Bundesministerium
Inneres

Bundeskriminalamt

Cybercrime Report 2020

Lagebericht über die Entwicklung von Cybercrime

Cybercrime Report 2020

Cybercrime Report 2020

Lagebericht über die Entwicklung von Cybercrime

Wien 2021

www.bundeskriminalamt.at/cybercrime

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres, Bundeskriminalamt
Josef-Holaubek-Platz 1, 1090 Wien
+43 1 24836 985025 (Single Point of Contact)
bundeskriminalamt.at
Druck: Digitaldruckerei des BMI, Herrengasse 7, 1010 Wien
Wien 2021

Inhalt

Vorwort 5

1 Einleitung 6

Über die Broschüre 7

2 Trends,Entwicklungen und Beispiele 9

Cybercrime im Aufwind 10

Covid-19-Pandemie und ihre Auswirkungen 10

Internetbetrug 11

Crime as a Service 12

Fraud Calls, Cyber Trading Fraud, Investment Scam, Tech Support Scam 13

Phishing 14

Ransomware 14

SIM-Swapping 16

Datenleaks 16

DDoS-Angriffe 17

Call-ID-Spoofing 17

Suchtgifthandel im Darknet 18

Pornographische Darstellungen Minderjähriger 20

3 Recht und Strategie 21

Stärkung der Cybercrimebekämpfung in allen Bereichen 22

Carrier Grade NAT 22

Sicherheitspolizeigesetz und Strafprozessordnung 23

4 Jahresrückblick 25

Zahlen und Fakten im Überblick 26

Cybercrime im engeren Sinn 27

Cybercrime im weiteren Sinn 28

Dunkelziffer und Anzeigeverhalten 29

5 Aufbauorganisation und Abläufe 31

Drehscheibe und wichtige Ansprechstelle 32
C4-Meldestelle 32
C4-Forensik 34
Entwicklung und Innovation 36
Wissensvermittlung durch Ausbildung und internationalen Austausch 37
Zentrale Anfragestelle für Social Media und Online Service Provider (ZASP) 38
Zusammenarbeit mit der Polizei 39
6 Kriminalprävention 41
Schulter an Schulter mit dem Digitalisierungsministerium 42
7 Zusammenfassung und Ausblick 46
8 Summary and Outlook 49
9 Glossar 51

Vorwort

Liebe Leserinnen, liebe Leser!

Bundesminister für Inneres
Karl Nehammer, MSc
und Direktor des
Bundeskriminalamtes
General Mag. Andreas
Holzer, MA

Cybercrime ist ein Deliktsfeld, das immer weiter zunimmt und uns vor immer neue Herausforderungen stellt. Covid-19 hat auch diesen Deliktsbereich maßgeblich bestimmt: Die Verlagerung des realen Lebens in die virtuelle Welt hat Cyberkriminellen einen Nährboden bereitet. Besonders die Schließungen des stationären Handels hat Auswirkungen auf den Internetbetrug und mangelnde Sicherheitsvorkehrungen begünstigten Cyberattacken auf Heim- und Arbeitsnetzwerke. Durch die Digitalisierung und den Zugang zu Diensten, wie „Crime as a Service“ oder technischen Neuerungen haben es die Täter einfacher ihre Reichweite zu steigern, wodurch auch erhöhte Schadenssummen entstehen.

Um dieses Kriminalitätsfeld nachhaltig zu bekämpfen, müssen Rahmenbedingungen laufend angepasst werden. Ebenso braucht es dazu die notwendigen personellen, technischen und logistischen Ressourcen sowie eine Stärkung der Widerstandsfähigkeit gegen kriminelle Cyberangriffe. Eine erhöhte Bewusstseinsbildung für mehr Sicherheit und Eigenverantwortung sowie eine schnelle und wirksame Reaktion auf Cybervorfälle müssen ebenfalls garantiert werden.

Die politischen und rechtlichen Rahmenbedingungen sind für diese Thematik global sehr unterschiedlich. Das Bemühen für die im Bericht genannten, konkreten Problembereiche auch umfassende, strategische Ansätze zu entwickeln, muss weiterhin forciert werden.

Kriminalpolizeilich werden weiterhin jene operativen Maßnahmen umgesetzt, die im Rahmen der vorgegebenen, strategischen Leitlinien von EU-Cybersicherheitsstrategien, nationalen Strategien im Bundeskanzleramt und innerhalb des Bundesministeriums für Inneres entwickelt werden.

Ihr

Karl Nehammer, MSc
Bundesminister für Inneres

General Mag. Andreas Holzer, MA
Direktor des Bundeskriminalamtes

1 Einleitung

Über die Broschüre

Der vorliegende Bericht soll den alljährlichen Überblick in die komplexen Themenbereiche von Cybercrime bieten und aufzeigen, wo die größten Herausforderungen für die Exekutive liegen. Betrachtet werden hier nur die in Österreich geltenden Definitionen und Abgrenzungen von Cyberkriminalität. Die Aufgaben der Cybersicherheit und der Cyberabwehr unterliegen den Verantwortungen anderer Organisationen.

Die Ergebnisse aus den Analysen basieren auf Untersuchungen von Informationen, die in der fachlichen Zentralstelle des Bundeskriminalamtes (BK), dem Cybercrime Competence Center (C4) zusammenlaufen und auf gesammelten Meldungen, Anzeigen, Statistiken, internationalen Kooperationen, Informationsaustausch mit Mitgliedstaaten, Ausbildungen, Positionspapieren sowie Studien von Dritten. Die Bestandsaufnahme der quantitativen Daten und qualitativen Inhaltsanalysen fand zwischen Jänner und März 2021 statt, wobei die eingetretenen Entwicklungen von Jänner bis Dezember 2020 berücksichtigt wurden.

Die wichtigsten Phänomene werden im Detail beschrieben und fallweise mit vorbeugenden Handlungsempfehlungen ergänzt. Zudem werden die rechtlichen Rahmenbedingungen und hiermit einhergehende Herausforderungen des kriminalpolizeilichen Alltags dargestellt.

Der Jahresrückblick mit den kriminalstatistischen Analysen ist ein wesentlicher Faktor für die strategische Ausrichtung zur Kriminalitätsbekämpfung und wird als Grundlage für die Fokussierung auf die kontinuierliche Verbesserung der präventiven und repressiven Maßnahmen herangezogen. Trotz des erneut hohen Anstiegs von Cybercrime-Delikten von 26,3 Prozent im Vergleich zum Vorjahr konnte die Aufklärungsquote mit 33,4 Prozent annähernd konstant gehalten werden. Insgesamt wurden 2020 im Vergleich zu 2019 bei absoluter Betrachtung 1.820 Straftaten mehr aufgeklärt. Die von Jahr zu Jahr steigende Zahl der Anzeigen stellt die zuständigen Organisationseinheiten des BK vor große personelle und technische Herausforderungen, wobei sich gerade die Personalrekrutierung als durchwegs schwierig gestaltet.

Die Aufbauorganisation und ihre Abläufe sind auch aufgrund der technischen Komplexität mit ständigem Wissensaufbau und einhergehender Spezialisierung sehr flexibel gestaltet. Das C4 möchte mit der ausgeübten zentralen Fachaufsicht einen Einblick in Vorgehensweisen geben und das Anzeigeverhalten in der Bevölkerung verbessern.

Der Wissensaufbau übernimmt mittels Ausbildungskonzepten und durchgeführten Schulungen einen wichtigen Stellenwert in der strategischen Ausrichtung zur Bekämpfung von Cybercrime. Im C4 wurden neben der Gremienarbeit mit Europol und Interpol auch wichtige Veranstaltungen mit internationaler Beachtung organisiert. So wurde eine

internationale Konferenz für Ermittlungen bei Transaktionen virtueller Währungen veranstaltet sowie zahlreiche Schulungen abgehalten.

Die Dunkelziffern im vorgegeben Deliktsbereich werden als sehr hoch eingeschätzt. Um wichtige Ermittlungshinweise durch Anzeigeerstattungen zu erhalten, sollen eine hohe Transparenz und eine illustrierte Erklärung von Abläufen helfen, möglichen Ängste, Scham oder Hemmungen bei Geschädigten zu überwinden.

Da Ermittlungsansätze im Zuge der Strafverfolgung aufgrund von steigender Anonymisierung zunehmend begrenzt werden, wird weiterhin vermehrt auf die Eigenverantwortung der Userinnen und User gesetzt und ein Fokus auf präventive Maßnahmen in der Bevölkerung gesetzt.

Informationen zu kriminalpräventiver Arbeit sowie einen strategischen Ausblick für das Thema Cybercrime und die Zusammenfassung des Berichtes runden den Cybercrime Report 2020 ab.

2 Trends, Entwicklungen und Beispiele

Cybercrime im Aufwind

Zu Beginn des Jahres 2020 stiegen die Angriffe auf Computersysteme oder Netzwerke mit Hilfe von Schadsoftware erneut an. Ebenso läuteten zahlreiche Erpressungsversuche auf Unternehmen unter Verwendung pornografischer Darstellungen Minderjähriger sowie Kontaktdaten und Lichtbilder der erpressten Empfängerinnen und Empfänger das neue Jahr ein.

Das bereits im Vorjahr aufgetauchte Phänomen von widerrechtlichen Zugriffen mittels alter, wiederverwendeter E-Mail-Adressen und Online Accounts von sozialen Medien sowie Zahlungs- und Webshopping-Dienstleistern, setzte sich 2020 fort. Widerrechtliche Zugriffe auf Online Accounts nahmen aufgrund von Datenleaks ebenfalls zu. Die Deliktsbereiche zum Internetbetrug, insbesondere jene mit Covid-19-Bezug, Datenleaks, Ransomware, Verbreitung von Remote Access Trojaner (RATs) und Distributed Denial of Service-Angriffe (DDoS-Angriffe) waren die größten Herausforderungen im vergangenen Jahr.

Die massive Steigerung der Deliktsformen im Bereich Cybercrime im weiteren Sinn sind auf den ganzjährig auftretenden Internetbetrug, dem Anstieg der sonstigen Kriminalität im Internet (besonders die Paragraphen 207a, 208a Srafgesetzbuch) und einer seit Jahren zunehmenden Verlagerung des Suchtgifthandels in den digitalen Raum zurückzuführen. Auch Straftaten in Zusammenhang mit § 3g Verbotsgesetz stiegen an. Erpressungen konnten aufgrund intensiver Ermittlungsarbeit und der Etablierung einer eigenen Arbeitsgemeinschaft „ARGE Erpressungsmails“ erfolgreich zurückgedrängt werden. Der Internetbetrug wurde fokussiert und kooperierend im Rahmen der Linienorganisation bearbeitet. Darüber hinaus zeigte sich bei den Tätern weiterhin ein Trend zur Nutzung von Ransomware, RATs, eBanking Trojaner und anderen maßgeschneiderten Crime as a Service-Leistungen (CaaS).

Die markanten Entwicklungen im Bereich Cybercrime sind aber auch auf die geänderten Lebensbedingungen und Verhaltensweisen während der anhaltenden Covid-19-Pandemie zurückzuführen.

Covid-19-Pandemie und ihre Auswirkungen

Ab dem ersten Quartal 2020 war das weitere Geschehen von der Pandemie geprägt. Nach Neuregistrierung mehrerer tausender Domains wurde in Zusammenhang mit Covid-19 eine starke Zunahme betrügerischer Webseiten zwecks Phishing beziehungsweise der Verbreitung von Schadsoftware beobachtet. So wurden beispielsweise Erpressungs-E-Mails versendet, in denen die Opfer zur Zahlung von 4.000 US-Dollar in Form von Bitcoins aufgefordert wurden, da ansonsten deren Familien mit Covid-19 infiziert würden.

Durch Malspam, Phishing und Ransomware teilte man in zahlreichen Aussendungen von Fake-E-Mails vermeintlicher Paketzustelldienste mit, dass aufgrund von Covid-19 keine Zustellungen möglich seien und die E-Mail-Empfängerin oder der -Empfänger entweder per Direktlink oder per Dateianhang die Optionen zum Paketempfang auswählen könne. Beim Öffnen des Links beziehungsweise Dateianhangs wurde dann die Schadsoftware am Zielcomputer installiert.

Zeitgleich mit dem ersten Lockdown folgte eine starke Abnahme der Anzeigen in allen Deliktsbereichen, was in erster Linie auf die Ausgangsbeschränkungen und auch dem damit einhergehenden geänderten Anzeigeverhalten der Bevölkerung zurückzuführen ist. Mit Sommerbeginn häuften sich aber die Verdachtslagen vor allem im Zusammenhang mit Phishing- und Schadsoftwarefällen.

Generell erfuhr der Bereich Cybercrime durch das allgemeine Social Distancing auch einen starken Anstieg von Betrugshandlungen durch Love Scam oder „Stranded Travellers“.

In Fakeshops, aber auch über handelsübliche, reguläre Plattformen wurden vermehrt Betrugshandlungen mit Desinfektionsmitteln und Atemschutzmasken sowie Fake Apps und Bank-Trojanern wahrgenommen.

Allgemein wurde über die letzten Jahre ein sehr starker Anstieg bei Internetbetrugsdelikten verzeichnet. Aufgrund zunehmender Arbeitsteilung und Vernetzung der Tätergruppen, besonders im Bereich von Ransomware, wird eine erfolgreiche Strafverfolgung erschwert.

Internetbetrug

Die Vorgehensweisen im Bereich des Internetbetrugs umfassen eine Vielzahl von Modi Operandi, die von Anlagebetrügereien, Gewinnversprechen bis zu vorgetäuschten Warenlieferungen reichen. Das Medium Internet wird dabei als ein Werkzeug zur Begehung der Tat eingesetzt. Dies bedeutet für die Täter, dass sie nicht nur die Möglichkeiten der Anonymität und der Verschleierung der eigenen Identität nutzen, sondern auch mit wenig Aufwand mit einer Vielzahl von potenziellen Opfern rasch und unkompliziert weltweit in Kontakt treten können.

In diesem Deliktsfeld scheint besonders wichtig, dass gerade durch präventive Maßnahmen Schäden verhindert werden können. Die Realität hat in den letzten Jahren gezeigt, dass repressive Handlungen und Maßnahmen durch die Kriminalpolizei zur Aufklärung der Tat durch die fast immer notwendigen internationalen Ermittlungsschritte häufig erschwert werden. Das BK setzt daher neben der Präventionsarbeit auch auf eine

intensive Zusammenarbeit zwischen der Bevölkerung, der Privatwirtschaft und der Polizei, um den Internetbetrug in allen seinen Facetten effektiv zu bekämpfen.

Auch im Bereich des Internetbetrugs waren auch Auswirkungen der Covid-19-Pandemie spürbar. Nachdem der klassische analoge Betrug aufgrund der verhängten Lockdowns abgenommen hatte, verzeichnete der Internetbetrug übers Jahr gesehen weiter Zuwächse. Diese Zunahmen sind jedoch nicht Covid-19 zuzuschreiben. So zeigt sich, dass aus der Pandemie kein neuer Modus Operandi per se abgeleitet wurde, jedoch wurden alt bekannte Vorgehensweisen durch die Täter auf die Pandemie und ihre Auswirkungen adaptiert.

Der Internetbetrug hat 2020 mit 18.780 Anzeigen einen neuen Höchststand erreicht. Auf Basis der Vorjahreszahlen ergibt das eine Steigerung um 1.949 Anzeigen zum Jahr 2019. Auf den gesamten Bereich Cybercrime gerechnet, stellt somit der Internetbetrug den größten Teil der Anzeigen im Deliktsbereich dar. Bei der Aufklärungsquote im Bereich Internetbetrug ist 2020 mit 35,3 Prozent nur ein durchschnittliches Ergebnis erzielt worden. Wie auch in den vergangenen Jahren muss dies auf die Verschleierungsmöglichkeiten der Täter im Internet und der zunehmenden Professionalisierung der Tätergruppierungen zurückgeführt werden.

Zusätzlich ist gerade beim Internetbetrugs zumeist von Massendelikten auszugehen. Die spezialisierten Tätergruppierungen gehen arbeitsteilig, technisch versiert und dementsprechend überlegt vor. In diesem Deliktsfeld wird durch den zuständigen Fachbereich des BK besonders im Bereich Bestellbetrug ein Schwerpunkt gesetzt. Dabei stehen betrügerische Bestellungen über das Internet bei österreichischen Onlinehändlerinnen und -händler im Fokus. Im letzten Jahr wurde diesbezüglich wieder gemeinsam mit Europol die „E-Commerce Action Week“ abgehalten. Aufgrund des gemeinsamen Zieles den Bestellbetrug in Europa zu bekämpfen, wurde der Fokus 2020 auf die Prävention und die Aufklärung von Onlinehändlerinnen und -händlern gerichtet. Dazu wurde gemeinsam mit dem österreichischen Handelsverband die Sicherheitsstudie durchgeführt, diese auch medial präsentiert und mit einer Informationsveranstaltung kombiniert. Ziel der Maßnahme war es einerseits den Onlinehändlerinnen und -händlern Möglichkeiten zum eigenen Schutz aufzuzeigen, andererseits aber auch Möglichkeiten zum Austausch zwischen der Privatwirtschaft und der Polizei im Rahmen des Projekts Gemeinsam.Sicher zu geben.

Crime as a Service

Die angebotenen Leistungen von CaaS-Diensten nehmen im Internet weiterhin zu. Dabei handelt es sich vorwiegend um Hackingtools, Schadsoftware, wie beispielsweise Verschlüsselungstrojaner, aber darüber hinaus auch um spezielle Dienstleistungen zur Geldwäsche, für Übersetzungen oder für den Opfer-Support. Auch die Nutzung von Bot-Netzwerken, die DDoS-Angriffen oder zum Versand von Spam-E-Mails dienen, konnte vermehrt registriert werden. Ebenso wurde ein Anstieg beim in Verkehr bringen von Falschgeld, Online-Kindesmissbrauch, Kreditkartendaten und gefälschten Urkunden bemerkt.

Durch die im Darknet angebotenen Dienste stiegen vor allem Massenerpressungs-E-Mails und gezielte Erpressungen durch Ransomware mit Bitcoin-Forderungen an. Die Täterschaft benötigte damit keinesfalls mehr tiefgreifendes Wissen zur technischen Durchführung, sondern konnte sich durch CaaS-Leistungen das fehlende Wissen zukaufen. Mit einem Ransomware as a Service Modell (RaaS) lassen sich nach wie vor beträchtliche Gewinne erzielen.

Fraud Calls, Cyber Trading Fraud, Investment Scam, Tech Support Scam

Betrügerinnen und Betrüger gehen mit der Zeit und finden immer wieder Wege Geld von ihren Opfern zu bekommen. 2020 nutzten die Täter die Covid-19-Pandemie, die in der Bevölkerung große Verunsicherungen auslöste und brachten viele Menschen um ihr Erspartes. Im Folgenden wird auf einige Betrugsarten kurz eingegangen:

Stromkundinnen und -kunden wurden 2020 Opfer von Fraud Calls. Mit der richtigen Nennung der Internationalen Bankkontonummer (IBAN), der Höhe der letzten Stromrechnung und weiteren wahrheitsgemäßen Details schufen die Betrügerinnen und Betrüger eine Vertrauensbasis, wodurch ihnen die Kundinnen und Kunden leichter zum Opfer fielen.

Ebenso konnte ein Anstieg des CEO-Frauds mit Beginn der Jahresmitte 2020 beobachtet werden. Der im Herbst erneut festgestellte Cyber Trading Fraud oder Investment Scam erzeugte finanzielle Schäden in Millionenhöhe. Der Erstkontakt erfolgte hierbei über das Telefon, Online-Werbungen, Social Media oder E-Mails. Anschließend wurden die Opfer unter falscher Versprechung hoher Gewinne, vor allem in den Bereichen Forex Trading, Handel mit binären Optionen oder bei Investitionen in Kryptowährungen, zu immer höheren Investments gedrängt.

Unabhängig von Covid-19 waren Trading-Fraud beziehungsweise Anlagebetrügereien in Verbindung mit Kryptowährungen zu verzeichnen, wobei weiterhin massiv mit hohen Investitionsgewinnen im Zusammenhang mit Kryptowährungen wie Bitcoins geworben wurde. Im Spätsommer 2020 wurden auch SMS-Nachrichten vermehrt zum Daten-Phishing verwendet: Es kursierten mehrere Spam-Kampagnen, die einen Hinweis auf eine angebliche Zustellbenachrichtigung und weiterführende Links enthielten. Hierbei wurde

zu Portonachzahlungen von 1,50 Euro aufgefordert, wobei das wahre Ziel der Täterschaft das Phishing von Kreditkartendaten war.

2020 wurden auch weiterhin zahlreiche Fälle von Tech Support Scam („Microsoft Betrug“) zur Anzeige gebracht. Dabei wurden die Opfer entweder gleich direkt telefonisch kontaktiert oder es erschien am Gerät des Anzeigers eine Warnmeldung, dass der Computer kompromittiert sei und ein zertifizierter Support als Unterstützung für die Bereinigung zur Verfügung stehe. In weiterer Folge wurde das Opfer vom „Support Mitarbeiter“ überzeugt, vollen Zugriff auf das eigene Gerät (Computer, Smartphone, Tablet und dergleichen) zu erteilen, bei dem nicht nur die Daten des Opfers gestohlen wurden, sondern auch im Fall einer Nichtzahlung der Gebühren das Gerät gesperrt bleiben würde.

Ebenso wurde ab Mitte November 2020 vielfach versucht, WhatsApp Accounts von Userinnen und Usern zu stehlen, um damit weitere Betrugshandlungen durchzuführen. Gegen Jahresende war auch wieder die saisonal beobachtbare Anzahl an kriminellen Webshops (Fake- und Phishing-Shops) in der Vorweihnachtszeit deutlich angestiegen. Auch waren wieder zahlreiche Spamwellen mit Erpressungs-E-Mails (Sextortion) und E-Mails mit Phishing von Bankdaten im Umlauf.

Phishing

Phishing E-Mails oder -Webseiten traten 2020 gehäuft in Erscheinung. Der berühmteste Fall war der Betrug mit FinanzOnline: E-Mails mit der falschen Absende-E-Mail-Adresse finanzOnline@bmf.gv.at versprachen Steuerrückerstattungen von über tausend Euro. Folgte man dem Link, gelangte man auf eine Phishing-Webseite, die die Eingabe von persönlichen Informationen und Kreditkartendaten forderte.

Alle größeren Bankinstitute in Österreich waren mittels Phishings von Zugangsdaten für eBanking betroffen, wobei mit schädlichen Android-Applikationen mobile TANs für das Onlinebanking abgegriffen wurden. Besonders im Rahmen der Anubis Android-Malware waren mehrere Phishing- und Malware-Verbreitungskampagnen im Umlauf. Der Link zur Phishing-Seite lässt sich nur über Android-Browser (Android User Agent) öffnen. Nach Eingabe der Daten erfolgte die Aufforderung zum Download einer sogenannten Sicherheits-App.

Ransomware

Ransomware wurde in den letzten Jahren zu einem der wichtigsten Werkzeuge von Cybercrime-Tätern. Ransomware verschlüsselt Nutzerdaten, um für deren Wiederherstellung die Bezahlung von Lösegeldern, meist in Form von Bitcoins, zu fordern. Es existieren mittlerweile zahlreiche Varianten mit unterschiedlichen Verbreitungswegen und verschiedenen Verschlüsselungsalgorithmen. Die Gefahr eigene Daten durch eine Schadsoftware zu verlieren, indem diese verschlüsselt und zum Zeitpunkt der Verschlüsselung vorhandene Sicherungen unbrauchbar gemacht werden, ist nach wie vor noch sehr hoch.

Auch 2020 führte die zentrale Bearbeitung von Ransomware-Fällen zur erfolgreichen Ermittlung von Tatverdächtigen. Ein Schwerpunkt galt den Organisationsstrukturen zum Vertrieb von Ransomware, die ebenfalls erforscht werden konnten. Die Angriffe richteten sich vorwiegend gegen kleine und mittlere Unternehmen (KMU) und weniger gegen Einzelpersonen, wodurch sich das Risikopotential für die österreichische Unternehmenslandschaft deutlich erhöhte.

Als primäre Infektionsquellen gelten:

- Fernzugriffe, die für Firmen für die Fernwartung und Datenzulieferung häufig notwendig sind,
- E-Mails mit schädlichem Dateianhang oder mit Links über die Schadsoftware nachgeladen wird,
- Schadsoftware über die die Verschlüsselungssoftware nachgeladen wird, zum Beispiel Emotet sowie
- zahlreiche andere Wege sich mit einem Verschlüsselungstrojaner infizieren zu können, wie beispielsweise Drive-by-Downloads, Supply Chain Attacks oder Malvertising

Die Täter gingen auch 2020 zielgerichtet gegen ihre Opfer vor und mit einer technischen Kompromittierung des Computersystems des Opfers von durchschnittlich vierzehn Tagen wurden auch deren Methoden viel aufwendiger und ausgeklügelter. So wurden die Höhen von Erpressungssummen an den Umsatz und die Verschlüsselungsprozesse an die Backup-Strategien ihrer Opfer angepasst.

Zusammenfassung aktueller Informationen zu Ransomware:

- Ransomware bleibt eine der größten Gefahren im Internet, um persönliche Daten zu verlieren.
- Bestehende Varianten von Ransomware werden technisch ständig weiterentwickelt und der Modus Operandi, vom Weg der Infektion bis zur Lösegeldforderung, den Umständen und Opfern flexibler angepasst.
- Angriffe mit Ransomware erfuhren auch im letzten Jahr eine zielgerichtete Spezialisierung auf Unternehmen, bei denen die Geldforderungen der Täterschaft an die wirtschaftliche Leistungsfähigkeit beziehungsweise an die vorhandene IT-Infrastruktur mit ihren Backup-Lösungen angepasst wurden.

- Die Infektion in Unternehmen hatte immer häufiger den Ursprung in einer anderen Schadsoftware (Trojaner), die wochen- oder monatelang vor der eigentlichen Datenverschlüsselung das komplette Netzwerk oder Computersystem ausspäht.
- Die Angriffe lassen immer öfter auf großes Fachwissen und Kenntnisse organisierter Tätergruppen beziehungsweise Anbietern von RaaS schließen.
- Um Druck zur Zahlung auszuüben, wurden Veröffentlichungen sensibler Daten angekündigt und auch durchgeführt.
- Lösegeldverhandlungen werden nicht mehr nur im Darknet, sondern auch telefonisch geführt.

SIM-Swapping

Mit der SmartCash-Funktion ist es möglich, an Geldausgabeautomaten, die sich zum Beispiel im Foyer von Bankfilialen befinden, ohne Bankomatkarte Geld zu beheben. Dies geschieht mittels eines Zahlencodes (mobile PIN), der auf das Mobiltelefon gesendet wird. Im Zuge von Ermittlungen nach betrügerischem Datenverarbeitungsmissbrauch konnten 17 Tatverdächtige ausgeforscht und 15 davon in mehreren europäischen Ländern festgenommen werden. Diese wandten SimSwapping Techniken an, um die Rufnummern von Mobiltelefonen umzuleiten. Dadurch erhielten die Täter den Zahlencode, um bei Bankomaten ohne Bankkarte Geldbeträge von den Konten ihrer Opfer abzuheben.

Datenleaks

Der bereits in den letzten Jahren bemerkbare Trend setzte sich auch 2020 fort. Mitte des Jahres fand eine Verschiebung von Ransomware-Angriffen hin zu Datenleaks statt, mit denen Lösegeld von Unternehmen erpresst werden sollte. So nahm die Anzahl von Einbrüchen in Computernetzwerke von Unternehmen, bei denen unbekannten Täter Unternehmensdaten extrahierten und dann Lösegeld erpressten, zu. Im Fall von Nichtzahlung wurden Daten tatsächlich über Tor-Seiten veröffentlicht. Durch die Häufung verschiedener Datenleaks erhöhte sich auch die Anzahl der Anzeigen wegen widerrechtlichen Zugriffs auf Benutzerkonten bei Online Service Providern (OSP). Die Zugangsdaten wurden anschließend von den Tätern meistens in betrügerischer Absicht verwendet. Der Missbrauch von Zugangsdaten mittels Credential Stuffing zählte zu den meist genutzten kriminellen Angriffswerkzeugen im Netz. Die entwendeten Daten lösen oftmals auch Jahre später Folgekriminalität aus.

DDoS-Angriffe

National wie international wurden ab Herbst mehrere Wellen von DDoS-Angriffen vor allem im Banken- und Finanzsektor und auf Internetanbieter (ISPs) gemeldet. In einigen Fällen handelte es sich um Trittbrettfahrer, die in den Erpresserschreiben Namen bekannter Tätergruppen, wie Fancy Bear oder Lazarus verwendeten. Beobachtet wurden dort bis zu 100 GBit/s teilweise wurden Wochen später weitere Kontaktaufnahmen durch die Täter beobachtet. Andere beharrliche Tätergruppen erreichten auch deutlich höhere Angriffsbandbreiten.

Call-ID-Spoofing

Als gängige Vorbereitungshandlung für klassische Betrugshandlungen, aber auch für den stark ansteigenden Internetbetrug, wurden die operativen Ermittlungsbereiche in den Landeskriminalämtern (LKA) vermehrt auf das Tatmittel des Call-ID-Spoofing aufmerksam.

Beim Call-ID-Spoofing werden oftmals, aber nicht ausschließlich, Callcenter im Ausland engagiert, um sich zunächst der Daten einer angerufenen Person noch einmal zu vergewissern. Meist stammen die Namen und angerufenen Telefonnummern aus Listen von (un)seriösen Datenhändlerinnen und -händlern oder Quellen im Darknet. Diese Callcenter senden zumeist eine falsche Telefonnummer (Caller-ID) mit, um ihre wahre Herkunft zu verschleiern und somit auch eine mögliche Rückverfolgung zu erschweren. Die Täter gehen hier meist ungezielt vor und lassen diese Listen sogar automatisiert von ihren sehr freundlich wirkenden Mittätern abarbeiten. Dies dient oft einer schnellen Auswahl an möglichen Opfern. Es werden falsche Telefonnummern beispielsweise mit einer österreichischen Vorwahl mitgesendet, um falsches Vertrauen zu wecken. Mittlerweile können die Nummern dieser Callcenter für jeden einzelnen Anruf automatisch generiert werden.

Klassische Tatmodi, bei denen Call-ID-Spoofing verwendet wird, sind telefonische Gewinnzusagen, Cyber Trading Fraud, CEO-Fraud oder es werden unberechtigt ausstehende Beträge aus angeblichen Käufen oder Verträgen eingefordert. 2020 gab es ab dem Herbst einen deutlichen Anstieg von Anruferinnen und Anrufern, die sich vor allem im Osten Österreichs als Kriminalpolizistinnen und -polizisten ausgaben und mit Hinweis auf die Pandemie meist ältere Personen mit angekündigten Abholungen von Geldbeträgen und Sachwerten um ihr Vermögen brachten. In diesem Zusammenhang konnten Personen von international kooperierenden Tätergruppen angezeigt und festgenommen werden.

Diese Anrufe werden über die Voice-over-IP (VoIP) Technologie abgewickelt und teilweise über Server in exotische Länder ohne Abkommen zur internationalen Strafverfolgung weitergeleitet. Damit sind weiterführende Erhebungen stark erschwert. Dies ist ebenfalls ein Grund, warum auch bei diesem Phänomen der kriminalpolizeiliche Schwerpunkt sehr stark auf der Prävention liegt.

Suchtgifthandel im Darknet

Der Onlinehandel mit verbotenen Substanzen hat sich mittlerweile zu einer gängigen Begehungsform der Suchtmittelkriminalität entwickelt. Sowohl Einzeltäter als auch kriminelle Organisationen bedienen sich des Darknets zur Abwicklung ihres organisierten Suchtmittelhandels und generieren damit ihre illegalen Gewinne. Von der Kontaktaufnahme über Verkaufsverhandlungen bis hin zur Bezahlung wird der gesamte Ablauf über verschlüsselte Netzwerke abgewickelt. Ermittlungen zeigen bislang, dass der Online-Drogenhandel den Straßenhandel nicht verdrängt. Vielmehr wird der Handel auf Online-Plattformen dazu genutzt, illegale Suchtmittel höherer Qualität zu erwerben, um diese im Straßenverkauf gewinnbringend weiterzuverkaufen. Der klassische Straßenhandel wird somit durch den Internethandel erweitert und ergänzt. Wie sehr Österreich vom Online-Suchtmittelhandel betroffen ist, zeigen die nachstehenden Zahlen. Seit September 2016 werden durch den deutschen Zoll Schwerpunktkontrollen bei den zu exportierenden Briefsendungen durchgeführt. Dabei wurden im internationalen Briefzentrum Frankfurt am Main bisher etwa 28.500 Briefsendungen durch das Zollfahndungsamt sichergestellt, die insgesamt rund 2.000 Kilogramm Suchtmittel beinhalteten. Adressiert waren die Briefsendungen an Empfängerinnen und Empfänger aus über 90 verschiedenen Nationen. Dabei belegte Österreich seit Beginn der Kontrollen, gemessen an der Anzahl der Empfängerinnen und Empfänger, den zweiten Platz hinter den USA und liegt vor Destinationen, wie Großbritannien, Frankreich oder Australien. Seit dem zweiten Halbjahr 2019 führt Österreich die Reihung sogar konstant an erster Stelle an. Die für Österreich bestimmten Postsendungen enthielten insgesamt über 240 Kilogramm Suchtgift, hauptsächlich Amphetamin und MDMA, einschließlich 38.000 Stück Ecstasy-Tabletten und 1.200 LSD-Trips. Auch in Österreich werden im Zuge von Kontrollen regelmäßig Postsendungen mit illegalen Suchtmitteln sichergestellt. Die Folgeermittlungen zu den bisherigen Sicherstellungen ergaben, dass das Suchtgift der aufgegriffenen Briefsendungen ausschließlich über Darknet-Marktplätze bestellt wurde. Etwa 80 Prozent der in Österreich sichergestellten Postsendungen wurde aus den Niederlanden versandt.

Um dieser Begehungsform der Suchtmittelkriminalität entgegenzutreten, wurde zu deren Bekämpfung bereits 2018 ein spezialisiertes Referat im Büro zur Bekämpfung der Suchtmittelkriminalität im BK eingerichtet. Dieses führt unter anderem schwerpunktmäßig Ermittlungen gegen in Österreich aufhältige Online-Suchtmittelhändlerinnen und -händler und koordiniert die polizeilichen Maßnahmen gegen die Käuferinnen und Käufer.

Neben den operativen Ermittlungsmaßnahmen werden durch das Fachreferat, teils im Wege des internationalen polizeilichen Informationsaustausches, fortwährend neue Strategien entwickelt und aktuelle Entwicklungen analysiert. Dadurch konnte festgestellt werden, dass zur Bekämpfung dieser Kriminalitätsform, die Zerschlagung der Vertriebswege eines der effektivsten Mittel darstellt. Die auf Darknet-Marktplätzen veräußerten Suchtmittel, werden in erster Linie über den herkömmlichen Postweg versandt. Daher werden seit Beginn 2020 die operativen Ermittlungen mit Schwerpunktkontrollen der Postwege kombiniert. Diese Kontrollmaßnahmen werden in enger Kooperation mit der österreichischen Zollverwaltung durchgeführt. Um auch seitens der Kriminalpolizei den dadurch entstandenen Mehraufwand abdecken zu können, wurde mit Jänner 2020 die Arbeitsgemeinschaft „FLAVUS“ innerhalb des genannten Fachreferats installiert.

Auswirkungen der Covid-19-Pandemie auf den Online-Suchtmittelhandel

Im Bereich des Suchtmittelhandels über Darknet-Marktplätze konnte hinsichtlich der Covid-19-Situation im Jahr 2020 betreffend Österreich Folgendes festgestellt werden:

Allgemeine und internationale Erkenntnisse

- Die Online-Suchtmittelhändlerinnen und -händler (Vendoren) befürchteten eine mögliche Verstärkung der Kontrollen von Paketsendungen und Verzögerungen bei der Zustellung von Postsendungen.
- Einige Vendoren versenden seitdem nur mehr im eigenen nationalen Bereich.
- Es gab Beschwerden von Abnehmerinnen und Abnehmern über nicht erhaltene Bestellungen beziehungsweise dass bei Verlust kein Ersatz versandt wurde. Es war eine vermehrte Unzufriedenheit unter den Käuferinnen und Käufern zu bemerken. Es stand der Vorwurf im Raum, die Händlerinnen und Händler würden die Covid-19-Situation als Ausrede für nicht erhaltene Bestellungen nutzen.
- Es kann davon ausgegangen werden, dass es durch die beschränkten Liefermöglichkeiten zu einem Engpass bei der Zulieferung von Drogenausgangstoffe für die Herstellung synthetischer Suchtmittel kam. Dies wirkte sich deshalb vor allem auch auf den Online-Suchtmittelhandel aus, da über die Darknet-Marktplätze in erster Linie synthetische Suchtgifte vertrieben werden.

Nationale Erkenntnisse

- Grundsätzlich konnte festgestellt werden, dass sich die Anzahl der bisher aktiven und bekannten österreichischen Vendoren auf den gängigen Darknet-Marktplätzen verringerte. Dies dürfte auf die Covid-19-Situation allgemein sowie auf die verstärkt durchgeführten Maßnahmen seitens Polizei und Zoll zurückzuführen sein.

- Auch die in Österreich ortsansässigen Vendoren nahmen Abstand von ihrem bisher international geführten Handel und belieferten zum größten Teil nur mehr ihre Kundschaft im Inland.
- Eine Zu- oder Abnahme in den Verkaufszahlen konnte jedoch nicht festgestellt werden.
- Es wurden nach wie vor die klassischen Suchtmittel sowie auch neue psychoaktive Substanzen angeboten.
- Die Preise waren stabil und unverändert.

Conclusio

- International waren in der Darknet-Community verzögerte oder nicht erhaltene Lieferungen gehäuft Thema. Ansonsten konnten keine bemerkenswerten Veränderungen festgestellt werden.
- Mit den Spezialisten des C4 werden in diesem Zusammenhang die Fachbereiche des BK sowie die LKA tatkräftig bei der Ausforschung von Tätern unterstützt.
- Die speziell in diesem Bereich eingesetzten Kriminalisten des C4 nahmen zusätzlich mehrmals an international, im Rahmen von Europol durchgeführten Amtshandlungen, wie zum Beispiel der Darknet Action Week teil.

Pornographische Darstellungen Minderjähriger

Im Bereich des Tatbestandes stellte sich 2020 nach Analyse der an das BK übermittelten Fallzahlen die Gesamtsituation ähnlich wie im Vorjahr dar. Das ist auf den Umstand eines verstärkten Kampfes gegen die Verbreitung von Daten mit Online-Kindesmissbrauch durch soziale Medien zurückzuführen. Die Inhalte der Benutzerinnen und Benutzer werden vor allem in den USA vermehrt auf Pornographie überprüft. Inhalte mit Online-Kindesmissbrauch werden bei einem entdeckten Fall gesichert und der betroffene Account gesperrt. Damit einhergehend erfolgt eine entsprechende Verdachtsmeldung an das jeweilige Land, dem der Verursacher zugeordnet werden kann.

2020 kam es zur Übermittlung von 5.658 derartiger Verdachtsmeldungen durch Internet Service Provider an das BK. Der in Zusammenhang mit der Covid-19-Situation prognostizierte signifikante Anstieg ist zumindest in Österreich ausgeblieben. Die Fallzahlen haben sich auf einem hohen, wenngleich unter dem Vorjahr liegenden Niveau eingependelt.

Positiv hervorzuheben ist jedoch die Tatsache, dass es dem BK mit 895 identifizierten Verdächtigen gelungen ist, die Aufklärungsquote gegenüber dem Vorjahr signifikant zu verbessern und dadurch das Dunkelfeld gefährdeter Kinder weiter aufzuhellen.

3 Recht und Strategie

Stärkung der Cybercrimebekämpfung in allen Bereichen

Eine Cyber-Sicherheitsstrategie kann nur erfolgreich sein, wenn sie umfassend gestaltet ist und trotz erforderlicher Abgrenzungen und Verantwortungen alle betroffenen Akteure gemeinsam ihre jeweilige Aufgabe wahrnehmen. Drohende Gefahren müssen in diesem Bereich sehr schnell erkannt werden. Alle Erkenntnisse aus den kriminellen Aktivitäten fließen zudem umgehend in präventive Maßnahmen und Schulungen ein. Dieser Wissensaufbau stellt mit der Aus- und Weiterbildung von Polizistinnen und Polizisten auch im Bereich der IT-Kriminalität eine hohe Priorität in der gesamten Sicherheitsstrategie des Bundesministeriums für Inneres dar. Die Situation der Pandemie führte zu besonders großen Herausforderungen, wobei es gelang virtuelle Lernumgebungen zu schaffen und die Präsenzschulungen auf Webinare zu verlagern.

Nach wie vor fehlen nötige rechtliche Rahmenbedingungen in Hinblick auf die Problematiken bei Carrier Grade NAT (CGN), Domainnamen und Kryptowährungen, die derzeit die kriminalpolizeiliche Arbeit massiv erschweren beziehungsweise sogar verhindern. Eine Aktualisierung der Strategie und Konzepte zur Bekämpfung von Cybercrime wurde wie im Vorjahr geplant vorgenommen. Dazu wurden ebenso viele maßgebliche Empfehlungen des Rechnungshofes eingearbeitet.

Die Bereiche IT-Ermittlungen und die digitale Beweismittelsicherung werden in den kommenden Jahren personell verstärkt. Verbesserungen in Prozessen und Technologien finden kontinuierlich statt, gerade um neuen technischen Herausforderungen gerecht werden zu können. Dabei wird verstärkt auf aktuelle und künftige Phänomene im Internet eingegangen sowie die Kooperation mit anderen Ermittlungseinheiten verstärkt. Insbesondere im Bereich der elektronischen Beweismittelsicherung wird auf künftige Speicher- und Übertragungstechnologien Bedacht genommen.

Aufgrund des wachsenden personellen und technischen Bedarfs ist im Laufe des Jahres 2021 der Umzug des C4 an einen neuen Standort vorgesehen, um es zu einer neuen und modernen Cybercrime-Einheit zu gestalten und den internationalen Standards auch weiterhin gerecht zu werden.

Carrier Grade NAT

Hervorzuheben ist die Problematik mit CGN, bei der aufgrund der beschränkten Anzahl von IP-Adressen vom jeweiligen Betreiber zur gleichen Zeit ein- und dieselbe IP-Adresse einer Mehrzahl von Handy- und PC-Nutzerinnen beziehungsweise -Nutzern im Netz des Serviceproviders zugewiesen werden kann. Generell ist diesbezüglich anzumerken, dass eine IP-Adresse häufig einen der wenigen Ermittlungsansätze bei Cybercrime-Ermittlungen, wie zum Beispiel bei Ermittlungen im Zusammenhang mit Online-Kindesmissbrauch, Erpressungs-E-Mails oder auch Ransomware sowie Selbstmordankündigungen darstellt.

Mögliche Lösungsansätze, um die einzelne Nutzerin oder den einzelnen Nutzer auch bei der Verwendung von CGN nachvollziehbar und somit individualisierbar zu machen, existieren bereits. Des Weiteren besteht die Problematik mit § 76a Absatz 1 Zeile 1 Strafprozessordnung (StPO), bei dem die Regelung „… es sei denn, dass diese Zuordnung eine größere Zahl von Teilnehmern erfassen würde“ (zusammen mit dem TKG) geändert beziehungsweise gestrichen werden müsste. Diese Formulierung wird oft als Grund für die Verweigerung der Auskunft angeführt. Mit der CGN Problematik beschäftigt sich Europol schon seit 2017 und hat erkannt, welche Probleme dadurch entstehen und dass auf diesem Gebiet etwas unternommen werden muss. Bereits gefundene internationale Ansätze sind noch auf ihre österreichische Umsetzbarkeit zu prüfen.

Sicherheitspolizeigesetz und Strafprozessordnung

Wahrscheinlich wurden noch nie zuvor so viele Daten produziert, wie zu Zeiten der Covid-19 Pandemie. Es ist eine enorme Datenmenge im Umlauf, nicht nur aufgrund von Homeoffice, Streaming-Diensten oder Online-Gaming. Denn auch die Menge an verarbeiteten Gesundheitsdaten steigt und ist ein begehrtes Ziel von Cyber-Kriminellen. Somit ist auch unter anderem das Aufkommen vieler betrügerischer Seiten im Internet, sogenannter Fakeshops, Fake-Internetseiten, und dergleichen für Kriminelle noch lukrativer geworden. Sie nutzen die Angst der Bevölkerung und bieten mittlerweile vermehrt diverse medizinische Produkte in solchen Fakeshops an. Aus diesem Grund sollte bereits im Vorfeld gegen diese vorgegangen werden. Das bedarf einer Anpassung im Sicherheitspolizeigesetz (SPG), damit der Nahebezug zwischen Erkennung der Gefahr, Gefahrenerforschung und Gefahrenabwehr neu überdacht wird. Hierbei liegt die Herausforderung, das historisch gewachsene SPG an die Anforderungen der heutigen digitalen Zeit anzupassen, um flexibler mit den aktuellen Herausforderungen umgehen zu können.

Die steigende Komplexität digitaler Systeme und damit verbunden die Häufigkeit der auftretenden Sicherheitslücken erhöht die Anzahl der Systemangriffe und dadurch auch die Menge der exfiltrierten Daten, sogenannter Datenleaks. Daher braucht es auch eine Anpassung im Strafgesetzbuch (StGB) bei Cybercrime-Delikten. 2020 gab es einen deutlichen Anstieg an Datenleaks. Diese können aber nicht unter den § 118a StGB (widerrechtlicher Zugriff auf ein Computersystem) subsumiert werden, da häufig Sicherheitslücken aus mangelnder Sorgfalt oder Unkenntnis nicht geschlossen werden und die Täter daher keine Sicherheitsvorkehrungen umgehen müssen. Die dadurch erlangten (meist personenbezogenen) Daten werden im Internet geteilt. Dies ist in Österreich (noch) nicht strafbar ist. Strafrechtliche Ermittlungen sind dadurch nicht oder nur bedingt möglich. Bei Ermittlungen im Zusammenhang mit Cybercrime sind fast ausschließlich internationale

Ermittlungsansätze zu verfolgen. Um jedoch über die Justiz ein Rechtshilfeersuchen in ein anderes Land zu erhalten, ist die Grundbedingung, dass bei dem zu ermittelnden Sachverhalt ein Strafrahmen von über einem Jahr vorliegt. Die Grundtatbestände der klassischen Cybercrime-Delikte in Österreich weisen jedoch einen Strafrahmen von bis zu sechs Monaten Freiheitsstrafe auf. Diesbezüglich ist jedenfalls eine Angleichung des „digitalen“ Cyber-Strafrechts an das „analoge“ Strafrecht notwendig.

Eine bereits eingerichtete Arbeitsgruppe widmet sich genau diesen Problematiken. Conclusio der rechtlichen Herausforderungen ist, dass man Gesetzmaterien überarbeiten muss, um im digitalen Zeitalter anzukommen.

4 Jahresrück-blick

Zahlen und Fakten im Überblick

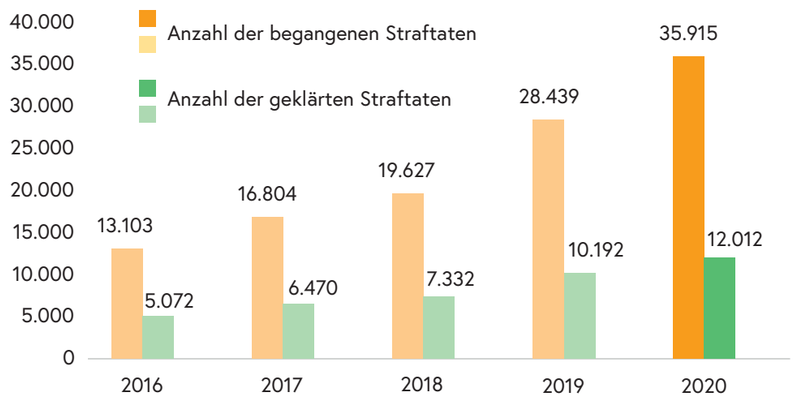
Die nachfolgenden Zahlen und Daten stammen ausschließlich aus der öffentlich verfügbaren und offiziell verlautbarten Polizeilichen Kriminalstatistik (PKS). Zuvor erwähnte Faktoren, wie die Covid-19-Krise im besonderen Ausmaß und beispielsweise rechtliche Herausforderungen spiegeln sich deutlich in der Kriminalitätsentwicklung wider. Eine starke Zunahme der begangenen Straftaten im Cybercrime-Bereich konnte beobachtet werden. Dieser Trend wurde durch die Pandemie und die vermehrte Verlagerung vieler Lebensaspekte in die digitale Welt zusätzlich verstärkt.

Tabelle: Entwicklung der Anzeigen, der aufgeklärten Fälle und der Aufklärungsquote von Cybercrime 2016 bis 2020

Jahr	Anzahl der angezeigten Fälle	Anzahl der geklärten Straftaten	Aufklärungsquote (gerundet)
2016	13.103	5.072	38,7 %
2017	16.804	6.470	38,5 %
2018	19.627	7.332	37,4 %
2019	28.439	10.192	35,8 %
2020	35.915	12.012	33,4 %
Veränderung 2019/2020	26,3 %	17,9 %	-2,4%-Punkte

2020 wurden 35.915 Cybercrime-Delikte zur Anzeige gebracht. Gegenüber dem Vorjahr mit 28.439 angezeigten Straftaten wurde ein Anstieg von 26,3 Prozent verzeichnet. Trotz des erneut beachtlichen Zuwachses der Anzeigen konnte die prozentuelle Aufklärungsquote mit 33,4 Prozent im gleichen Zeitraum nahezu konstant gehalten werden. Die absolute Anzahl der geklärten Straftaten stieg in diesem Bereich von 10.192 auf über 12.000 Fälle. Es konnten somit insgesamt deutlich mehr Fälle aufgeklärt werden als im Vorjahr.

Abbildung: Entwicklung der Anzeigen und der aufgeklärten Fälle von Cybercrime 2016 bis 2020



In der PKS wird im Sinne internationaler Vereinbarungen und in Anlehnung an die Budapester Konvention eine Einteilung von Cybercrime vorgenommen, deren Überarbeitung auch national ein Thema von interministeriellen Diskussionen ist. Im letzten Jahr wurden national auch Strafrechtsdelikte und Suchtmitteldelikte hinzugenommen und in den nachfolgenden Tabellen besonders gekennzeichnet.

Cybercrime im engeren Sinn

Cybercrime im engeren Sinne umfasst kriminelle Handlungen, bei denen Angriffe auf Daten oder Computersysteme unter Verwendung der Informations- und Kommunikationstechnik (IKT) begangen werden. Die Straftaten sind gegen die Netzwerke selbst oder aber gegen Geräte, Dienste oder Daten in diesen Netzwerken gerichtet, wie zum Beispiel bei der Datenbeschädigung, dem Hacking oder DDoS-Angriffen.

2020 musste bei Tatbeständen zu Cybercrime im engeren Sinn ein deutlicher Gesamtanstieg der Anzeigen von 69,4 Prozent gegenüber dem Vorjahr verzeichnet werden. Massive Steigerungen wurden beim betrügerische Datenverarbeitungsmissbrauch (§ 148a StGB) registriert. Mit über 10.000 angezeigten Fällen verdoppelte sich dieser nahezu im Vergleich zu 2019. Steigerungsraten jenseits der 40 Prozent im Vergleich zum Vorjahr wurden auch beim Missbräuchlichen Abfangen von Daten (§ 119a StGB), Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB) und bei der Datenfälschung (§225a StGB) verzeichnet.

Trotz der Zunahme an angezeigten Fällen konnten 2.459 Straftaten aufgeklärt werden und das Vorjahresniveau in absoluten Zahlen um 558 in diesem Bereich übertroffen werden. Die relative Aufklärungsquote sank jedoch aufgrund der verzeichneten Anzeigenzuwächse auf 19 Prozent.

Delikt	Angezeigte Fälle 2019	Angezeigte Fälle 2020	Geklärte Straftaten 2019	Geklärte Straftaten 2020
§ 107c StGB	330	329	255	253
§ 118a StGB	684	816	96	113
§ 119 StGB	11	12	10	5
§ 119a StGB	47	67	8	12
§ 126a StGB	467	361	68	78
§ 126b StGB	93	71	12	10
§ 126c StGB	243	354	54	66
§ 148a StGB	5.537	10.603	1.262	1.723
§ 225a StGB	210	301	136	199
Gesamt	**7.622**	**12.914**	**1.901**	**2.459**

Tabelle: Angezeigte Fälle und geklärte Straftaten von Cybercrime im engeren Sinn nach Paragraphen des Strafgesetzbuches 2020 im Vergleich zu 2019

Cybercrime im weiteren Sinn

Unter Cybercrime im weiteren Sinne werden Straftaten verstanden, bei denen die Informations- und Kommunikationstechnik als Tatmittel zur Planung, Vorbereitung und Ausführung von herkömmlichen Kriminaldelikten eingesetzt wird, wie zum Beispiel Betrugsdelikte, Drogenhandel im Darknet, Online-Kindesmissbrauch, Cybergrooming oder Cybermobbing. In der PKS umfasst Cybercrime im weiteren Sinne die Paragrafen des Internetbetrugs und der sonstigen Kriminalität im Internet.

Tabelle: Jahresvergleich 2019 – 2020 Angezeigte Fälle von Cybercrime im weiteren Sinn nach Paragraphen

Delikt	Angezeigte Fälle 2019	Angezeigte Fälle 2020	Geklärte Straftaten 2019	Geklärte Straftaten 2020
Internetbetrug				
§ 146 StGB	14.494	16.279	5.512	5.639
§ 147 StGB	1561	1761	437	580
§ 148 StGB	776	740	433	407
Internetbetrug-Gesamt	**16.831**	**18.780**	**6.382**	**6.626**
Sonstige Kriminalität im Internet				
§ 107a StGB		1		1
§ 144 StGB	1.874	778	80	83
§ 145 StGB	84	72	18	13
§ 207a StGB	1.666	1.702	1.541	1.528
§ 207b StGB	4	22	4	21
§ 208a StGB	101	142	69	102
§ 218 StGB	12	7	7	4
§ 223 StGB	42	45	35	30
§ 224 StGB	21	23	9	16
§ 228 StGB		1		1
§ 229 StGB		1		0
§ 231 StGB	16	38	8	15
§ 232 StGB	62	13	54	10
§ 241a StGB	4	1	3	1
§ 27 SMG		1.154		905
§ 28 SMG		9		8
§ 283 StGB		2		2
§ 28a SMG		63		58
§ 297 StGB	5		5	
§ 30 SMG		29		26
§ 3g VerbotsG	95	118	76	103
Sonstige Kriminalität im Internet gesamt	**3.986**	**4.221**	**1.909**	**2.927**
Internet-kriminalität gesamt	**28.439**	**35.915**	**10.192**	**12.012**

Der Internetbetrug erreichte 2020 mit 18.780 angezeigten Delikten wie im Vorjahr einen neuen Höchststand. Die Anzahl der angezeigten Fälle von Betrugsformen im Internet §§ 146 bis 148 StGB folgten mit einem Anstieg von 11,6 Prozent dem stetig steigenden Trend der vergangenen Jahre. Auf den gesamten Bereich Cybercrime gerechnet, stellt somit der Internetbetrug etwas mehr als die Hälfte der Anzeigen dar. Auch die sonstige Kriminalität im Internet stieg an. Dennoch konnte in nahezu allen Bereichen die Zahl der geklärten Straftaten deutlich erhöht werden. Die Aufklärungsquote beim Internetbetrug ging mit einem Minus von 2,6 Prozentpunkten gegenüber dem Vorjahr hingegen leicht zurück, bei der sonstigen Kriminalität im Internet stieg sie um 21,5 Prozentpunkte.

Zuwächse im Bereich der sonstigen Kriminalität im Internet sind aufgrund gestiegener Zahlen bei beispielsweise Online-Kindesmissbrauch (§ 207a StGB), Anbahnung von Sexualkontakten zu Unmündigen (§ 208a StGB) und vor allem durch die Neuaufnahme mehrerer Paragrafen des Suchtmittelgesetzes zu verzeichnen, wie zum Beispiel § 27 SMG unter dem die meisten diesbezüglichen Anzeigen subsumiert wurden. Die Erpressung (§144 StGB), die im Internet in den vergangenen Jahren besonders durch die Versendung von Massenerpressungs-E-Mails und die Infizierung mit Ransomware begangen wurde, nahm hingegen nicht zuletzt aufgrund konsequenter Ermittlungsarbeit deutlich ab.

Dunkelziffer und Anzeigeverhalten

Die Dunkelziffern im Bereich der Internetkriminalität sind unter Berücksichtigung internationaler Studien besonders hoch. Viele Betroffene scheuen die Anzeige bei der nächsten Polizeidienststelle, teils aus Scham, Angst vor Reputationsverlust oder weil angenommen wird, dass der Fall ohnehin nicht verfolgt werden könnte.

Jedoch kann mit jedem angezeigten Vorfall die Beweismittellage zu verdächtigen Tätergruppen weiter verdichtet werden. Außerdem verbessert die Anzahl der Anzeigen die frühere Erkennung von neuen Massenphänomenen für die ermittelnden Strafverfolgungsbehörden. Ebenso können Präventionsmaßnahmen früher gesetzt werden und mit zielgerichteten Warnhinweisen an die Bevölkerung die Anzahl der Geschädigten reduziert werden. Eine Wiedererlangung abhanden gekommener Vermögenswerte gelingt jedoch selbst nach internationaler Ausforschung der Täter nur in den seltensten Fällen. Deshalb

muss im Bereich des Internetbetrugs der Verhinderung von Straftaten durch verstärkte Bewusstseinsbildung und Aufklärung erhöhte Aufmerksamkeit geschenkt werden. Die Täter nutzen menschliche Schwächen, wie Gier und Sehnsüchte nach Anerkennung oder Beziehungen aus, um sich zu bereichern. Auch im vergangenen Jahr blieb Social Engineering eine maßgebliche Gefahr.

5 Aufbau-organisation und Abläufe

Drehscheibe und wichtige Ansprechstelle

Das C4 wurde 2011 zur Bekämpfung von Computerkriminalität als eigene Einheit innerhalb der Abteilung Kriminalpolizeiliche Assistenzdienste des BK etabliert. Es ist nationale und internationale Koordinierungs-, Ermittlungs- und Meldestelle im Zusammenhang mit Cybercrime im engeren Sinn sowie für die elektronische Beweismittelsicherung und deren Auswertung zuständig. Darüber hinaus ist die C4-Meldestelle nicht nur als rund um die Uhr erreichbare Kontaktstelle gemäß der Budapest Cybercrime Convention und anderen internationalen Vereinbarungen eingerichtet. Die C4-Meldestelle agiert auch als wichtige Ansprechstelle für die Bevölkerung und Unternehmen, wodurch im Schadensfall eine rasche Unterstützung erfolgt und neue Phänomene frühzeitig erkannt werden können. Das C4 dient aber auch allen Polizeidienststellen als wichtige Drehscheibe und Koordinationspunkt.

Es gliedert sich mit seinen Schnittstellen zum Cyber Security Center (CSC) des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT) als wesentlicher Bestandteil in die Strategie des Bundeskanzleramts ein. In diesem Zusammenhang ist das C4 Teil des Inneren Kreises der operativen Koordinierungsstrukturen (IKDOK). Weiterführende Informationen finden sich unter

https://www.bundeskanzleramt.gv.at/themen/cyber-sicherheit-egovernment.html

C4-Meldestelle

Die Meldestelle zur Bekämpfung der Internetkriminalität ist seit knapp zehn Jahren im C4 etabliert und ist in einem 24/7 Betrieb rund um die Uhr erreichbar. Durch diese können umgehend die erforderlichen Maßnahmen zur Gefahrenabwehr eingeleitet werden. Anfragen erhält die Meldestelle, wie ursprünglich vorgesehen, von den behördeneigenen Dienststellen und zunehmend in Form von Mitteilungen durch Bürgerinnen und Bürger, Unternehmen sowie nationalen und internationalen Polizeidienststellen. Im Jahr 2020 erhielt die Meldestelle 14.988 Anfragen. 2019 waren es noch 13.936. 11.576 der Anfragen aus 2020 hatten einen Bezug zu Cybercrime.

In ihrer zentralen Funktion als Cybercrime-Schnittstelle innerhalb polizeiinterner Strukturen sowie als Meldestelle für Bevölkerung und Wirtschaft, agiert die Meldestelle als Koordinierungs- und Informationszentrum für diesen Themenkreis. Zusätzlich umfasst diese Tätigkeit auch proaktive, präventive Maßnahmen in Form von Warnmeldungen und Newslettern, die von speziell geschulten Mitarbeiterinnen und Mitarbeitern erstellt werden. Die deutlich erkennbare Sensibilisierung und Bewusstseinsbildung zum Thema Cybercrime erfolgte einerseits durch die fortlaufende Kooperation mit unterschiedlichen Institutionen aus dem Bereich der Wirtschaft und Vereinen, wie beispielsweise der Wirtschaftskammer Österreich (WKO) oder der Initiative „Watchlist Internet“, die unter www.watchlist-internet.at erreichbar ist. Ebenso führen Erstanalysen der eingehenden Meldungen zu schnellen Informationsweitergaben aktueller Phänomene, damit die akuten negativen Auswirkungen minimiert werden können. Für diese Aufgaben ist ein technischer Journaldienstbetrieb eingerichtet, der in dringenden Fällen organisationsübergreifende Sofortmaßnahmen einleiten kann.

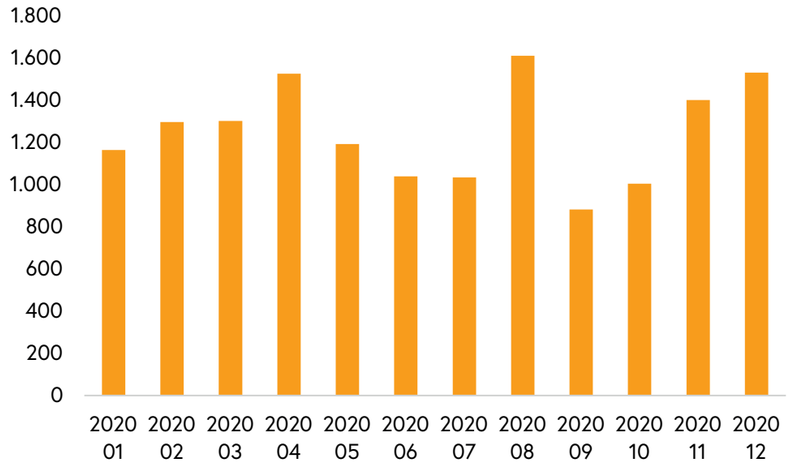
Zur raschen und effizienten Gewährleistung internationaler Ermittlungen erfolgt die Zusammenarbeit der Meldestelle als Drehscheibe zu anderen internationalen Dienststellen und Polizeieinheiten, wie dem Interpol Digital Cyber Center (IDCC), dem Europäischen Cybercrime Center (EC3) und den jeweiligen High-Tech Crime Units anderer Staaten (NCPs).

Kontakt:
Bundeskriminalamt - Meldestelle Cybercrime
Josef-Holaubek-Platz 1, 1090 Wien
Email: against-cybercrime@bmi.gv.at

Monat	Anzahl der relevanten E-Mail-Meldungen	Anzahl der E-Mail-Eingänge - Ohne Relevanz	Anzahl der Telefon-Meldungen	Summe der relevanten Meldungen (mit Cybercrime Bezug)	Summe aller Meldungen
Januar	803	277	85	888	1.165
Februar	944	273	80	1.024	1.297
März	916	324	62	978	1.302
April	1.125	282	119	1.244	1.526
Mai	904	236	53	957	1.193
Juni	753	228	58	811	1 039
Juli	853	85	97	950	1.035
August	768	769	74	842	1 611
September	754	98	31	785	883
Oktober	777	166	62	839	1.005
November	1.089	242	70	1.159	1.401
Dezember	1.053	432	46	1.099	1.531

Tabelle: Übersicht der Meldungen an die C4-Meldestelle nach Monaten 2020

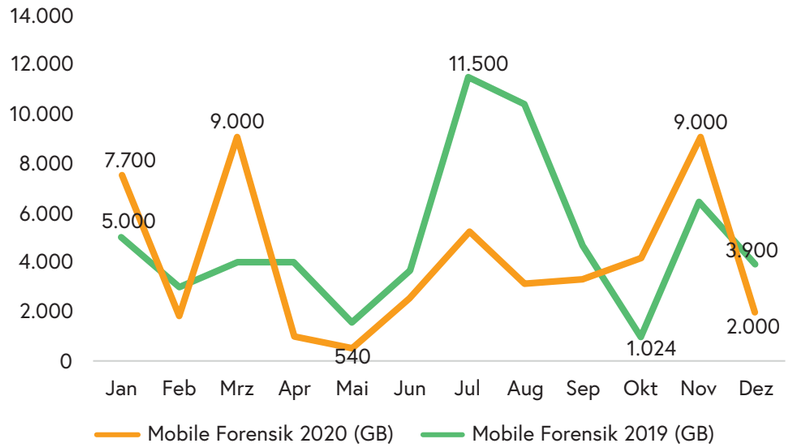
Abbildung: Meldungen an die C4-Meldestelle nach Monaten – Jahresverlauf 2020



C4-Forensik

Die Auswertung von IT- und Speichermedien stellte die Ermittlerinnen und Ermittler, insbesondere nach dem Terroranschlag im November 2020, vor eine enorme Herausforderung. Es waren unzählige Geräte mit sehr hohen Datenmengen aufzubereiten, um die ressourcenintensive Unterstützung der ermittelnden Beamtinnen und Beamten zu gewährleisten.

Abbildung: Mobile Forensik, Jahresvergleich der ausgewerteten Datenmengen in Gigabyte (GB)



2020 war der Support der C4-Forensik, wie auch die Jahre zuvor, ein unverzichtbarer, wesentlicher Bestandteil strafrechtlicher Ermittlungen. Die gesamte Datenmenge forensischer Auswertungen war Pandemie-bedingt rückläufig, da über das Jahr verteilt deutlich weniger Hausdurchsuchungen stattfanden als im Jahr zuvor. Dennoch kam der elektronischen Beweismittelsicherung im C4 und den LKA weiterhin essenzielle Bedeutung in der Ermittlungsarbeit zu.

Aufgrund der rasanten technischen Entwicklung wird die Auswertung diverser Medien allerdings immer schwieriger. Herstellerspezifische Systeme mit ausgeprägten Verschlüsselungsverfahren stellen die elektronische Beweissicherung immer wieder vor große Herausforderungen. Insbesondere im Bereich der mobilen Forensik werden Datensicherungen und Auswertungen immer komplexer. Die steigenden Zahlen zu forensischen Tätigkeiten erklären sich mit den zunehmend umfassenden Auswertungen von Smartphones und Clouds, die zum Teil von den LKA nicht mehr bewältigt werden können.

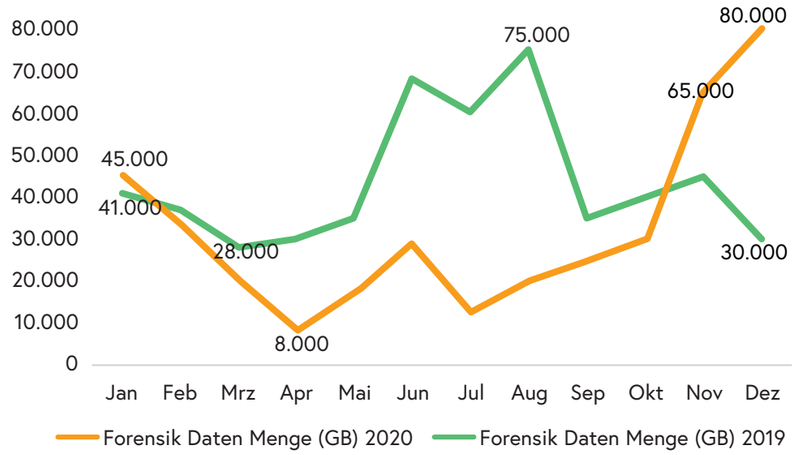


Abbildung: IT-Forensik, Jahresvergleich der ausgewerteten Datenmengen in GB

Fahrzeugforensik / Automotive-IT

Im Bereich der Fahrzeugforensik / Automotive-IT, die sich als eigener Fachbereich innerhalb der IT-Forensik entwickelt hat, waren abermals steigende Anforderungen zur digitalen Beweismittelsicherung aus Fahrzeugsystemen erkennbar. Durch die zunehmende Digitalisierung in der Fahrzeugindustrie stellen die im Fahrzeug gespeicherten Daten ein wichtiges Beweismittel für das Strafverfahren dar, wodurch Kraftfahrzeugsysteme (Kfz) zunehmend in den Fokus von Ermittlungen gerückt sind. Während beispielsweise die Zahl der Auswertungen in Zusammenhang mit Kfz-Diebstahl und -Verschiebungen rückläufig waren, kam es vermehrt zu Auswertungen in Zusammenhang mit schweren Straftaten.

Das zeit- und ressourcenaufwendige sowie hochspezialisierte Chip Off-Verfahren sowie die Kfz-Forensik, können nur zentral im C4 durchgeführt werden. Mit 83 Chip Off-Verfahren 2020 wurde gegenüber dem Vorjahr ein starker Anstieg von rund 50 Prozent verzeichnet.

Ein weiterer Anstieg von Anfragen konnte im Zusammenhang mit schweren und / oder tödlichen Verkehrsunfällen festgestellt werden, wobei der Schwerpunkt auf der Sicherung von Crashdaten (EDR-Event Data Recorder) gerichtet war. Diese können in Verbindung mit herkömmlichen Untersuchungsschritten maßgeblich zur Rekonstruktion des Unfall-

hergangs beitragen, da wichtige digitale Informationen über Fahrmanöver kurz vor dem Unfall analysiert werden können. Dieser Umstand wurde auch seitens der EU-Kommission thematisiert, wodurch konventionelle Personenkraftfahrzeuge ab 2022 verpflichtend mit einem EDR-System ausgestattet werden sollen. Der aktuelle Entwurf sieht allerdings vor, dass diese Crashdaten zukünftig keine Orts-, Datums- und Zeitangaben mehr enthalten sollen, weshalb diesen Informationen keine faktische Beweiskraft mehr zukommen würde. Derartige Entwicklungen werden genauestens durch den Fachbereich beobachtet und in internationalen Gremien behandelt. Die Mitarbeiter der Kfz-Forensik sind beispielsweise Teil der Fachgruppe Automotive-IT bei Europol, stehen laufend in Kontakt mit Interpol, aber auch mit der Automobilindustrie und deren Vertreterinnen und Vertreter. Hierbei gilt es zukünftige Entwicklungen zu erkennen, die nicht vernachlässigbare Auswirkungen auf die polizeiliche Ermittlungsarbeit und digitale Beweissicherung haben. Dazu zählt beispielsweise der stetig steigende Anteil an Elektrofahrzeugen, die Vernetzung von intelligenten Kfz untereinander und mit der Verkehrsinfrastruktur sowie die fortschreitende Technik in Bezug auf teilautonomes beziehungsweise autonomes Fahren.

Entwicklung und Innovation

Um die Bereiche der Cybercrime-Ermittlungen und digitalen Forensik unterstützen zu können, werden im C4 auch eigene Tools und Skripte entwickelt. Schwerpunkte dazu waren 2020 die Bereiche der Kryptowährungen, digitalen Ermittlungen und Forensik. Diese Werkzeuge werden grundsätzlich nicht nur national, sondern auch international, über das Europol Projekt SIRIUS, für Strafverfolgungsbehörden zur Verfügung gestellt. Gerade im Bereich der digitalen Ermittlungen ist es erforderlich, flexibel große Datenmengen effizient abzuarbeiten, das Wesentliche daraus zu erkennen und optimal für die weitere Tätigkeit der Kriminalpolizei zu verwerten. Dabei ist es notwendig, Synergien zwischen den Entwicklungsbereichen verschiedener Strafverfolgungsbehörden optimal zu verbinden.

Um organisatorische und technische Strukturen von Tätern besser abschätzen zu können, war die Sicherheitsforschung im Bereich von Cybercrime ebenfalls einer der zentralen Punkte des vergangenen Jahres. Die Praxisorientierung ist notwendig, um operativen Ermittlerinnen und Ermittlern die erworbenen Kenntnisse und Informationen für zielführende Ermittlungen weiterzugeben. Durch den raschen und flexiblen Informationsaustausch, den weiter anwachsenden „Cybercrime Communities“ sowie den zahlreichen CaaS-Angeboten wird es deutlich schwerer, verschiedene Vorgehensweisen der Täter und kriminelle Strukturen zu verstehen. Daher ergeben sich ähnlich gelagerte Ziele mit dem Bereich der Cybersicherheit, die jedoch für den Kriminalitätsbereich andere Fragestellungen erfordern.

Wissensvermittlung durch Ausbildung und internationalen Austausch

Bereits seit 2012 findet eine grundlegende Ausbildung von Bezirks-IT-Ermittlerinnen und -ermittler statt. Mittlerweile unterstützen mehr als 300 speziell ausgebildete Kolleginnen und Kollegen durch fachgemäße Erstmaßnahmen und Ermittlungen auf lokaler Ebene. Die Vortragenden werden aus den besten Expertinnen und Experten der LKA und dem BK bereitgestellt. Das Thema Cybercrime wird insbesondere im Rahmen der Kriminaldienstfortbildungsrichtlinie (KDFR) sowie in den Grundausbildungslehrgängen behandelt.

2020 wurde der Ausbildungsbereich durch Covid-19 und den damit verbundenen Schutzmaßnahmen vor eine große Herausforderung gestellt. Die Präsenzkurse konnten nicht wie geplant durchgeführt werden. Das C4 hat ab dem zweiten Quartal mit der Entwicklung eines Learning Management Systems (LMS) in Verbindung mit einer Webinar Plattform auf eigenen sicheren Servern begonnen. Bis Ende des Jahres konnten bereits einige der Module für die Bezirks-IT-Ermittlerschulung auf dieses System umgestellt werden. Zusätzlich wurde ein Online-Format „C4-Fachvorträge“ ins Leben gerufen, das sich an einen erweiterten Personenkreis richtet. Hier wird regelmäßig aktuelles Wissen zu unterschiedlichen Cybercrime-relevanten Themen an alle interessierten Ermittlerinnen und Ermittler weitergegeben.

Um den weiteren Ausbau der Expertise im BK und den LKA zu gewährleisten, wurde im Auftrag des Herrn Bundesministers die Entwicklung einer universitären Ausbildung für die Bereiche Digitale Forensik und Digitale Ermittlungen gestartet.

Aufgrund von Covid-19 mussten besonders geschulte Präventionsbeamtinnen und -beamte, die insbesondere für Klein- und Mittelbetriebe, aber auch für die interessierte Allgemeinheit im Einsatz waren, die meisten Präsenzveranstaltungen absagen.

Fachkonferenz „Blockchain und virtuelle Währungen“

Neben der Gremienarbeit bei Europol und Interpol organisierte das C4 wichtige Veranstaltungen mit internationaler Reichweite. Vor Beginn der Covid-19-Pandemie lud das C4 vom 22. bis 24. Jänner 2020 rund 200 Polizistinnen und Polizisten sowie Vertreterinnen und Vertreter von Strafverfolgungsbehörden zur Konferenz „Blockchain und Virtuelle Währungen. Gezielt ermitteln und sicherstellen“. Im Rahmen dieser größten deutschsprachigen Tagung zu Kryptowährungen im kriminalpolizeilichen Kontext konnten die Teilnehmerinnen und Teilnehmer den Umgang mit Kryptowährungen und sogenannten Smart Contracts lernen. Dazu entwickelten die IT-Spezialistinnen und -Spezialisten des C4 eigens einen „BK-Token“, der mit einem selbst geschriebenen Smart Contract in die Ethereum Blockchain hochgeladen wurde und öffentlich einsehbar war. Er stellt keinen finanziellen Gegenwert dar und wird nicht gewerblich gehandelt. Um die Aufgaben

plastischer zu gestalten wurde ein eigener „Coin-O-Mat“ entwickelt, der mit dem Smart Contract interagieren kann. Wenn die Benutzerin oder der Benutzer des Automaten die Übung mit dem BK-Token richtig abschließt, wirft der Automat eine Challenge-Coin aus. In Expertenworkshops wurden die Transaktionen der Konferenzteilnehmerinnen und -teilnehmer mit dem BK-Token auf forensische Spuren untersucht. So wurde eine ideale Übungsumgebung für Ermittlungen geschaffen. Trainings mit dem BK-Token werden auch künftig im Rahmen weiterer nationaler und internationaler Schulungen abgehalten. Die Konferenz wurde von der Europäischen Union über den Fonds für die innere Sicherheit (ISF) kofinanziert.

Das C4 vertritt Österreich zudem im Bereich der Aus- und Fortbildung auf internationaler Ebene in der European Cybercrime Training and Education Group (ECTEG).

Zentrale Anfragestelle für Social Media und Online Service Provider (ZASP)

Bei bestimmten Ermittlungen sind internationale Anfragen an Social Media Plattformen und ausländische Diensteanbieter im Internet erforderlich. In der Vergangenheit wurden diese von fast jeder Polizeidienststelle in Österreich selbst durchgeführt, jedoch gab es keinen einheitlichen Prozessablauf. Durch unterschiedliche Rechtsauslegungen und Gesetzesmaterien kam es daher oft zu keiner positiven Beantwortung der gestellten Anfrage beziehungsweise wurden langwierige Rückfragen seitens der Anbieter geführt. Diese Zeitverzögerungen können für Ermittlungen sehr nachteilig sein. Durch die gewonnenen Informationen der Provideranfragen können Täter rascher ausgeforscht werden. Aus diesem Grunde wurde das C4 beauftragt, eine zentrale Anfragestelle für Social Media und Online Service Provider, kurz ZASP, einzurichten, um einheitliche, klare und einfach geregelte Ablaufprozesse künftig zentral abzuwickeln und das dort gewonnene Knowhow den Kolleginnen und Kollegen zur Verfügung zu stellen. Damit entstand eine verstärkte Unterstützung für die einzelnen Ermittlungsbereiche und es konnte ein höherer Output generiert werden. Ebenso plädieren zahlreiche Diensteanbieter ihrerseits bereits ausdrücklich auf eine zentrale Kontaktstelle in den jeweiligen europäischen Staaten, um die an sie gestellten Anfragen gezielter abarbeiten zu können. Die ZASP steht nicht nur im regelmäßigen Austausch mit den Vertretern der Social Media Anbieter, sondern ist auch Ansprechstelle für Anfragen polizeilicher Dienststellen und der Justiz.

Derzeit läuft der Probebetrieb der ZASP mit dem Bundesministerium für Justiz, drei Bundesländern und drei Social Media Diensteanbietern. Vor diesem Projekt gab es in Österreich allgemein 20 Prozent bis 40 Prozent positive Rückmeldungen von Online Service Providern. Anhand des von Facebook veröffentlichten Transparenzberichtes für das erste Halbjahr 2020 ergibt sich eine Beantwortungsquote von 44 Prozent bundesweit. Vom Projektstart bis zur Evaluierung am 25. Februar 2021 ist eine Quote von 80 Prozent positiver Rückbeantwortungen ersichtlich. Bei den restlichen 20 Prozent der angeforderten Daten aus dem Probetrieb lag noch kein Ergebnis vor. Nach Abschluss des Probebetriebs ist geplant, die zentrale Anfragemöglichkeit für Social Media und Online Service Provider auf das gesamte Bundesgebiet auszurollen und weitere einzubinden.

Zusammenarbeit mit der Polizei

Erstattung einer Anzeige

Sind Sie Opfer einer Straftat aus dem Feld der Cyberkriminalität geworden, haben Sie die Möglichkeit diesen Sachverhalt in jeder Polizeidienststelle prüfen zu lassen beziehungsweise gegebenenfalls anzuzeigen.

Um sich hierfür optimal vorzubereiten:

- Wenn es um einen konkreten aktuellen Notfall geht (Angriff auf Leib/Leben), dann rufen Sie den Polizeinotruf 133 an.

- Stellen Sie relevante(s) Beweismittel / Datenmaterial wie beispielsweise E-Mails, Chat-Verläufe, Zahlungsbelege, Screenshots, digitale Fotos oder Videos entsprechend zusammen. Wenn bestimmte Inhalte nicht abgespeichert werden können, erstellen Sie Screenshots oder fotografieren Sie den Bildschirm notfalls ab.

- Stellen Sie sicher, dass Sie die Unterlagen und Daten, die Sie der Polizei zur Verfügung stellen, im Originalzustand befinden, das bedeutet keine Manipulation, keine Ergänzungen oder Ähnliches damit durchzuführen. Bei E-Mails würde das bedeuten, diese nicht einfach weiterzuleiten, sondern die Original-E-Mail abzuspeichern und die gespeicherte Kopie als Anhang zu übermitteln.

- Häufig haben Sie auch selbst die Möglichkeit, bei den von Ihnen betroffenen Accounts, Informationen zu erfragen, die für eine Täterausforschung notwendig sind, wie zum Beispiel IP-Adressen über widerrechtliche Zugriffe inklusive Zeitstempel, Logdaten und dergleichen. Überprüfen Sie dazu am besten selbst, welche der für die Tat relevanten Daten beim jeweiligen Account-Anbieter beziehungsweise Online Service Provider gespeichert werden und für Sie zugänglich sind oder deren Bekanntgabe über diesen angefordert werden kann.

- Wenn es sich um komplexere Taten handelt, dokumentieren Sie den Tathergang in chronologischer Weise und stellen Sie sicher, dass die Geschehnisse zeitlich richtig eingeordnet sind.

- Wenn Sie Probleme haben die Beweismittel technisch zu sichern beziehungsweise abzuspeichern, bitten Sie eine Person Ihres Vertrauens diese Beweise mit Ihnen gemeinsam zu sichern.

- Stellen Sie die gesicherten Daten der Polizei nach Absprache in geeigneter Form zur Verfügung (beispielsweise über https://cryptshare.bmi.gv.at). Die Daten zur Verfügung zu stellen ist wichtig für die weiteren Ermittlungen, um den Verlust von Spuren im Netz zu vermeiden.

- Bitte haben Sie Verständnis dafür, dass Sie bei einem ersten Gespräch mit der Polizei nicht unmittelbar auf spezialisierte Cybercrime-Expertinnen und -Experten treffen und deshalb in den meisten Fällen erst in einem zweiten Schritt an eine spezialisierte Fachdienststelle weitergeleitet werden oder von dort Rückfragen erhalten.

- Darüber hinaus kann Ihnen die Meldestelle für Cybercrime professionelle Auskunft über die weitere Vorgangsweisen und Schritte bei Cybercrime-Vorfällen erteilen. Für die formelle Anzeigenerstattung sind in der Regel die örtlich und sachlich zuständigen Polizeidienststellen verantwortlich. Derzeit ist eine formelle Anzeigeerstattung über die Meldestelle nicht vorgesehen.

6 Kriminal-prävention

Schulter an Schulter mit dem Digitalisierungsministerium

Covid-19 hat die Situation für viele Personen verändert. Die Pandemie hatte nicht nur Auswirkungen auf das tägliche Leben, sondern auch auf die Kriminalitätsformen. Klassische Delikte, wie Einbruch und Taschendiebstahl sind in den Hintergrund getreten, weil eine Vielzahl von Menschen im Homeoffice oder zu Hause anzutreffen sind. Dadurch verlagern sich alltägliche Handlungen und das berufliche Leben zunehmend ins Internet, wodurch mehr Möglichkeiten für Straftaten geschaffen werden. Die Polizei klärt in der Präventionsarbeit im Bereich der Computer- und Internetkriminalität über Gefahren, Phänomene und Problemfelder auf.

Das BK bietet gemeinsam mit dem Digitalisierungsministerium an, sich im Bereich Sicherheit in der digitalen Welt zu informieren. Zu diesem Zweck steht die fit4internet-Hotline zur Verfügung, bei der Exekutivbedienstete in ganz Österreich für Beratungen und Vorträge angefordert werden können. Die Vorträge stehen mittlerweile bereits als Webinar zu Verfügung und können als solches gebucht werden. In den Vorträgen und Beratungen werden einfache Handlungsanleitungen erklärt und eine entsprechende Sensibilisierung bei besonders häufigen Delikten vorgenommen, um das Risiko Opfer von Cybercrime zu werden, zu senken.

Um möglichst viele Menschen zu erreichen, wurde durch gezielte Social Media Auftritte auf aktuelle Kriminalitätsformen eingegangen und mit Präventionstipps verbreitet. Dabei haben sich die Social Media Kanäle des BK und der Landespolizeidirektionen als gute Plattform erwiesen.

Für diese Tätigkeit stehen in ganz Österreich Präventionsbedienstete zur Verfügung. Diese können über das jeweilige LKA erreicht werden. Die Polizistinnen und Polizisten sind bei Beratungen auf den Polizeiinspektionen, durch Vorträge bei Organisationen, Unternehmen, Gemeinden oder bei Elternabenden in Schulen und Kindergärten aktiv.

Abbildungen: Informationsblätter über Cyberangriffe und sichere Telearbeit von Europol auf den Seiten 43, 44 und 45

Sichere Telearbeit

TIPPS UND HINWEISE FÜR UNTERNEHMEN

Legen Sie Unternehmensrichtlinien und -prozesse für Telearbeit fest und testen Sie diese nach Möglichkeit vorab

Legen Sie eine klare Richtlinie für Telearbeit fest, die den Zugriff auf Unternehmensressourcen und Ansprechpartner bei Problemen vorgibt. Legen Sie klare Prozesse für Sicherheitsvorfälle fest. Setzen Sie zusätzliche Maßnahmen hinsichtlich Dokumentation an das mittlere und obere Management um Unterschriften, Genehmigungen / Feedback und Informationen zu erhalten.

Sichern Sie Ihre Telearbeitsgeräte

Implementieren Sie Maßnahmen wie Festplattenverschlüsselung, Zeitlimits für Inaktivität, Blickschutz für Displays, starke Authentifizierung und Kontrolle sowie Verschlüsselung von Wechseldatenträgern (z. B. USB-Laufwerke). Implementieren Sie einen Prozess für die Remote-Deaktivierung von Zugriffen auf verloren gegangene oder gestohlene Geräte.

Sicherer Remote-Zugriff

Erlauben Sie Ihren Mitarbeitern nur über einen vom Unternehmen bereitgestellten/genehmigten VPN-Zugang mit Mehrfaktor Authentifizierung („multi-factor authentication“) eine Verbindung zum Unternehmensnetzwerk herzustellen. Stellen Sie sicher, dass Remote-Verbindungen nach einer bestimmten Zeit der Inaktivität automatisch getrennt werden („time out“) und nach Ablauf eine erneute Authentifizierung erforderlich ist.

Halten Sie Betriebssysteme und Apps auf dem neuesten Stand

Dies wird das Risiko verringern, dass Cyberkriminelle vom Hersteller behobene Sicherheitslücken ausnutzen.

Sichern Sie Ihre Unternehmenskommunikation

Bestehen Sie auf die Verwendung von Multi Faktor Authentifizierung für den Zugriff auf Unternehmens-E-Mail-Konten. Stellen Sie Ihren Mitarbeitern sichere Kommunikationskanäle Verfügung, damit sich diese leicht erreichen und mit externen Partnern kommunizieren können.

Erhöhen Sie Ihr Sicherheitsmonitoring

Überprüfen Sie ungewöhnliche Remotebenutzeraktivitäten und erhöhen Sie Ihre Warnstufen für VPN-bezogene Angriffe.

Sensibilisieren Sie Mitarbeiter für die Risiken der Telearbeit

Informieren Sie die Mitarbeiter über die Telearbeitsrichtlinien des Unternehmens. Nehmen Sie sich die erforderliche Zeit, um auf Cyber-Bedrohungen aufmerksam zu machen und insbesondere auf Phishing und Social Engineering zu sensibilisieren.

Treten Sie mit Ihren Mitarbeitern regelmäßig in Verbindung

Setzen Sie realistische Ziele, und gestalten Sie Arbeitspläne und Follow-up-Mechanismen nach Möglichkeit flexibel, um die persönlichen Umstände der Mitarbeiter zu berücksichtigen.

Bundesministerium Inneres
Bundeskriminalamt
EUROPOL EC3 European Cybercrime Centre

Sichere Telearbeit

TIPPS UND HINWEISE FÜR MITARBEITER

Zugriff auf Unternehmensdaten mit Unternehmensausstattung

Verwenden Sie nur vom Unternehmen bereitgestellte Geräte und Software. Erstellen Sie sichere Kennwörter (verwenden Sie vertrauenswürdige / genehmigte Kennwortmanager, falls verfügbar). Schreiben Sie Ihre Kennwörter nicht auf und schützen Sie sich davor, bei der Eingabe beobachtet zu werden. Vermeiden Sie Workarounds, auch wenn diese scheinbar genau das bieten, was Sie benötigen.

Stop.Think.Connect

Machen Sie sich vor Beginn der Telearbeit mit den Geräten, Richtlinien und Abläufen des Unternehmens vertraut. Vergewissern Sie sich, dass Sie die Bedienung der Geräte, sowie die Verhaltensregeln für deren Verwendung verstanden haben und die Kontakte für Hilfe kennen.

Sicherer Fernzugriff

Stellen Sie nur über das vom Unternehmen bereitgestellte/genehmigte VPN eine Verbindung zum Unternehmensnetzwerk her und schützen Sie die für die VPN-Verbindung erforderlichen Token (z. B. Smartcard).

Schützen Sie Ihre Arbeitsgeräte und Ihre unmittelbare Arbeitsumbebung, die Sie für die Telearbeit benötigen

Erlauben Sie Familienmitgliedern keinen Zugriff auf Ihre Arbeitsgeräte. Sorgen Sie für eine geeignete Sperre Ihrer Geräte, wenn diese unbeaufsichtigt sind und bewahren Sie sie an einem sicheren Ort auf, um Verlust, Beschädigung oder Diebstahl zu vermeiden. Verhindern Sie das unberechtigte Ablesen Ihres Bildschirms durch Verwendung eines Display-Sichtschutzes und positionieren Sie Bildschirme niemals vor Fenstern oder Kameras.

Informieren Sie Ihren Arbeitgeber

Sollten Sie ungewöhnliche oder verdächtige Aktivitäten auf Ihrem Arbeitsgerät bemerken, wenden Sie sich sofort über die entsprechenden Kanäle an Ihren Arbeitgeber.

Bleiben Sie wachsam

Achten Sie auf verdächtige Aktivitäten und Anfragen, insbesondere im Zusammenhang mit finanziellen Forderungen. Es könnte sich um CEO-Fraud oder Tech-Support-Scam durch Betrüger handeln! Rufen Sie im Zweifelsfall den Anforderer zur Verifizierung an. Klicken Sie nicht auf Links oder Anhänge in E-Mails und Textnachrichten unbekannter Herkunft.

Geben Sie keine persönlichen Informationen weiter

Antworten Sie niemals mit persönlichen Informationen auf Nachrichten, auch wenn diese angeblich von legitimen Unternehmen stammen. Wenden Sie sich stattdessen direkt an das Unternehmen, um die Anfrage zu verifizieren.

Entwickeln Sie neue Routinen

Besprechen Sie Arbeitspläne, Aufgabenverteilung, Fristen und Kommunikationskanäle während der Telearbeitszeit mit Ihrem direkten Vorgesetzten und den Teammitgliedern.

Verwendung von privaten Geräten

Wenn die Verwendung Ihres persönlichen Geräts die einzige und von Ihrem Arbeitgeber zugelassene Option ist, stellen Sie die Aktualität des Betriebssystems und der Software - insbesondere des Antivirus Programms - sicher. Zusätzlich sollten Sie nur von Ihrem Unternehmen genehmigte VPN Lösungen zur Verbindung ins Unternehmen nutzen.

Privates und Berufliches trennen

Verwenden Sie das Telearbeitsgerät nicht für private Zwecke und installieren Sie keine vom Arbeitgeber ungenehmigten Applikationen.

Bundesministerium Inneres
Bundeskriminalamt
EUROPOL EC3 European Cybercrime Centre

7 Zusammenfassung und Ausblick

Fazit

Der ununterbrochene Anstieg der Cybercrime-Delikte sowie die immer komplexer werdenden Modi-Operandi erfordern eine stetige Anpassung der Ressourcen und Strukturen in den Cybercrime-ermittelnden Organisationseinheiten. Insbesondere die strukturelle Anpassung des C4 als neue Abteilung im Bundeskriminalamt und der Umzug in ein modernes Gebäude stellen dabei wichtige Meilensteine dar. Parallel dazu sollen personelle Verstärkungen der Cybercrime-Ermittler/innen in den Landeskriminalämtern und den Bezirken erfolgen. Im Vordergrund stehen dabei die Spezialisierung auf aktuelle und künftige Phänomene sowie die nationale und internationale Zusammenarbeit.

Die schnellen Änderungen bei Tätern und Technologien fordern eine stetige Weiterentwicklung und eine laufende Fortbildung des Kriminaldienstes und der uniformierten Polizei. Diese werden zum Teil durch die Bezirks-IT-Ermittler Schulungen erfüllt. Geplant ist auch hier ein lang notwendiger Ausbau, welcher bereits in einem Projekt zu einem vollständigen Ausbildungskonzept weiterentwickelt wurde. Zusätzlich dient der Cybercrime Experts Circle (CEC), der vom Cybercrime Competence Center (C4) aufgebaut wurde, als internationale Plattform zum Austausch von unmittelbar praktisch anwendbarem Wissen mit Expertinnen und Experten aus Partnerländern.

Herausfordernd bleibt es eine rasche und effiziente Reaktion auf internationale Cybervorfälle im operativen, kriminalpolizeilichen Dienst setzen zu können. Mit der Entsendung eines Spezialisten für Cybercrime zur europäischen Polizeibehörde Europol wird künftig eine schnelle und technisch kompetente Informationsweitergabe bei operativen Fällen gewährleistet.

Mit der Einrichtung einer zentralen Ansprechstelle als bundesweite Kontaktstelle zwischen den Betreibern sozialer Medien und inländischen Polizeieinheiten werden künftig Anfragen effektiv und effizient gestaltet. Dies hat nicht nur positive Auswirkungen bei der Kriminalitätsbekämpfung, sondern dient auch der raschen Informationsgewinnung bei Hilfeleistungen im Falle verunglückter oder vermisster Personen.

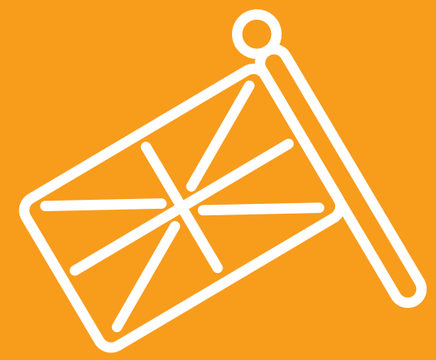
Da dienliche und notwendige forensische Aufgaben meist direkt vor Ort durchzuführen sind, wird eine mobile Referenzlösung im Rahmen eines Projekts des BMI erstellt werden. Mittels eines forensischen Auswertungsclusters, einer speziell eingerichteten Serverlandschaft soll eine qualitativ hochwertige Auswertung der vermehrt sichergestellten Daten effizienter und schneller möglich werden. Dem zunehmenden Einsatz von Verschlüsselungstechnologien auf Seiten der Täter, wird mittels nationaler Forschungsinitiativen und Projekten zum Ausbau der Entschlüsselungskapazitäten entgegengewirkt.

Der kontinuierlich starke Anstieg der Cyberdelikte erfordert ein größeres Problembewusstsein in allen gesellschaftlichen Bereichen. Präventivmaßnahmen zur Steigerung

der Widerstandsfähigkeit gegen Cyber-Angriffe werden auch künftig über bestehende Kooperationen weiter ausgebaut.

Zur Umsetzung und Finanzierung der Cybersicherheitsstrategie und der damit verbundenen Bekämpfung von Cybercrime werden für Projektvorhaben vermehrt spezielle EU-Budgets herangezogen.

8 Summary and Outlook



Conclusion

Constantly increasing numbers of cybercrime offences and more and more complex modi operandi likewise call for a constant adjustment of resources and structures of those units investigating cybercrime. In particular, the structural adaptations and moving C4 to a modern building is a highly important milestone. At the same time, the cybercrime investigations in the provincial CIDs and on district level will be strengthened by additional personnel. Most important is the specialization in current and future phenomena as well as national and international cooperation.

The rapidly changing offenders as well as new technologies require a constant development and training of the criminal police officers as well as uniformed police. This is done partly by IT investigators in the districts. A necessary expansion has already been developed in the course of a project as a complete training concept is planned. In addition, the Cybercrime Experts Circle (CEC), established by the Cybercrime Competence Centre (C4), is an international platform for the exchange of practical knowledge with experts from partner countries.

A swift and efficient reaction to international cyber events of operational CID services continues to be a challenge. In order to guarantee that knowledge in an operational case can be swiftly exchanged, a cybercrime expert will be sent to the European police authority Europol.

A central point of contact established for the providers of social media in cooperation with Austrian police units will help to deal with inquiries efficiently and effectively. This will not only have positive effects on the fight against crime but will also serve to quickly obtain information in case of missing persons or victims of accidents.

Necessary forensic examinations mostly have to be carried out on site; therefore, a mobile reference solution will be established in the course of a project of the Federal Ministry of the Interior. With the help of forensic analysis, a specially equipped server landscape, high-quality analysis of the growing number of seized data shall be guaranteed in a more swift and efficient way. The increased use of encryption technologies on the part of the offenders is countered by national research initiatives and projects to develop the decryption capacities.

The continuous increase in cybercrime requires a greater awareness for the problem in all social levels. Preventive measures and existing cooperation to increase resilience against cyber attacks will be further developed in the future.

In order to finance and implement cyber security strategies and thus the fight against cybercrime dedicated EU budgets are used for planning projects.

9 Glossar

Anonymisierungsdienst

Bei Anonymisierungsdiensten handelt es sich um Services und Techniken im Internet, die dazu dienen, bestimmte Informationen, die auf die Identität einer Internetnutzerin oder eines Internetnutzers hindeuten könnten, zu verschleiern.

Antivirenprogramm

Ein Antivirenprogramm (synonym mit Virenscanner oder Virenschutz) ist eine Software, die bekannte Schadsoftware, wie beispielsweise Computerviren in einem Computersystem aufspüren kann, blockiert und gegebenenfalls beseitigt. Auch wenn damit ein grundlegender Schutz gegeben ist, erfolgt dieser nicht zu hundert Prozent, da es laufend neue Schadsoftware gibt, die noch nicht erkannt wird.

Applikation / App

Eine Applikation, kurz App oder Anwendungssoftware, ist ein Computerprogramm. Häufig wird der Begriff App im Zusammenhang mit Anwendungen für mobile Endgeräte, wie Tablets oder Smartphones verwendet.

BEC (Business Email Compromise)

Angreifer kompromittieren bei einem BEC den E-Mail-Schriftverkehr eines Unternehmens mit dem Ziel, eine Mitarbeiterin oder einen Mitarbeiter der Firma zu einer Geldtransaktion auf das Bankkonto der Täter zu veranlassen. Es handelt sich hier um gezielte Angriffe gegen bestimmte Unternehmen, da die Täter im Vorfeld teilweise umfangreiche Recherchen anstellen und sich häufig mittels Social Engineering zusätzliche Informationen verschaffen. Um derartige Fälle zu vermeiden, ist eine Sensibilisierung der Unternehmensmitarbeiterinnen und -mitarbeiter durchzuführen und es ist ratsam im Schriftverkehr mit Handelspartnerinnen und -partnern vorsichtig zu sein. Bei unklaren oder eigenartigen Sachlagen über eine andere Technologie (Telefon) sind die Sachverhalte zu überprüfen.

Behördenwallets

Das C4 ist seit 2018 rechtlich und technisch in der Lage Sicherstellungen von Kryptowährungen durchzuführen. Hierfür werden unter höchsten Sicherheitsvorkehrungen sogenannte Behördenwallets erstellt und zur Aufbewahrung von virtuellen Währungseinheiten verwendet.

Das BK verfügt jederzeit über etwa 1.000 Behördenwallets von verschiedenen Kryptowährungen, die rund um die Uhr für Sicherstellungen von Strafverfolgungsbehörden zur Verfügung stehen.

Bitcoin

Bitcoin (englisch für „digitale Münze“) ist ein weltweit verwendbares dezentrales Register und der Name eines immateriellen Vermögenswertes. Überweisungen werden von einem Zusammenschluss von Rechnern über das Internet mittels Blockchain (durchgehende Kette von Transaktionsblöcken) abgewickelt, sodass anders als im herkömmlichen Bankverkehr keine zentrale Abwicklungsstelle benötigt wird. Eigentumsnachweise können in einer persönlichen digitalen Brieftasche, einem sogenannten Wallet, gespeichert werden.

Collége Européen de Police (CEPOL)

Die European Union Agency for Law Enforcement Training beziehungsweise Europäische Polizeiakademie ist eine durch Beschluss des Rates der europäischen Justiz- und Innenminister im Jahr 2000 gegründete europäische Einrichtung zur Ausbildung der europäischen Polizei.

CaaS (Crime as a Service)

Die für die Begehung einer Straftat benötigten Dienste werden gleichsam eines Puzzles individuell zusammengestellt und gleich online erworben. Dabei handelt es sich vorwiegend um Hackingtools, Schadsoftware, wie beispielsweise Verschlüsselungstrojaner, aber auch um spezielle Dienstleistungen zur Geldwäsche, für Übersetzungen oder für den vermeintlichen Opfer-Support. Die Täter benötigen damit kein tiefgreifendes technisches Wissen zur Straftatbegehung, sondern kaufen sich das fehlende Wissen schlichtweg zu.

Cybermobbing

Der Begriff Cybermobbing bezeichnet das absichtliche und über einen längeren Zeitraum anhaltende Beleidigen, Bedrohen, Bloßstellen, Belästigen oder Ausgrenzen von Personen über digitale Medien, wie beispielsweise über soziale Netzwerke, Messenger Apps oder in Videoportalen.

Darknet

Große Teile des Internets sind für übliche Suchmaschinen nicht zugänglich. Diese zeigen oft nur Inhalte des offenen Internets, dem Clearweb, an. Dort liegen alle Daten unverschlüsselt vor und können durchsucht sowie meist über eine Adresse, den so genannten Uniform Resource Locator (URL), aufgerufen werden. Um in das Darknet beziehungsweise Tor-Netzwerk zu gelangen, benötigt man beispielsweise einen speziellen Browser, wie den Tor-Browser. Daten werden im Darknet anonym und verschlüsselt über verschiedene Server geschickt. Das Darknet war ursprünglich für Personen und Organisationen gedacht, die von Zensur bedroht waren. Heutzutage reicht das Spektrum an illegalen Aktivitäten

im Darknet vom Drogen- und Waffenhandel über Dokumentenfälschung, Geldfälschung, Datenhandel bis hin zu Online-Kindesmissbrauch und weit darüber hinaus.

DDoS-Angriffe

DDoS-Angriffe (Distributed Denial of Service-Angriffe) sind Attacken auf die Verfügbarkeit der Ressourcen und Dienste eines IT-Systems oder von Netzwerken meistens mit dem Ziel, diese zu blockieren und somit regulären Benutzerinnen und Benutzern keinen Zugriff mehr zu ermöglichen. Die Angriffe erfolgen häufig von vielen verschiedenen Ressourcen aus dem Internet. Neben politisch oder persönlich motivierten Angriffen versuchen Täter auch häufig Geld mit DDoS-Angriffen zu erpressen.

Domain Name System (DNS)

Das DNS ist einer der wichtigsten Dienste im Internet. Seine Hauptaufgabe ist die Auflösung des Domainnamens, wie zum Beispiel www.bmi.gv.at, in eine IP-Adresse, um eine Kommunikation zwischen den Computersystemen zu ermöglichen.

European Cybercrime Center (EC3)

Das EC3 ist ein Teil von Europol und wurde eingerichtet, um in folgenden drei Bereichen signifikante Unterstützung für die Mitgliedsstaaten zu schaffen:

- Bekämpfung von Cybercrime, begangen durch organisierte Gruppierungen, die beispielsweise durch Online-Betrug große Geldmengen erbeuten.
- Bekämpfung von Formen von Cybercrime, die die Opfer massiv schädigen, wie beispielsweise sexueller Missbrauch von Kindern.
- Bekämpfung von Cybercrime (inklusive Cyberattacken), die gegen kritische Infrastruktur und Informationssysteme der EU-Mitgliedsstaaten gerichtet ist.

Firewall

Eine Firewall ist ein System aus hardware- und/oder softwaretechnischen Komponenten, um Netzwerke sicher miteinander zu verbinden. Die Firewall analysiert den Netzwerkverkehr und hat beispielsweise die Aufgabe, unerwünschte Zugriffe von außen wie dem Internet zu blockieren.

IP-Adresse

Eine IP-Adresse dient zur eindeutigen Adressierung von Computern und anderen Geräten in einem Netzwerk, das auf dem Internetprotokoll (IP) basiert. Sie wird jedem Gerät in einem Netzwerk zugewiesen und macht somit jedes Gerät adressierbar und damit erreichbar. Die IP-Adresse entspricht funktional der Rufnummer in einem Telefonnetz. Technisch wird unterschieden zwischen IP-Version 4 (IPv4) und IP-Version 6 (IPv6) unterschieden. Letzteres wurde unter anderem eingeführt, da die Anzahl der möglichen öffentlichen Adressen bei IPv4 stark beschränkt sind und mittlerweile als aufgebraucht gelten.

Kryptowährungen und Blockchain

Kryptowährungen sind digitale Zahlungsmittel, die auf verschlüsselten Datensätzen basieren. Mit dieser Form der Zahlungsmittel ist ein digitaler Zahlungsverkehr ohne ein dazwischen geschaltetes Geldinstitut möglich. Der Besitz des Code-Schlüssels stellt dabei das Eigentum dar. Zahlungstransaktionen mit Kryptowährungen werden in sogenannten Blöcken gespeichert. Das Buchungssystem nennt man Blockchain. Die bekannteste Kryptowährung ist der Bitcoin. Das Bitcoin-Zahlungssystem wurde 2008 unter dem Pseudonym Satoshi Nakamoto erstmals veröffentlicht. Obwohl Kryptowährungen in den vergangenen Jahren auch Kursverluste hinnehmen mussten, ist ein steigender Trend bei legalen als auch illegalen Bezahlvorgängen zu beobachten. Insbesondere im Bereich Cybercrime haben sich „Cryptos“, vor allem bei Massenerpressungs-E-Mails und im Suchtgifthandel durchgesetzt. Auch wenn Bitcoin immer noch an erster Stelle rangiert, wird mittlerweile ebenso mit anderen, als „Altcoins“ bezeichneten, Kryptowährungen bezahlt.

Love Scam / Romance Scam

Bei Love Scam handelt es sich um eine Art von Partnervermittlungsbetrug. Der Täter stellt meist den ersten Kontakt per E-Mail oder soziale Medienplattformen her und versucht eine Vertrauensbasis durch zum Beispiel die Zusage von persönlichen Treffen zu schaffen. Durch das Vortäuschen einer Notsituation wird in Folge der elektronischen Kommunikation versucht, das Opfer zum Übersenden von Geld und Wertgegenständen zu überreden. Tatsächlich existiert die dargestellte, geliebte Person aber nicht, sondern dient dem Täter nur als Tarnung. Die Betrügerinnen und Betrüger schrecken dabei auch nicht davor zurück die Identität und den Internetauftritt von realen Personen zu missbrauchen.

Malspam

Bei Malspam beziehungsweise „Malicious Spam“ handelt es sich um Spam-E-Mails, die zur Verbreitung von Schadsoftware dienen. Diese E-Mails können bereits Schadsoftware oder schädliche Elemente, versteckt als JavaScript, eingebettet in komprimierten Dateien oder anderen Datenformaten, beinhalten. Oder diese E-Mails beinhalten einen Link, der aktiv von der Empfängerin der dem Empfänger angeklickt werden muss, damit die schädlichen Komponenten auf dem Gerät des Opfers installiert werden.

Money Mules

Wie die deutsche Übersetzung der Bezeichung Money Mule, nämlich Geldesel, vermuten lässt, wird von einer Person illegal erworbenes Geld im Rahmen von Kurierdiensten transferiert, um die Strafverfolgung zu erschweren. Meist erhält die Person ein Entgelt für den Geldtransfer, ist sich aber dabei nicht bewusst, dass sie aktiv an Geldwäsche beteiligt ist. Die Anwerbung erfolgt oft über E-Mail.

Network Address Translation (NAT)

Bei Carrier Grade NAT teilt der Provider eine IPv4-Adresse aus dem privaten Adressbereich „10.0.0.0/8“ den Endkundenanschlüssen zu – keine „öffentliche IP Adresse“ (§ 92 Abs 3 Z 16 TKG). Auf diese Weise spart er mittlerweile sehr rare öffentliche IPv4-Adressen. Zwischen dem privaten Provider-Netz und dem öffentlichen IPv4-Netz vermittelt dann die NAT oder Port Address Translation (PAT). Der dafür zuständige vermittelnde Server kümmert sich um die Adressübersetzung zwischen den privaten und öffentlichen IPv4-Adressen und reicht die Pakete zwischen den Netzwerken weiter. NAT wurde ursprünglich für lokale Netzwerke, wie dem WLAN-Router zu Hause, entwickelt, die nur eine öffentliche IPv4-Adresse zugeteilt bekommen haben. Diese wird aber von mehreren Clients als Zugang zum öffentlichen Netz genutzt. NAT findet hier in kleinem Rahmen mit wenigen Clients statt. Bei Carrier Grade NAT sind davon meist mehrere tausend Clients betroffen und gleichzeitig wird doppelt geNATet, weil die Kundin oder der Kunde immer noch nur eine IPv4-Adresse für mehrere Clients bekommt.

Bei jedem NAT- oder PAT-Vorgang wird nicht nur die private IP-Adresse in eine öffentliche übersetzt, sondern auch die zu der Netzwerkadressierung (IP-Adresse und Port, Schreibweise zum Beispiel 194.203.112.23:80) gehörenden Ports ändern sich. Das bedeutet, dass bei jedem NAT Vorgang von dem NAT Verbindungsserver einer bestimmten IP-Adresse aus dem internen Netz eine bestimmte Portnummer der öffentlichen IP im externen Netz (dem Internet) eindeutig zugewiesen wird, damit der Kommunikationsvorgang nachvollziehbar bleibt. Sonst wüsste der Verbindungsserver nicht, wer welche Kommunikation durchführt. Das Identifikationsmerkmal des Nutzeranschlusses ist daher nicht mehr nur die IP-Adresse, sondern auch der sogenannte Source-Port oder sozusagen als „Rückrechnung“ für die Provider die Ziel-IP und der Ziel-Port.

Open Source Intelligence (OSINT)

OSINT befasst sich mit der Gewinnung von Informationen, die über offene Quellen frei verfügbar im Internet zu finden sind. Diese Daten werden für weitere Ermittlungen und Analysen herangezogen, um gezielte Erkenntnisse daraus herzuleiten.

Phishing

Mit Phishing wird versucht, beispielsweise über gefälschte Webseiten, E-Mails oder andere Messenger-Nachrichten an persönliche Daten zu gelangen. Phishing steht häufig im Zusammenhang mit zumindest versuchten Betrugshandlungen und Identitätsmissbrauch.

Ransomware

Als Ransomware wird Schadsoftware bezeichnet, die den Zugriff auf Daten und elektronische Systeme durch Verschlüsselung von Daten oder Bereichen des Betriebssystems einschränkt oder verhindert. Diese Ressourcen werden erst wieder nach Bezahlung eines Lösegeldes („ransom“), meist in Form von Kryptowährung, freigegeben.

RAT (Remote Access Trojaner)

Hierbei handelt es sich um ein Schadprogramm, das eine Hintertür (backdoor) für administrative Kontrolle auf dem Zielsystem öffnet. RATs werden üblicherweise im Hintergrund durch ein Programm heruntergeladen, das der Anwender aufgerufen hat, bspw. ein Spiel oder ein E-Mail-Anhang. Sobald das Zielsystem kompromittiert ist, macht sich der Eindringling diesen Umstand zunutze, um RATs auf andere anfällige Computer zu verteilen.

Schadsoftware

Bei Schadsoftware (synonym mit den Begriffen Schadprogramme, Schadcode oder Malware) handelt es sich um Programme oder Skripte, die mit dem Ziel entwickelt wurden, eine unerwünschte und meistens schädliche Funktion auf Computersystemen auszuführen.

Smart Contracts

Dabei handelt es sich um Computerprotokolle, die Verträge abbilden, überprüfen oder die Verhandlung und Abwicklung eines (Kauf-)Vertrages technisch unterstützen.

Social Engineering

Bei Social Engineering werden vermeintliche menschliche Schwächen wie Neugier oder Angst ausgenutzt, um Zugriff auf sensible Daten oder Informationen zu erhalten. Bei Cyber-Angriffen verleiten Täter ihre Opfer dazu, eigenständig wichtige Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadsoftware auf ihren Systemen zu installieren. Während vor vielen Jahren noch der Müll nach Dokumenten

und Datenträgern durchsucht wurde, geschieht das Ausforschen von Informationen heutzutage oft durch das Ausspähen von Daten auf Social Media Plattformen und Anrufen mit falschen Identitäten.

Spam

Als Spam bezeichnet man elektronische, unerwünschte Nachrichten, die massenhaft und gezielt über verschiedene Kommunikationsdienste verbreitet werden. Teilweise beinhaltet Spam in harmlosen Varianten unerwünschte Werbung. Häufig jedoch enthält Spam auch Schadsoftware im Anhang, Links zu infizierten Webseiten oder wird für Phishing Angriffe genutzt.

Stranded Traveller Scam

Die Opfer erhalten eine E-Mail von jemandem den sie meist persönlich kennen und in der behauptet wird, dass das Gegenüber wegen eines Raubüberfalls in einem fremden Land gestrandet wäre und gerade Sie braucht, um ihm/ihr zu helfen, nach Hause zurückzukehren. Gefordert werden Geldbeträge in unterschiedlicher Höhe. Tatsächlich wurde das E-Mail-Konto gehackt und die Nachricht an alle Kontakte im Adressbuch gesendet. Die Hacker können E-Mails an das Konto des Opfers umleiten und so das weitere Geschehen steuern.

Trojaner (Trojanisches Pferd)

Als Trojanisches Pferd bezeichnet man ein Computerprogramm oder Applikation, das als nützliche oder harmlose Anwendung getarnt ist, im Hintergrund aber ohne Wissen der Anwenderin oder des Anwenders eine andere, meist schädliche Funktion erfüllt.

Uniform Resource Locator (URL)

Ein URL identifiziert und lokalisiert Ressourcen im Internet, wie beispielsweise Webseiten. Das URL-Format macht eine eindeutige Bezeichnung von Dokumenten im Internet möglich und beschreibt die Internetadresse von Objekten, die von einem Browser gelesen werden können, zum Beispiel http://www.bmi.gv.at.

Virus

Bei (Computer-)Viren handelt es sich um die älteste Art von Schadsoftware, die sich selbstverbreiten und unterschiedliches Schadpotenzial in sich tragen. Sie treten in Kombination mit einem Wirt auf, das heißt mit einem infizierten Dokument oder einer Applikation.

Verschlüsselung

Verschlüsselung transformiert Daten in Abhängigkeit von einer Zusatzinformation, dem Schlüssel, in einen zugehörigen Geheimtext, der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation, das heißt die Zurückgewinnung des Klartextes aus dem Geheimtext, wird Entschlüsselung genannt.

Wallet

Ein Wallet, der englische Begriff für „Geldbeutel“ oder „Portemonnaie“, ist eine virtuelle Geldtasche, in der der Benutzer Bitcoins oder auch andere Kryptowährungen aufbewahrt. Insofern kann ein Wallet mehrere unterschiedliche Kryptowährungen beinhalten. Darüber hinaus gibt es unterschiedliche Arten von Wallets.

WHOIS

WHOIS ist ein Service im Internet, das vor allem zur Abfrage von Daten zu Domainnamen genutzt wird. Vor der Datenschutz-Grundverordnung (DSGVO) war es uneingeschränkt möglich den Eigentümer und den Ansprechpartner der Domain (siehe Domain Name System) sowie IP-Adressen über diesen Dienst abzufragen, da alle Daten öffentlich zugänglich gewesen sind.

Deliktsbezeichnungen nach Paragrafen

Strafgesetzbuch (StGB)

- § 107a StGB — Beharrliche Verfolgung
- § 107c StGB — Fortdauernde Belästigung im Wege einer Telekommunikation oder eines Computersystems
- § 118a StGB — Widerrechtlicher Zugriff auf ein Computersystem
- § 119 StGB — Verletzung des Telekommunikationsgeheimnisses
- § 119a StGB — Missbräuchliches Abfangen von Daten
- § 126a StGB — Datenbeschädigung
- § 126b StGB — Störung der Funktionsfähigkeit eines Computersystems
- § 126c StGB — Missbrauch von Computerprogrammen oder Zugangsdaten
- § 144 StGB — Erpressung
- § 145 StGB — Schwere Erpressung
- § 146 StGB — Betrug
- § 147 StGB — Schwerer Betrug
- § 148 StGB — Gewerbsmäßiger Betrug
- § 148a StGB — Betrügerischer Datenverarbeitungsmissbrauch
- § 207a StGB — Pornographische Darstellungen Minderjähriger
- § 207b StGB — Sexueller Missbrauch von Jugendlichen
- § 208a StGB — Anbahnung von Sexualkontakten zu Unmündigen
- § 218 StGB — Sexuelle Belästigung und öffentliche geschlechtliche Handlungen
- § 223 StGB — Urkundenfälschung
- § 224 StGB — Fälschung besonders geschützter Urkunden
- § 225a StGB — Datenfälschung
- § 228 StGB — Mittelbare unrichtige Beurkundung oder Beglaubigung
- § 229 StGB — Urkundenunterdrückung
- § 231 StGB — Gebrauch fremder Ausweise
- § 232 StGB — Geldfälschung
- § 241a StGB — Fälschung unbarer Zahlungsmittel
- § 283 StGB — Verhetzung
- § 297 StGB — Verleumdung

Suchtmittelgesetz (SMG

- § 27 SMG — Unerlaubter Umgang mit Suchtgiften
- § 28 SMG — Vorbereitung von Suchtgifthandel
- § 28a SMG — Suchtgifthandel
- § 30 SMG — Unerlaubter Umgang mit psychotropen Stoffen

Verbotsgesetz (VerbotsG)

- § 3g VerbotsG — Wiederbetätigung