Bundeskriminalamt

BKA

Cybercrime

Bundeslagebild 2019

Inhaltsverzeichnis

1 Vorbemerkung

In der Polizeilichen Kriminalstatistik (PKS) werden die bekannt gewordenen Straftaten nach Abschluss der polizeilichen Ermittlungen erfasst. Diese Statistik bildet insofern das polizeiliche Hellfeld ab.

Dass im Bereich Cybercrime von einem weit überdurchschnittlichen Dunkelfeld ausgegangen werden kann, lässt sich aus folgenden – für das Deliktsfeld z. T. spezifischen – Aspekten ableiten:

- Eine große Anzahl strafbarer Handlungen im Internet kommt aufgrund zunehmender technischer Sicherungseinrichtungen über das Versuchsstadium nicht hinaus und wird von den Geschädigten nicht bemerkt.
- Die betroffenen Personen erkennen nicht, dass sie Geschädigte einer Cyber-Straftat geworden sind (z. B. bei Diebstahl ihrer Identität bei einem Online-Shop) bzw. von ihnen eingesetzte technische Geräte unbemerkt zur Begehung von Cybercrime-Straftaten missbraucht wurden (z. B. Nutzung infizierter PCs oder Router als Teil eines Botnetzes zur Ausführung von DDoS[1]-Angriffen oder Infektion mit Cryptomining-Malware).
- Straftaten werden durch Geschädigte nicht angezeigt, insbesondere, wenn noch kein finanzieller Schaden entstanden ist (z. B. bloßer Virenfund auf dem PC) oder der eingetretene Schaden von Dritten (z. B. Versicherung) reguliert wird.
- Geschädigte, insbesondere Firmen, zeigen erkannte Straftaten nicht an, um bspw. die Reputation als „sicherer und zuverlässiger Partner“ im Kundenkreis nicht zu verlieren.
- Geschädigte erstatten z. B. in Erpressungsfällen oftmals nur dann Anzeige, wenn trotz Zahlung eines Lösegelds keine Dekryptierung des durch die Täterseite zuvor verschlüsselten Systems erfolgt.

Um den Kriminalitätsbereich Cybercrime – trotz dieser Faktoren – möglichst realitätsnah zu beschreiben, wurden – wie in der polizeilichen Strategie zur Bekämpfung der Cybercrime festgelegt – auch für das Berichtsjahr Informationen unterschiedlicher polizei- und behörden-externer Institutionen (z. B. Forschungseinrichtungen und IT-Sicherheitsdienstleister) einbezogen. Ferner wurde der Kooperationspartner des Bundeskriminalamts (BKA), das German Competence Centre against Cyber Crime e.V. (G4C)[2], samt der dem Verein zugehörigen Unternehmen in die Erstellung des Lagebilds eingebunden.
Die auf dieser Basis erstellte qualitative Analyse der Lage Cybercrime ist im aktuellen Lagebild der quantitativen Betrachtung auf Basis der PKS vorangestellt.

[1] Denial-of-Service (DoS)-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff (DDoS = Distributed Denial of Service). DDoS-Angriffe erfolgen häufig durch eine sehr große Anzahl von Computern oder Servern, die ein Botnetz bilden.
[2] G4C-Mitglieder: Commerzbank, ING-DiBa, HypoVereinsbank, Kreditanstalt für Wiederaufbau, Schufa, Bank-Verlag, R+V, Broadcom, Diebold Nixdorf, Link11, G-Data; G4C-Kooperationspartner: BKA und BSI.

2 Prägende Cyberangriffe 2019

Januar
- Ein Tochterunternehmen der Deutschen Kreditbank (DKB) wird von einem DDoS-Angriff getroffen – die Online-Dienste sind zeitweise nicht mehr verfügbar.

Februar
- Kunden verschiedener Banken werden Opfer von SIM-Swapping[3] und anschließendem TAN-Abfang.

März
- Die Ransomware *LockerGoga* befällt den internationalen Industriekonzern NorskHydro.
  GandCrab erpresst mehrere Unternehmen in Deutschland.

April
- Verschiedene DAX-Unternehmen sollen mit Hilfe der Malware Winnti ausspioniert worden sein.

Mai
- Eine Welle der Malware *Emotet* trifft u. a. diverse Finanzämter.

Juni
- Die IT-Systeme des internationalen Forensik-Dienstleisters Eurofins werden durch eine Ransomware verschlüsselt. Partner von Eurofins beenden daraufhin die Kooperation.

[3] Beim SIM-Swapping lassen die Täter die Rufnummer eines Ziels auf eine vom Angreifer gehaltene SIM-Karte übertragen. Um beim jeweiligen Telekommunikationsanbieter an eine SIM-Karte mit der Rufnummer des Opfers zu gelangen, sammeln die Täter häufig im Vorfeld über verschiedene Methoden die dafür notwendigen Daten über das potenzielle Opfer. Die SIM-Karte mit der Rufnummer des Opfers ermöglicht es den Tätern dann, bei einigen Anbietern Passwörter von Konten des Opfers (z. B. bei E-Commerce-Plattformen oder Banking-Apps) neu zu vergeben.

Juli

- Die Ransomware *Sodinokibi* infiziert mehrere Einrichtungen des Deutschen Roten Kreuzes.

August

- Die Ransomware *GermanWiper* verbreitet sich im Inland. Selbst nach Zahlung des Lösegeldes bleiben die verschlüsselten Daten unbrauchbar.

September

- Die Systeme der Rheinmetall-Automotive-Gruppe werden mit Malware infiziert.

Oktober

- Während die Malware *Emotet* die Arbeit des Kammergerichts Berlin massiv beeinträchtigt, verschlüsselt eine Ransomware die Systeme der Universität Regensburg.

November

- Die Pilz GmbH wird gezwungen, ihren Betrieb zeitweise einzustellen. Anlass ist eine Ransomware.

Dezember

- Zum Jahresende tritt wieder verstärkt *Emotet* auf: Sowohl das Klinikum Fürth, die Stadt Frankfurt am Main als auch die Stadt Homburg werden von dem Trojaner infiziert.
- Zudem wird die Universität Gießen Opfer eines Ransomeware-Angriffs.

3 Cybercrime in Deutschland

Die Professionalität von Cyberkriminellen steigt weiter an.

Cybercrime erschafft und basiert auf kriminellen Wertschöpfungsketten.

Ransomware bleibt die größte Bedrohung für Wirtschaftsunternehmen.

Anzahl und auch Intensität von DDoS-Angriffen steigen rapide an.

Die Täter sind global vernetzt und agieren international, arbeitsteilig und höchst organisiert.

Die wichtigsten Schutzmechanismen gegen Cybercrime sind weiterhin sensible Internetnutzer.

3.1 DIEBSTAHL DIGITALER IDENTITÄTEN / ID-THEFT

Zu Beginn der meisten Cybercrime-Straftaten steht der Diebstahl einer digitalen Identität. Durch den Abgriff eines Passworts für einen E-Commerce-Account, zu E-Mail- oder Messengerdiensten, zur Cloud oder zu firmeninternen Ressourcen ist es Cyberkriminellen möglich, diese missbräuchlich zu nutzen. Die Auswirkungen von Diebstählen der digitalen Identität sind mannigfaltig und Grundlage der wirtschaftlichen Wertschöpfungsketten von Cybercrime – angefangen von der Nutzung kostenpflichtiger Streaming-Dienste über das widerrechtliche Abschließen von Verträgen und Warenbestellungen, Mobbing, Stalking oder das Tätigen von Online-Überweisungen.

Was ist die digitale Identität?

Der Begriff „digitale Identität" bezeichnet die Summe aller Möglichkeiten und Rechte des einzelnen Nutzers sowie seiner personenbezogenen Daten und Aktivitäten innerhalb der Gesamtstruktur des Internet.
Konkret beinhaltet dies auch alle Arten von Nutzer-Accounts, also auch Zugangsdaten in den Bereichen

- *Kommunikation (E-Mail- und Messengerdienste),*
- *E-Commerce (Online-Banking, Online-Aktienhandel, internetgestützte Vertriebsportale aller Art),*
- *berufsspezifische Informationen (z. B. für den Online-Zugriff auf firmeninterne, technische Ressourcen),*
- *E-Government (z. B. elektronische Steuererklärung) sowie*
- *Cloud-Computing (Nutzung von als Dienstleistung angebotenem Speicherplatz, von Software oder Rechenleistung).*

Der Diebstahl von digitalen Identitäten durch die Cybertäter kann auf verschiedene Weise erfolgen. Die häufigsten Methoden sind dabei:

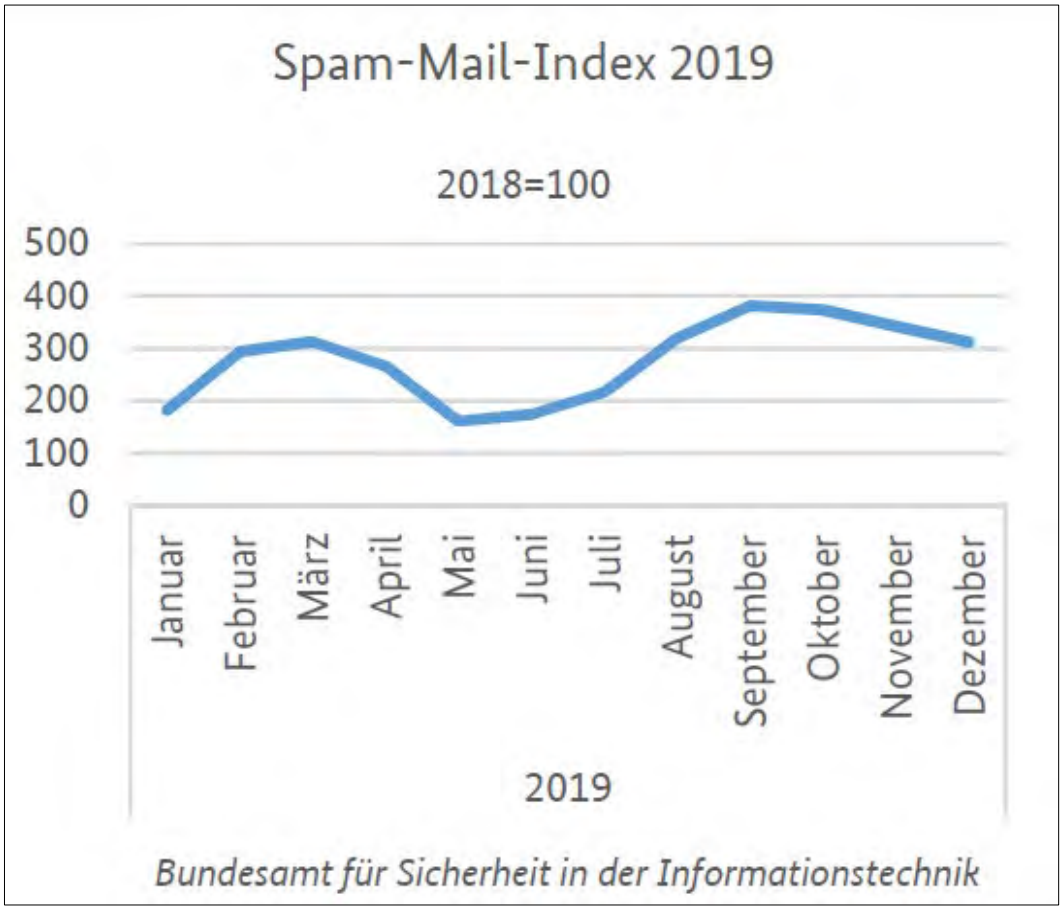
- Phishing- und Spam-Mails,
- Schadsoftware (z. B. Keylogger, welche Tastatureingaben mitschneiden),
- analoges Social Engineering (z. B. über sog. Tech-Support-Scam[4]),
- Datenlecks (der oftmals ungewollte Abfluss von Daten) oder Data-Breaches (das aktive Abgreifen, Abfangen oder Ausleiten von Daten durch Dritte).

[4] Kriminelle rufen bei Zielpersonen an und geben sich als ein IT-Support-Team aus. Unter dem Vorwand, dass auf dem Rechner ein Fehler aufgetreten sei oder eine falsche Betriebssystem-Lizenz verwendet werde, soll das Opfer den Kriminellen via Fernsteuerung Zugriff auf den Rechner gewähren oder Passwörter offenlegen.

Jedes gestohlene Passwort, jede geleakte Mail-Adresse, jede erbeutete Kreditkartennummer kann für kriminelle Zwecke missbraucht und weiterverkauft werden.

Die Verbreitung von Spam-Mails ist ein Angriffsvektor, der den meisten Bürgern bereits persönlich begegnet sein dürfte: Dubiose E-Mail-Absender verschicken offenbar willkürlich Mails zu höchst unterschiedlichen Themen. Die Spam-Mail zielt darauf ab, dass der Nutzer entweder den Anhang herunterlädt oder einem Link folgt. Beides führt zur Kompromittierung des IT-Systems: Sowohl der Mail-Anhang als auch die verlinkte Webseite können maliziösen Code enthalten, welcher zum Abgriff von Daten auf dem Zielsystem verwendet wird.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) führt den sog. Spam-Mail-Index, der die Betroffenheit der Netze des Bundes hinsichtlich der dort identifizierten Spam-Mails misst. Der Index umfasst dabei alle unerwünschten Mails, z. B. Werbung, aber auch Mal-Spam.[5]



[5] Mal-Spam bezeichnet eine mit Malware beladene Spam-Mail.

Deutlich sichtbar ist die quantitative Erhöhung des Index in 2019 gegenüber dem Vorjahresdurchschnitt. Zu keinem Zeitpunkt des Jahres 2019 liegt der Spam-Mail-Index unterhalb des Basiswerts 2018 – die Anzahl an Spam-Mails hat im Jahr 2019 drastisch zugenommen, lag im Durchschnitt bei 277,8 und ist somit knapp 2,8-mal so hoch wie im Jahresdurchschnitt 2018. Besonders ab August zeigt der Index starke Abweichungen zum Vorjahresdurchschnitt.

Data-Breaches oder durch technische Mängel verursachte, versehentliche Abflüsse von Daten können jeweils Millionen von Datensätzen beinhalten. Jeder verlorene Datensatz kann als Nährboden für weitere kriminelle Zwecke dienen und weiterverkauft werden. Das kriminelle Potenzial, das der Verlust von Datensätzen mit einer Größenordnung von über 100 Millionen betroffenen Kunden aufweist, ist daher enorm: So berichtete das Nationale Cyber-Abwehrzentrum[6] Anfang 2019 von einem veröffentlichten Data-Dump, der ca. 773 Millionen E-Mail-Adressen und 21 Millionen Passwörter im Klartext beinhaltete. Auch wenn ein Großteil der veröffentlichten Zugangsdaten vermutlich zu diesem Zeitpunkt bereits nicht mehr aktuell war, so besteht durch derartige Veröffentlichungen ein hohes Risiko der illegitimen Übernahme digitaler Identitäten durch Dritte.

Schwerwiegend dabei: Oftmals ist es den Betroffenen nicht bewusst, dass ihre Daten abgegriffen wurden bzw. anderweitig abhandengekommen sind. Ursache für den Verlust von Daten ist oftmals der unzureichend gesicherte Umgang mit selbigen.

Fallbeispiel: weleakinfo.com

Ab dem 04.01.2019 wurde im BKA ein Ermittlungsverfahren gegen einen damals 21-jährigen deutschen Staatsangehörigen geführt, der über Social Media-Kanäle unbefugt persönliche Daten und Dokumente von Politikern, Journalisten und Personen des öffentlichen Lebens im Rahmen eines sog. „Adventskalenders“ veröffentlichte. Der Beschuldigte gab nach seiner vorläufigen Festnahme an, bei der Plattform *weleakinfo.com* Zugangsdaten und Passwörter angekauft und diese für das anschließende Eindringen in die Accounts seiner Opfer genutzt zu haben.

Am 21.05.2019 hat die Generalstaatsanwaltschaft Frankfurt/Main (ZIT) ein Verfahren wegen des Verdachts des Ausspähens von Daten (§202a StGB) sowie der Datenhehlerei (§202d StGB) gegen die Betreiber der Plattform *weleakinfo.com* eingeleitet und das BKA mit den Ermittlungen beauftragt. Weitere Ermittlungsverfahren wurden gegen die beiden Administratoren der Plattform in den Niederlanden, Großbritannien und den USA geführt.

Die Administratoren dieser Plattform konnten am 15.01.2020 in Großbritannien festgenommen werden. Im Verlauf der weiteren Maßnahmen konnten mehrere Server in den Niederlanden sichergestellt werden, die in Verbindung zur Plattform *weleakinfo.com* standen. Das BKA führte weitere Beweissicherungsmaßnahmen von in Deutschland angemieteten Servern der Beschuldigten durch. Die Domain *weleakinfo.com* konnte durch das FBI übernommen und mit einem sog. „seizure banner“ versehen werden.

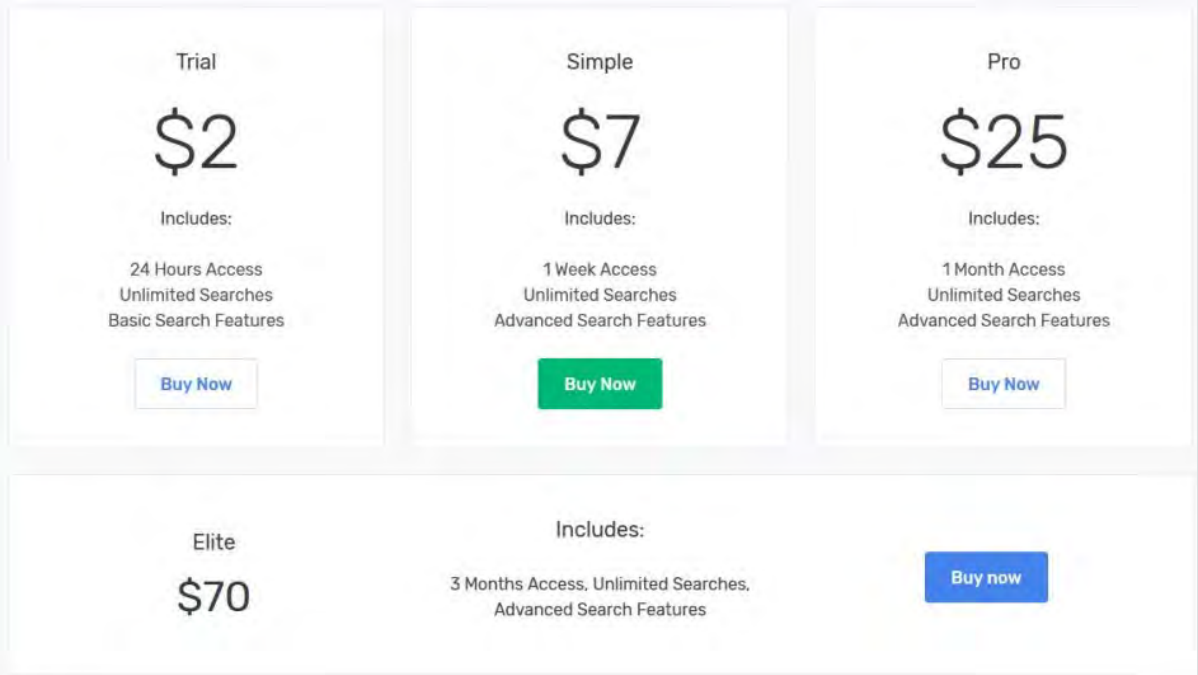
[6] Das Nationale Cyber-Abwehrzentrum ist eine behördenübergreifende Informations-, Koordinations- und Kooperationsplattform, in der u. a. arbeitstäglich sicherheitsrelevante Cybervorfälle gesammelt, analysiert und bewertet werden.

Fallbeispiel: weleakinfo.com

Weleakinfo.com bot im Januar 2020 **12,4 Milliarden Datensätze** aus über 10.000 in der Vergangenheit aufgetretenen Daten-Leaks zum Kauf an.

Die Daten stammten aus im Internet verbreiteten Datenleaks, wurden auf *weleakinfo.com* von den Plattformbetreibern zusammengetragen und gegen Bezahlung den angemeldeten Käufern zur Verfügung gestellt.

Fallbeispiel: weleakinfo.com



Auf der Plattform erfolgte, entgegen den Standards seriöser Seiten wie beispielsweise dem „Identity Leak Checker“ des Hasso-Plattner-Instituts, keine Überprüfung durch den Webseitenbetreiber, ob die angefragten Daten tatsächlich vom rechtmäßigen Eigentümer abgerufen werden. Somit war es beispielsweise möglich, dass die zahlenden Kunden auf *weleakinfo.com* Vor- und Nachnamen, Benutzernamen und E-Mail-Adressen von Dritten abfragen und bei einem Treffer die dazugehörigen Passwörter erhalten konnten.

Kurzbewertung:
Die arbeitsteiligen Ermittlungen mit unterschiedlichen Schwerpunkten in den beteiligten Staaten (GB/NL = Personenansatz, DE = Infrastrukturermittlung und US = Domainsicherung) führten zu einer effizienten und schnellen Aufarbeitung des Ermittlungskomplexes. Durch den engen polizeilichen Informationsaustausch wurde die internationale Koordination der unterschiedlichen Maßnahmen erfolgreich gewährleistet.

Jede digitale Identität kann Kriminellen als Basis für die Begehung einer Vielzahl von Straftaten dienen.

Jeder Internetnutzer sollte sich bewusst sein, dass seine digitale Identität eine ähnliche Sensibilität aufweist, wie z. B. sein physischer Personalausweis, Reisepass oder seine Kreditkarte, und deshalb geschützt werden muss. Auch trivial anmutende Maßnahmen wie die Nutzung eines sicheren Passworts tragen entscheidend zur Sicherheit der eigenen Daten bei.

3.2 MALWARE / SCHADPROGRAMME

Was ist Malware?

Unter dem Begriff Malware versteht man alle Programme, welche schädliche Funktionen auf einem IT-System ausführen.

Zu diesen maliziösen Funktionen gehören u.a.

- *Ausspähen und Weiterleiten von Account-Daten wie Usernamen und Passwörtern,*
- *Manipulation bzw. Zerstörung von Daten,*
- *illegitime Nutzung von Rechenleistung zum Kryptomining,*
- *Verschlüsseln von Daten,*
- *Einbindung in ein Bot-Netz und zum Missbrauch für DDoS-Angriffe,*
- *missbräuchliche Fernsteuerung eines fremden IT-Systems.*

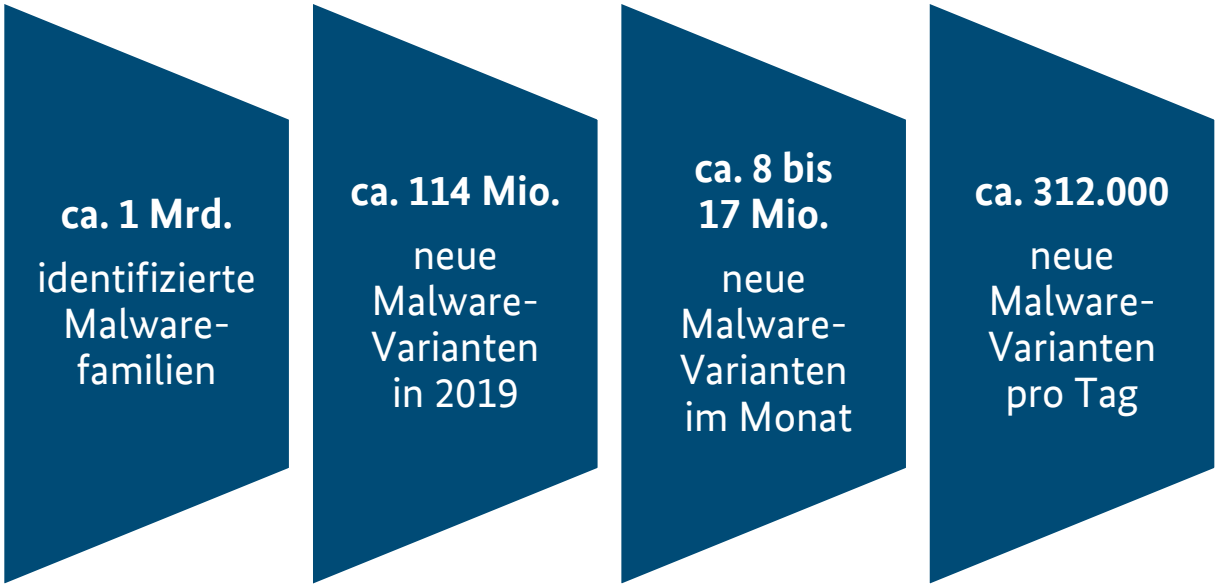
Ein Großteil von Cyberstraftaten wird mittels Malware begangen, welche in fremde Systeme eindringt und dort eine Vielzahl an schädlichen Funktionen ausführen kann. Die Distribution von Malware-Familien kann auf unterschiedliche Weise erfolgen.

Die am häufigsten ausgenutzten Eintrittsvektoren in ein fremdes System sind infizierte Anhänge von Spam-Mails. Dabei wird der Benutzer aufgefordert, einen Anhang herunterzuladen (oftmals ein Word- oder PDF-Dokument). Nach dem Öffnen des Anhangs installiert sich die Malware und verbreitet sich im System. Ebenso häufig befinden sich Links in Spam-Mails, welche zu maliziösen Webseiten führen. Unbemerkt wird über derartige Seiten Malware auf das System des Betroffenen geladen (Drive-By-Infection).

Über 1 Milliarde Malware-Familien festgestellt

Die Anzahl an Malware-Familien kann nicht exakt beziffert werden. Der Grund dafür liegt in der hyperaktiven Dynamik von Cybercrime – jeden Tag werden dutzende neue Varianten bereits bekannter Malware-Familien identifiziert.

Der IT-Sicherheitsdienstleister AV-Test beziffert das Ausmaß an Malware-Distribution im Jahr 2019 wie folgt[7]:



Diese Zahlen stellen nur einen Teil der insgesamt identifizierten Malware-Varianten dar. Die genaue Anzahl fällt aufgrund des erheblichen Dunkelfeldes im Phänomenbereich Cybercrime weitaus höher aus. Cyberkriminelle arbeiten ständig daran, bestehende Malware-Varianten zu überarbeiten und mit weiteren Schadfunktionen auszustatten.

Einer Auswertung von G Data[8] zufolge sind nachfolgend aufgeführte Malware-Varianten sowohl weltweit unter den zehn häufigsten Schadprogrammen vertreten als auch in Deutschland weit verbreitet:

- Die Ransomware *GandCrab*, welche Systeme verschlüsselt und ein Lösegeld für die Entschlüsselung verlangte. Mitte 2019 gab die Gruppierung hinter *GandCrab* an, ihre Aktivitäten einzustellen – trotzdem befindet sich *GandCrab* noch immer im Umlauf und wird aktiv gestreut. Es wird vermutet, dass die 2019 neu identifizierte Ransomware *Sodinokibi* den Nachfolger von *GandCrab* darstellt.
- Der „Loader“ *Emotet* – Ausführungen zur stetigen Bedrohung durch *Emotet* siehe Seite 17.
- *AZORult* - ein Info-Stealer, der verschiedene digitale Identitäten abgreift.
- *njRAT*, ein Remote Access Tool, das Tastaturanschläge mitschneidet (sog. Keylogging) sowie Dritten Zugang zu Mikrofon und Web-Cam verschafft.

[7] AV-Test – Malware, abrufbar unter: https://www.av-test.org/en/statistics/malware/
[8] G DATA – Malware-Wop-10 2019: Angriffe im Sekundentakt, abrufbar unter: https://www.gdata.de/news/2020/01/35714-malware-top-10-2019-angriffe-im-sekundentakt

Hohe Professionalisierung der Malwareentwicklung

Die Bandbreite an illegitimen Funktionalitäten von Malware ist sehr hoch und häufig verfügt eine Malware-Familie über mehrere dieser Schadfunktionen.

Ein Trend, der sich in den letzten Jahren abzeichnet, ist die zunehmende Professionalisierung der Malware-Programmierer und des sog. Malware-Cryptings: Sowohl der eigentliche Schadcode als auch dessen Verschlüsselung/Verfremdung (Crypting) entwickeln sich stets weiter und werden komplexer. Ziel von Cyberkriminellen ist dabei die Verbesserung der sog. Obfuskationsfähigkeit[9] der Schadsoftware, um dadurch möglichst lange vor Sicherheitssystemen unentdeckt zu bleiben.

Ebenfalls testen Entwickler ihre Malware vor ihrem Einsatz dahingehend, ob diese durch aktuelle Antiviren (AV)-Software erkannt wird. Coding, Crypting und Tests mit AV-Scannern stellen zentrale Elemente erfolgsträchtiger Cybercrime dar (hierzu Kapitel 4.6). Wenngleich dieser Dreiklang der Malware-Entwicklung bereits langjährig existiert, gewinnt er weiter an Bedeutung.

Eine zunehmende Professionalisierung spiegelt sich zudem in den angewendeten Modi Operandi und hier im Speziellen den gewählten Eintrittsvektoren wieder. Ähnlich staatlichen Akteuren agieren allgemeinkriminelle Cybergruppierungen zunehmend im Rahmen sog. APT (Advanced Persistent Threat, siehe Kapitel 6): Vor dem eigentlichen Angriff auf ein IT-System wird das Ziel umfassend ausgespäht. Unternehmenspolitik, monatliche Umsätze, Personalien und Webauftritte werden erkundet und die IT-Systeme auf etwaige Schwächen untersucht, um den geeignetsten Eintrittsvektor zu bestimmen. Befindet sich der Angreifer erst einmal im angegriffenen Zielsystem, nimmt er sich Zeit, um das IT-System verdeckt auszuspionieren und spezifische Daten als Ziel zu markieren.

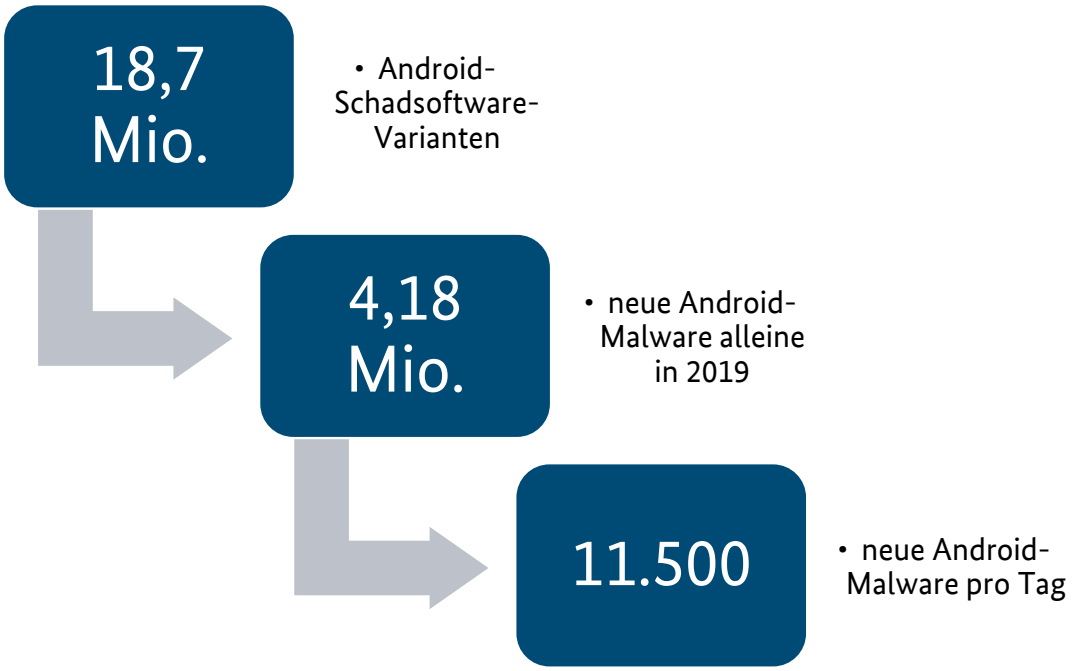
Im Phänomenbereich Malware ist zunehmend zu beobachten, dass Schadprogramme gezielt Betriebssystem-spezifische Schwachstellen ausnutzen. Auch Kompromittierungen des Remote-Desktop-Protokolls[10] von Windows-Systemen bilden einen Schwerpunkt. Die Nutzung von Exploits[11] und CVE[12] wird, neben der Kompromittierung von Accounts durch den Missbrauch gestohlener digitaler Identitäten, als Ausgangspunkt für die Installation von RATs[13] genutzt – besitzt der Cyberkriminelle dann Zugriff auf das IT-System, kann er weitere Malware nachladen.

[9] Verschleierung vor Sicherheitsmechanismen, wie z. B. Antiviren-Scannern
[10] Bei Remote-Desktop-Protokollen handelt es sich um Netzwerkprotokolle von Microsoft für den Fernzugriff auf Windows-Rechner.
[11] Exploits sind Programme, die Sicherheitslücken ausnutzen.
[12] Common Vulnerabilities and Exposures: Sicherheitslücken und Schwachstellen in IT-Systemen und Software
[13] Remote Acces Trojan – Malware, welche über eine technische „Hintertür“ administrative Kontrolle über den angegriffenen Rechner ermöglicht

Mobile Malware

Der G4C-Kooperationspartner G DATA analysierte[14] für den Berichtszeitraum die Verbreitung von Mobile-Malware – also Schadsoftware, welche spezifisch gegen mobile Endgeräte eingesetzt wird. Vor allem das Betriebssystem Android ist dabei primäres Ziel von Angriffen.

11.500 neue Mobile-Malware-Varianten pro Tag



Mobile-Malware kann unterschiedliche Ausprägungen besitzen: von Info-Stealern, die Passwörter und Kontodaten stehlen, bis hin zu Ransomware, die das Gerät verschlüsselt. Besonders häufig findet man zwei Arten von Mobile-Malware: Adware und Spyware.

Adware ist darauf ausgelegt, den Bildschirm mit unerwünschter Werbung zu überschwemmen. Obwohl dies dem Internetnutzer häufig nur lästig erscheint, kann das Aufrufen angezeigter Werbung schwerwiegende Folgen haben –die aufgerufene Werbung kann zu einer maliziösen Webseite führen und dort weitere, aggressivere Schadsoftware übertragen.

Spyware kundschaftet das infizierte System aus und leitet diese Daten (z.B. aktuelle Standortdaten) an Dritte weiter. Ähnlich wie Adware tarnt sich Spyware häufig als legitime Software, z. B. in Form einer App. Daher wird empfohlen, Apps von offiziellen Stores zu beziehen.

[14] G DATA – G DATA Mobile Malware Report 2019, abrufbar unter: https://www.gdata.de/news/2020/05/36125-g-data-mobile-malware-report-2019-neuer-hoechststand-bei-schaedlichen-android-apps

Die Sicherheitsüberprüfungen auf offiziellen App-Stores (z.B. Google Play Stores) wurden in den letzten Jahren weiter verschärft[15].

Fallbeispiel: *Emotet*

Die Malware Emotet beeinträchtigte im Jahr 2019 in Deutschland zahlreiche Behörden, Firmen und Unternehmen, darunter die Bundesanstalt für Immobilienaufgaben, eine Niederlassung des Industriekonzerns Norsk Hydro, das Kammergericht in Berlin sowie verschiedene lokale Stadtverwaltungen.

So wurde am 12.12.2019 die Zentrale Ansprechstelle Cybercrime (ZAC) des Bayerischen Landeskriminalamts telefonisch durch das Klinikum Fürth darüber in Kenntnis gesetzt, dass deren IT-Systeme kompromittiert wurden. Eine erste Analyse ergab die Infizierung von mindestens 53 Clients mit verschiedenster Schadsoftware, darunter *Emotet* und *Trickbot*. Eintrittsvektor war eine E-Mail mit maliziösem Anhang. Diese ging am 04.12.2019 im Klinikum ein und wurde samt Anhang (Dokument im .doc-Format) und darin befindlicher Makros geöffnet. Analysen ergaben, dass die im Anhang eingebetteten Makros auf verschiedene URLs (Webseitenadressen) verwiesen und über eine dieser URLs der Hinweis auf den Download einer schadhaften Datei mit Bezug zu *Emotet* festgestellt wurde.

Durch das Eingreifen der IT-Verantwortlichen des Klinikums Fürth konnte ein großflächiger Schaden verhindert werden. Der eingerichtete Krisenstab bat um dringende Unterstützung durch die Polizei.

Im Rahmen weiterer Analysen wurde weiterer Schadcode auf sog. "File Share"-Servern festgestellt. Ferner wurden bislang nicht im Fokus gestandene Rechner mit inaktuellem Virenschutz aufgefunden.

Der Krankenhausbetrieb selbst wurde durch den Cyber-Angriff nicht beeinträchtigt.

Exkurs/Hintergrund:
Emotet gilt aktuell als eine der schädlichsten Malware weltweit und hat auch in Deutschland IT-Systeme zahlreicher Unternehmen/Institutionen infiziert. Es handelt sich bei *Emotet* um einen sog. „Loader“ bzw. „Dropper“, dessen primäre Funktion im Nachladen weiterer Schadsoftware besteht (z. B. Ransomware). Standortabhängig erfolgt das Nachladen weiterer Malware, in Deutschland insbesondere von den Malware-Varianten *Trickbot* und *Ryuk*. Das Geschäftsmodell kann als „Infection-as-a-Service“ bezeichnet werden.

Ein typischer Ablauf der Infektion durch den Malware-Verbund *Emotet-TrickBot-Ryuk* beginnt mit einem maliziösen Word-Dokument, welches via Spam-Mails verbreitet wird. Durch das Öffnen des Dokuments und dem Zulassen von Makros wird ein im Dokument eingebetteter, maliziöser Code ausgeführt und der eigentliche *Emotet*-Trojaner auf das Zielsystem geladen. Ab diesem Zeitpunkt können Cyberkriminelle Informationen über das Zielsystem ausspähen und diese an den sog. Command and Control(C2) - Server der Täter senden sowie Keylogging durchführen.

[15] Siehe z. B. heise.de – Mehr Warnungen sollen Android-Nutzer schützen, abrufbar unter: https://www.heise.de/security/meldung/Google-Play-Protect-Mehr-Warnungen-sollen-Android-Nutzer-schuetzen-4322166.html

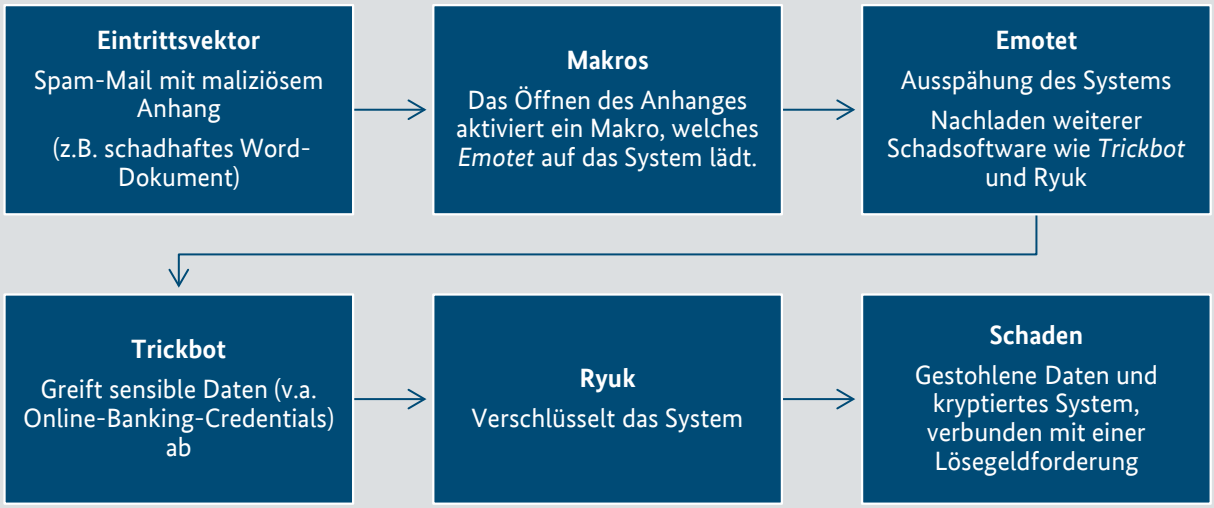
Fallbeispiel: *Emotet*

Darüber hinaus war festzustellen, dass *Emotet* weitere Module nachladen kann, darunter solche zur/zum

- Manipulation des Online-Bankings,
- Ausspähen von gespeicherten Passwörtern in Web-Browsern und E-Mail-Programmen,
- Ausführung von DDoS-Angriffen und
- Extraktion von Informationen aus E-Mail-Adressbüchern (Namen und E-Mailadressen).

Häufig wird nach der initialen Infektion mit *Emotet* der Trojaner *TrickBot* nachgeladen. *TrickBot* ist ein überwiegend in den USA und Großbritannien aktiver Banking-Trojaner[16], welcher weitere sensible Daten im Zielsystem abgreift und an einen C2-Server überträgt.

Am Ende der Infektionskette wird die Ransomware *Ryuk* nachgeladen, welche das Zielsystem verschlüsselt und ein Lösegeld für die Entschlüsselung verlangt.



Kurzbewertung:
Von *Emotet* gehen erhebliche Gefahren aus. Die Malware wird für zielgerichtete Angriffe auf Kritische Infrastrukturen, Behörden und große Unternehmen eingesetzt. Primäre Fähigkeit von Emotet ist das Nachladen weiterer Malware. Reagiert eine angegriffene Institution nicht schnell und professionell genug, kann das gesamte IT-Netzwerk durch eine nachgeladene Ransomware verschlüsselt werden.

[16] Bei Banking-Trojanern handelt es sich um Schadsoftware, welche bevorzugt (Zugangs-)Daten bzgl. Nutzung vom E-Commerce und Online-Banking stiehlt.

Angriffe auf Geldautomaten

Logische/digitale Angriffe auf Geldautomaten gewinnen zunehmend an Bedeutung, wenn auch in vergleichsweiser geringer Fallzahl. Dieser Phänomenbereich ist vor allem durch drei Modi Operandi geprägt:

a) Jackpotting mit Malware (Angriffe auf den Rechner/PC eines Geldautomaten mittels Schadsoftware),

b) Jackpotting über eine mitgeführte sog. Blackbox (Variante des Jackpotting-Angriffs auf das Auszahlungsmodul des Geldautomaten mittels tätereigener Hardware) und

c) 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 geldautomatenbetreibende Bank, um einen direkten Zugriff auf die im Netzwerk verbundenen Geldautomaten zu erhalten und einen sog. kartenungebundenen „Cash Out“ durchzuführen).

Nach einem signifikanten Anstieg der Fälle in 2018 blieben die Fallzahlen im Jahr 2019 auf einem Vergleichsweise konstanten Niveau:

Jahr	Jackpotting mit Malware	Jackpotting mit Blackbox	Netzwerkattacken
2017	11	3	3
2018	20	43	3
2019	21	47	1

Die Mehrzahl der Jackpotting-Angriffe mit Blackbox in Deutschland im Jahr 2019 erfolgte auf einen bestimmten Geldautomatentypen, welcher für derartige Angriffe besonders anfällig war. Bei den festgestellten Tätern handelte sich hauptsächlich um russische und ukrainische Staatsgehörige.

Von den registrierten 21 Jackpotting-Angriffen mit Malware fanden 19 Fälle in Berlin statt, welche einer rumänischen Tätergruppierung zuzurechnen sind.

Die Schadenssummen der Jahre 2018 und 2019 variierten stark, was u. a. auf die verschiedenen Sicherungsmaßnahmen bei den Geldautomaten zurückzuführen sein dürfte.

Jahr	Jackpotting mit Malware	Jackpotting mit Blackbox	Netzwerkattacken
2018	540.000 €	450.000 €	37.000 €
2019	125.000 €	940.000 €	10.000 €

Über das Darknet wird u. a. Schadsoftware für Geldautomaten vertrieben, die es auch technisch weniger versierten Tätern ermöglichen soll, Geldautomaten zu manipulieren und einen sog. „Cash Out“ durchzuführen.

Aufgrund der potenziell hohen „Gewinnerwartung“ für die Täter ist von einer anhaltend hohen Bedrohung durch logische/digitale Angriffe auf Geldautomaten auszugehen.

Fallbeispiel: Angriffe auf Geldautomaten

Seit November 2019 führte die Kriminalpolizei Osnabrück ein Ermittlungsverfahren der dortigen Staatsanwaltschaft wegen des Verdachts des gewerbsmäßigen Computerbetrugs gegen zwei ukrainische Staatsangehörige.

Die Ermittlungen führten zur Aufklärung von insgesamt elf Fällen von Jackpotting mit Blackbox im Zeitraum 24.10.2019 bis 10.11.2019 in vier Bundesländern. Insgesamt erlangten die Beschuldigten bei diesen Taten Bargeld in Höhe von 214.970 Euro, wovon ein Drittel sichergestellt werden konnte. Die Ermittlungen führten zu einer Täterstruktur, bei der sog. Läufer für die technische Umsetzung der Tat am Geldautomaten verantwortlich sind. Diese Läufer hielten Kontakt zu einem Täter, welcher als „Vorgesetzter“ der Läufer und als Kontakt zu den mutmaßlich im Ausland aufhältigen Hintermännern agierte.

Bemerkenswert ist, dass die Beschuldigten in zwei Fällen vermutlich aus den Taten erlangte Bargeldbeträge in Höhe von 29.640 Euro und 26.850 Euro an entsprechenden Geldautomaten in Bitcoins umgewandelt haben.

Im Juli 2020 wurden beide Beschuldigte zu Freiheitsstrafen von vier Jahren und drei Monaten wegen gewerbsmäßigen Computerbetrugs verurteilt.

Kurzbewertung:
Der technische Modus Operandi ist – auch ausweislich der gerichtlichen Würdigung – im Phänomenbereich Cybercrime im engeren Sinne (CCieS)[17] zu verorten. Die Tatbegehungs-komponenten – Rekrutierung von Läufern, Remote-Steuerung der Blackbox aus dem Ausland und Finanzflüsse mit Bitcoin auf russische Darknet-Markplätze - deuten auf international organisierte, kriminelle Strukturen hin.

[17] CCieS umfasst die Straftaten, die sich gegen das Internet[17], weitere Datennetze[17], informationstechnische Systeme[17] oder deren Daten richten. Eine Auflistung der Straftatbestände befindet sich in Kapitel 8.4.

3.3 RANSOMWARE – DIGITALE ERPRESSUNG

Wie bereits in 2018 festgestellt, setzte sich der Trend von zielgerichteten, hochprofessionellen Ransomware-Angriffen auf Unternehmen fort. Die Intensität dieser Angriffe hat im Jahr 2019 weiter zugenommen – vor allem die dadurch entstandenen Auswirkungen.

Was ist Ransomware?

Ransomware verschlüsselt die Daten eines digitalen Systems und führt in vielen Fällen auch zur Sperrung anderer, in einem Netzwerk erreichbarer Endgeräte (bspw. in Firmennetzwerken).

Es gibt unterschiedliche Arten von Ransomware:

a) *Erpressungssoftware, die tatsächlich keine Verschlüsselung der Festplatte durchführt, sondern durch eine Manipulation lediglich den Zugriff auf das System versperrt. Die wohl bekanntesten Ausprägungen sind Schadprogramme, bei denen bekannte Namen und Logos von Sicherheitsbehörden[18] missbraucht werden, um der kriminellen Zahlungsaufforderung einen vermeintlich offiziellen Charakter zu verleihen.*

b) *Sog. Krypto-Ransomware, welche die Daten auf den infizierten Endsystemen und aktuell auch mittels netzwerkverbundener Systeme (Server, Dateiablagen etc.) verschlüsselt. Diese Variante birgt für den Betroffenen ein sehr hohes Schadenspotenzial, da die genutzten Verschlüsselungen nicht in allen Fällen überwunden werden können. Die Zahlung des geforderten Lösegelds führt darüber hinaus häufig nicht zur Entschlüsselung des infizierten Systems.*

c) *Ein sog. Wiper weist gegenüber einer „herkömmlichen" Ransomware einen entscheidenden Unterschied auf: Die Funktionalität zum Entschlüsseln und Wiederherstellen von Daten auf einem System ist nicht vorhanden– die Daten werden somit unbrauchbar und irreversibel zerstört. Selbst nach der Bezahlung des Lösegeldes können die Daten nicht wiederhergestellt werden.*

Strafrechtlich betrachtet handelt es sich beim Einsatz von Ransomware um eine Kombination der Delikte Computersabotage gem. §303 b StGB und Erpressung gem. §253 StGB.

Ransomware-Angriffe auf Unternehmen besitzen das Potenzial, existentielle Bedrohungen auszulösen. Auch wenn der Fokus von Cyberkriminellen 2019 eindeutig auf Unternehmen und staatlichen Einrichtungen lag, so können auch Privatpersonen Opfer von Ransomware werden. Hier bedeutet ein erfolgreicher Angriff oftmals den Verlust von vielen und sehr privaten Daten.

[18] Bekannte Beispiele für derartige Phishing-Mails sind der sog. BKA-Trojaner und der GVU-Trojaner (GVU: Gesellschaft zur Verfolgung von Urheberrechtsverletzungen).

Ransomware ist und bleibt DIE Bedrohung für Unternehmen und öffentliche Einrichtungen.

Eine der ersten Phasen eines typischen Ransomware-Angriffs ist der Versand einer Phishing-Mail. Diese beinhaltet ein maliziöses Dokument, das nach dem Öffnen die Schadsoftware lädt. [19]
Der allgemeine Hinweis, keine E-Mails von Unbekannten zu öffnen, stellt Unternehmen häufig vor Schwierigkeiten in der Umsetzung. So stellten im Jahr 2019 vermeintliche Initiativbewerbungen einen häufigen Aufhänger für Ransomware-Attacken dar. Überdies war festzustellen, dass Cyberkriminelle Mailverkehr, den sie aus vergangenen Cyberangriffen erlangt haben, auswerten, um so vertraute Absenderadressen vorzutäuschen. Auf diese Weise werden E-Mails von vermeintlich bekannten Absendern mit für das potenzielle Opfer realistischen Themen und Gesprächszusammenhängen bestückt, um die Opfer zur Öffnung des maliziösen Dokuments oder zum Aufrufen eines täterseitig kontrollierten Links zu veranlassen.

Erhöhtes Schadenspotenzial durch Double Extortion

Seit 2019 erhielt dieser typische Modus Operandi eine weitere, äußerst kritische Facette – das sog. Double Extortion. Dabei verschlüsseln Ransomware-Akteure nicht mehr nur die IT-Systeme ihrer Ziele, sondern leiten vor der Kryptierung sensible Daten aus und drohen damit, diese zu veröffentlichen. Hierbei werden in modularisierter Vorgehensweise

- zunächst persönliche Kontakt- und Zugangsdaten ausgespäht,
- anschließend der Abfluss von Bankverbindungen, Geldtransfers und weiteren sensiblen Informationen veranlasst und zuletzt
- der Abfluss von Betriebsgeheimnissen zum Zwecke der Erpressung (Dekryptierung gegen Lösegeld und Drohung mit Verkauf bzw. Veröffentlichung) durchgeführt.

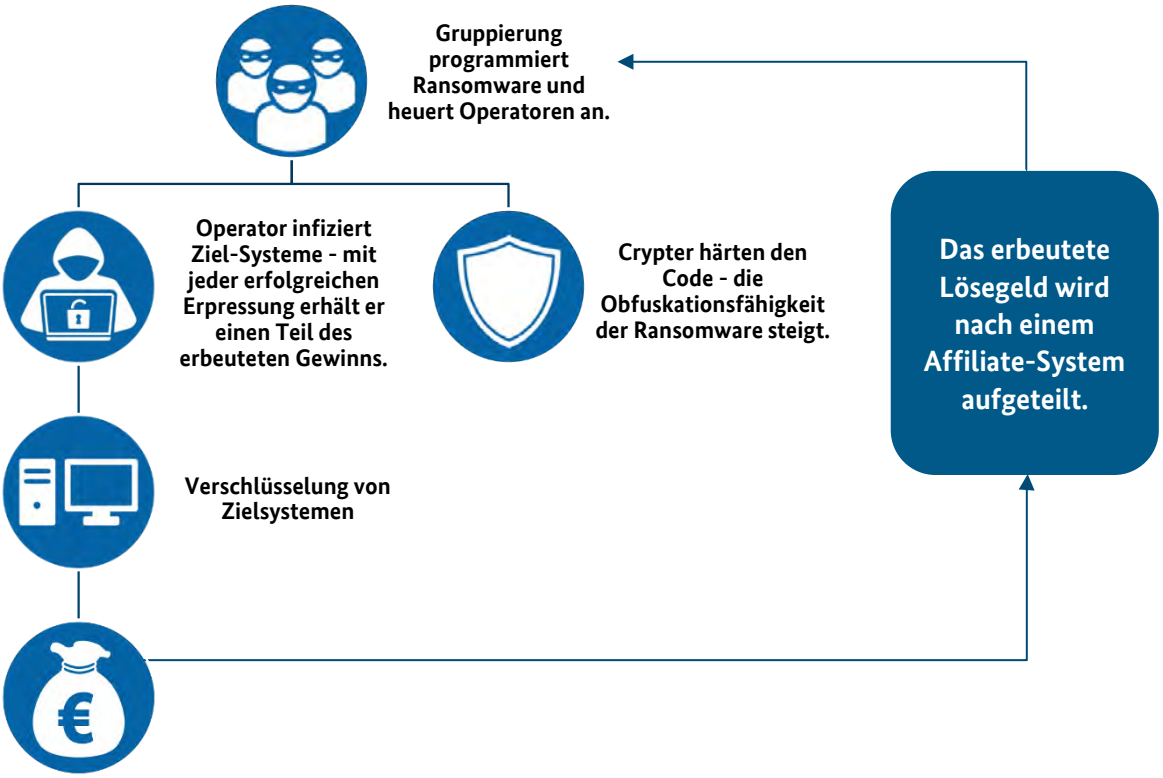
Damit werden die Betroffenen unter verstärkten Druck gesetzt, die Lösegeldsummen zu zahlen. Hier ist nicht nur die Verfügbarkeit der kryptierten Daten bedroht, sondern auch deren Vertraulichkeit und damit die Reputation des Opfers.

Im Jahr 2019 begannen die Entwickler der Ransomware *Maze,* diesen neuen Modus Operandi umzusetzen. Dabei publizierten sie die Daten von Betroffenen, welche der Lösegeldforderung nicht nachkamen, auf einer „Public-Shaming"-Webseite. Weitere Akteure wie die Gruppierungen hinter den Ransomware-Familien *Nemty* und *Sodinokibi,* folgten dem Beispiel von *Maze*.

Aufgrund des als lukrativ empfundenen Geschäftsmodells ist anzunehmen, dass weitere Täter diesen Modus Operandi übernehmen werden.

[19] Besonders häufig werden Microsoft Office-Dokumente verwendet.

Ransomware-Akteure handeln, wie auch der Rest der Cybercrime-Szene, organisiert und arbeitsteilig, sodass sich innerhalb der Underground Economy (siehe Kapitel 4) das Ransomware-as-a-Service-Modell etabliert hat: Dabei programmiert eine Gruppe von Kriminellen eine Ransomware und heuert weitere sog. Operatoren an, die die Software auf die Zielsysteme laden. Über ein Affiliate-System profitieren alle Beteiligten: Für jede erfolgreiche Erpressung erhalten die Operatoren einen Teil der erpressten Lösegeldsumme – der Rest fließt den Ransomware-Codern zu. Ein mittlerweile standardmäßiges Element derartiger Vorgehensweisen ist das sog. Malware-Crypting. Hierbei wird der Code der Ransomware optimiert, um ihn so vor Sicherheitsmechanismen der Zielsysteme zu verbergen.



Zusammenfassend:
Von allen hier dargestellten Phänomenen hat Ransomware das in Summe höchste Schadenspotenzial für Unternehmen, öffentliche Einrichtungen, Behörden und Kritische Infrastrukturen. Eine Infektion mit Ransomware und eine damit zusammenhängende Verschlüsselung des Systems kann für jede Art von Unternehmen zu massiven und kostenintensiven Geschäfts- bzw. Funktionsunterbrechungen führen.

Vor allem Betroffene, die keine regelmäßigen Backups erstellen, müssen bei einem Ransomware-Befall mit auch langfristig schädigenden Folgen für ihr Unternehmen rechnen. Aber auch das Erstellen regelmäßiger Backups ist alleine keine Garantie, den Geschäftsbetrieb zeitnah wieder aufnehmen zu können. Fortschrittliche Ransomware-Varianten sind in der Lage, auch auf Backups zuzugreifen und diese ebenfalls zu verschlüsseln. Daher ist es empfehlenswert, Offline-Backups zu führen, die nicht jederzeit per Netzwerk oder File Shares erreicht und damit verschlüsselt oder überschrieben werden können.

Um die befallenen Unternehmensprozesse schnellstmöglich wieder aufzunehmen, neigen viele Betroffene zur Zahlung des Lösegeldes. Davon rät das BKA ab: Hierdurch wird das kriminelle Geschäftsmodell Ransomware weiter gestärkt und es werden weitere Täterkreise zur Nachahmung motiviert. Zudem ist keineswegs sichergestellt, dass verschlüsselte Daten nach einer Zahlung des Lösegeldes tatsächlich wiederhergestellt werden.

Betroffene sollten sich immer an die zuständige Kriminalpolizei wenden. Im Rahmen der Selbsthilfe können Betroffene darüber hinaus nach frei verfügbaren Entschlüsselungstools recherchieren, so bspw. über das von EUROPOL und der Niederländischen Polizei in Zusammenarbeit mit der Privatwirtschaft initiierte Projekt „NoMoreRansom“[20]. Das BKA unterstützt dieses Projekt und ist seit 2017 offizieller „Supporting Partner“ von „NoMoreRansom“.

Fallbeispiel: Infektion von DRK-Kliniken mit *Sodinokibi*

Am 13. Juli 2019 kam es zu einem Ransomware-Angriff auf die IT-Infrastruktur der Trägergesellschaft Süd-West des Deutschen Roten Kreuzes (DRK) mit Sitz in Mainz. Bei dem Angriff wurden die IT-Systeme in zwölf Einrichtungen der Gesellschaft in Rheinland-Pfalz in großem Umfang verschlüsselt. Die Arbeitsabläufe waren dadurch erheblich eingeschränkt.

Die forensische Auswertung im Rahmen des beim LKA Rheinland-Pfalz geführten Ermittlungsverfahrens ergab, dass es sich bei der Schadsoftware um die Ransomware *Sodinokibi* handelte. *Sodinokibi* (auch bekannt als *Sodin* und *REvil*) ist eine Ransomware, welche erstmalig im Mai 2019 identifiziert wurde und seitdem weltweit für kriminelle Zwecke eingesetzt wird.

Die Ransomware wurde über einen extern erreichbaren Terminalserver eingeschleust, um sich zentrale Benutzerrechte zu sichern und die Verschlüsselung des internen Systems zu starten. Befindet sich *Sodinokibi* im angegriffenen System, deaktiviert es Windows-eigene automatische Reparaturfunktionen. Dem Nutzer des betroffenen Systems wird dann, je nach Betriebsprogramm und Oberfläche, ein Erpresserschreiben auf dem Desktop angezeigt. Sowohl die technische Infrastruktur der Ransomware als auch der betriebene Aufwand der Entwickler ist höchst professionell.

Im TOR-Netzwerk betreiben die Kriminellen hinter *Sodinokibi* eine eigene Seite, über welche die Erpresserschreiben und die jeweils aktuelle Höhe der geforderten Lösegeldsumme in Bitcoins dokumentiert werden. Darüber hinaus wird ein Zeitfenster angezeigt, ab wann sich diese Summe verdoppelt.

Sodinokibi gehört seit dem Jahr 2020 zu jenen Ransomware-Familien, welche Daten vor der Kryptierung des Systems ausleitet und mit der Veröffentlichung der Daten droht.

Kurzbewertung:
Obwohl die Patientenversorgung stets gewährleistet war, zeigt dieser Fall erneut auf, dass Kritische Infrastrukturen in Deutschland durch Cyber-Angriffe erheblich gefährdet sind: Ein einziger Angriff auf eine zentrale Serverstruktur kann ausreichen, um eine Kettenreaktion auszulösen und mehrere angeschlossene Einrichtungen handlungsunfähig zu machen.

[20] https://www.nomoreransom.org/

Nach Auskunft der Fa. Coveware[21], einem Partner des „NoMoreRansom“-Projekts, ist *Sodinokibi* noch vor *Maze*, *Phobos* und *Ryuk* die am häufigsten eingesetzte Ransomware weltweit.

Verschiedene Quellen deuten darauf hin, dass *Sodinokibi* der „inoffizielle“ Nachfolger von *GrandGrab* ist.

Seit die weitere Entwicklung von *GandCrab* eingestellt wurde, gewinnt *Sodinokibi* deutlich an Marktsignifikanz; weitere Angriffe mit dieser Ransomware sind wahrscheinlich.

[21] https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report

3.4 DDOS-ANGRIFFE

Mit dieser Methode zielen Cybertäter darauf ab, Webpräsenzen, Server und Netzwerke von Personen oder Organisationen durch Überlastung stark einzuschränken bzw. eine Nichterreichbarkeit der Dienste herbeizuführen. Die Angriffsprogramme werden dabei von einer großen Anzahl von Rechnern koordiniert und laufen zeitgleich, sodass die Zielsysteme durch eine Vielzahl von IT-Prozessen überlastet werden.

Distributed Denial of Service (DDoS)-Angriffe

Durch gezielt herbeigeführte Überlastung wird versucht, die Verfügbarkeit eines Internetdienstes oder eines Zielsystems zu stören.

Der DDoS-Angriff zeichnet sich dadurch aus, dass der Angriff i. d. R. von einer Vielzahl einzelner Anfragen bzw. einer großen Zahl an Rechnern – vielfach mittels großer, ferngesteuerter Botnetze – erfolgt.

Wie entstehen Botnetze?

Botnetze entstehen durch die zumeist für den Besitzer unbemerkte Installation einer Schadsoftware auf dem PC des Geschädigten.

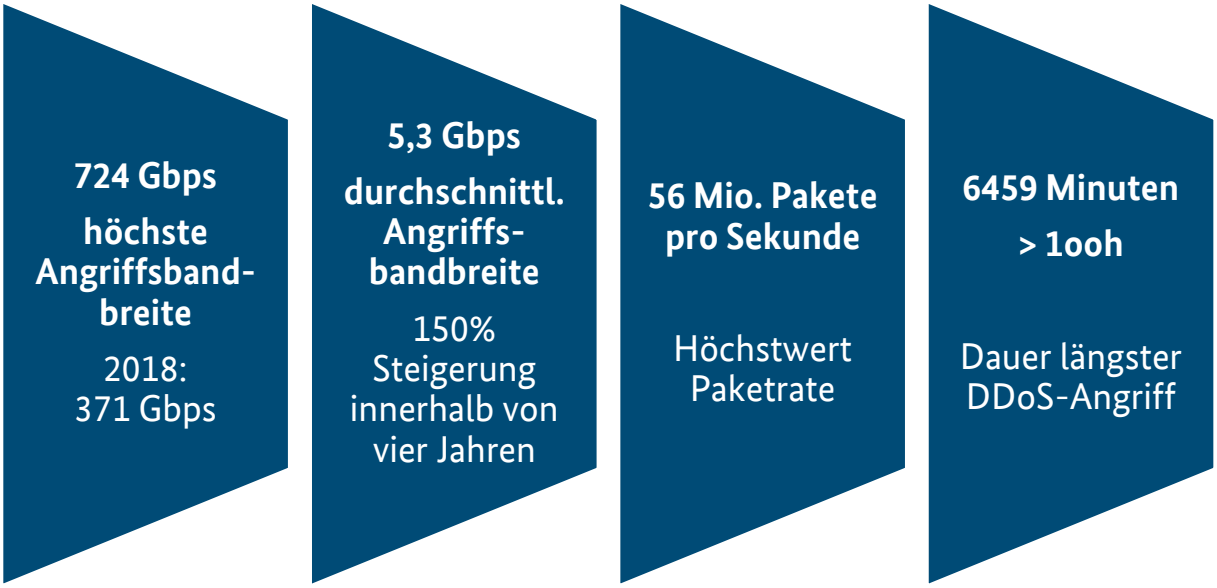
Durch diese Schadsoftware hat der Täter einen nahezu vollständigen Zugriff auf das infizierte System. Die zahlreichen, per Schadcode infizierten Geräte der Geschädigten werden ohne Wissen ihrer Besitzer mittels sog. „Command and Control-Server" kontrolliert und gesteuert.
Grundsätzlich wird der „befallene" PC so als Angriffsressource genutzt – nicht selten für DDoS-Attacken.

Die Täter setzen für den koordinierten Angriff häufig Botnetze ein. Diese bestehen aus einer großen Zahl von zuvor infizierten Computern, die vielfach weltweit verteilt sind. Ein Command and Control-Server, der diese Bot-Rechner fernsteuert, bestimmt Zeitpunkt und Ziel von Massenanfragen. Da prinzipiell alle internetfähigen Geräte in ein solches Botnetz eingebunden werden könnten, spielt das Internet der Dinge (IoT – Internet of Things) mit allen seinen vernetzten Geräten wie Fernseher, Kameras, Router etc. eine große und weiter steigende Rolle im Bereich von Cybercrime.

Das BKA arbeitet im Bereich der Lageberichterstattung zu DDoS-Angriffen eng mit dem G4C-Mitglied Link11 zusammen. Die nachfolgenden Ausführungen beziehen sich auf Erkenntnisse dieses IT-Sicherheitsdienstleisters, der regelmäßig die in seinem Netzwerk registrierten Attacken analysiert, sowie ergänzende Informationen.

Sowohl in Bezug auf die Anzahl als auch die Intensität (Dauer, Bandbreite) war in den letzten Jahren eine stetige Steigerung von DDoS-Angriffen zu verzeichnen.

Laut DDoS-Report 2019 von Link11[22] konnte bei der Analyse der Angriffe, die in dem dortigen Netzwerk registriert wurden, folgende Bedrohungslage für dieses Berichtsjahr festgestellt werden:



Innerhalb der EU nutzt lediglich ein Sechstel der Firmen schnelle Internetanbindungen von über 100 Mbps[23]. Die Mehrheit hat einen deutlich schmalbandigeren Anschluss. Angriffe von mehreren 100 Gbps[24] sind demzufolge für das jeweilige Ziel fast immer überdimensioniert. Da die Täter versuchen, durch minimalen Einsatz von Mitteln eine maximale Wirkung zu erzielen, passen sie ihre Attacken an und können mit einer deutlich niedrigeren, zielangepassten Bandbreite zwischen 1 und 10 Gbps agieren– dies erklärt auch die große Diskrepanz zwischen der höchsten und der durchschnittlichen Angriffsbandbreite.

Angriffsvektoren beschreiben den Weg und das Vorgehen, wie die Cybertäter Zugriff auf Computer und Server im Netzwerk erhalten. Sobald Angreifer in einer Attacke mehrere Protokolle missbrauchen, spricht man von komplexen bzw. Multivektor-Attacken. Im Link11-Netzwerk lag der Anteil komplexer Attacken, bei denen mehrere Angriffsvektoren zum Einsatz kamen, im Jahr 2019 bei 67%. Die innerhalb eines Angriffs wechselnden Vektoren stellen die Sicherheitsdienstleister hierbei vor Herausforderungen. Auch wenn DDoS-Angriffe grundsätzlich stets die Überlastung des Zielsystems herbeiführen wollen, sind bestimmte Typausprägungen zu unterscheiden:

Volumetrische Angriffe (volumetric attacks)
Bei diesem Angriff wird von Täterseite versucht, durch die Belegung der kompletten Bandbreite zwischen Ziel und Internet eine Überlastung zu erzeugen. Massiver Datenverkehr bzw. große Datenmengen werden eingesetzt, um das Zielsystem zu beeinträchtigen.

Protokollattacken (protocol attacks)
Schwachstellen in verschiedenen Schichten des Internetprotokolls werden vom Täter ausgenutzt, um das Ziel unzugänglich zu machen und so den Service des angegriffenen Ziels zu unterbrechen.

[22] **https://www.link11.com/en/downloads/ddos-report-for-the-full-year-2019/**
[23] Mbps: „Megabits per second“, Maßeinheit für Geschwindigkeiten beim Datentransfer
[24] Gbps: „Gigabits per second“

Angriffe auf die Anwendungsschicht (application attacks)
Gezielte Angriffe auf die Anwendungsschicht[25] einer Webseite und eine damit einhergehende Störung ihrer Dienste erfordern lediglich eine geringe Bandbreite und eine begrenzte Anzahl von „Paketen". Da sich der böswillige nur schwer vom legitimen Datenverkehr unterscheiden lässt, ist diese Form des Angriffs für die IT-Security-Dienstleister problematisch und stellt eine wachsende Herausforderung dar.
Derartige, sogenannte Layer-7-Angriffe gewinnen zunehmend an Bedeutung.

IoT-Geräte und Cloud-Server als Verstärker bei DDoS-Angriffen

Eine Vielzahl von Netzwerkprotokollen, die als Basis der elektronischen Datenübertragung fungieren, können von den DDoS-Angreifern als Verstärker für ihre Attacken – sog. Amplification Vektoren – missbraucht werden. So beobachtete Link11 Ende des Jahres 2019 verstärkt die Strategie des sog. „Carpet Bombings". Hierunter versteht man eine Flut von einzelnen Angriffen, die nicht nur gegen ein einzelnes Internetprotokoll des Ziels gerichtet sind, sondern zeitgleich gegen das gesamte Netzwerk ausgeführt werden. Der manipulierte Datenverkehr verteilt sich so auf sehr viele Attacken und Internetprotokolle innerhalb dieses Netzwerkes. Die Datenmenge jedes einzelnen Angriffs ist jedoch so klein, dass deren Identifizierung als manipulierter Datenverkehr schwierig und deren Filterung nicht möglich ist. In den Auswirkungen ist dieser Angriff aber gleichzusetzen mit hochvolumigen Angriffen.

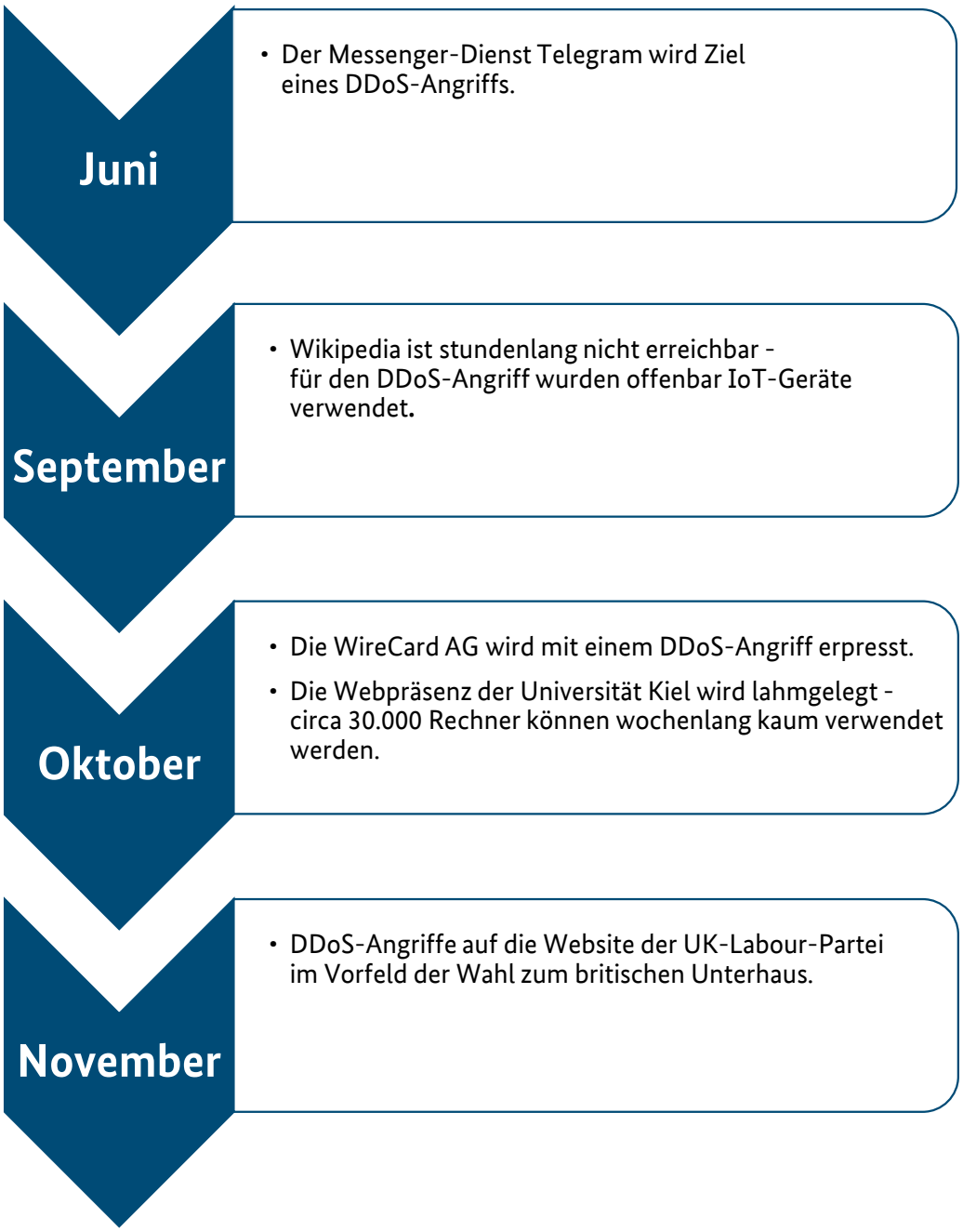
Das Cloud-Computing bietet nicht nur zahlreiche Vorteile für Unternehmen, sondern bietet auch für Cyber-Täter erweiterte Möglichkeiten. Innerhalb des Link11-Netzwerks konnte im Berichtsjahr 2019 festgestellt werden, dass der Anteil von DDoS-Attacken, bei denen Cloud-Server eingebunden waren, bei 45 Prozent lag – Tendenz steigend.
Zunehmend werden DDoS-Attacken auch mit Erpressungsforderungen der Täter gekoppelt.
Wie bei Attacken mittels Ransomware werden Zahlungen in Form von Bitcoin gefordert, damit die großvolumigen DDoS-Attacken eingestellt werden.

DDoS-Angriffe verursachen gezielt Schäden bei den angegriffenen Personen und Organisationen/ Unternehmen. Die Beweggründe sind vielfältig und reichen von der Schädigung geschäftlicher Konkurrenz bis hin zu rein politischer Motivation. Insgesamt spielen monetäre Interessen in Form von DDoS-Erpressungen eine wachsende Rolle.

Durch die Nichterreichbarkeit der Webpräsenzen entstehen den Betreibern nicht nur Ausfälle in Geschäftsabläufen, Einbrüche von Verkaufszahlen und damit erhebliche wirtschaftliche Schäden, sondern ebenso Reputations- und Vertrauensverlust bei Partnern, Kunden und sogar Wählern. DDoS-Angriffe sind deshalb nicht selten für existenzielle Notlagen von Betrieben verantwortlich.

[25] Die Anwendungsschicht dient z. B. zur Datenein- und ausgabe sowie zur Generierung von Webseiten auf Servern. Ebenfalls werden hier auch Antworten für Besucher dieser Webseiten bereitgestellt.

Im Jahr 2019 wurden die in der folgenden Übersicht beispielhaft aufgeführten DDoS-Angriffe festgestellt:



4 Underground Economy

Illegale Foren oder Marktplätze im Clearnet, Deepweb und im Darknet spielen eine weiter zunehmende Rolle bei der Begehung von Cybercrime.

Begriffsbestimmungen

Clearnet *(auch Visible Web, Surface Web, Open Web): Für jedermann mit marktgängigen Browserprogrammen zugänglich, unterstützt durch einfache Handhabung mittels Suchmaschinen. Auch im Clearnet sind vielfältige illegale Inhalte verfügbar, z. B. solche mit Bezug zu Politisch Motivierter Kriminalität oder Plattformen und Foren der sog. „Underground Economy (Straftaten überwiegend aus dem Bereich der Cybercrime im engeren Sinne).*

Deep Web *(auch Invisible Web): Der Teil des Internets, dessen Inhalte nicht durch Suchmaschinen auffindbar sind, weil z. B. Webseiten nicht indexiert/in Suchmaschinen verlinkt wurden oder weil sie zugriffsbeschränkt sind. Inhalte des Deep Webs können z. B. Datenbanken, Intranets oder Fachwebseiten sein und sind – sofern die URL bekannt ist und eine Zugangsberechtigung besteht – mit Browsern erreichbar.*

Darknet: *Die Inhalte im Darknet sind ausschließlich durch Nutzung spezieller Software, die der Anonymisierung dient, einsehbar. Bestandteile des Darknets sind z. B. Foren, Blogs/Wikis mit unterschiedlichsten – legalen wie illegalen – Zielrichtungen. Einen bedeutenden Teil machen sog. Darknet-Marktplätze aus, bei denen anonym größtenteils inkriminierte Güter gehandelt werden. Auch werden zahlreiche und bedarfsorientierte Angebote für Crime-as-a-Service (Durchführung bzw. Unterstützungsleistungen krimineller Handlungen im Auftrag) oder Darknet-Seiten mit kinderpornografischen Inhalten zur Verfügung gestellt. Viele Bereiche des Darknets unterscheiden sich vom Aufbau und von der Art der Nutzung her nicht vom Clearnet: Auch im Darknet werden in Foren Meinungen geäußert und Diskussionen geführt, Wikis liefern Erklärungen und Erläuterungen. Allerdings beziehen sich diese Inhalte im Darknet häufig auf illegale Aktivitäten und Inhalte (z. B. Betäubungsmittel).*

Digitale Schwarzmärkte im Darknet betreffen nahezu alle Deliktsbereiche klassischer Kriminalitätsphänomene. Hierbei sind die Herstellung, Besorgung und der Handel bzw. Austausch folgender angebotenen Güter bzw. Services zu verzeichnen:

- Betäubungsmittel und verschreibungspflichtige Arzneimittel,
- erlaubnispflichtige Chemikalien,
- Waffen, Kriegswaffen und Explosivstoffe,
- kinder- und jugendpornografische Schriften,
- Falschgeld, gefälschte Urkunden und sonstige Dokumente,
- Hehlerware und gefälschte Markenprodukte,
- Datenhehlerei ausgespähter Zugangs- oder Kreditkartendaten,
- Schadsoftware und Sicherheitslücken,
- Handlungsanleitungen zur Begehung von Straftaten,
- Informationen und Serviceleistungen zur Geldwäsche und
- Hosting und Infrastrukturdienstleistungen für kriminelle Aktivitäten.

Nach wie vor stellt der Betäubungsmittelhandel im Darknet den größten illegalen Marktanteil dar. Die Handelsplätze orientieren sich hierbei an den allgemeinen marktwirtschaftlichen Prinzipien von Angebot und Nachfrage. Demgegenüber werden durch diverse Seitenbetreiber Richtlinien zur Selbstregulation aufgestellt. Insbesondere kinder- und jungendpornografisches Material, Schusswaffen und Fentanyl sind in Reaktion auf intensive, international abgestimmte polizeiliche Strafverfolgungsmaßnahmen der letzten Jahre von der Mehrheit der Marktplätze verschwunden.

Tor-Netzwerk

Das im allgemeinen Sprachgebrauch oftmals synonym mit dem Darknet verwendete Tor-Netzwerk (The Onion Router) bezeichnet ein im Internet gehostetes, aus mehreren Tausend Knotenpunkten bestehendes, paralleles Netzwerk. Erreicht wird das Netzwerk über einen speziell konfigurierten Tor-Browser, wobei der Datenverkehr durch mehrere Instanzen geleitet und dabei verschleiert wird. Webangebote im Tor-Netzwerk werden daher Hidden-Services genannt.

Die beobachtete Lage des inkriminierten Teils des Darknets ergibt das Bild einer durch Forenkommunikation gestütztes und wesentlich durch den Community-Gedanken vorangebrachtes, loses Netzwerk. Auf die wesentlichen Bestandteile der inkriminierten Darknet-Szene wird im Folgenden eingegangen.

4.1 MARKTPLÄTZE

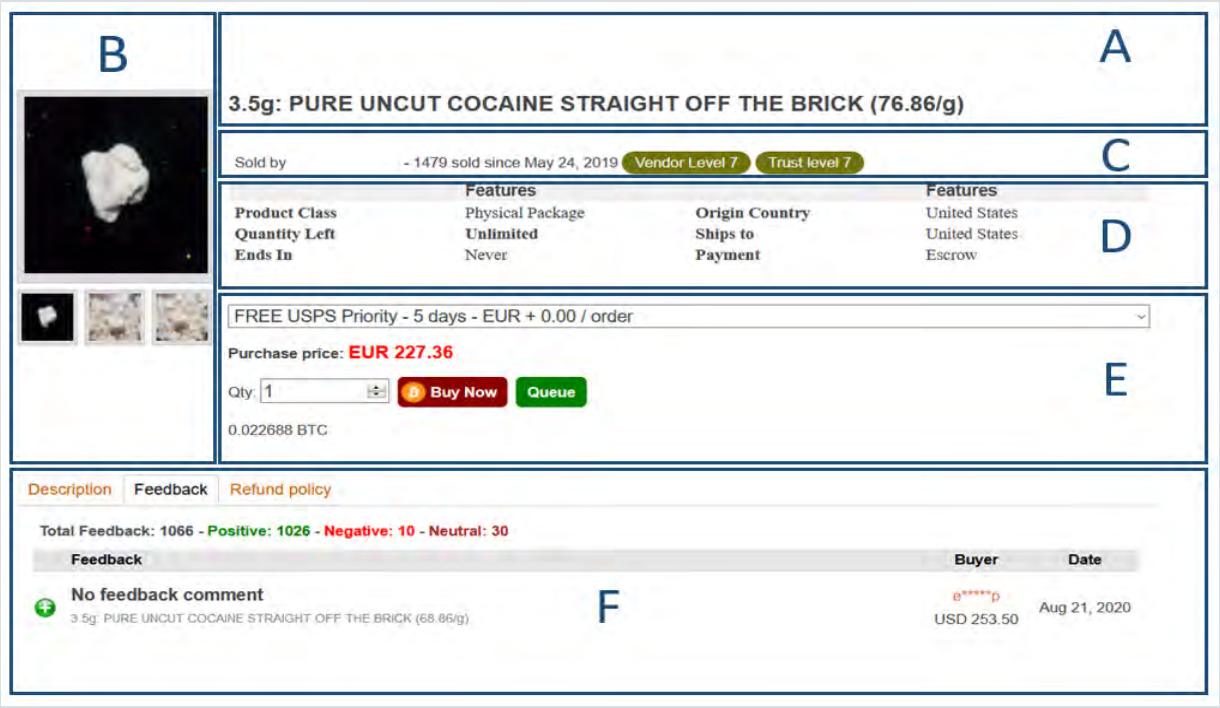
Einen bedeutenden Anteil der strafrechtlich relevanten Inhalte und des inkriminierten Finanzvolumens im Darknet stellen weiterhin Marktplätze dar. Diese nach dem Vorbild bekannter E-Commerce Plattformen aufgebauten Seiten bieten den jeweiligen Verkäufern die Möglichkeit des komfortablen und anonymen Handels. Über Marktplätze erfolgt der illegale internationale Warenverkehr inkriminierter Güter mit einem hohen Grad an Professionalität. Die Betreiber dieser illegalen Plattformen profitieren hieran durch Verkaufsgebühren.

Bitcoin bleibt das beliebteste Zahlungsmittel.

Der Geldtransfer erfolgt aufgrund ihrer dezentralen und teilanonymen Charakteristiken hauptsächlich in Kryptowerten. Die Kryptowährung Bitcoin stellt weiterhin die mit Abstand verbreitetste Zahlungsmethode dar. Zur Reduzierung von Warenkredit- und Warenbetrügereien werden Gelder durch die Plattformbetreiber für bestimmte Verweildauer treuhänderisch verwaltet. Dieser Umstand bietet wiederum eine Tatgelegenheit für die Seitenbetreiber, die Geldwerte zu unterschlagen. Diese als sogenanntes „Exit-Scam“ bekannte Masche konnte in den letzten Jahren vielfach beobachtet werden.

Die Kommunikation zu marktplatzbezogenen Themen erfolgt entweder über von der Marktplatzadministration betriebene oder separate Foren. Einige Plattformen betreiben darüber hinaus einen ticketbasierten Support für ihre Käufer und Händler.

Fallbeispiel: Kokainangebot auf einem Darknet-Marktplatz



(A) Kurzbeschreibung bzw. Titel.

(B) Fotografien der Güter. Teilweise enthalten Bilder Aspekte von sog. Proof-Pics wie Händlernamen oder Datum.

(C) Informationen zum Verkäufer. Neben dem Benutzernamen werden Informationen zur Anzahl der Verkäufe sowie Rang und Vertrauenswürdigkeit angezeigt.

(D) Meta-Informationen zum Artikel. Bspw. verfügbare Menge, Angaben zur Befristung des Angebots, Produktkategorien. Besonders Angaben zur Sendungsherkunft sind von Relevanz, da Zollkontrollen vermieden werden sollen. Bei der Art der Zahlungsabwicklung handelt es sich hier um eine treuhänderische Abwicklung ("escrow service") durch den Betreiber der Plattform. Die Zahlung wird dem Verkäufer also erst dann gutgeschrieben, wenn der Käufer den Erhalt der Ware meldet oder ein vorgegebener Zeitrahmen verstreicht.

(E) Bestellmenge, Versandoptionen und resultierender Gesamtpreis. Dieser wird primär in konventionellen Währungen angezeigt und in die Nutzwährung, hier Bitcoin, umgerechnet.

(F) Im unteren Teil befindet sich der Reiter "Feedback", der die angebotsbezogenen Rückmeldungen und Bewertungen der Käufer auflistet. Der Reiter "Description" dient der detaillierten Beschreibung des Produkts. Unter "Refund Policy" sind die Erstattungsrichtlinien des Verkäufers einzusehen. Oftmals wird der Kaufpreis von Produkten, die mit Sendungsverfolgung versendet werden und ihren Bestimmungsort nicht erreichen, erstattet.

4.2 FOREN

Foren der kriminellen Darknet-Szene unterscheiden sich in ihrem Aufbau und ihren Funktionalitäten kaum von marktgängigen Foren des Clearnets. Zur Teilnahme bedarf es eines Nutzerkontos ohne Angabe von persönlichen Informationen. Teilweise werden durch Einladungscodes, limitierte Forenabschnitte oder „Pay-to-Join"-Kriterien Beitrittshürden geschaffen und spezielle Bereiche gesondert geschützt.

Polizeiliche Zugriffe und Maßnahmen werden genau beobachtet.

Die Foren bieten eine Plattform für Diskussionen, Erfahrungsberichte, Ankündigungen und sonstige Kommunikation zwischen Nutzern. Beispielsweise werden die Qualität und Vertrauenswürdigkeit von Markplätzen, Händlern und Produkten bewertet. Eine große Rolle beim Austausch von Nutzern im Darknet spielen Vorkehrungen zur Verschleierung der Nutzeridentitäten.
Unter dem Begriff OPSEC (Operations/ Operational Security) erfolgt in Unterforen reger Wissens- und Erfahrungsaustausch über Methoden, Werkzeuge und Verhaltensweisen, die auf eine möglichst effektive Absicherung eigener Daten gegen Strafverfolgung abzielen. Neben der Anwendung von Verschlüsselungen und anonymen E-Mail-Dienstleistern sind auch die vermuteten Fähigkeiten und Ermittlungsinstrumente der Polizei und Sicherheitsbehörden ein häufiges Thema. Die Betreiber von Marktplätzen drängen daher ebenfalls ihre Nutzer zunehmend zur Implementierung von Sicherheits- und Verschleierungsmaßnahmen.

Einige Foren bieten zusätzlich separate Handelsbereiche an, die eine konkrete Platzierung von Angeboten und Gesuchen ermöglichen. Die Inhalte und Themen der Foren sind divers und die einzelnen Foren unterscheiden sich stark in ihren thematischen Schwerpunkten. Das Spektrum reicht von Hacking über die Herstellung von Betäubungsmitteln bis hin zu legalen Inhalten. Die Moderation der Foren beschränkt sich in der Regel auf die Durchsetzung der durch die vom jeweiligen Betreiber gesetzten Regeln. Diese sehen häufig lediglich ein Verbot kinder- und jugendpornografischer und terroristischer Inhalte vor. Teilweise wird auch das Doxxing von Nutzern (Sammeln und Leaken personenbezogener Daten) sanktioniert.

Foren im Darknet stellen insgesamt eine tragende Funktion als Informations-, Vernetzungs- und Veröffentlichungsplattform für die Nutzer des Darknets dar. Aufgrund der allgegenwärtigen Anonymität wird Vertrauen durch den persönlichen Austausch untereinander kompensiert.

4.3 VERTRAUEN IM DARKNET

Um trotz des Mangels an Vertrauen die Echtheit von Aussagen zu validieren, kommen unter Nutzern diverse technische Verfahren zur Anwendung. Um die Authentizität von Nachrichten (z. B. öffentlicher Post oder vertrauliche Direktnachricht) sicherzustellen, kommen regelmäßig digitale Signaturen mittels Public-Key-Verschlüsselungsverfahren (insb. OpenPGP) zur Anwendung. Anhand jener können Informationen bei Bedarf zudem verschlüsselt werden. Insgesamt ist das PGP-Schlüsselpaar eines Nutzers im Darknet ein wichtigerer Teil seiner Online-Identität als der Benutzername.

Eine Methode zur Herstellung von Vertrauen auf Seiten von Plattformbetreibern ist der Einsatz von sogenannten „Canary Messages“. Hierbei wird eine bestimmte Textnachricht des Betreibers eines Hidden-Services in regelmäßigen Abständen digital signiert und öffentlich publiziert. Weiteren Nutzern soll dies frühzeitig anzeigen, wenn die Plattform durch staatliche Stellen sichergestellt oder der Betreiber festgenommen wurde. Der Name Canary ist dabei an die Warnfunktion der Kanarienvögel im Bergbau angelehnt. Verstummt der Vogel, stimmt etwas nicht.

4.4 LINKSAMMLUNGEN UND NEWSBLOGS

Linklisten geben eine Übersicht über vorhandene URLs der unterschiedlichen Hidden Services. Sie sind häufig auch aus dem Clearnet zu erreichen. In Ermangelung leistungsfähiger Suchmaschinen dienen sie als Portal, auf dem die Hidden Services bekannt gemacht werden.

Wie Suchmaschinen im Clearnet, sind Linksammlungen zentrale Anlaufstellen für das Darknet.

Da es im Darknet im Vergleich zum Clearnet häufiger vorkommt, dass URLs geändert werden, dienen diese Link-Listen auch zur Verbreitung aktualisierter URLs. Teilweise stellen die Betreiber der Link-Listen Anforderungen in Bezug auf Sicherheitsaspekte (siehe auch Canary und OpenPGP), deren Einhaltung Voraussetzung für eine Aufnahme in die Liste ist. Die Linksammlungen sind somit essentiell für die Orientierung von Nutzern im Darknet.

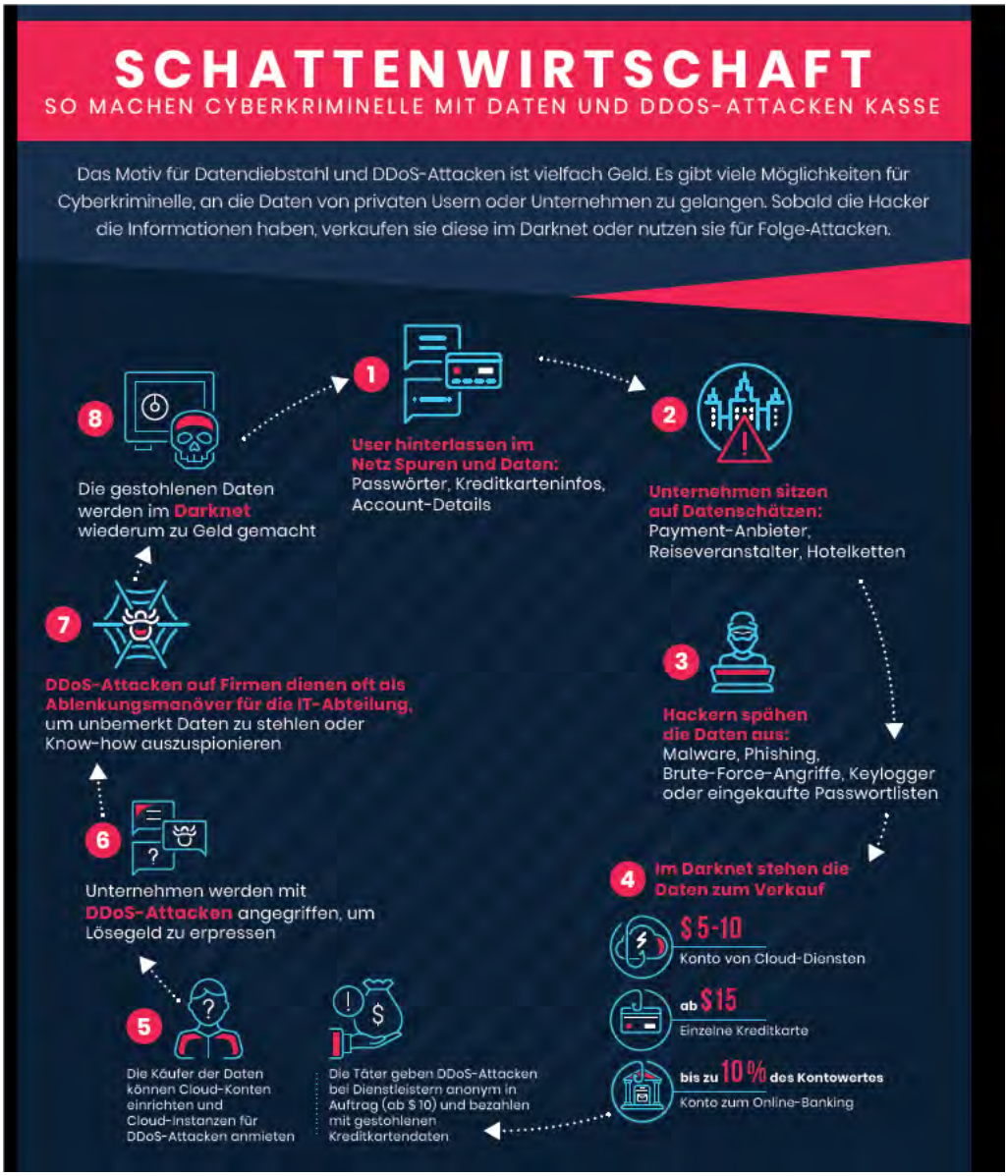
Szenespezifische Newsblogs informieren über Ereignisse in Bezug auf Marktplätze und Händler, z. B. Festnahmen und polizeiliche Ermittlungen. Die Blogs dienen der Community als wichtige Informationsquelle, auch um individuelle OPSEC-Maßnahmen an das eigene Handeln anzupassen.

4.5 SERVICES

Ein weiterer wichtiger Teil der Darknet-Infrastruktur sind die digitalen Services. Dienstleistungen wie E-Mail-Postfächer, Server-Hosting oder VPNs[26] werden speziell für die Darknet-Klientel angeboten. Auch sogenannte Bitcoin-Mixer oder Krypto-Exchanger erfahren große Beliebtheit im Darknet und spielen eine große Rolle zur Verschleierung von Finanzströmen. Die Vielzahl an Services macht das Darknet vom Clearnet unabhängig und deckt alle Bedarfe der Nutzer, Händler und Plattformbetreiber im Darknet ab.

Welche Relevanz der Diebstahl digitaler Identitäten und im Darknet angebotene Services für die gesamte Wertschöpfungskette im Bereich Cybercrime haben können, zeigt nachfolgende von Link11 erstellte Grafik am Beispiel von DDoS-Angriffen:

[26] VPN seht für „Virtual Private Network“. Die Nutzung solcher grundsätzlich legalen Netzwerke ermöglicht die anonyme und verschlüsselte Internetkommunikation und Datenübertragung. Dazu wird die IP-Adresse des Nutzers durch die IP-Adresse des VPN-Servers ersetzt.



Copyright Grafik: Link11

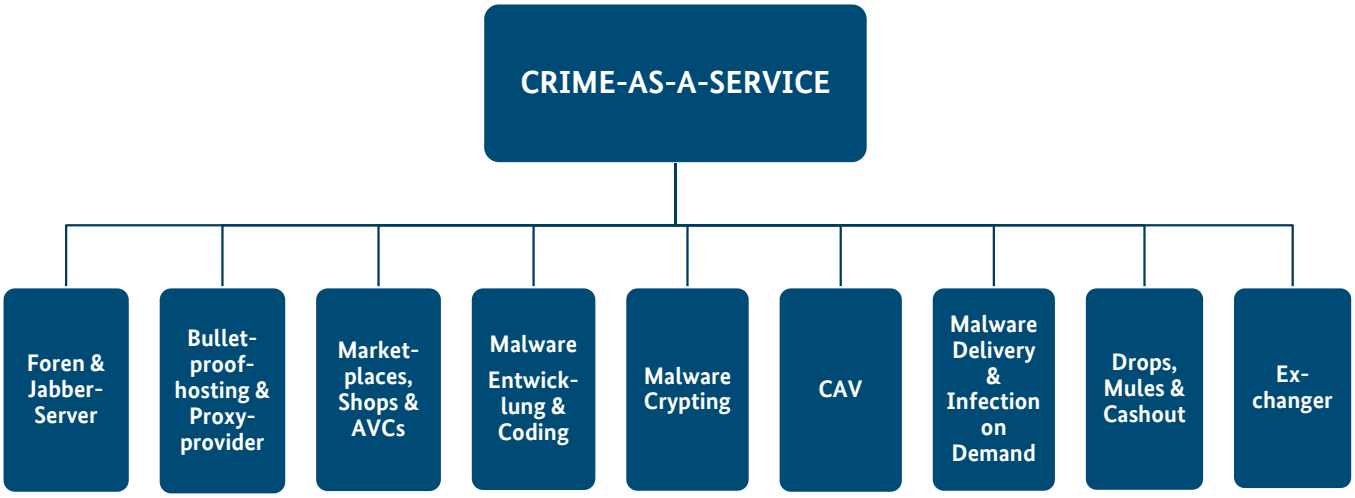
4.6 CYBERCRIME AS A SERVICE / DAS NEUN-SÄULEN-MODELL

Im Rahmen der in den letzten Jahren beim BKA geführten Ermittlungsverfahren konnte festgestellt werden, dass im Phänomenbereich „Cybercrime-as-a-Service“ (CCaaS; Cyberstraftat als Dienstleistung) eine hohe Arbeitsteilung zwischen den Tatbeteiligten und eine Spezialisierung Einzelner auf ausgewählte relevante Tatteilbeiträge vorherrschen.

Cyberkriminelle fokussieren sich vermehrt auf eine auftragsorientierte Begehung bzw. dienstleistungsorientierte Ermöglichung von Straftaten. So wurde festgestellt, dass aktive Straftäter einzelne Tatbeiträge an Außenstehende und auf bestimmte Cybercrime-Dienstleistungen spezialisierte Tätergruppen auslagern bzw. von diesen ankaufen. Die damit einhergehende Zergliederung ermöglicht es auch weniger Cyber-affinen Straftätern, technisch komplexere Straftaten zu realisieren.

Nach hiesigen Erkenntnissen stützt sich dieses Phänomen bzw. kriminelle Öko-System auf neun Säulen[27], die nachfolgend beschrieben und für mehrere Säulen mit Sachverhalten aus dem Berichtsjahr 2019 exemplarisch näher vorgestellt werden:

Säule 1: Foren und Jabber-Server



Foren[28] und Jabber[29]-Server funktionieren als zentrale kommunikative Knotenpunkte, als „Branchenbücher" zwischen Anbietern und Interessenten krimineller Dienstleistungen. In diesen Kontaktbörsen können Akteure ihre Anfragen und Bedürfnisse sowie angebotene Fähigkeiten und Produkte darlegen.

Zudem wird durch Foren sehr maßgeblich die „Qualitätssicherung" von kriminellen Dienstleistungen im Darknet gewährleistet: Durch ein Bewertungssystem können Kunden bspw. mit der Abgabe von Sternen das Produkt bzw. den Service des Cybercrime-Anbieters benoten. Anzahl und Ausprägung positiver Bewertungen spiegeln so den Ruf bzw. das Ansehen des Händlers in der Community wider und sind somit für diesen wichtig, um weitere Aufträge zu erlangen und Preisgestaltungen durchzusetzen.

Fallbeispiel: Polizeiliche Maßnahme gegen Foren-Betreiber

Im Rahmen eines Ermittlungsverfahrens der Polizei Rheinland-Pfalz konnte Anfang Juli 2019 nach umfangreichen Ermittlungsmaßnahmen einer der Hauptbetreiber des größten deutschen Underground-Economy-Forums *Fraudsters* in Pinneberg festgenommen werden.

Über das Forum wurden u. a. Geld- und Urkundenfälschungs- sowie Betäubungsmitteldelikte verübt und widerrechtlich erlangte Daten getauscht. Es zählte circa 30.000 registrierte Nutzer. Der Beschuldigte wurde im Verfahren durch das LG Bad Kreuznach zu einer Freiheitsstrafe von 6 Jahren und 8 Monaten verurteilt.

[27] Die folgenden Fallbeispiele behandeln ausschließlich Fälle mit Relevanz für das Jahr 2019/Anfang 2020.
[28] Ein Online-Forum ist ein virtueller Platz zum Austausch von Gedanken, Meinungen und Erfahrungen.
[29] Jabber ist ein anbieterunabhängiger virtueller Sofort-Nachrichten-Dienst zur Kommunikation.

Kurzbewertung:
Es handelte sich um die erste Verurteilung wegen der Bildung einer kriminellen Vereinigung gem. §129 StGB in Verbindung mit Straftaten aus dem Bereich Cybercrime in Deutschland. Da in vergleichbaren Verfahren den Tätergruppierungen bislang keine konkreten vereinigungsimmanenten Straftaten nachgewiesen werden konnten, stellt dieses Urteil einen Meilenstein bei der Bekämpfung von Cybercrime dar.

Säule 2: Bulletproofhosting- und Proxyprovider

Da eine Vielzahl von Modi Operandi im Bereich CCieS interventionsfeste technische Infrastrukturen voraussetzen, haben sich kriminelle Hosting-Dienstleister darauf spezialisiert, sichere Serverstrukturen (IP-Adressen, Domains) oder Proxy[30]- bzw. VPN-Provider bereitzustellen. Die kriminellen Hosting-Dienstleister mieten hierzu häufig Server bei gewerblichen Datacenter-Betreibern an und stellen diese gegen Bezahlung kriminellen Kunden zu Verfügung. Diese Kunden verfolgen das Ziel, dass die betriebenen Serverstrukturen möglichst lange online bleiben. Da bei Beschwerden zu missbräuchlicher Nutzung des Servers die Nachrichten in der Regel zunächst an den kriminellen Host selbst geleitet werden, hat dieser die Möglichkeit, diese lange genug zu ignorieren, ehe sich letztlich der reguläre Datacenter-Betreiber einschaltet und den Server ggf. abstellt. Bis zu diesem Zeitpunkt könnten die Cyberkriminellen die Begehung der Straftat bereits vollendet haben.

Fallbeispiel: Bulletproofhosting – „Cyberbunker“

Das LKA Rheinland-Pfalz führte seit 2013 umfangreiche Ermittlungen gegen die Betreiber eines Bulletproofhosting-Rechenzentrums in einem ehemaligen Atomschutzbunker, welcher auch unter dem Szenenamen „Cyberbunker“ bekannt gewesen ist. Dort wurden zahlreiche Seiten gehostet, über die international agierende Kriminelle inkriminierte Waren wie Betäubungsmittel, gefälschte Dokumente und gestohlene Daten vertrieben, Kinderpornografie verbreitet und flächig angelegte Cyberangriffe durchgeführt haben.

Im Zuge der Ermittlungen konnte der Tatverdacht gegen insgesamt 13 Tatverdächtige wegen Bildung einer kriminellen Vereinigung (§129 StGB) und wegen Beihilfe zu Hunderttausenden Fällen von schweren Drogendelikten, Falschgeldgeschäften, Datenhehlerei und der Beihilfe zur Verbreitung kinderpornografischer Schriften erhärtet werden.

Im Rahmen von konzertierten Durchsuchungen im September 2019 wurden vielfältige Beweismittel, u.a. 400 Server, sichergestellt.

Kurzbewertung:
Am 07.04.2020 erhob die Landeszentralstelle Cybercrime (LZC) der Generalstaatsanwaltschaft Koblenz Anklage gegen die Verdächtigen. Die Staatsanwaltschaft wertet den Verfahrenskomplex strafrechtlich als Gründung und Beteiligung an einer kriminellen Vereinigung.

[30] Ein Proxy ist eine Kommunikationsschnittstelle in einem Netzwerk, welcher als Vermittler auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen.

Säule 3: Marketplaces, Shops und Automated Vending Carts (AVCs)

Für eine Vielzahl von Cybercrime-Straftaten benötigen bzw. nutzen kriminelle Täter kompromittierte Zugangsdaten. Automatisierte Marktplätze/Shops im Darknet bieten derartige Daten an.

Die mit weitem Abstand beliebtesten Produkte zum Kauf und Verkauf stellen Betäubungsmittel dar.

Der äußere Aufbau derartiger Markplätze ähnelt häufig dem regulärer Online-Handelsplattformen aus dem Clearnet. Als typische Angebote auf Darknet-Marktplätzen gelten z. B.

- digitale Identitäten,
- Online-Zugangsdaten (z. B. E-Mail-Adressen, Online Banking-Accounts),
- Zahlungskartendaten,
- Bereitstellung von Servern,
- Betäubungsmittel und
- Waffen.

Säule 4: Malware-Entwicklung/Coding

Die Entwicklung von Schadsoftware erfolgt in der Regel nach den Anforderungen der Abnehmer, welche die Grundfunktionalitäten der benötigten Malware skizzieren und sich über Foren auf die Suche nach geeigneten Programmierern begeben. Nach aktuellem Stand gelten als am häufigsten vorkommende Malware-Familien: *Emotet*, *Dridex*, *Ryuk*, *Trickbot* und *Maze*.

Säule 5: Malware-Crypting

Aufgrund der signifikanten Weiterentwicklungen sowohl von AV-Produkten als auch von Betriebssystemen sind die Anforderungen an funktionierende und vor allem nicht detektierbare Malware für die Täterseite in den vergangenen Jahren gestiegen. So haben sich Crypting-Dienstleister der Aufgabe verschrieben, Schadcode so zu verfremden bzw. zu verschlüsseln, dass eine Erkennung der Malware durch Antivirus-Produkte verhindert werden soll.

Fallbeispiel: Malware-Crypting

Im Rahmen eines seit 2018 geführten Ermittlungsverfahrens konnte das BKA einen in Deutschland lebenden tunesischen Staatsangehörigen identifizieren, der im Verdacht steht, unter einer virtuellen Identität auf einem Darknet-Forum von ihm kryptierte Malware zum Upload freigegeben zu haben.

Durch die Ermittlungen konnte nachvollzogen werden, dass der Beschuldigte für einen gesondert verfolgten Nutzer des Darknet-Forums als Crypter gearbeitet und insgesamt als langjähriger Dienstleister für Cryptingdienste in der Cybercrime-Szene fungiert hatte.

Die ausgewertete Kommunikation zeigte, dass der Beschuldigte seit Jahren Werbung auf zahlreichen, für Cyberkriminelle attraktiven Foren machte, um Kunden für Cryptingdienste zu gewinnen. Gegen ihn besteht der Verdacht, Schadsoftware im großen Stil – insbesondere im Auftrag der russischen Cyberkriminellen-Szene –kryptiert und damit gegen eine Detektierung abgesichert zu haben. Dadurch soll er Beihilfe zu den mit der Schadsoftware begangenen Folgetaten geleistet haben.

Kurzbewertung:
Das Fallbeispiel ist Beleg, dass Crypting einen elementaren Bestandteil der Malware-Entwicklung und auch einen eigenen Wirtschaftszweig der Underground Economy darstellt. Es unterstreicht zudem die herausragende Bedeutung internationaler polizeilicher Zusammenarbeit für erfolgreiche Cybercrime-Ermittlungen.

Säule 6: Counter-Antivirus-Services (CAV)

Wird das Schadprogramm durch AV-Produkte entdeckt, bedeutet dies i. d. R. den Verlust des infizierten Opfersystems für weitere kriminelle Handlungen. Daher bieten technisch hochspezialisierte Counter-Antivirus-Dienstleister in der Underground Economy an, Malware-Samples auf ihre Erkennungsrate durch AV-Produkte zu testen. Die Anbieter dieser Services arbeiten sehr agil, sodass ihre Kunden stets eine tagesaktuelle Bewertung für die Vitalität bzw. Funktionalität ihrer Malware erhalten.

Säule 7: Malware Delivery / Infection on Demand

Schadprogramme können erst dann ihre kriminelle Energie entfalten, wenn sie Opfersysteme infizieren und sich verbreiten. Im CCaS-Ökosystem existieren sog. Content-Delivery-Netzwerke, welche sich auf die Verbreitung und die Installation von Schadsoftware ihrer Kunden spezialisiert haben. Diese Netzwerke verfügen häufig über eine Vielzahl von bereits mit anderer Schadsoftware infizierten Rechnern (Botnetze). Den für sie bestehenden Zugang zu diesen Geräten können sie nutzen, um deren Systeme mit der durch den kriminellen Auftraggeber zugelieferten Schadsoftware zu infizieren. Bezahlt werden die kriminellen Content-Delivery-Dienstleister auf Erfolgshonorarbasis, welche sich nach der Anzahl erfolgreicher Installationen der Malware auf fremden Systemen richtet (sog. „Pay-per-Install“).

Säule 8: Drops, Mules und Cashout

Hauptaufgabe dieser Dienstleister ist, den monetären Mehrwert des kriminellen Handels zu verwirklichen. Es handelt sich um die aus Tätersicht risikoreichste Aktivität, da es eines Auftretens außerhalb der digitalen Welt bedarf. Inkriminierte Zahlungen müssen auf Konten geleitet und an Geldautomaten abgehoben werden. Betrügerisch bestellte Warensendungen müssen an Packstationen oder „toten" Briefkästen abgeholt werden. Für diesen sog. „Cashout" beauftragen die Hinterleute eines Cyberangriffs nicht selten einen gesonderten kriminellen Dienstleister, welcher wiederum Subunternehmen – sog. „Runner" oder „Drops" – mit der tatsächlichen Abholung der Gelder bzw. der Waren beauftragt. Der Rückfluss an die eigentlichen kriminellen Auftraggeber erfolgt dabei i. d. R. mittels Kryptowährungen.

Säule 9: Exchanger

Diese Säule der CCasS betrifft die Geldwäsche im digitalen Raum. Ziel ist es, einen kostengünstigen Wandel von einer digitalen Währung in eine oder mehrere andere staatliche oder digitale Währungen nach Wahl durchzuführen (sog. Mixing-Dienste). Zusätzlich soll parallel eine weitestmögliche Verschleierung der inkriminierten Transaktionen erfolgen. Die kriminellen sog. „Exchanger" verfügen über weitrechendes Wissen über Technologie und Geschäftsabläufe im Bereich von Kryptowährungen sowie den Rahmenbedingungen im Finanzsektor.

Polizeiliche Erfahrungen zu Mixing-Diensten

- *Die Polizei hat bereits verschiedene Mixing-Dienste abgeschaltet und entsprechende Transaktionsdaten gesichert.*
- *Ein sog. „De-Mixing" ist möglich; Kryptowährungen sind nicht so anonym, wie viele Täter denken – auch Kryptowährungen liefern erfolgversprechende Ermittlungsansätze.*
- *Die Qualität der Verschleierung richtet sich oft nach dem Preis des Exchangers.*
- *Phänomen der betrügerischen Mixing-Dienste: Diese nehmen Kryptowährungen des Kunden entgegen, wandeln diese jedoch nicht um bzw. zahlen diese nicht wieder aus. Ein geprellter Cybertäter erstattet selten Strafanzeige.*

5 Angriffe auf Wirtschaft und KRITIS

Die deutsche Wirtschaft ist ein beliebtes Ziel für Cyberkriminelle – laut BITKOM-Studie[31] vom Februar 2020 ist die Anzahl der 2019 tatsächlich von einem Cyberangriff betroffenen Unternehmen erneut stark gestiegen.

[32]

Drei von vier Unternehmen wurden 2019 Opfer von Cyberkriminellen – 2017 nur jedes zweite.

Unternehmen sehen sich einer großen Bandbreite an Cybergefahren ausgesetzt - sei es die Ausspähung von sensiblen Daten, ihre missbräuchliche Veränderung, die Beeinträchtigung von Erreichbarkeiten von Servern und Webpräsenzen, die Manipulation von Webseiten, die Infizierung mit Schadsoftware, die Verschlüsselung oder gar Zerstörung von Daten. Durch eine zunehmende Professionalisierung der Täterseite hat sich diese Situation im letzten Jahr weiter und deutlich verschärft – die Modi Operandi werden komplexer und ihr jeweiliges Zusammenspiel sowie die Art des verwendeten Angriffsvektors ausgefeilter und vielfältiger. Eintrittsvektor für die Cyberattacke ist nicht immer das Unternehmen selbst – oftmals nutzen Cyberkriminelle die Lieferkette des Unternehmens oder die IT-Systeme des Partners aus, um das eigentliche Ziel zu kompromittieren.

[31] Abrufbar unter: https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf
[32] Anzahl der jeweils Befragten (n):
2015: n = 1074
2017: n = 1069
2019: n = 1070

Zudem wurde auch in 2019 der Modus Operandi festgestellt, bei dem täterseitig aktiv das Internet nach Systemen gescannt wird, welche Fernwartungszugänge anbieten. Auf die Passwörter dieser Systeme wird eine sog. Brute-Force-Attacke ausgeführt und bei erfolgreichem Login Mal- und Ransomware installiert.

Kleine und vermehrt große private Unternehmen, aber auch öffentliche Einrichtungen stehen verstärkt im Fokus von Cyberkriminellen.

Das G4C sowie der BITKOM identifizierten eine weitere Entwicklung: Lag in 2018 der Fokus der Angriffe auf Wirtschaftsunternehmen vor allem auf kleinen und mittleren Unternehmen (KMU), setzten Cyberkriminelle im Jahr 2019 vermehrt auf das sog. „Big Game Hunting", d.h. zielgerichtete Angriffe auf große Unternehmen und Institutionen.

Zusammen mit dem in Kapitel 4.1 erwähnten Modus Operandi der Double Extortion lässt sich insgesamt eine qualitative Steigerung hinsichtlich Intensität und Dimension von Cyberangriffen auf die deutsche Wirtschaft erkennen.

Im Jahr 2019 entstand ein Schaden von circa 102,9 Mrd. Euro durch Cyberangriffe auf Wirtschaftsunternehmen.

BITKOM bezifferte die von ihm hochgerechneten Schäden, die im Jahr 2019 durch Cyberangriffe verursacht wurden, auf 102,9 Milliarden Euro – dies stellt annähernd eine Verdopplung gegenüber dem Untersuchungszeitraum 2017/2018 mit 55 Milliarden Euro dar.

Die sog. Kritischen Infrastrukturen (KRITIS)[33], das institutionelle „zentrale Nervensystem" der Gesellschaft und der öffentlichen Ordnung, richten sich zunehmend auf die Abwehr und das Management von Cybergefahren ein. Der Ausfall einer KRITIS würde fundamentale Prozesse der Öffentlichkeit einschränken, sodass ihrem Schutz auch im Rahmen polizeilicher Gefahrenabwehr und Strafverfolgung eine herausragende Bedeutung zukommt.

KRITIS-Unternehmen sind bei festgestellten Störungen verpflichtet, diese an das BSI zu melden. Laut IT-Sicherheitslagebericht 2019[34] weist das BSI 252 Meldungen für den Berichtszeitraum 31.05.2018 bis 01.06.2019 aus. Im Gegensatz zum Vorjahr stammte das Gros der Meldungen aus dem Finanzsektor, dicht gefolgt vom IT- und Telekommunikationssektor. Die Anzahl der beim BSI erfassten Meldungen im Vergleich zur Vorjahresberichterstattung (145 Meldungen) stieg damit prozentual sehr deutlich an.

[33] Unter KRITIS fallen die Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Finanz- und Versicherungswesen, Transport und Verkehr, Gesundheit, Medien und Kultur sowie Staat und Verwaltung.
[34] Die Lage der IT-Sicherheit in Deutschland 2019, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf

Von einer weiteren Zunahme der Cyberangriffe auf KRITIS ist, in Anbetracht der hier geschilderten Entwicklungen, auszugehen.

Fallbeispiel: 2,4 Millionen Euro Schaden durch Ransomware-Angriff

Das LKA Schleswig-Holstein berichtete, dass ein im dortigen Zuständigkeitsbereich ansässiges Unternehmen ab Anfang September 2019 von unbekannten Tätern erpresst wurde (§253 StGB). Die Täter waren in die IT-Systeme dieser Firma eingedrungen und hatten dort alle relevanten Daten und Systeme mit der Ransomware *iEncrypt* verschlüsselt.

Wie bei vielen Ransomware-Varianten üblich, wurde nach der Verschlüsselung ein Erpressertext angezeigt, in dem die Zahlung eines Lösegelds zur Entschlüsselung der Daten gefordert und für weitere Informationen an verschiedene E-Mail-Adressen verwiesen wurde. Nach Kontaktaufnahme über diese Email-Adressen, die mit der Ransomware *iEncrypt* in Verbindung standen, erhielt das Unternehmen folgende Antwortmail der Täter:

„Hello,
Attached is one decrypted file
We have an error with the second one "tablfertigung Berechtigung.xlsx", the file was modified in your environment AFTER the encryption process (we cannot help if you manipulate the files intentionally)
If you want to test it again, make sure the file itself and _readme are not corrupted in any way (do not rename or change the file name/format or its content)
The price is $2,600,000 (two million six hundred thousand)
The bitcon address for the payment: 3DCCbrz1FZRDqRLNRiJ63UzAVPqNUnDu8B
It takes around 40-80 minutes to get enough confirmations form the blockchain, in order to validate the payment
Upon receipt we send you the tool“

Kurzbewertung:
Bei dem geschilderten Sachverhalt ist von einer gewerbsmäßigen Tatbegehung auszugehen. Neben den Ermittlungen in Schleswig-Holstein wurden weitere gleichgelagerte Fälle im Bundesgebiet bekannt, die eindeutige Tatzusammenhänge aufwiesen. Die zur Entschlüsselung geforderten Lösegelder lagen alle mindestens im sechsstelligen Bereich. Dies zeigt, welche enorme Dimension ein Ransomware-Befall haben kann. Schadenssummen dieser Höhe können für Unternehmen existenzbedrohend sein. Aus diesem Grund ist es gerade für Unternehmen unabdingbar, regelmäßige Backups zu erstellen, um im Falle eines Ransomware-Befalls dem Täter nicht ausgeliefert zu sein (Siehe hierzu auch Kapitel 9.4).

In den Medien und auf Kanälen von IT-Security-Dienstleistern ist im Zusammenhang mit Angriffen auf Wirtschaftsunternehmen des Öfteren von besonders komplexen Cyberangriffen, den sog. APT, die Rede.

Kennzeichnend für APT-Angriffe ist, dass sie sowohl zur Spionage, das heißt zum Ausspähen von Daten, als auch zur Sabotage, also zum Stören von Abläufen, genutzt werden. Oftmals werden APT von staatlich unterstützten oder nachrichtendienstähnlichen Gruppierungen ausgeführt.

Advanced Persistent Threat (APT)

Bei einem APT handelt es sich um einen zielgerichteten Cyber-Angriff auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten auf Seiten der Angreifer aus und sind i. d. R. schwierig zu detektieren.

Allerdings adaptieren in den vergangenen Jahren zunehmend auch nicht-staatliche Gruppierungen diese Form des Angriffes und verschaffen sich durch ein professionelles Vorgehen langfristige, tiefgreifende Zugriffe auf fremde Systeme. APT ist demnach kein Alleinstellungsmerkmal staatlicher oder staatsnaher Gruppierungen mehr, sondern eine Angriffsform, welche von einer wachsenden Zahl von Cybercrime-Akteuren verwendet wird.

APTs stellen existentielle Bedrohungen für Unternehmen dar.

Das BKA stellt im Bereich der staatlich gesteuerten Cyberangriffe Folgendes fest:

- Cyber-Angriffe gegen Deutschland bleiben weiterhin eine wichtige Methode der Informationsgewinnung für ausländische Nachrichtendienste.
- Weltweit werden bei Cyberspionage-Angriffen immer wieder dynamisch gestaltete Serverinfrastrukturen sowie hoch professionelle und einer steten Weiterentwicklung unterliegenden Schadsoftwarekomponenten verwendet.
- Gruppierungen passen auch ihre Angriffs-Narrative den aktuellen politischen und gesellschaftlichen Situationen und Herausforderungen an und nutzen Ängste und Informationsbedürfnisse der Bevölkerung für ihre Zwecke aus.
- Den meisten Angriffen gehen gezielte „Social Engineering-Operationen“ voraus. Hauptangriffsvektor ist dabei der Versand von „Spear-Phishing-E-Mails“[35], sowohl mit maliziösen Links als auch mit Schadanhang, mittels derer die Systeme der Geschädigten infiziert werden. Den Cyberspionage-Angriffen gehen i. d. R. professionelle Abklärungen der Zielpersonen voraus. Dies geschieht nicht nur durch gezielte Aufklärung im Internet und in Sozialen Medien, sondern auch durch klassische Spionage in Form von Fernmeldeaufklärung und den Einsatz von Agenten.

[35] „Spear-Phishing“ bezeichnet ein verfeinertes Phishing mit einem gezielteren persönlichen Ansatz („spear“ – steht für Speer).

- Veröffentlichungen zahlreicher IT-Sicherheitsunternehmen weisen regelmäßig auch auf eine Betroffenheit Deutschlands bei Cyberspionage-Angriffen hin. Eine konkrete und belastbare Attribution ist bei diesen staatlich/nachrichtendienstlich gesteuerten Angriffen nur schwer möglich.
- Es ist von einer hohen Dunkelziffer durch nicht erkannte bzw. nicht angezeigte Angriffe auszugehen.
- Das Sicherheitsunternehmen FireEye gibt in einer Analyse[36] verschiedener APT-Gruppen an, dass deren Operationsbasen vorwiegend in China, Russland, Nordkorea, Vietnam und dem Iran zu finden seien.

Der Wirtschaftsstandort Deutschland ist aufgrund der vergleichsweise hohen Konkurrenzfähigkeit und technologischen Expertise der angesiedelten Unternehmen weiterhin ein interessantes Ziel für Cyberspionage und/oder allgemeinkriminelle Hacker. Ungeachtet aktueller wirtschaftlicher Entwicklungen dürften Unternehmen in Deutschland im Fokus von Cybertätern bleiben.
Die zunehmende Professionalisierung allgemeinkrimineller Cybertäter führt dazu, dass diese vermehrt APT-Vorgehensweisen einsetzen und somit ebenfalls zu einer kritischen Bedrohung für Unternehmen werden. Dieser Trend wird dadurch begünstigt, dass vertiefte IT-Kenntnisse nicht mehr zwingend erforderlich sind und benötigte Komponenten über das CCaaS-Ökosystem bezogen werden können – die Wahrscheinlichkeit von hochkomplexen und schwerwiegenden Angriffen durch ein erweitertes Täterspektrum steigt damit weiter an.

Fallbeispiel: SOFACY/APT 28

Das BKA ermittelt seit 2015 im Auftrag des Generalbundesanwalts beim Bundesgerichtshof (GBA) gegen unbekannte Mitglieder des russischen militärischen Geheimdienstes GRU[37] u. a. wegen der elektronischen Ausspähung des Deutschen Bundestags im Frühjahr 2015.
Das Ermittlungsverfahren umfasst zahlreiche weitere Taten, die dem GRU bzw. der Cyber-Angriffskampagne *SOFACY/APT28* zugeordnet werden.
Bei den verfahrensgegenständlichen Tatkomplexen handelt es sich um elektronische Angriffe auf interne IT-Netze, u. a. von Parteien, politischen Stiftungen sowie gesellschaftspolitischen Forschungseinrichtungen.

Die Untersuchung bzw. forensische Analyse der bisher sichergestellten Server lieferte umfangreiche Erkenntnisse hinsichtlich der unterschiedlichen Erscheinungsformen der durch die *SOFACY/APT28*-Gruppierung verwendeten Malware sowie Erkenntnisse zu handelnden Personen. Gegen eine dieser Personen erließ der Ermittlungsrichter des Bundesgerichtshofs am 29.04.2020 Haftbefehl wegen des elektronischen Angriffs auf den Deutschen Bundestag.

Kurzbewertung:
Die Tatkomplexe belegen, dass die Akteure hinter *SOFACY/APT28* über eine weltweite IT-Infrastruktur verfügen und für die Durchführung der Cyber-Angriffe ein komplexes Netzwerk von Servern nutzen. Im Rahmen der Ermittlungen wurde eine Vielzahl von Servern bei in Deutschland ansässigen Internet-Dienstleistern, die Anonymität sowie Identitätsschutz angeboten und anonyme Zahlungsmittel akzeptiert hatten, sichergestellt.

[36] **https://www.fireeye.de/current-threats/apt-groups.html**
[37] Glawnoje Raswedywatelnoje Uprawlenije, Übersetzung: Hauptverwaltung für Aufklärung

6 Polizeiliche Kriminalstatistik (PKS)

6.1 ERFASSUNGSMODALITÄTEN

Cybercrime als Phänomen unterscheidet die Bereiche Cybercrime im engeren Sinne (CCieS) und im weiteren Sinne (CCiwS)[38].

Das Bundeslagebild Cybercrime 2019 informiert über die polizeilich bekannt gewordenen Entwicklungen von CCieS. Ergänzend werden mit Blick auf die sog. Underground Economy als einem wesentlichen Bereich von Cybercrime auch Ausführungen zur CCiwS gemacht.

Bei der Betrachtung von polizeilich erfassten statistischen Daten müssen die besonderen Erfassungs- bzw. Zählmodalitäten in der Polizeilichen Kriminalstatistik (PKS) berücksichtigt werden. So ist bei der Interpretation der Statistik zu beachten, dass z. B. einzelne relevante Phänomene wie Erpressungshandlungen im Zusammenhang mit gezielten DDoS-Attacken oder auch mit Ransomware in der PKS i. d. R. nicht als Cybercrime-Delikt, sondern als schwerwiegendere bzw. speziellere Tat, in diesem Fall als Erpressung, erfasst werden.

Trotz der eingeschränkten Aussagekraft der PKS hinsichtlich der Gesamtheit der in Deutschland verübten Cybercrime-Straftaten liefert diese eine Datenbasis, auf deren Grundlage zumindest Trendaussagen für den Phänomenbereich getroffen werden können.

Die Polizei weist auf die Notwendigkeit zur Anzeige entsprechender Cybercrime-Straftaten durch die Geschädigten hin: Eine zeitnahe Strafanzeige wirkt der Flüchtigkeit digitaler Spuren wirksam entgegen und erhöht die Erfolgswahrscheinlichkeit bei der Täterermittlung. Gemeinsame Ziele sind, die Urheber für Cyber-Angriffe zu identifizieren, zur Verantwortung zu ziehen, abschreckende Wirkung auf potenzielle Täter zu entfalten und so Wiederholungs- bzw. Nachahmungstaten zu unterbinden. Zudem ergeben sich aus einem umfassenden Lagebild neue Ermittlungsansätze für eine effektivere Bekämpfung (durch z. B. Analyse der Angriffsvektoren oder Feststellung von Tatzusammenhängen).

6.2 FALLZAHLEN CYBERCRIME

Im Jahr 2019 war erneut ein Anstieg der Straftaten von CCieS zu verzeichnen. Die PKS wies insgesamt 100.514 Fälle aus. Dies bedeutet eine Steigerung gegenüber dem Vorjahr um 15,4 Prozent (2018: 87.106 Fälle). Die Aufklärungsquote betrug 32,3%, was einem Rückgang gegenüber dem Vorjahr um 6,6 Prozentpunkte entspricht.

Mehr als Drei Viertel aller Straftaten wurden als Fälle von Computerbetrug registriert. Für das Jahr 2019 wurde in diesem Deliktsfeld ein Anstieg von 18,0 Prozent verzeichnet. In den meisten Fällen wurden hierunter Sachverhalte erfasst, bei denen das Internet lediglich als Tatmittel fungierte.[39] Insofern stellen diese Fälle keine CCieS dar. Auch aus diesem Grund sind die Fallzahlen der PKS differenziert zu betrachten und zu bewerten.

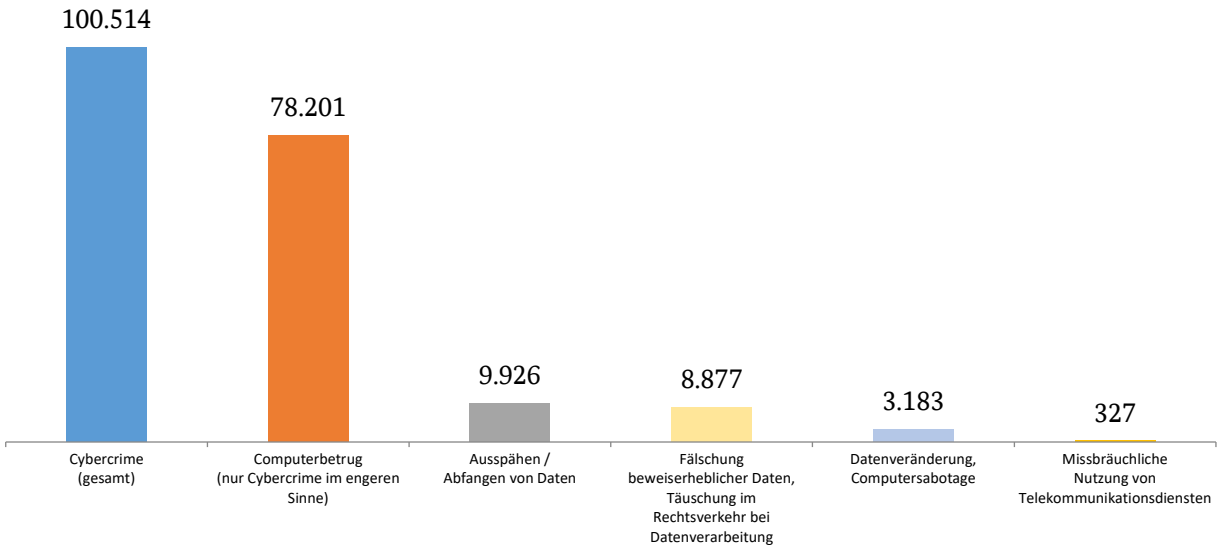
Die Fallzahl zur missbräuchlichen Nutzung von Telekommunikationsdiensten gem. §263a StGB sank im Berichtsjahr um 49,2 Prozent auf 327 Fälle (2018: 644 Fälle). Dieser Rückgang ist hauptsächlich auf den Abschluss eines komplexen Ermittlungsvorgangs der Staatsanwaltschaft Oldenburg

[38] CCiwS beschreibt alle Straftaten, bei denen das Internet als Tatmittel eingesetzt wurde.
[39] Z. B. der Waren- oder Leistungskreditbetrug in folgender Form: Beim Versuch, eine Ware oder Dienstleitung über das Internet zu erlangen, erfolgt durch die Betrüger keine Bezahlung der Bestellung.

und der Polizeiinspektion Osnabrück[40] mit zahlreichen (aufgeklärten) Einzelfällen zurückzuführen, der für die hohe Fallzahl im Jahr 2018 verantwortlich war.

Bei Datenveränderung/Computersabotage gem. §§303a, 303b StGB wurde ein Anstieg von 10,7 Prozent verzeichnet. Diesbezüglich wurden 3.183 Fälle registriert (2018: 2.875 Fälle).

Fälle von Cybercrime im engeren Sinne (2019)



Da in der PKS ausschließlich Schäden in Fällen des Computerbetrugs und der missbräuchlichen Nutzung von Telekommunikationsdiensten ausgewiesen werden, lassen sich nur eingeschränkte statistische Aussagen zum monetären Gesamtschaden durch Cybercrime treffen.
Die für das Jahr 2019 erfasste Schadenssumme in den beiden Deliktsbereichen belief sich auf 88,0 Mio. Euro (2018: 61,4 Mio. Euro). Dies entspricht einem Anstieg von 43,3 Prozent gegenüber dem Vorjahr. 87,7 Mio. Euro entfallen dabei auf den Computerbetrug (2018: 60,7 Mio. Euro).

6.3 TATVERDÄCHTIGE

Im Jahr 2019 wurden insgesamt 22.574 Tatverdächtige (TV) von Cybercrime-Delikten registriert. Gegenüber dem Vorjahr entspricht das einem Anstieg um 2,4 Prozent (2018: 22.051 TV).
68,3 Prozent der Tatverdächtigen waren männlich, 31,7 Prozent weiblich.

Auffällig ist, dass weibliche TV damit im Phänomenbereich CCieS im Verhältnis zu allen Straftaten der PKS (Anteil 25,0%) überrepräsentiert sind. Ausschlaggebend dafür ist der Straftatbestand des Computerbetrugs, hier vornehmlich des Warenkreditbetrugs. Dieser weist eine hohe Fallzahl und einen hohen Anteil weiblicher Tatverdächtiger auf (Computerbetrug gem. §263a StGB:

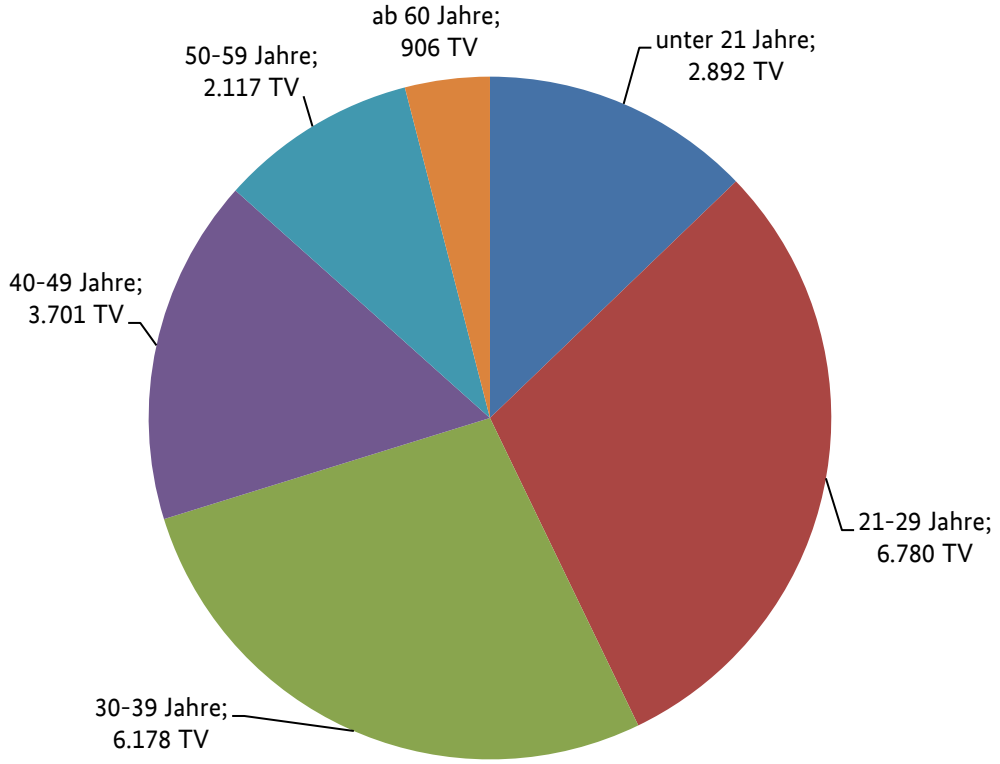
[40] In dem Ermittlungskomplex erlangte ein Beschuldigter über das Internet Zugriff auf sog. FRITZ!-Boxen und programmierte Rufumleitungen zu Mehrwertnummern. Anschließend wurden die Rufumleitungen automatisiert ausgelöst, so dass es zu kostenpflichtigen Verbindungen vom jeweils manipulierten Router/Telefonanschluss kam. Der Beschuldigte „mietete“ unter Verschleierung seiner Identität die zuvor programmierten nationalen und internationalen Mehrwertrufnummern und erlangte einen Teil der angefallenen Telefongebühren.

34,1% weibliche TV; Warenkreditbetrug gem. §§ 263, 263a StGB: weibliche TV 33,9%).
Bei Cybercrime-Delikten mit geringeren Fallzahlen ist der Anteil der weiblichen TV wiederum fast konform mit dem Anteil an den Gesamtstraftaten (z. B. Ausspähen von Daten, Abfangen von Daten, Datenhehlerei gem. §§202a-d StGB: 25,2%) oder fällt sogar geringer aus (z. B. Datenveränderung, Computersabotage gem. §§303a, b StGB: 22,4%).

Im Jahr 2019 waren 17.015 der festgestellten Tatverdächtigen (75,4%) deutsche Staatsangehörige. 5.559 Tatverdächtige waren Nichtdeutsche, wobei türkische (13,2%), rumänische (9,2%) und polnische (6,1%) Staatsangehörige am häufigsten in Erscheinung traten. Bei allen drei Staatsangehörigkeiten ist der Warenkreditbetrug für den hohen Anteil verantwortlich.

Mehr als die Hälfte (57,4%) der registrierten Delikte der CCieS wurde von Tatverdächtigen begangen, die zwischen 21 und 39 Jahre alt waren.

Altersstruktur der Tatverdächtigen (2019)



Das Täterspektrum reicht von Einzeltätern bis hin zu international organisierten Tätergruppierungen. Gemeinsam agierende Täter arbeiten im Bereich Cybercrime nur selten in hierarchischen Strukturen. Sie kennen sich häufig nicht persönlich und bevorzugen auch bei arbeitsteiligem Vorgehen die erhöhte Anonymität des Internet.

Die Täterseite reagiert flexibel und schnell auf neue technische Entwicklungen und passt ihr Verhalten entsprechend an. Dienste, die nicht selbst erbracht werden können, werden in der Underground Economy hinzugekauft (s. Kapitel 5).

6.4 ORGANISIERTE KRIMINALITÄT

Auch Gruppierungen der Organisierten Kriminalität (OK) betätigen sich im Kriminalitätsbereich Cybercrime. Zehn der für das Jahr 2019 insgesamt gemeldeten 579 OK-Verfahren wurden im Bereich Cybercrime geführt (2018: 13 OK-Verfahren).

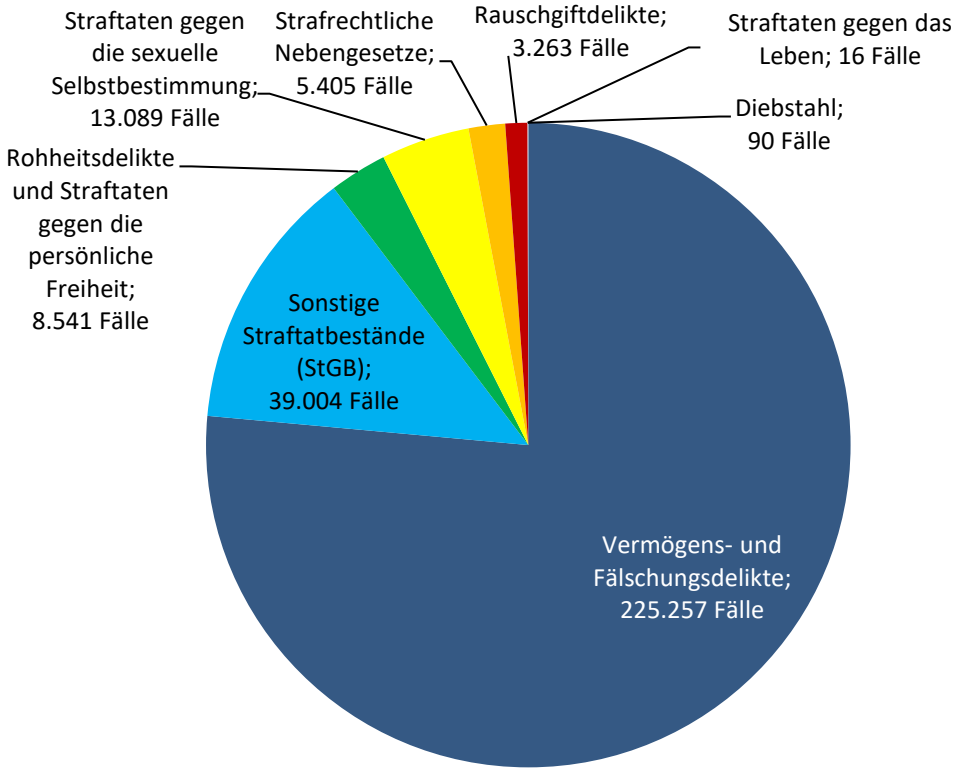
Die organisierten Strukturen begingen dabei die gleichen Cybercrime-Delikte, die auch bei Einzeltätern und loseren Netzwerken festzustellen sind. Es handelt sich dabei überwiegend um Computerbetrug, Angriffe auf das Online-Banking und um die Verbreitung von Ransomware mit dem Ziel der digitalen Erpressung.

6.5 TATMITTEL INTERNET

Im Jahr 2019 wurden in der PKS insgesamt 294.665 Fälle erfasst, bei denen das Internet als Tatmittel genutzt wurde. Dies entspricht einem Anstieg um 8,4 Prozent gegenüber dem Vorjahr (2018: 271.864 Fälle).

Die PKS-Sonderkennung[41] „Tatmittel Internet“ wird bei der Erfassung berücksichtigt, wenn das Internet im Hinblick auf die Tatverwirklichung eine wesentliche Rolle spielt, z. B. bei Erpressungshandlungen i. Z. m. DDoS-Attacken oder bei der Abwicklung von Geschäften bei Online-Versandhäusern. Die Sonderkennung wird allerdings nicht verwendet, wenn z. B. im Vorfeld der eigentlichen Tat lediglich lose Kontakte zwischen Täter und Geschädigtem über das Internet bestanden.

Tatmittel Internet – Verteilung nach Deliktsbereichen (2019)



[41] Sonderkennungen sind in der PKS Merkmale, die bei der Erfassung einer Straftat optional ausgewählt werden können. Mit Sonderkennungen werden bestimmte PKS-relevante Kriminalitätsformen gekennzeichnet.

Im Jahr 2019 handelte es sich bei 74,1 Prozent (218.270 Fälle) aller Straftaten mit dem Tatmittel Internet um Betrug (2018: 75,7%; 205.735 Fälle). Darunter waren 156.966 Fälle von Waren- und Warenkreditbetrug (2018: 154.773 Fälle), bei denen Tatverdächtige über das Internet Waren zum Verkauf anboten, diese jedoch entweder nicht oder nur in minderwertiger Qualität lieferten oder bei denen Tatverdächtige die Waren bestellten und nicht bezahlten.

7 Gesamtbewertung und Ausblick

Cybercrime gewinnt weiter an Bedeutung. Dies belegen die polizeilichen Fallzahlen sowie auch zahlreiche Studien und Phänomenanalysen. So kommt der Branchenverband BITKOM zu dem Schluss, dass Cyberangriffe sowohl quantitativ als auch qualitativ zugenommen haben – diesen Schluss legen auch die Daten der PKS 2019 nahe. Darüber hinaus bestätigen diverse weitere Studien, dass von einem großen Dunkelfeld im Bereich Cybercrime auszugehen ist und allein der polizeiliche Datenbestand dieses Kriminalitätsfeld nicht realitätsnah abbilden kann.

Einer Umfrage des eco-Verbands[42] aus dem Jahr 2020 zufolge schätzen 91 Prozent der befragten Unternehmen die allgemeine Bedrohungslage bei der Internetsicherheit als wachsend bzw. stark wachsend ein. Keiner der Befragten gab an, dass sich das Gefährdungspotenzial durch Cybergefahren verringert hätte. Bei einer Forsa-Befragung[43] von 300 repräsentativen Entscheidern bei KMU im Frühjahr 2019 zum Thema „Cyberrisiken im Mittelstand“ gaben 24 Prozent der Befragten an, durch Attacken von Cyberkriminellen bereits Schäden erlitten zu haben. Überwiegend handelte es sich dabei um Kosten zur Aufklärung und Datenherstellung bzw. um Schäden durch Unterbrechungen des Betriebsablaufs. Aber auch mittelbare wirtschaftliche Schäden durch Reputationsverluste oder den Diebstahl von Betriebsgeheimnissen spielen nach solchen Gefährdungssachverhalten für die betroffenen Unternehmen eine Rolle.

Bei der Erstellung des „Allianz Risiko Barometer 2020“[44] wurden über 2.700 Personen aus verschiedenen Industrie- und Wirtschaftsbereichen in 102 Staaten zu den wichtigsten Unternehmensrisiken befragt. „Cybervorfälle“ wie z. B. Cybercrime, IT-Ausfälle und Data Breaches wurden dabei von 39 Prozent der Befragten und damit im Jahr 2019 erstmals als das wichtigste Geschäftsrisiko angesehen. Im Jahr 2013 rangierte das Risiko mit einem Antwortanteil von 6 Prozent noch auf dem 15. Platz dieses Rankings. Die Unternehmen sehen sich dabei immer häufiger Datenskandalen und einer steigenden Anzahl sonstiger Cyberangriffe wie Erpressungs- und Spoofing-Attacken ausgesetzt.

Die Studie „e-Crime in der deutschen Wirtschaft 2019“[45] der Wirtschaftsprüfungsgesellschaft KPMG spricht von 39 Prozent der Unternehmen in Deutschland, die in den letzten zwei Jahren von Cybercrime betroffen waren. Für die Studie wurden 1.001 repräsentativ ausgewählte Unternehmen befragt. Große Schwierigkeiten bereitet den Unternehmen insbesondere die Identifikation der Täter. 80 Prozent der Betroffenen können lediglich erkennen, dass Unbekannte von außerhalb des eigenen Unternehmens für den Angriff verantwortlich sind. So besteht eine große Wahrscheinlichkeit, dass nicht nur die Täter, sondern auch die jeweiligen Delikte an sich unerkannt bleiben.

---

[42] Auszug abrufbar unter: https://www.eco.de/presse/eco-it-sicherheitsstudie-2020-unternehmen-ruesten-sich-fuer-den-ernstfall/

[43] Cyberrisiken im Mittelstand. Ergebnisse einer Forsa-Befragung. Frühjahr 2019, abrufbar unter: https://www.gdv.de/resource/blob/48506/a1193bc12647d526f75da3376517ad06/cyberrisiken-im-mittelstand-2019-pdf-data.pdf, S. 5

[44] Allianz Risk Barometer 2020 – Cyber incidents, abrufbar unter: https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2020-cyber-incidents.html, veröffentlicht am 14.01.2020

[45] E-Crime in der deutschen Wirtschaft 2019, abrufbar unter: https://hub.kpmg.de/studie-e-crime-in-der-deutschen-wirtschaft-2019

Die bereits 2018 identifizierten Entwicklungen in den einzelnen Phänomenbereichen von Cybercrime haben sich im Jahr 2019 weiter fortgesetzt. Die Bedrohungslage, welche durch Cybercrime-Straftaten besteht, befindet sich auf einem hohen Niveau und wird angesichts weiterer technischer Entwicklungen und einer fortschreitenden Digitalisierung ansteigen. So zeigt sich im Berichtsjahr erneut, dass das IoT für die Verstärkung von DDoS-Angriffen aktiv ausgenutzt wird.

Die Täterseite betreibt eine organisierte, arbeitsteilige und hochprofessionelle Wirtschaft, die nahtlos ineinandergreift und durch jeden erfolgreichen Angriff wächst.

Charakteristisch für Cyberangriffe im Jahr 2019 ist die Verbindung von Wertschöpfungsketten: Daten werden zunächst auf kriminelle Weise entwendet, um als Basis für weitere kriminelle Aktivitäten zu dienen. Es können mit dem Kauf und dem Weiterverkauf dieser Daten und deren unterschiedliche Nutzung im Cyberbereich illegale Gewinne an verschiedenen Punkten dieser Ketten generiert werden.

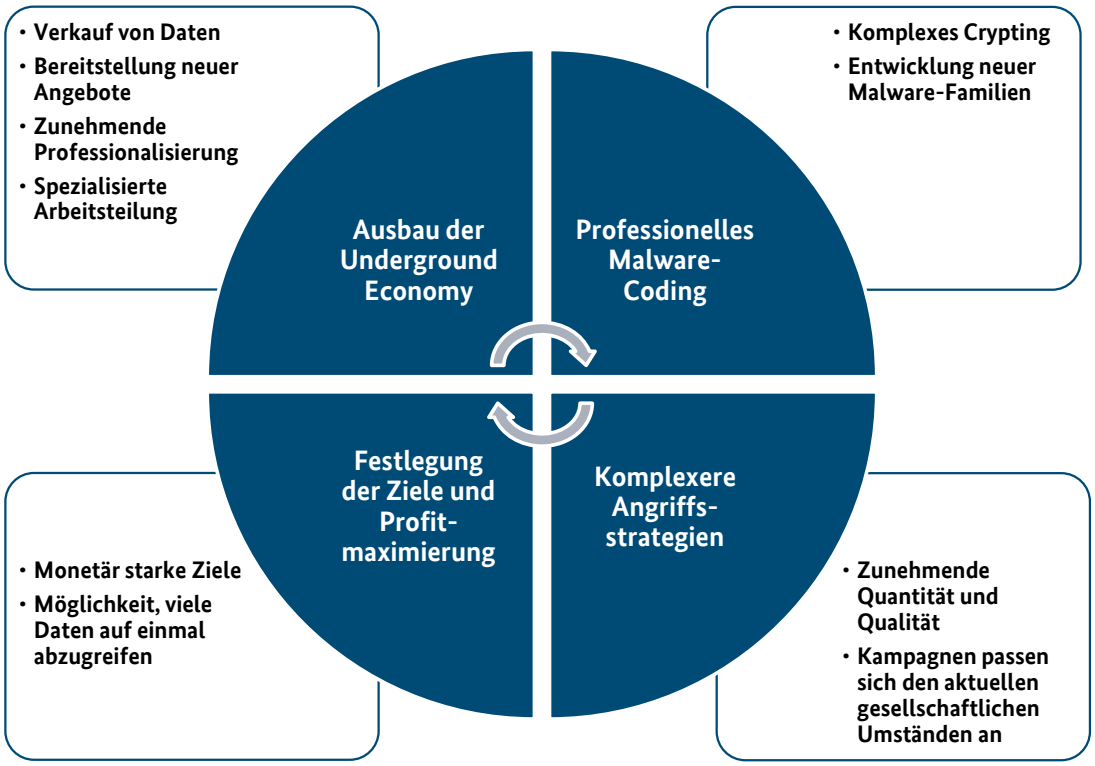
Das vorliegende Lagebild Cybercrime zeigt vier wesentliche Entwicklungen auf:

1. Die Täterseite professionalisiert sich zunehmend – nicht nur in Bezug auf Malware-Coding, sondern auch auf die spezialisierende Arbeitsteilung in der Underground Economy. So etabliert sich eine organisierte, autonome Wirtschaft, deren Wirkung die Schädigung von (elementaren) Bestandteilen der Gesellschaft darstellt.

2. Durch diese Professionalisierung steigen Quantität und Qualität von Cyberangriffen an: Während die eingesetzten Malware-Familien und Angriffskampagnen ausgefeilter und technisch komplexer werden, etablieren sich kompetente und fachkundige Akteure, welche die Infrastrukturen der Underground Economy perfektionieren und so die Grundlage für weitere, ressourcenaufwändige Cyberangriffe ermöglichen.

3. Um maximalen Gewinn zu generieren, richten Cyberkriminelle ihre Angriffe auf Wirtschaftsunternehmen und öffentliche Einrichtungen. Nicht nur, dass die Cyberkriminellen monetär lukrativ erscheinende Institutionen angreifen – auch wissen sie, dass der Ausfall eines dieser Elemente weitreichende Konsequenzen nach sich ziehen und daher Lösegeldforderungen zusätzlicher Nachdruck verliehen werden kann. Mit diesem Kalkül schlagen Cyberkriminelle dort zu, wo es die Gesellschaft am empfindlichsten trifft.

4. Jeder erfolgreiche Angriff dient als Nährboden für die Cybercrime-Szene. Durch den Gewinn monetärer Mittel wächst die Underground Economy, entstehen neue Angebote, werden neue Daten verkauft und neue Akteure treten hervor. Die Wertschöpfungskette beginnt an dieser Stelle – mit einer gestiegenen Intensität – erneut.



Mit Blick auf die Privatwirtschaft, die Betreiber öffentlicher Einrichtungen und KRITIS zeigen diese Entwicklungen auf: Cyberkriminelle werden ihre Angriffe fortsetzen und hierzu eine Vielzahl und hohe Diversität an Angriffsvektoren einsetzen, um Malware-Varianten auf Zielsysteme zu schleusen und dort Daten abzugreifen, zu verschlüsseln oder zu zerstören.

Die Bedrohungslage durch Cyberangriffe stieg im Jahr 2019 stark an und wird sich auch 2020 weiter erhöhen.

Handlungsaufforderungen und Hinweise an ein angemessenes Gefahrenbewusstsein im Cyberraum richten sich jedoch auch an die Bürgerinnen und Bürger: Sie müssen auf ihre Daten im Internet achten und bei E-Mails von Unbekannten skeptisch sein. Darüber hinaus sind regelmäßig Back-Ups durchzuführen, es ist kein Lösegeld zu zahlen und die Polizei zu informieren.

Für Unternehmen gilt, dass ein IT-Sicherheitskonzept unabdingbar ist und die Belegschaft für die Gefahren durch Cybercrime sensibilisiert werden sollte. Eine E-Mail mit einer Ransomware im Anhang etwa kann fatale Folgen für das gesamte Unternehmen haben.

Cybercrime durchdringt die gesamte Gesellschaft – Unternehmen, öffentliche Einrichtungen, kritische Infrastrukturen und auch das Privatleben von Personen werden durch die fortschreitende Digitalisierung im digitalen Raum abgebildet. Dadurch kann grundsätzlich jeder zur Zielscheibe von Cyberkriminellen werden – in Anbetracht des zunehmenden Bedrohungspotenzials der Cyber-kriminalität muss diese demzufolge als gesamtgesellschaftliche Herausforderung betrachtet werden.

Besonders ersichtlich wird dies in der Anpassungsfähigkeit der Cyberkriminellen: Politische Entwicklungen, soziale Bewegungen, öffentliche Diskussionen dienen umgehend als Narrativ für Spam- und Phishing-Mails.

Die Täterseite greift hochflexibel aktuelle gesellschaftliche Entwicklungen auf – dies muss auch für notwendige Sensibilisierungs- und Schutzmaßnahmen gelten.

Das BKA und weitere Sicherheitsbehörden geben Warnmeldungen heraus, wenn eine neue Bedrohungslage identifiziert wurde. So können sich Unternehmen und Bürger schnell über neue Gefahren informieren und entsprechend handeln.

Der Schutz eines Unternehmens vor einem Angriff beginnt aber stets bei den Mitarbeitenden: Diese müssen dahingehend sensibilisiert werden, E-Mails von zweifelhaften Absendern zu löschen oder auch bei ungewöhnlich erscheinenden E-Mails von (vermeintlichen) Partnern skeptisch zu reagieren, bevor Anhänge geöffnet werden.

Die erfolgreiche Bekämpfung von Cybercrime ist auf nationale und internationale Kooperation angewiesen. Cybercrime ist ein Phänomen, das keine nationalen Grenzen kennt, das sowohl Privatpersonen als auch Unternehmen und die Gesellschaft als Ganzes angreift. Nur durch eine ausgeprägte und vertrauensvolle Zusammenarbeit zwischen Strafverfolgungsbehörden, der Wirtschaft, der Wissenschaft, der Justiz und der Politik kann diesem Bereich der Kriminalität effektiv entgegengetreten werden. Der Ausbau dieser Kooperationen steht im Fokus der Cybercrimefachdienststellen der Sicherheitsbehörden von Bund und Ländern.

Cybersecurity und IT-Kenntnisse müssen als Standards der heutigen Gesellschaft erkannt werden.

Mit fortschreitenden Entwicklungen wie dem IoT, der Industrie 4.0 oder der Entwicklung von intelligenter Software wird das Spektrum potenzieller Ziele für Cyberkriminelle stetig erweitert. So sehr der technische Fortschritt das Leben der Menschen im Positiven verändern mag, birgt er immer auch die Möglichkeit einer kriminellen Nutzung, z. B. als „lernende Schadsoftware“.

IT-spezifische Themen, vor allem im Kontext der Cybersecurity, werden im öffentlichen Diskurs mitunter abstrakt diskutiert. Dies hält einen Teil der Bevölkerung ab, sich überhaupt mit derartigen Themen zu beschäftigen. Durch eine breite Aufmerksamkeit für diese Themen kann jedoch die Resilienz der Bevölkerung vor Cyberkriminellen und ihren Methoden gestärkt werden. So wird von Beginn an verhindert, dass Täter erfolgreich agieren.

In der Gesamtschau der sicherheitsbehördlichen und privatwirtschaftlichen Erkenntnisse ist davon auszugehen, dass sich die für das Jahr 2019 festgestellte Erhöhung des Gefahrenpotenzials durch Cybercrime auch 2020 fortsetzen wird.

8 Appendix

8.1 WICHTIGES KOMPAKT

Diebstahl digitaler Identitäten	• Handelsware der Underground Economy • Jede gestohlene digitale Identität ist Nährboden für weitere kriminelle Aktivitäten.
Malware	• *Emotet* bleibt größte Malware-Bedrohung – v. a. im Verbund mit *TrickBot* und *Ryuk* • Anzahl der Malware-Familien steigt stetig an • Professionelles Crypting, das die Malware gegenüber AV-Scannern unsichtbar werden lässt
Ransomware	• Die primäre, existentielle Bedrohung für Unternehmen • Systeme werden nicht mehr nur verschlüsselt – Akteure drohen mit der Veröffentlichung der kryptierten Daten.
DDoS	• Sowohl Quantität als auch Qualität steigend • Vermehrter Nutzen von IoT und Clouds zur Verstärkung von DDoS-Angriffen
Underground Economy	• Arbeitsteilige, hochspezialisierte Wirtschaft • Basiert auf neun Säulen – jede mit ihrem eigenen Fachgebiet • Jede Säule sorgt für den reibungslosen Ablauf von kriminellen Aktivitäten.
Angriffe auf Unternehmen	• APT-ähnliches Verhalten durch kriminelle Organisationen • Schaden durch z. B. einen Ransomware-Angriff liegt im mind. 6-stelligen Bereich

8.2 STRAFTATBESTÄNDE CYBERCRIME IM ENGEREN SINNE

Nachfolgend werden die relevanten Straftatbestände von Cybercrime im engeren Sinne beschrieben.

Computerbetrug als Cybercrime im engeren Sinne (§263a StGB).
Dieses Delikt wird seit 01.01.2016 in der PKS in folgende Betrugsarten aufgeschlüsselt:

- Betrügerisches Erlangen von Kraftfahrzeugen gem. §263a StGB,
- weitere Arten des Kreditbetruges gem. §263a StGB,
- Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten gem. §263a StGB,
- Betrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel gem. §263a StGB,
- Leistungskreditbetrug gem. §263a StGB,
- Abrechnungsbetrug im Gesundheitswesen gem. §263a StGB,
- Überweisungsbetrug gem. §263a StGB.

Sonstiger Computerbetrug (§263a Abs. 1 und 2 StGB sowie Vorbereitungshandlungen gem. §263a Abs. 3 StGB, soweit nicht unter die nachfolgenden Betrugsarten bzw. die „Missbräuchliche Nutzung von Telekommunikationsdiensten“ gefasst).

Ausspähen und Abfangen von Daten einschl. Vorbereitungshandlungen und Daten-Hehlerei (§§202a, 202b, 202c, 202d StGB) umfasst den Diebstahl und die Hehlerei digitaler Identitäten, Kreditkarten-, E-Commerce- oder Kontodaten (z. B. Phishing). Die entwendeten Daten werden i. d. R. als Handelsware auf digitalen Schwarzmärkten zum Kauf angeboten und täterseitig missbräuchlich eingesetzt. Die Verwertung erfolgt damit in zwei Stufen: dem Verkauf der Daten und dem betrügerischen Einsatz erworbener Daten. Auf beiden Ebenen werden erhebliche Gewinne generiert.

Hehlerei (§§202a, 202b, 202c, 202d StGB) umfasst den Diebstahl und die Hehlerei digitaler Identitäten, Kreditkarten-, E-Commerce- oder Kontodaten (z. B. Phishing). Die entwendeten Daten werden i. d. R. als Handelsware auf digitalen Schwarzmärkten zum Kauf angeboten und täterseitig missbräuchlich eingesetzt. Die Verwertung erfolgt damit in zwei Stufen: dem Verkauf der Daten und dem betrügerischen Einsatz erworbener Daten. Auf beiden Ebenen werden erhebliche Gewinne generiert.

Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr (§§269, 270 StGB) -
Diese Tatbestände beinhalten die Täuschung (einer Person) durch die Fälschung von Daten. Durch einen Dateninhaber werden Daten gefälscht bzw. verfälscht und zur Täuschung im Rechtsverkehr genutzt. Dies geschieht z. B. durch die Zusendung von E-Mails unter Vorspiegelung realer Identitäten oder Firmen. Unter Vortäuschung einer Legende soll der Geschädigte z. B. zur Preisgabe von Account-Informationen, Kreditkartendaten oder auch zu Zahlungen bewegt werden. Ebenso erfasst ist das Zusenden von als Rechnungen getarnter Schadsoftware in E-Mail-Anhängen.

Datenveränderung/Computersabotage (§§303a, 303b StGB) – Hierbei handelt es sich um eine Art digitaler Sachbeschädigung. Es wird die Veränderung von Daten in einem Datenverarbeitungssystem bzw. das Verändern des Systems durch andere als den Dateninhaber unter Strafe gestellt. Die §§303a, 303b StGB umfassen typischerweise Denial of Service-Angriffe (DoS-/DDoS-Angriffe), ebenso wie die Verbreitung und Verwendung von Schadsoftware unterschiedlicher Art (Trojaner, Viren, Würmer usw.).

Missbräuchliche Nutzung von Telekommunikationsdiensten (§263a StGB) – Dies ist eine besondere, separat erfasste Form des Computerbetrugs gem. §263a StGB. Unter Ausnutzung von Sicherheitslücken oder schwachen Zugangssicherungen werden sowohl bei Firmen als auch Privathaushalten, z. B. durch den unberechtigten Zugriff auf Router, teure Auslandstelefonverbindungen angewählt oder gezielt Premium- bzw. Mehrwertdienste in Anspruch genommen.

8.3 WIE SICH BÜRGERINNEN UND BÜRGER SCHÜTZEN KÖNNEN

Seien Sie skeptisch bei E-Mails von unbekannten Absendern!

Halten Sie Sicherheitsprogramme und andere Software stets auf dem neusten Stand!

Legen Sie komplexe Passwörter an – "Passwort1234" ist kein sicheres Passwort!

Vertrauen Sie nur offiziellen Webseiten und App-Stores!

Legen Sie regelmäßig Back-Ups Ihres Systems an!

8.4 WIE SICH UNTERNEHMEN SCHÜTZEN KÖNNEN

Entwickeln Sie ein angemessenes IT-Sicherheitskonzept für Ihr Unternehmen

- Entwerfen Sie Verfahrensweisen und Anleitungen, wie sich Ihre Mitarbeitenden im Falle eines Cyberangriffs verhalten sollen.
- Aktualisieren Sie Ihr Sicherheitskonzept regelmäßig.
- Schulen Sie Ihre Mitarbeitenden hinsichtlich Cybersicherheit.
- Legen Sie (vom System getrennte) Back-Ups Ihres Systems an.

Wie Sie helfen können

- Seien Sie zurückhaltend bei der Weitergabe von vertraulichen und persönlichen Informationen.
- Haben Sie gesundes Misstrauen, wenn Ihnen etwas ungewöhnlich vorkommt.
- Überprüfen Sie E-Mails auf die richtige Absenderadresse.
- Öffnen Sie keine verdächtigen E-Mails.
- Seien Sie misstrauisch bei Links oder Anlagen in E-Mails unbekannter Absender.

Maßnahmen nach einer Ransomware-Infektion

- Trennen Sie unverzüglich die Netzwerkverbindung von infizierten Rechnern und schalten Sie betroffene Geräte umgehend aus.
- Isolieren Sie Backups, damit diese nicht ebenfalls verschlüsselt werden.
- Sichern Sie relevante Dateien, die Aufschluss über den Infektionshergang geben können. Hierzu zählen beispielsweise Log-Dateien oder E-Mails.
- Ändern Sie sämtliche Benutzer- und Netzwerkkennwörter, sofern diese durch den Vorfall kompromittiert sein könnten.
- Erstatten Sie unverzüglich Strafanzeige bei Ihrer Zentralen Ansprechstelle Cybercrime (ZAC).

Wenden Sie sich an die Polizei!

- Erstatten Sie auf jeden Fall Anzeige.
- Informieren Sie sich über die ZAC-Dienststellen: https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html
- Wir appellieren dringend, bei Cyberangriffen jeder Art unverzüglich Strafanzeige zu erstatten – erfolgreiche Cyberkriminelle werden Angriffe wiederholen!

Impressum

Herausgeber
Bundeskriminalamt, 65173 Wiesbaden

Stand
September 2020

Gestaltung
Bundeskriminalamt, 65173 Wiesbaden

Bildnachweis
Bundeskriminalamt

Weitere Publikationen 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.