelne Dienststelle sämtliche Kompetenzen und technischen Fähigkeiten vollständig abbildet. Diese müssen als Gegenentwurf zum täterseitigen Vorgehen vielmehr „as-a-Service“ schnell und bedarfsorientiert im polizeilichen Verbund für alle bereitgestellt werden.

Impressum

Herausgeber
Bundeskriminalamt, 65173 Wiesbaden

Stand
Mai 2022

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.