Bundesministerium
Inneres

Bundeskriminalamt

Cybercrime Report 2019

Lagebericht über die Entwicklung von Cybercrime

Cybercrime Report 2019

Lagebericht über die Entwicklung von Cybercrime

Wien 2020

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 2020

Inhalt

Vorwort **5**

1 Einleitung **6**

Über die Broschüre 7

Entwicklungen und Trends 8

2 Rechtliche Herausforderungen **9**

Anpassung des Cyberstrafrechts 10

Datenschutz-Grundverordnung und „WHOIS“ Abfragen 10

Carrier Grade NAT Problematik 10

Pseudoanonyme Transaktionen von virtuellen Währungen 11

3 Jahresrückblick **13**

Zahlen und Fakten im Überblick 14

Cybercrime im engeren Sinn 15

Cybercrime im weiteren Sinn 16

Dunkelziffer und Anzeigeverhalten 17

4 Phänomeneund Ermittlungen **18**

„Crime as a Service“ 19

Ransomware 19

Bitcoin-Mixer und deren erfolgreiche Bekämpfung 20

Erpressungs-E-Mails 21

Internetbetrug 21

Voice over IP-Spoofing 22

Suchtmittelhandel im Darknet 23

Pornographische Darstellungen Minderjähriger 24

5 Bekämpfung **26**

Kriminalpolizeiliche Struktur zur Bekämpfung von Cybercrime 27

Meldestelle 28

Zentrale Aufgaben 30

Forensik 30
IT-Ermittlungen 32
Entwicklung und Innovation 33
Bundesweite polizeiliche Zusammenarbeit 34
Neue Erfolgsmodelle in der Ablauforganisation 35
6 Zusammenarbeit mit der Polizei 36
Anzeigenerstattung 37
7 Events und internationale Gremien 39
Fachtagung IT-Beweismittelsicherung (ITB) 40
Symposium „Neue Technologien (NT)“ 40
8 Kriminalprävention 41
Verhinderung von Straftaten 42
9 Herausforderungen und Projekte 43
10 English Summary 45
11 Glossar 47

Vorwort

Liebe Leserinnen, liebe Leser!

Bundesminister für Inneres Karl Nehammer, MSc und geschäftsführender Direktor des Bundeskriminalamtes Gerhard Lang, BA MA

Cybercrime ist ein immer stärker zunehmendes Deliktsfeld. Die Opfer ziehen sich durch alle Altersgruppen und Gesellschaftsschichten. Waren vor einem Jahrzehnt noch wenige Delikte diesem Bereich zuzuordnen, steigen seit 2014 die Fallzahlen kontinuierlich und erreichten 2019 ein Rekordhoch. Durch die Digitalisierung und dem Zugang zu Diensten wie „Crime as a Service“ oder technischen Neuerungen haben es die Täter einfacher ihre Reichweite zu steigern, wodurch auch erhöhte Schadenssummen resultieren.

Um dieses Kriminalitätsfeld nachhaltig bekämpfen zu können, sind folgende Bereiche für die Sicherheitspolitik im Bereich Cybercrime von großer Wichtigkeit: verbesserte politische und rechtliche Rahmenbedingungen zur Eindämmung von Cybercrime, eine erhöhte Bewusstseinsbildung für mehr Sicherheit und Eigenverantwortung im Internet, eine Stärkung der Widerstandsfähigkeit gegen kriminelle Cyber-Angriffe in der Wirtschaft sowie eine schnelle und wirksame Reaktion auf Cyber-Vorfälle.

Die politischen und rechtlichen Rahmenbedingungen für Cybercrime sind in der EU und international sehr unterschiedlich. Das Bemühen für die im Bericht genannten, konkreten Problembereiche und auch umfassenden, strategischen Vorgehensweisen müssen weiterhin forciert werden.

Kriminalpolizeilich werden auch weiter jene operativen Maßnahmen überlegt und angeglichen, die im Rahmen der vorgegebenen strategischen Leitlinien von EU-Cyber-Sicherheitsstrategien, nationalen Strategien im Bundeskanzleramt und innerhalb des Bundesministeriums für Inneres entwickelt werden.

Ihr

Karl Nehammer MSc
Bundesminister für Inneres

Gerhard Lang, BA MA
Geschäftsführender 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 eine wirksame Umsetzung der politischen Rahmenbedingungen und deren effektive Vollziehung durch die Exekutive liegen. Betrachtet werden hier nur die in Österreich geltenden Definitionen und Abgrenzungen von Cyber-Kriminalität. Die Aufgaben der Cyber-Sicherheit, Cybercrime-Abwehr und Desinformation unterliegen den Verantwortungen anderer Organisationen.

Die Ergebnisse aus den Analysen basieren auf Informationen, die in der fachlichen Zentralstelle des Bundeskriminalamtes (BK), im Cybercrime Competence Center (C4) zusammenlaufen sowie aus gesammelten Meldungen, Anzeigen, Statistiken, internationalen Kooperationen, Informationsaustausch mit Mitgliedsstaaten, Ausbildungen, Positionspapieren und Studien von Dritten stammen. Die Bestandsaufnahme der quantitativen Daten und qualitativen Inhaltsanalysen fand von Jänner bis April 2020 statt, wobei Entwicklungen bis zum Dezember 2019 berücksichtigt wurden.

Der Bericht teilt sich in mehrere Kapitel: Im ersten Kapitel zu den rechtlichen Rahmenbedingungen werden die größten Herausforderungen für das kriminalpolizeiliche Handeln dargestellt. Der Jahresrückblick mit den kriminalstatistischen Analysen ist ein wesentlicher Faktor für die strategische Ausrichtung zur Kriminalitätsbekämpfung und wird als Grundlage für die Optimierung der präventiven und repressiven Maßnahmen herangezogen. Trotz des enormen Anstiegs der Cybercrime-Delikte von 44,9 Prozent im Vergleich zum Vorjahr konnte die Aufklärungsquote mit 35,8 Prozent annähernd konstant gehalten werden. Im Folgekapitel werden die wichtigsten Phänomene im Detail beschrieben und fallweise mit vorbeugenden Handlungsempfehlungen ergänzt. Die Aufbauorganisation und ihre Abläufe werden im nächsten Kapitel angeführt. Sie sind auch aufgrund der technischen Komplexität mit ständigem Wissensaufbau und einhergehender Spezialisierung sehr flexibel gestaltet. In diesem Kapitel folgt auch eine Beschreibung der zentralen Strategien zur Kriminalitätsbekämpfung im Bereich Cybercrime mit einer quantitativen Übersicht zu den stark ansteigenden Tätigkeiten der digitalen Forensik und der Meldestelle im C4. Im Anschluss wird auf die Wissensvermittlung und den internationalen Austausch eingegangen. Die Kriminalprävention bildet gemeinsam mit der Zusammenfassung und dem strategischen Ausblick den Abschluss des Berichts.

Die Nutzung der im Bericht angegebenen Daten (vollständig oder auszugsweise) ist nur mit der Quellenangabe „Polizeiliche Kriminalstatistik (PKS)“ gestattet.

Entwicklungen und Trends

Die markanten Entwicklungen im Bereich Cybercrime sind einerseits auf den massiven Anstieg von Massenerpressungs-E-Mails zu Jahresbeginn und andererseits dem ganzjährig stark auftretenden Internetbetrug zurückzuführen. Den Erpressungen wurde durch die Einrichtung einer eigenen Arbeitsgemeinschaft „ARGE Erpressungsmails“ begegnet und der Internetbetrug wurde kooperierend im Rahmen der Linienorganisation bearbeitet. Darüber hinaus zeigte sich ein Trend bei Tätern zur Nutzung von Ransomware und anderen „Crime as a Service“-Leistungen aus dem Darknet.

Nach wie vor fehlen nötige rechtliche Rahmenbedingungen im Hinblick auf die Problematiken bei Carrier Grade NAT, Domainnamen und Kryptowährungen, die derzeit die kriminalpolizeiliche Arbeit massiv erschweren und sogar verhindern. Eine Aktualisierung der Strategie und Konzepte zur Bekämpfung von Cybercrime ist geplant und betrifft die Bereiche IT-Ermittlungen sowie die digitale Beweismittelsicherung. Verbesserungen der Prozesse und Abläufe inklusive der einzusetzenden Technologien finden laufend statt, um den stetig fortschreitenden technischen Herausforderungen gerecht werden zu können.

2 Rechtliche Heraus-forderungen

Anpassung des Cyberstrafrechts

Bei kriminalpolizeilichen Ermittlungen in Zusammenhang mit Cybercrime-Delikten kommt es immer wieder zu Ermittlungshindernissen beziehungsweise Erschwernissen, die zum Teil auf die derzeitigen eng gefassten materiellen strafrechtlichen Bestimmungen zurückzuführen sind. So ist zum Beispiel ein Datendiebstahl, der nicht durch „Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem" erfolgt, gerichtlich nicht strafbar. Das BK spricht sich daher für eine Angleichung des „digitalen" Cyber-Strafrechts an das „analoge" Strafrecht wie, zum Beispiel in Zusammenhang mit Strafbestimmungen beim Diebstahl, aus. Bei der Beurteilung von begangenen Cyber-Delikten sollte eine entsprechende differenzierte Betrachtung und damit auch differenzierte Strafandrohungsbestimmungen erfolgen, je nach Datenumfang, Datenqualität oder Datensensibilität.

Datenschutz-Grundverordnung und „WHOIS" Abfragen

Domainnamen, wie „www.bundeskriminalamt.at", machen Informationen im Internet leichter auffindbar. Die dafür benötigten Domänen können bei Registries und Registraren angemietet werden. „WHOIS" Abfragen im Internet führten in der Vergangenheit häufig noch direkt zum Inhaber einer Domäne und zu einer technischen Kontaktperson. Diese Domainnamen zählen zu den Grundbausteinen des Internets. Personenbezogene Auskünfte sind für weiterführende Ermittlungen von hoher Bedeutung und waren bis zum Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2018 auch öffentlich zugänglich. Durch die Vielzahl von Registries und Registraren, die für die Verwaltung von Domainnamen zuständig sind, ergeben sich weitere Herausforderungen bei den Nachforschungen. Waren vormals nur einfache Abfragen in öffentlichen Datenbanken erforderlich, müssen bei Auskunftsersuchen an internationalen Standorten verwaltungstechnisch höchst aufwändige Prozesse durchlaufen werden. Diese erheblichen Ermittlungshürden werden als Folge der DSGVO auch in technischen und rechtlichen Gremien mit der Dachorganisation der Domänenverwaltung ICANN behandelt. Bis dato konnten keine von diesen Organisationen in Aussicht gestellte Konzepte final umgesetzt werden

Weitere Informationen:
https://www.icann.org/public-comments/epdp-phase-2-addendum-2020-03-26-en

Carrier Grade NAT Problematik

Aufgrund der häufigen Nutzung der Carrier Grade NAT Technologie, bei denen mehreren Internetnutzerinnen und Internetnutzer zeitgleich idente IP-Adressen vom Netz Provider zugewiesen werden, können viele Straftaten nicht geklärt und auch die Verfasser von Hasspostings sowie Fakenews nicht ausgeforscht werden. Dies führt im Rahmen der Ermittlungen zu erheblichen Problemen bei der Zuordnung und Identifizierung krimineller Userinnen und User, wenn vom Netzanbieter die üblichen Protokollierungen von Userinnen und Usern beispielsweise auf Grund der fehlenden rechtlichen Rahmenbedingungen nicht gespeichert werden dürfen und daher nicht übermittelt werden können. Überdies gibt es international und auch auf europäischer Ebene selbst zwischen den einzelnen Mitgliedstaaten sehr große Unterschiede in deren rechtlichen Rahmenbedingungen zu dieser Thematik.

Das Beispiel eines aktuellen Ermittlungsfalles zeigt die negativen Folgen unzureichender Rechtsrahmen:
In Serbien wurde eine ermordete Frau aufgefunden, die nach Ermittlungen identifiziert werden konnte. Das Opfer war bereits sieben Tage tot, aber die Nachforschungen ergaben, dass zur Verschleierung auch nach ihrer Ermordung von ihrem Account auf sozialen Medien gepostet wurde. Diese Nachrichten werden dem mutmaßlichen Mörder zugeordnet, der mehrere österreichische IP-Adressen für diese Postings verwendet hatte. Der österreichische Kabelanbieter konnte aufgrund der Verwendung von Carrier Grade NAT mit dem österreichischen Rechtsrahmen keine Auskunft erteilen. Zum besseren Verständnis zur diesbezüglichen Thematik wird angeführt, dass die Speicherung über den Inhaber einer dynamischen IP-Adresse in Österreich nicht erlaubt ist, wenn die Zuordnung eine größere Zahl von Teilnehmern erfasst – was im Fall von Carrier Grade Nat immer zutrifft. Der Mord konnte bis dato nicht geklärt werden.

Eine diesbezügliche Harmonisierung auf europäischer Ebene wäre insofern erstrebenswert.

Pseudoanonyme Transaktionen von virtuellen Währungen

Kryptowährungen wie Bitcoins sind unter anderem auch ein beliebtes Mittel für Finanztransaktionen, bei der Geldwäsche und für Käufe illegaler Waren im Internet. Jeder kann selbst anonym eigene Wallets erstellen, die wie eine digitale Geldbörse zur Aufbewahrung und wie ein Bankkonto für den Versand und Empfang von virtuellen Währungen genutzt werden. Der Einsatz von Computerprogrammen ermöglicht es zudem eine Vielzahl von Schritten beim Zahlungsverkehr zu automatisieren. Das reicht von der Generierung dieser Wallets, bis zu eigenständigen, maschinellen Überweisungen von

Geldbeträgen. Durch die Flut an anonymen Überweisungen werden Strafverfolgungsbehörden vor Herausforderungen gestellt, die bei den notwendigen Erhebungen nicht mehr bewältigt werden können.

Zum Zwecke der Strafverfolgung und zur Abwehr von Gefahren wäre für Ermittlungen die Schaffung verbesserter rechtlicher Rahmenbedingungen erstrebenswert. 2019 wurde die 5. Geldwäscherichtlinie umgesetzt, die bereits eine Verbesserung der Situation brachte. Dennoch gibt es in dieser Richtlinie bei virtuellen Währungen noch offene Gesetzeslücken wie zum Beispiel den Grenzwert für Transaktionen ab dem die Identität des Inhabers durch die so genannten Krypto Exchange, die vor allem virtuelle Währungen in reales Geld tauschen und umgekehrt, protokolliert werden muss. Einen Lösungsweg zeigt die Schweizer Finanzmarktaufsicht Finma auf, die altbekannte Regeln auch für Kryptozahlungen gegen Bedenken und Widerstände von Lobbyisten durchsetzen konnte. Die Legislative erweiterte einfach ein Verfahren, das schon seit langem für gewöhnliche Finanztransaktionen bei der Durchführung durch Banken gilt. Die mittlerweile in der Schweiz geltende verpflichtende Übermittlung von Sender und Geldempfänger bei Transaktionen von virtuellen Währungen versetzt die Schweiz nun in die Lage organisierte Kriminalität, Geldwäsche und Terrorismusfinanzierung wesentlich besser bekämpfen zu können.

3 Jahresrück-blick

Zahlen und Fakten im Überblick

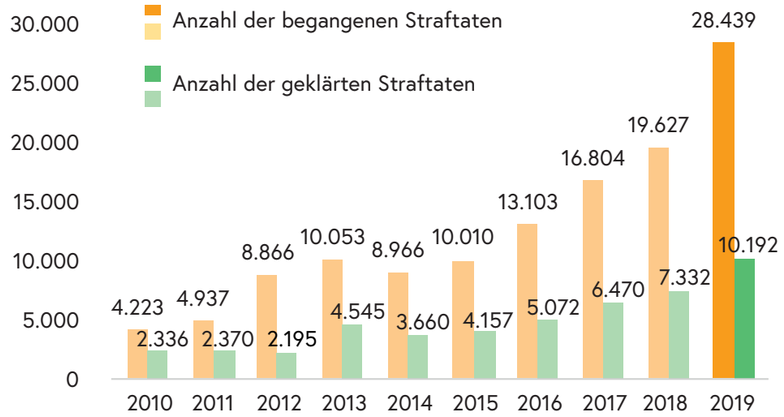
Die vorangehend angeführten rechtlichen Herausforderungen wirken sich entsprechend auf die IT-Ermittlungen und in Folge auch auf die Kriminalitätsentwicklung aus. Die nachfolgenden Zahlen und Daten stammen ausschließlich aus der Polizeilichen Kriminalstatistik (PKS).

Tabelle: Entwicklung der Anzeigen, der aufgeklärten Fälle und der Aufklärungsquote von Cybercrime 2010 bis 2019

Jahr	Anzahl der begangenen Straftaten	Anzahl der geklärten Straftaten	Aufklärungsquote (gerundet)
2010	4.223	2.336	55,30%
2011	4.937	2.370	48,00%
2012	8.866	2.195	24,80%
2013	10.053	4.545	45,25%
2014	8.966	3.660	40,80%
2015	10.010	4.157	41,50%
2016	13.103	5.072	38,70%
2017	16.804	6.470	38,50%
2018	19.627	7.332	37,40%
2019	28.439	10.192	35,80%

Die Abbildung der Entwicklung von Cybercrime in den letzten zehn Jahren zeigt, dass mit 28.439 Delikten 2019 gegenüber dem Vorjahr ein Anstieg von 44,9 Prozent zu verzeichnen ist (2018: 19.627). Trotz des enormen Zuwachses der Anzeigen konnte die Aufklärungsquote im gleichen Zeitraum nahezu konstant gehalten werden. Die Anzahl der geklärten Straftaten stieg in diesem Bereich von 7.332 erstmals auf über 10.000 Fälle, wodurch eine Aufklärungsquote von 35,8 Prozent erreicht werden konnte. Weitere Details können der Tabelle zur Entwicklung von Cybercrime der letzten zehn Jahre entnommen werden.

Abbildung: Entwicklung der Anzeigen und der aufgeklärten Fälle von Cybercrime 2010 bis 2019



Die Internetkriminalität wird in Cybercrime im engeren Sinne und weiteren Sinne unterteilt.

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 sogenannten „Distributed Denial of Service“ (DDoS) Angriffen.

2019 musste bei Tatbeständen zu Cybercrime im engeren Sinn ein überdurchschnittlich hoher Anzeigenanstieg von 148,3 Prozent gegenüber dem Vorjahr verzeichnet werden. Die beiden häufigsten Deliktsarten waren der widerrechtliche Zugriff auf ein Computersystem § 118a Strafgesetzbuch (StGB) und der betrügerische Datenverarbeitungsmissbrauch § 148a StGB.

Der § 118a StGB hat eine Steigerung von 69,7 Prozent bei einer Reduktion der Aufklärungsquote von -13,3 Prozent zu verzeichnen. Der § 148a StGB hat sich mit 5.537 Delikten und einer Zunahme von 291,3 Prozent beinahe verdreifacht. Trotz dieser großen Steigerung konnten 1.262 Straftaten aufgeklärt werden. Damit konnte die Aufklärungen in diesem Delikt gegenüber 2018 immerhin um 254,5 Prozent gesteigert werden.

Delikt	Angezeigte Fälle 2018	Angezeigte Fälle 2019	Geklärte Straftaten 2018	Geklärte Straftaten 2019
§ 107c StGB	308	330	230	255
§ 118a StGB	403	684	110	96
§ 119 StGB	11	11	8	10
§ 119a StGB	45	47	7	8
§ 126a StGB	415	467	73	68
§ 126b StGB	102	93	10	12
§ 126c StGB	201	243	51	54
§ 148a StGB	1.415	5.537	356	1.262
§ 225a StGB	170	210	141	136
Gesamt	**3.070**	**7.622**	**986**	**1.901**

Tabelle: Angezeigte Fälle und geklärte Straftaten von Cybercrime im engeren Sinn nach Paragraphen des Strafgesetzbuches 2019 im Vergleich zu 2018

Cybercrime im weiteren Sinn

Unter Cybercrime im weiteren Sinne werden Straftaten verstanden, bei denen die IKT als Tatmittel zur Planung, Vorbereitung und Ausführung von herkömmlichen Kriminaldelikten eingesetzt wird, wie zum Beispiel Betrugsdelikte, Drogenhandel im Darknet, pornographische Darstellungen Minderjähriger im Internet, Cybergrooming oder Cybermobbing.

Tabelle: Angezeigte Fälle von Cybercrime im weiteren Sinn nach Paragraphen des Strafgesetzbuches 2019 im Vergleich zu 2018

Delikt	Angezeigte Fälle 2018	Angezeigte Fälle 2019	Geklärte Straftaten 2018	Geklärte Straftaten 2019
Internetbetrug				
§ 146 StGB	11.417	14.494	4.237	5.512
§ 147 StGB	1.248	1.560	366	436
§ 148 StGB	663	777	353	434
Internetbetrug-Gesamt	**13.328**	**16.831**	**4.956**	**6.382**
Sonstige Kriminalität im Internet				
§ 144 StGB	1.599	1.874	49	80
§ 145 StGB	92	84	13	18
§ 207a StGB	1.161	1.666	1.037	1.541
§ 207b StGB	1	4	1	4
§ 208a StGB	108	101	67	69
§ 218 StGB	10	12	3	7
§ 223 StGB	24	42	15	35
§ 224 StGB	7	21	5	9
§ 229 StGB	1		1	
§ 231 StGB	15	16	6	8
§ 232 StGB	35	62	33	54
§ 241a StGB		4		3
§ 297 StGB		5		5
§ 3g VerbotsG	176	95	160	76
Sontige Kriminalität gesamt	**3.229**	**3.986**	**1.390**	**1.909**
Cybercrime gesamt	**19.627**	**28.439**	**7.332**	**10.192**

Der Internetbetrug erreichte 2019 mit 16.831 Anzeigen einen neuen Höchststand. Die Anzahl der angezeigten Fälle von Betrugsformen im Internet §§ 146 bis 148 StGB folgten mit einem Anstieg von 26,3 Prozent dem stetig steigenden Trend der vergangenen Jahre. Auf den gesamten Bereich Cybercrime gerechnet, stellt somit der Internetbetrug etwas mehr als 59 Prozent der Anzeigen dar. Der Anteil der aufgeklärten Delikte konnte, trotz des erheblichen Anstiegs gegenüber dem Vorjahr, mit 28,8 Prozent dennoch stabil gehalten werden.

Dunkelziffer und Anzeigeverhalten

Im Bereich der Internetkriminalität sind die Dunkelziffern, insbesondere unter Beachtung internationaler Studien, besonders hoch. Die diesbezüglichen Gründe sind mannigfaltig. Viele Betroffene scheuen die Anzeige bei der Polizeidienststelle, teils aus Scham, Angst vor Reputationsverlust oder weil angenommen wird, dass der Fall ohnehin nicht verfolgt werden könne.

Jedoch kann mit jedem angezeigten Fall 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 zeitnaher gesetzt und mit zielgerichteten Warnhinweisen an die Bevölkerung die Zahl der Geschädigten reduziert werden. Eine Wiedererlangung abhanden gekommener Vermögenswerte gelingt jedoch selbst nach internationaler Ausforschung der Täter nur in den seltensten Fällen. Deshalb gebührt im Bereich des Internetbetrugs, der Verhinderung von Straftaten durch angeregte Bewusstseinsbildung und Aufklärung, erhöhte Aufmerksamkeit. 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 der maßgebliche Angriffspunkt.

4 Phänomene und Ermittlungen

„Crime as a Service“

Die Leistungen an sogenannten „Crime as a Service“-Diensten, die im Internet angeboten werden, nahmen weiterhin zu. Es handelt sich dabei vorwiegend um Hackingtools, Schadsoftware, wie beispielsweise Verschlüsselungstrojaner oder spezielle Dienstleistungen der Geldwäsche. Auch die Nutzung von Bot-Netzwerken, die DDoS-Angriffen oder zum Versand von Spam-E-Mails dienten, konnten vermehrt wahrgenommen werden. Ebenso wurde ein Anstieg beim in Verkehr bringen von Falschgeld, Material mit Online-Kindesmissbrauch, Kreditkartendaten und gefälschten Urkunden bemerkt.

Mit den im Darknet angebotenen Diensten stiegen vor allem Massenerpressungsmails und gezielte Erpressungen durch Ransomware und Bitcoin-Forderungen an. Die Täterschaft benötigte damit keinesfalls mehr tiefgreifendes Wissen zur technischen Durchführung, sondern wird mit den „Crime as a Service“-Leistungen in die Lage versetzt, das fehlende Wissen mit entsprechenden Diensten zukaufen zu können. Mit einem „Ransomware as a Service“-Modell machten beispielsweise die Entwickler der Ransomware „GandCrab“ im Zeitraum von Anfang 2018 bis Mitte 2019, ihren eigenen Angaben zufolge, mehr als zwei Milliarden US Dollar Gewinn.

Weitere Informationen:
https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/

Ransomware

Ransomware wurde in den letzten Jahren zu einem der wichtigsten Werkzeuge von Cybercrime-Tätern. Diese Schadsoftware 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, seine Daten durch Schadsoftware zu verlieren, die die eigenen Daten verschlüsselt und auch häufig die Sicherungen durch Backups, die zum Zeitpunkt der Verschlüsselung erreichbar waren, unbrauchbar macht, ist immer noch sehr groß.

Im letzten Jahr wurden zentral 220 Fälle von Ransomware bearbeitet . Dabei konnten einige Tatverdächtige erfolgreich ausgeforscht werden. Ein Schwerpunkt galt den Organisationsstrukturen für den Vertrieb von Ransomware, die ebenfalls ermittelt werden konnten. Die Angriffe richteten sich vorwiegend gegen kleine und mittlere Unternehmen (KMU) und weniger gegen Einzelpersonen. Dadurch hatte sich das Risikopotential für die österreichische Unternehmenslandschaft deutlich erhöht.

Als Gefahren für eine Infektion gelten:

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

Im Laufe des Jahres gingen die Täter immer zielgerichteter 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.

Ransomware bleibt zusammengefasst eine der größten Gefahren im Internet, um seine Daten zu verlieren. Bestehende Varianten von Ransomware werden technisch ständig weiterentwickelt und auch der Modus Operandi vom Weg der Infektion bis zur Lösegeldforderung den Umständen und Opfern flexibler angepasst. Angriffe mit Ransomware erfuhren im letzten Jahr eine zielgerichtete Spezialisierung auch auf Unternehmen, bei denen die Geldforderungen der Täterschaft an die wirtschaftliche Leistungsfähigkeit beziehungsweise an die vorhandene IT-Infrastruktur mit ihren Backup-Lösungen angepasst werden. Die Infektion in Unternehmen hat immer häufiger den Ursprung in anderer Schadsoftware (Trojaner), die wochen- oder monatelang vor der eigentlichen Datenverschlüsselung das komplette Netzwerk oder Computersystem ausgespäht hat. Die Angriffe lassen immer öfter auf großes Knowhow organisierter Tätergruppen beziehungsweise Anbietern von „Ransomware as a Service“ schließen.

Bitcoin-Mixer und deren erfolgreiche Bekämpfung

In den vergangenen Jahren wurde bei kriminellen Transaktionen in der Blockchain ein erhöhter Anstieg von sogenannten Bitcoin-Mixern festgestellt. In einer im Juni 2018 gestarteten Ermittlung wurden im Mai 2019 die Betreiber der Webseite „Bestmixer.io“ ausgeforscht. Die Server wurden von den Behörden in den Niederlanden sichergestellt. Durch die Analyse von Kryptowährungstransaktionen konnte den Betreibern der Webseite ein Umsatz von umgerechnet 200 Millionen Euro nachgewiesen werden. Hierzu wurde in den Niederlanden ein Geldwäscheverfahren geführt. Das C4 hat hierbei mit einer selbst entwickelten Software die Beschuldigten den jeweilig zuständigen Mitgliedsstaaten zuordnen können und diese Erkenntnisse Europol übermittelt.

Weitere Informationen:
https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down

Erpressungs-E-Mails

Auf das Massenphänomen der betrügerischen Erpressungs-E-Mails wurde Anfang 2019 mit der Gründung einer eigenen Arbeitsgemeinschaft „ARGE-Erpressungs-E-Mail“ reagiert. Die Täter dieser Delikte versuchen durch das Versenden von E-Mails mit erpresserischem Text, der die Empfängerin oder den Empfänger in Angst und Schrecken versetzen soll, möglichst viele Opfer zu finden. Die dabei angedrohten Konsequenzen werden vom Täter nur vorgetäuscht.

Im Gegensatz zu den massenhaft auftretenden Erpressungsmails besteht bei Sextortion eine Täter-Opfer Beziehung. Was zunächst wie ein harmloser Flirt beginnt, endet letztlich mit hohen Geldforderungen. Sextortion bezeichnet eine Betrugsmasche im Internet, bei der Internetnutzerinnen und -nutzer von attraktiven Unbekannten in Videochats dazu aufgefordert werden, nackt zu posieren oder sexuelle Handlungen an sich vorzunehmen. Die Täter zeichnen das auf und erpressen ihre Opfer mit der Veröffentlichung der heimlich gemachten Fotos oder Videos.

Internetbetrug

Mit der fortschreitenden Digitalisierung verlagern sich Betrugsdelikte immer mehr ins Internet. Das Internet wird dabei als Werkzeug zur Begehung dieser Taten eingesetzt, denn es bietet für die Täter die Möglichkeit, mit der Anonymität und der weltweiten Vernetzung einfach und weitgehend unerkannt eine große Anzahl von potentiellen Opfern zu kontaktieren.

2019 waren neben den Zuwächsen bei den klassischen Betrugsdelikten auch beim Internetbetrug Steigerungen zu verzeichnen. Der Internetbetrug umfasst eine Vielzahl von Modi Operandi, die von Anlagebetrügereien, Gewinnversprechen in E-Mails oder Vortäuschen von Liebesbeziehungen bis hin zum Bestellbetrug durch vorgetäuschte Warenlieferungen reichen. Zusätzlich ist gerade im Bereich des Internetbetrugs zumeist von Massendelikten auszugehen. Die spezialisierten Tätergruppierungen gehen arbeitsteilig, technisch versiert und dementsprechend überlegt vor.

Häufige Tathandlungen waren auch das Vortäuschen besonders lukrativer Geschäftsmodelle, wie der Finanz-Online-Betrug oder der allgemeine Anlagebetrug unter Verwendung von Kryptowährungen oder das Anbieten vermeintlich technischer Unterstützung, wie der sogenannte Tech Support Scam oder der Microsoft-Betrug. Im Mai 2019 wurden bereits die ersten Fälle von versuchtem CEO Fraud via WhatsApp gemeldet, bei dem Unternehmer zur Überweisung hoher Geldbeträge verleitet wurden.

Im Herbst 2019 kam es zu einem exponentiellen Anstieg von Angriffen auf Social Media Accounts. Häufig wurden alte, von Vorbesitzern nicht mehr genutzte, aber durch Täter recycelte Accounts für zahlreiche Betrugshandlungen verwendet.

Die Bekämpfung des Bestellbetrugs ist ein Schwerpunkt des BK. Dabei stehen betrügerische Bestellungen über das Internet bei österreichischen Online-Händlern im Fokus. Im letzten Jahr wurde dazu unter der Leitung Österreichs gemeinsam mit Europol die „E-Commerce Action Week" abgehalten. So konnten in Zusammenarbeit mit dem C4 rund 200 neue falsche Onlineshops, vorwiegend im Technik- und Bekleidungsbereich ermittelt werden, die auf wenige Tätergruppierungen zurückzuführen waren. In der Vorweihnachtszeit 2019 wurde man auf eine Verdoppelung der Fake- und Phishingshops aufmerksam. Diese zeigte sich insbesondere durch durchschnittlich bis zu zehn neue Fake-Shops pro Tag. Ebenso wurden zahlreiche Betrugsfälle durch das Verwenden falscher Identitäten und Kontaktdaten bei Bestellungen im Internet, durch Kontaktaufnahme per Telefon, Email oder über Soziale Medien registriert.

Mit dem gemeinsamen Ziel den Bestellbetrug in Europa zu bekämpfen, wurde der Fokus im Jahr 2019 auf Prävention gerichtet. Gerade hier ist es wichtig, die Schäden durch präventive Maßnahmen zu verhindern. In der Praxis sind oft internationale Ermittlungen nötig, wo repressive Maßnahmen nur sehr schwer durchgeführt werden können. Das BK setzt daher neben der wirksamen Präventionsarbeit auch auf eine intensive Zusammenarbeit zwischen Wirtschaft und Polizei, um Internetbetrug effektiv bekämpfen zu können. Dazu wurde gemeinsam mit der Wirtschaftskammer Österreich (WKO) eine Informationsveranstaltung für Online-Händlerinnen und -Händler abgehalten und eine Roadshow durch alle Bundesländer veranstaltet. Ziel der Maßnahme war es Möglichkeiten zum eigenen Schutz anzubieten und den Austausch mit der Privatwirtschaft und der Polizei im Rahmen des Projekts „Gemeinsam.Sicher" zu intensivieren.

Voice over IP-Spoofing

Als gängige Vorbereitungshandlung für klassische Betrugshandlungen, aber auch für den stark ansteigenden Internetbetrug wurden die operativen Ermittlungsbereiche in den Landeskriminalämtern (LKA) vermehrt auf den Modus Operandi des „Voice over IP-Spoofing" aufmerksam.

Beim Spoofing werden oftmals Callcenter im Ausland eingerichtet, um sich zunächst der Daten einer angerufenen Person noch einmal zu vergewissern. Meist stammen die Namen und angerufenen Telefonnummern aus Listen von unseriösen Datenhändlern oder Quellen im Darknet. Diese Callcenter senden zumeist eine falsche Telefonnummer mit, um ihre wahre Herkunft zu verschleiern. Die Täter gehen hier in der Regel ungezielt vor und lassen diese Listen sogar automatisiert von ihren freundlich wirkenden Mittätern abarbeiten. Dies dient oft einer schnellen Auswahl von möglichen Opfern. Inhalte der Gespräche sind in der Regel Angebote von Gewinnspielen oder es werden ausstehende Beträge aus angeblichen Käufen oder Verträgen eingefordert. 2019 gab es einen Anstieg von Anrufern, die sich als Kriminalpolizistinnen und Kriminalpolizisten ausgegeben und vor allem ältere Personen mit angekündigten Abholungen von Geldbeträgen und Sachwerten um ihre Vermögen gebracht haben. Die mitgesendeten falschen Telefonnummern haben oft eine österreichische Vorwahl, um beim Opfer Vertrauen zu wecken. Mittlerweile können die Nummern dieser Callcenter für jeden einzelnen Anruf automatisch generiert werden. Diese Anrufe werden über die Voice over IP (VoIP) Technologie abgewickelt und über Server in Länder ohne Abkommen zur internationalen Strafverfolgung weitergeleitet. Damit sind weiterführende Erhebungen nahezu aussichtslos. Die Polizei setzt daher ihren Schwerpunkt auf verstärkte Präventionsarbeit.

Suchtmittelhandel im Darknet

Der Online-Handel 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 13.200 Briefsendungen durch das Zollfahndungsamt sichergestellt, die insgesamt rund 1.200 Kilogramm Suchtmittel zum Inhalt hatten. Adressiert waren die Briefsendungen an Empfänger aus über 90 verschiedenen Nationen. Dabei belegt Österreich, gemessen an der Anzahl der Empfänger, seit Beginn der Kontrollen, den zweiten Platz hinter den USA und liegt noch vor Destinationen, wie Großbritannien, Frankreich oder Australien. Im zweiten Halbjahr 2019 wurde

diese Reihung von Österreich angeführt. Die für Österreich bestimmten Postsendungen enthielten insgesamt rund 163 Kilogramm Suchtgift, hauptsächlich Amphetamin und MDMA sowie 34.000 Stück Ecstasy-Tabletten und 1.080 LSD Trips. Der Ursprung dieser Postsendungen ist in der Regel auf die Niederlande zurückzuführen. Etwa 75 Prozent der in Österreich sichergestellten Postsendungen wurden von dort versandt. Auch in Österreich werden im Zuge von regelmäßigen Kontrollen Postsendungen mit Suchtmitteln sichergestellt. Insgesamt wurden im Zeitraum von Jänner 2016 bis Jänner 2020 rund 9.100 Postsendungen mit Suchtmitteln eingezogen. Diese Sendungen enthielten insgesamt rund 232 Kilogramm sowie 67.300 Stück Suchtmittel. Die Folgeermittlungen zu den bisherigen Sicherstellungen ergaben, dass das Suchtmittel der aufgegriffenen Briefsendungen ausschließlich über Darknet-Marktplätze bestellt wurde.

Eine ernstzunehmende Gefahr des Online-Handels zeigt sich auch mit dem ansteigenden Postversand von designten Derivaten, wie zum Beispiel Carfentanyl oder der Substanz U-47700. Diese Substanzen können schon beim Einatmen oder bei bloßem Hautkontakt zu beträchtlichen Gesundheitsschäden bis hin zum Tod führen. Eine große Anzahl der im Darknet verkauften illegalen Suchtmittel wird in den Niederlanden hergestellt und über diverse Vertriebskanäle am Postweg nach Österreich versandt.

Aber nicht nur Konsumentinnen und Konsumenten, sondern auch Suchtmittelhändlerinnen und -händler im Darknet konnten sich in Österreich etablieren. Seit der Gründung eines für den Suchtmittelhandel im Darknet spezialisierten Referates im BK mit Dezember 2018 konnten bereits zwölf in Österreich tätige Betreiber international agierender Darknet-Shops für Suchtmittel ausgeforscht werden. Mit nachgewiesenen Umsätzen in Millionenhöhe konnten diese zusammen mit ihren Mittätern festgenommen werden. Dabei wurden große Mengen an Kokain, Methamphetamin, Ecstasy-Tabletten sowie Benzodiazepine sichergestellt.

Pornographische Darstellungen Minderjähriger

Die Zahl der Anzeigen wegen pornographischer Darstellungen Minderjähriger (Paragraph 207a StGB) ist 2019 erneut um 43,5 Prozent auf 1.666 angestiegen (2018: 1.161 Anzeigen). Dies resultiert unter anderem daraus, dass die verschiedenen Anbieter von sozialen Medien in den USA bzw. Kanada den Kampf gegen die Verbreitung von kinderpornografischen Daten massiv verstärkt haben. So werden die einzelnen Dienste auf kinderpornografische Dateien überprüft und der betroffene Account gesperrt. Damit einhergehend erfolgt eine entsprechende Verdachtsmeldung an das jeweilige Land, dem der Verursacher zugeordnet werden kann.

Eine weitere Problematik in diesem Bereich ist immer noch das sogenannte „Liken“ beziehungsweise Weiterleiten von Videos, die vor allem via Facebook verbreitet werden und sexuelle Handlungen von Minderjährigen mit Tieren zeigen. Derartige Darstellungen werden oft gedankenlos als vermeintliche „Spaßvideos“ an andere Userinnen und User weitergeleitet ohne sich darüber im Klaren zu sein, dass schon der Besitz und die Verbreitung solcher Darstellungen ebenfalls strafbar sind.

5 Bekämpfung

Kriminalpolizeiliche Struktur zur Bekämpfung von Cybercrime

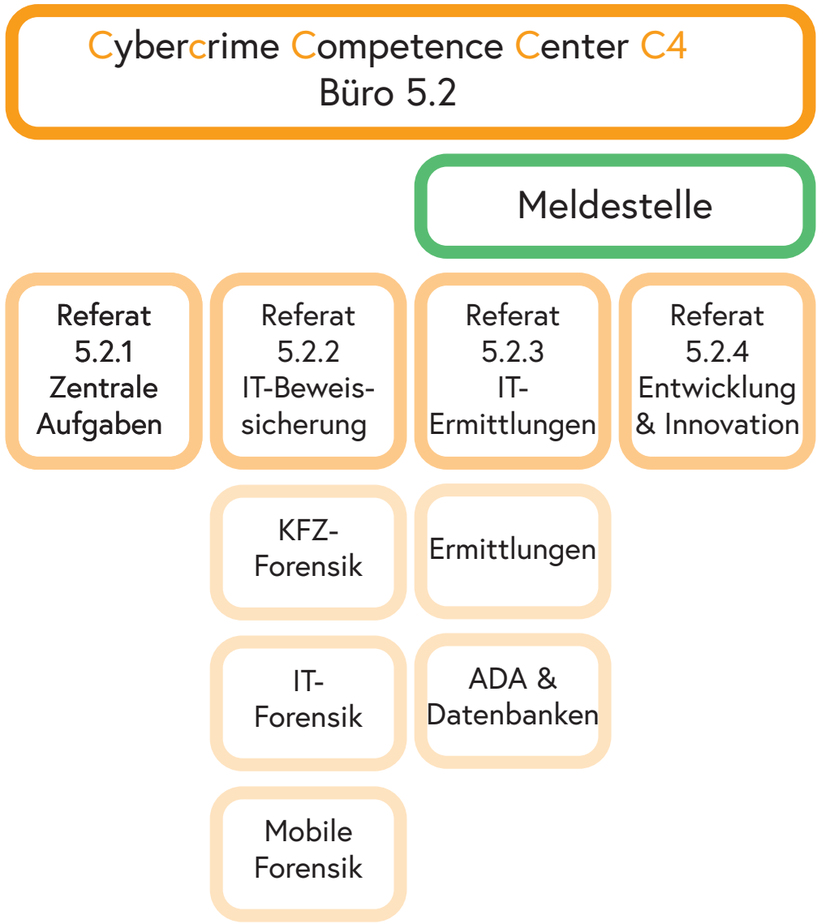
Für die Gewährleistung von mehr Sicherheit im virtuellen Raum ist es notwendig eine bundesweit umfassende Strategie zur Bekämpfung von Cybercrime zu verfolgen. Deshalb nimmt diese österreichweit bei der Polizei auf lokaler Ebene in den rund 900 Polizeiinspektionen und in über 100 Bezirks- und Stadtpolizeikommanden einen Schwerpunkt ein. Darüber hinaus sind auf Länderebene technisch ausgebildete Expertinnen und Experten zur Durchführung und Unterstützung von technischen Ermittlungs- und Beweissicherungsmaßnahmen tätig.

Die Zuständigkeit auf Bundesebene zur Bekämpfung von Cybercrime obliegt innerhalb der Abteilung Kriminalpolizeiliche Assistenzdienste des BK dem C4. 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. Eingerichtet ist die C4-Meldestelle als 24/7 erreichbare Kontaktstelle gemäß der Budapest Cybercrime Convention und anderen internationalen Vereinbarungen. Darüber hinaus agiert die C4-Meldestelle als wichtige Ansprechstelle für die Bevölkerung und Unternehmen, wodurch im Schadensfall eine rasche Unterstützung erfolgen und neue Phänomene frühzeitig erkannt werden können. Das C4 dient aber auch für alle Polizeidienststellen als wichtige Drehscheibe und als Koordinationspunkt.

Das C4 gliedert sich mit seinen Schnittstellen zum Cyber Security Center (CSC) des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung (BVT) sowie international zu Europols EC3 als wesentlicher Bestandteil in die Strategie des Bundeskanzleramts (BKA) ein. In diesem Zusammenhang ist das C4 Teil des Innerer Kreises der operativen Koordinierungsstrukturen (IKDOK).

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

Abbildung: Organigramm des C4

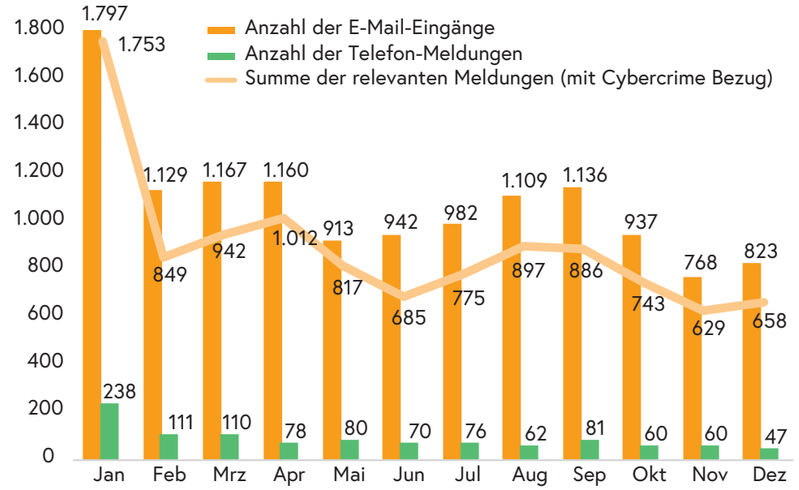


Meldestelle

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 die erforderlichen Maßnahmen zur Gefahrenabwehr umgehend eingeleitet werden.

Anfragen und Meldungen erhält die Meldestelle von Bürgerinnen und Bürgern, Unternehmen sowie nationalen und internationalen Polizeidienststellen. 2019 wurde die Meldestelle mit 13.936 Anfragen konfrontiert, wobei davon 10.646 einen Bezug zu Cybercrime hatten (2018: 8.331 Anfragen). Der detaillierten Betrachtung kann der starke Jahresbeginn und die leichte Reduktion an Meldungen im Jahresverlauf aus der Abbildung Meldungen an die C4-Meldestelle entnommen werden. Quelle der Daten zu den Anfragen an die C4-Meldestelle ist das C4.

Abbildung: Meldungen an die C4-Meldestelle 2019



In ihrer zentralen Funktion als Cybercrime-Schnittstelle innerhalb polizeiinterner Strukturen, sowie als Meldestelle für Bevölkerung und Wirtschaft agiert die Meldestelle als Koordinierungs- und Informationszentrum. Zusätzlich umfasst ihre Tätigkeit auch proaktive, präventive Maßnahmen in Form von Warnmeldungen, die von speziell geschulten Mitarbeiterinnen und Mitarbeitern erstellt werden. Die deutlich erkennbare Sensibilisierung und Bewusstseinsbildung für das Thema Cybercrime erfolgte in fortlaufender Kooperation mit unterschiedlichen Institutionen aus dem Bereich der Wirtschaft und Vereinen, wie beispielsweise der WKO oder der Initiative „Watchlist Internet“. Darüber hinaus führen Erstanalysen der eingehenden Meldungen zu schnellen Informationsweitergaben aktueller Phänomene, damit akut negative Auswirkungen auf potentiell weitere Opfer 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 stellt die Meldestelle eine 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 – National Contact Points (NCPs) dar.

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

Weitere Informationen:
Watchlist Internet: www.watchlist-internet.at
Europol: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Zentrale Aufgaben

Das Referat für zentrale Aufgaben zeichnet sich verantwortlich für Beschaffung, Bereitstellung und Instandhaltung der C4-internen Infrastruktur. Darüber hinaus übernimmt es administrative Tätigkeiten des C4 bei nationalen und internationalen Gremien, öffentlichen Veranstaltungen, im Berichtswesen und in der Koordination bei Aus- und Fortbildungsmaßnahmen für den Bereich IT-Ermittlungen, sowie in der elektronischen Beweismittelsicherung. Bereits seit 2012 findet eine grundlegende Ausbildung von Bezirks-IT-Ermittlerinnen und -ermittlern statt. Mittlerweile unterstützen mehr als 300 speziell ausgebildete Beamtinnen und Beamte durch fachgemäße Erstmaßnahmen und Ermittlungen auf lokaler Ebene. Für diese Ausbildung werden die Vortragenden aus dem Pool der besten Expertinnen und Experten des BK und der LKAs rekrutiert.

Als zusätzliche Fortbildungsmaßnahme für Kriminalbedienstete wird das Thema Cybercrime insbesondere im Rahmen der Kriminaldienstfortbildungsrichtlinie (KDFR) vermittelt.

Auf zahlreichen Veranstaltungen sind regional besonders geschulte Präventionsbeamtinnen und -beamte, insbesondere für Klein- und Mittelbetriebe, aber auch für die interessierte Allgemeinheit im Einsatz.

Neben der Gremienarbeit mit Europol und Interpol führte das C4 auch die Organisation wichtiger Veranstaltungen mit internationaler Beachtung durch. So wurde die ITB-Fachtagung abgehalten und entworfene Trainingsumgebungen für Ermittlungsschritte bei Transaktionen von virtuellen Währungen vorgestellt. Auf internationaler Ebene vertritt das C4 Österreich in der European Cybercrime Training and Education Group (ECTEG).

Forensik

IT und Speichermedien stellten sich auch 2019 als unverzichtbar für strafrechtlicher Ermittlungen dar, wobei wieder ein deutlicher Anstieg an forensischen Auswertungen verzeichnet wurde. Quelle der nachfolgenden Daten der Forensik ist das C4. Die elektronische Beweismittelsicherung im C4 sowie in den LKAs gewinnt damit weiterhin an ressourcenintensiver Bedeutung. Dies zeigt sich 2019 mit 524 Terabyte an forensisch ausgewerteten Daten von PC- und Serversystemen gegenüber 2018 mit noch 416 Terabyte.

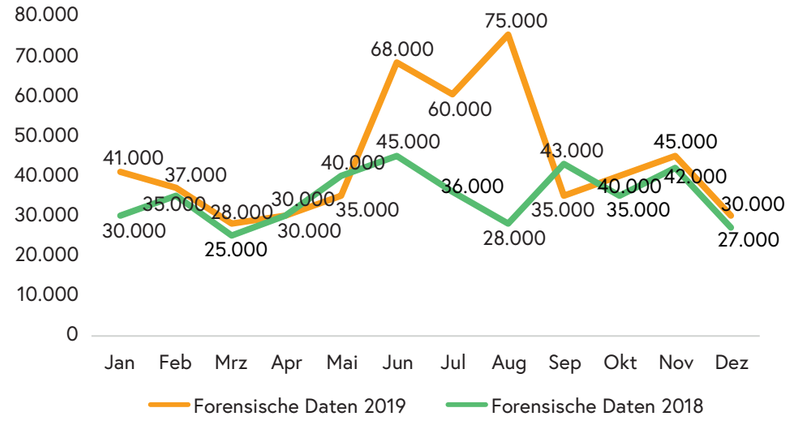


Abbildung: Ausgewertete forensische Daten 2018 und 2019 in Gigabyte

Aufgrund technischer Entwicklungen wird die Auswertung dieser Medien aber immer schwieriger. Herstellerspezifische Systeme mit Verschlüsselungsverfahren stellen die elektronische Beweissicherung laufend 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 aufwendigeren Auswertungen von Smartphones, die zum Teil von dem zuständigen Assistenzbereich „IT-Beweissicherung" der LKA nicht mehr bewältigt werden können. Somit stiegt 2019 die Anzahl der im C4 ausgewerteten Geräte auf 1.578 mit einer Gesamtdatenmenge von 59.260 Gigabyte gegenüber 964 mit 33.600 Gigabyte im Jahr 2018.

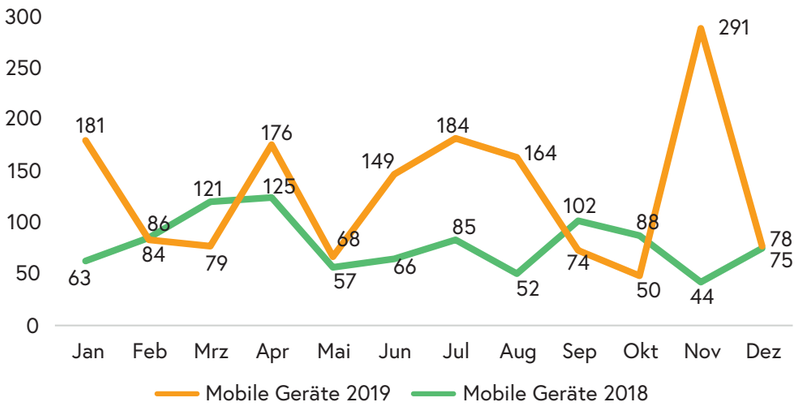
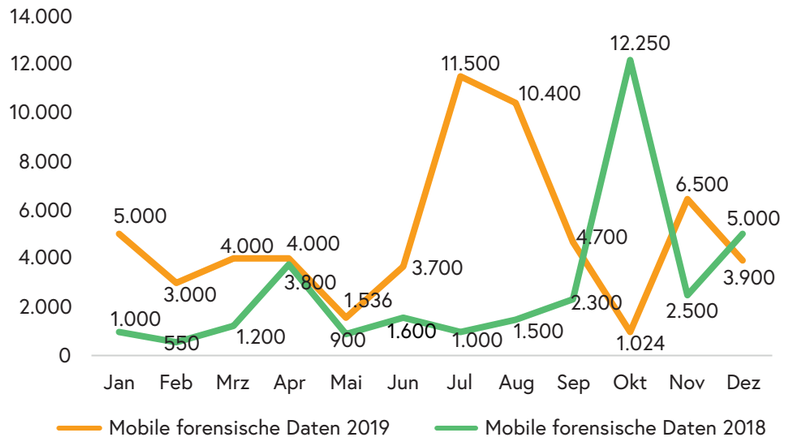


Abbildung: Ausgewertete mobile Geräte 2018 und 2019

Abbildung: Ausgewertete mobile forensische Daten 2018 und 2019 in Gigabyte



Das zeit- und ressourcenaufwendige sowie hochspezialisierte Chip Off-Verfahren, bei dem elektronische Bauteile aus den Geräten herausgelötet und ausgelesen werden, und die Kfz- Forensik können nur zentral im C4 durchgeführt werden.

Auch 2019 wurde die zentralen Leistungen der Fahrzeugforensik in steigendem Ausmaß bei der Beweismittelsicherung für 728 Fahrzeugen in Anspruch genommen. Die Fahrzeugforensik des C4 wurde als wichtige Säule durch Unterstützung der Ermittlungsarbeiten, forensische Schwerpunktkontrollen und Intensivierung der Zusammenarbeit mit ausländischen Dienststellen etabliert.

IT-Ermittlungen

Das Referat der IT-Ermittlungen ist mit der Leitung, Koordination und Durchführung nationaler sowie internationaler Ermittlungen zur zielgerichteten Aufklärung von Cybercrime-Delikten betraut. Dafür bedient sich das C4 der erfolgreichen bi- oder multilateraler Zusammenarbeit mit Europol und Interpol. Im Anlassfall führt der Fachbereich „ADA und Datenbanken“, Automatischer Daten Abgleich (ADA) neben Ermittlungsfällen und Projektunterstützungen auch die Koordination und Durchführung des automationsunterstützten Datenabgleichs durch. Darüber hinaus ist das Referat auch in der Lage technisch sehr komplexe Ermittlungen durchzuführen. Diesbezüglich gibt die Entwicklung von Cybercrime entsprechende Schwerpunkte vor, die von den IT-Ermittlern abgedeckt werden müssen. In diesem Zusammenhang sind besonders zu erwähnen Kryptowährungen und das Darknet, weil deren Nutzung durch Täter tendenziell steigt. Um dieser Entwicklung nachzukommen, ist im C4 eine entsprechende Expertise für Ermittlungen in diesen Bereichen aufgebaut worden.

Im Internet und insbesondere bei Cybercrime werden Kryptowährungen immer öfter genutzt. Dieser Trend entsteht vor allem durch den niederschwelligen Einstieg in Kryptowährungen durch einfach bedienbare Softwareprodukte. Dieser relativ einfachen Nutzung steht aber die Komplexität der Technologie, die Kryptowährungen erst ermöglicht, gegenüber. Deshalb ist gerade für Ermittlungen nicht nur technisches Spezialwissen erforderlich, sondern auch die richtige Ausrüstung ausschlaggebend. Im Bedarfsfall werden daher Hilfsmittel für die IT-Ermittlungen im Verbund mit dem Referat für Entwicklung und Innovation geschaffen, um die IT-Ermittlerinnen und IT-Ermittler bei ansonsten manuell sehr aufwändigen Tätigkeiten zu unterstützen. Ein gutes Beispiel dafür ist die genannte Unterstützung bei der Datenanalyse von Bestmixer.io im Punkt „Bitcoin Mixer und deren erfolgreiche Bekämpfung“, die eine Anwendung der gewonnenen Erkenntnisse auf europäischer Ebene zeigt. An diesem Beispiel ist weiters zu sehen, dass bei Cybercrime fast ausschließlich digitale Spuren vorliegen und oft nur deren Analyse zum Täter führt. Für die Koordinierung und Durchführung von kriminalpolizeilichen Tätigkeiten wurde im C4 eine Ermittlungsgruppe mit dem Thema betraut.

Der zweite Schwerpunkt bei Cybercrime Ermittlungen ist derzeit das Darknet, das von Tätern für die Abwicklung illegaler Geschäfte genutzt wird. Dies betrifft besonders die im Punkt „Crime as a Service“ genannten Dienstleistung, den Online-Handel mit verbotenen Substanzen sowie sexuelle Kindesmissbrauchsdarstellungen. Das Darknet befindet sich laufend im Wandel, da immer neuere Anonymisierungstechniken eingesetzt werden. Dabei kommen durchwegs sehr spezialisierte Lösungen zur Anwendung, sodass nicht unbedingt das bekannte TOR Netzwerk zur Anonymisierung genutzt werden muss. Ein Beispiel dafür ist die anonyme Handelsplattform OpenBazaar, die anonyme Geschäftsauftritte und Transaktionsabwicklung ermöglicht. Insofern ist es notwendig über die aktuelle Entwicklung im Darknet einen Überblick zu behalten. Mit dieser Aufgabe sowie der Unterstützung, Durchführung und Koordination von Ermittlungstätigkeiten im Darknet wurde im C4 ein Experte betraut.

Die Sonderermittlungskommission zu Ransomware wurde in der ersten Jahreshälfte 2019 als Ermittlungsgruppe in die Linienorganisation übernommen. Deren Aufgabe ist auch weiterhin das auf Bundesebene zentralisiertes Zusammenfassen, Bearbeiten und Ermitteln von Ransomware-Fällen. Dies ermöglicht umfassend die Ransomware-Arten und Tätergruppierungen zu klassifizieren. Durch internationale Kooperation, die vor allem durch das European Cybercrime Center (EC3) koordiniert wird, erfolgt ein laufender Austausch und gemeinsame Ermittlungen um Täter zu auszuforschen.

Entwicklung und Innovation

Das Referat für Entwicklung und Innovation setzt sich auf wissenschaftlicher Ebene mit dem Einsatz von neuen Technologien und deren Folgeabschätzung bei kriminellen Straf-

taten oder deren Potentiale für Aufklärungen auseinander. Dies umfasst die Forschung und das wissenschaftliche Arbeiten auf speziellen cybercrime-relevanten Gebieten durch Erforschung und Bewertung von Phänomen in den Bereichen der IKT und der digitalen Forensik. Dabei gewonnenes Wissen findet bei der Bewertung und Entwicklung von unterstützenden Tools, wie Software Werkzeugen, der Wissensvermittlung und Unterstützung bei der Bearbeitung von aktuellen Fällen eine Anwendung. Im Bereich der digitalen Forensik und bei Cybercrime Ermittlungen ist eine ständige Weiterbildung, aber vor allem die Entwicklung innovativer Ideen für eine Qualitäts- und Effizienzsteigerung gefordert, die durch dieses Referat gestützt werden.

Bundesweite polizeiliche Zusammenarbeit

Erhält die Sicherheitsbehörde Kenntnis über eine Straftat mit IT-Bezug, was in der Regel durch Mitteilung eines Geschädigten bei einer Polizeiinspektion erfolgt, kann insbesondere bei komplexeren Sachverhalten auf die Bezirks-IT-Ermittler und deren Fachexpertise zurückgegriffen werden. Darüber hinaus sind in den LKA Fachbereiche zur Klärung solcher Straftaten etabliert und fungieren auch als Bindeglied zum C4 im Bundeskriminalamt.

Die Polizistinnen und Polizisten in Polizeiinspektionen (PI), Stadtpolizeikommanden (SPK) und Bezirkspolizeikommanden (BPK) erhalten im Rahmen ihrer Grundausbildung IT-Basisschulungen unter anderem zu den Themen strafrechtliche Tatbestände oder Verhalten am Tatort. Auf dieser Ebene agieren speziell ausgebildete Polizeibeamte, die als erste Ansprechpartner für Geschädigte zur Verfügung stehen und über Basiswissen verfügen. Sie informieren und beauftragen in einem zweiten Schritt die Expertinnen und Experten. Darüber hinaus ist Cyber-Kriminalität mittlerweile ein wichtiger Bestandteil in der Ausbildung dienstführender Beamtinnen und Beamten.

In den LKA der Bundesländer sind fachlich ausgebildete Exekutivbedienstete tätig. Diese verfügen über eine spezielle polizeiliche Ausbildung und sind zusätzlich im IT-Bereich geschult. Sie servicieren die jeweiligen Ermittlungsbereiche bei digitalen, forensischen Sicherungen sowie deren Auswertungen und Aufbereitungen. Neben den forensischen Tätigkeiten umfasst deren Aufgabengebiet auch Ermittlungstätigkeiten im Cybercrime-Bereich auf nationaler Ebene. Aufbauend auf die Bezirks-IT-Ermittler-Ebene gewährleistet das LKA ein professionelles Einschreiten bei höherrangigen Strafrechtsdelikten mit entsprechendem IT-Bezug. Besonders bei internationalen Ermittlungen stellt das LKA durch seine Schnittstellenfunktion auf Bundesländerebene eine Hilfeleistung für das C4 im Bundeskriminalamt dar.

Neue Erfolgsmodelle in der Ablauforganisation

Um organisatorische Verbesserungen auszutesten wurde in der Außenstelle Zentrum Ost des Wiener LKA im Februar 2019 ein Probebetrieb mit IT-Ermittlerinnen und Ermittler sowie mit digitalen Forensikerinnen und Forensikern gestartet. Bereits in den ersten Wochen wurden diese von Kolleginnen und Kollegen anderer Bereiche konsultiert und mit steigender Akzeptanz im Rahmen der Aktenbearbeitung hinzugezogen. Das geforderte Spezialwissen wird insbesondere bei Einvernahmen, Hausdurchsuchungen und OSINT-Recherchen benötigt. Die Unterstützung umfasst neben der Sicherung von Videos, Bildextraktionen, Handyauswertungen auch die Bewältigung logistischer Herausforderungen.

Aus Sicht der IT-Ermittler wird die enge Abstimmung durch kurze Kommunikationswege und räumliche Nähe zu den Ermittlungsbereichen in der Außenstelle als Erfolgsmodell gewertet. So können die IT-Ermittler gleich bei Aufnahme der Arbeiten unmittelbare Ermittlungsansätze finden oder ausschließen.

Zahlreiche administrative und logistische Unterstützungshandlungen, wie die Erteilung von Auskünften und Beratungen, diverse Bildextraktionen oder die Sicherung und Konvertierung von Videodateien können so ohne unnötigen Aufschub zur Zufriedenheit von Ermittlerinnen und Ermittlern erledigt werden. Die frei gewordenen Kapazitäten werden dadurch auf den Kernbereich der Ermittlungstätigkeiten konzentriert.

Bereits bei der Konzeption des Modells wurden auch die notwendigen Zeiten für den stetigen Kompetenzaufbau und den Wissensaustausch mit anderen Organisationen vorgesehen. Durch die fortgesetzte Abstimmung mit dem täglichen Bedarf des Aufgabenbereiches, ist ebenso der unmittelbare und erhoffte Wissenstransfer feststellbar. Kurz nach Einführung dieses Probetriebs konnten zahlreiche Erfolge verzeichnet werden. Unter anderem konnte bei folgenden Amtshandlungen ein wesentlicher Beitrag zur Klärung der Straftat geleistet werden:

- Unterstützung bei einer Amtshandlung wegen mehrerer Vergewaltigungen teilweise unter Verwendung von KO-Mittel
- Ausforschung eines Beschuldigten nach einer Bombendrohung innerhalb von zwei Stunden
- Ausforschung eines Beschuldigten nach einem Raub
- Ausforschung von Verdächtigen nach schweren Betrügereien
- Ausforschung mehrerer Money-Mules nach einem Love-Scam

6 Zusammen-arbeit mit der Polizei

Anzeigenerstattung

Wenn Sie Opfer von Cyber-Kriminalität geworden sind, haben Sie die Möglichkeit diesen Sachverhalt in jeder Polizeidienststelle prüfen zu lassen beziehungsweise gegebenenfalls anzuzeigen.

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

Richtige Vorgehensweise:

- Sichern Sie bitte relevantes Beweismittel und Datenmaterial, wie beispielsweise Emails, Chat-Verläufe, Zahlungsbelege, Screenshots, digitale Fotos oder Videos oder ähnliches. Wenn bestimmte Inhalte nicht abgespeichert werden können, erstellen Sie Screenshots oder fotografieren Sie den Bildschirm notfalls ab.
- Stellen Sie sicher, dass sich die Unterlagen und Daten, die Sie der Polizei zur Verfügung stellen, im Originalzustand befinden. Das bedeutet, dass an ihnen keine Manipulation, keine Ergänzungen oder ähnliches durchgeführt wurden. Bei E-Mails würde das bedeuten, diese nicht einfach weiterzuleiten, sondern die Original-E-Mail abzuspeichern und die gespeicherte Kopie als Anhang zu übermitteln wäre.
- Häufig haben Sie auch selbst die Möglichkeit, bei den von Ihnen betroffenen Accounts, Informationen zu erfragen, die für eine Täterausforschung notwendig sind. Exemplarisch sind dies IP-Adressen über widerrechtliche Zugriffe inklusive Zeitstempel, Logdaten und so weiter. Überprüfen Sie dazu am besten selbst, welche der für die Tathandlung 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 Tathandlungen 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 dem aufnehmenden Beamten nach Absprache mit diesem 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 Polizeidienststellen zuständig. Derzeit ist eine formelle Anzeigeerstattung ist über die Meldestelle nicht vorgesehen.

E-Mail:
against-cybercrime@bmi.gv.at

7 Events und internationale Gremien

Fachtagung IT-Beweismittelsicherung (ITB)

Die 5. Fachtagung IT-Beweismittelsicherung (ITB) fand am 19. März 2019 in Wien statt und wurde vom C4 in Kooperation mit dem Bundesministerium für Landesverteidigung (BMLV) organisiert. Thema waren unter anderem neue Phänomene im Cyber-Bereich. IT-Ermittlerinnen und -Ermittler sowie Forensik-Expertinnen und –Experten vom Assistenzbereich in den LKAs – LKA AB6 ITB, von den Bezirken sowie aus den Fachabteilungen des BK, des BVT, von den Landesämtern für Verfassungsschutz und Terrorismusbekämpfung (LVT), vom Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung (BAK), vom BMLV, vom Bundesministeriums für Finanzen (BMF) und von der Bundeswettbewerbsbehörde nahmen an der Tagung teil.

Die Vortragenden kamen vom Institut für Strafrecht und Kriminologie der Universität Wien, vom „Computer Emergency Response Team Austria“ (CERT.at), vom Schweizer Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) sowie vom C4. Themenschwerpunkte waren das Phänomen Doxing und Internet of Things (IoT).

Symposium „Neue Technologien (NT)“

Am 5. und 6. November 2019 fand in Wien das 9. Internationale Symposium „Neue Technologien“ statt. Diese jährliche Veranstaltung wird gemeinschaftlich vom LKA Bayern, LKA Baden-Württemberg, dem BK Österreich und dem Eidgenössischem Bundesamt für Polizei (fedpol) organisiert. Die letztjährige Organisation wurde vom C4 durchgeführt. Über 200 Teilnehmende aus den Bereichen Polizei, Militär, Behörden, Wirtschaft und Forschung kamen dazu in den Räumlichkeiten der Landesverteidigungsakademie des Bundesheers in Wien für eine gemeinsame Technologiefolgenabschätzung zusammen.

Ziel dieser Veranstaltungsreihe ist es, laufend neue Technologieprojekte, die für Polizeibehörden von Bedeutung sind, im Rahmen hochkarätiger Vorträge vorzustellen und konkrete Ergebnisse zu präsentieren. Diese länderübergreifende Plattform trägt dazu bei, die möglichen Vorteile künftig bestmöglich nutzen zu können. Sie soll aber auch helfen, einhergehende potenzielle Gefahren für die Bevölkerung frühzeitig zu erkennen. Mit den Veranstaltungen wurde aus Sicht der Sicherheitsbehörden ein wichtiger Impulsgeber und eine bedeutende Plattform für die Sicherheitsforschung geschaffen.

8 Kriminal-prävention

Verhinderung von Straftaten

In der Präventionsarbeit wurde im vergangenen Jahr ein Schwerpunkt auf den Bereich der Computer- und Internetkriminalität gelegt. Es wurde über Gefahren, Phänomene und Problemfelder aufgeklärt. Mit gezielten Kooperationen kann der diesbezügliche Wissensaustausch intensiviert und gezielt an die Bevölkerung weitergegeben werden.

Für das Erkennen von Fake-Shops und andere Betrugsmethoden, wie Gewinnversprechen per E-Mail, Phishing-E-Mails und dergleichen wird die Bevölkerung über Social-Media-Kanäle und Beiträge auf der Homepage des BK informiert und gewarnt. Im Detail wurde in Vorträgen und Beratungen besonders auf die Vorgehensweisen und Methoden des Internetbetrugs eingegangen und dem stark ansteigenden Phänomen auch präventiv entgegenwirkt. Dabei wurden auch Unternehmen gezielt auf die Deliktsformen des CEO Fraud und das zugrundeliegende Social Engineering hingewiesen und Methoden zu dessen Erkennung und Verhinderung erarbeitet. Für diese spezialisierte Tätigkeit wurden 2019 in ganz Österreich bereits 150 Präventionsbedienstete ausgebildet, die über das jeweilige LKA erreicht werden können.

Verstärkt wird dazu die Wirkung der Public-Private-Partnership nicht nur in Form der Kooperation mit der WKO, sondern auch mit dem österreichischen Institut für angewandte Telekommunikation, eingesetzt. Dem Fachverband Unternehmensberatung und Informationstechnologie (UBIT) der WKO gehört die Experts Group IT Security an. Jene führt Unternehmensberater, IT-Dienstleister zusammen, die sich dem Thema der Informationssicherheit in all ihren Formen verschrieben haben und somit im Vorfeld bereits gegen Cybercrime wirksam werden können. Mit dem C4 und den Landespolizeidirektionen findet eine laufende Kooperation statt, die Maßnahmen, Vorträge und Veranstaltungen umfasst. So wurde auf dem E-Day, der jährlich das Interessen von Unternehmen an neue Technologien wecken soll, durch das C4 und das LKA Wien präventiv über aktuelle Gefahren von Cybercrime informiert und auf die Fragen der Besucher dazu eingegangen.

Wenn Serviceleistungen nicht mehr von österreichischen Sicherheitsbehörden geleistet werden können, gilt es den Klein- und Mittelunternehmungen (KMU) nicht nur den wichtigen präventiven Schutz zukommen zu lassen, sondern im Ereignisfall auch operative Hilfe zu leisten. Dies wird von der WKO durch die Cyber-Security Hotline 0800 888 133, an die sich betroffene Kammermitglieder wenden können, abgedeckt. Für Bürgerinnen und Bürger steht die Informationsplattform www.watchlist-internet.at zur Verfügung, auf der Informationen zu aktuellen Gefahren im Internet abgerufen werden können.

9 Herausforderungen und Projekte

Die Analysen des Reports zeigen die schnellen Veränderungen bei Tätern und Technologie, die eine Anpassung für die laufende Fortbildung der Kriminalpolizei und uniformierten Polizei notwendig machen. Dieser wird zum Teil durch die Schulungen der Bezirks-IT-Ermittler erfüllt. Geplant ist der notwendige Ausbau, der bereits in einem Projekt zu einem vollständigen Ausbildungskonzept weiterentwickelt wurde. Zusätzlich dient der Cybercrime Experts Circle (CEC), der vom C4 aufgebaut wurde, als internationalen Plattform zum Austausch von unmittelbar praktisch anwendbarem Wissen mit Expertinnen und Experten aus Partnerländern.

Herausfordernd bleibt es, rasche und effiziente Reaktionen auf internationale Cyber-Vorfälle in operativen, kriminalpolizeilichen Dienst setzen zu können. Dazu wird ein Spezialist für Cybercrime zu Europol entsandt werden, der künftig eine schnelle und technisch kompetente Informationsweitergabe bei operativen Fällen gewährleisten soll. Eine weitere Maßnahme ist die Einrichtung einer eigenen, zentralen Ansprechstelle als bundesweiter Kontakt- und Informationspunkt zwischen diesen Betreibern sozialer Medien sowie online-Diensteanbieter und inländischen Polizeieinheiten. Zusätzlich soll mit einer technischen Aufrüstung im Form eines forensischen Auswertungscluster die qualitativ hochwertige Auswertung der vermehrt sichergestellten Daten effizienter und schneller werden. Weiters werden im Bereich der Forensik Vereinfachungen und effizientere Gestaltungen für die Beweismittelsicherung vor Ort geprüft und deren Einsatz geplant werden.

Um den gerichtlichen Aufträgen Folge bei der zunehmenden Verschlüsselung noch Folge leisten zu können, wird mittels nationaler Forschungsinitiativen und Projekte der Ausbau von Kapazitäten zur Entschlüsselung angestrebt werden.

Grundsätzlich ist ein größeres Problembewusstsein in allen gesellschaftlichen Bereichen durch den starken Deliktsanstieg im Cybercrime Bereich notwendig geworden. Deshalb werden Präventivmaßnahmen über bestehenden Kooperationen zur Steigerung der Widerstandsfähigkeit gegen Cyber-Angriffe weiter ausgebaut werden.

Zur Umsetzung und Finanzierung der Cyber-Sicherheitsstrategie werden für die Projekte der Bekämpfung von Delikten im Cyberbereich vermehrt spezielle EU-Budgets herangezogen.

10 English Summary

The key developments in cybercrime in 2019 were the significant increase in mass blackmail messages at the beginning of the year and the year-round high level of Internet fraud. The former was taken into account by the establishment of a separate working group on blackmail emails and the latter was handled within the framework of the regular organisation. In addition, there is a trend among offenders to use Ransomware and other “Crime as a Service” deliverables from the darknet.

There is still a lack of a necessary legal framework for the problems of Carrier Grade NAT, G5, domain names and crypto-currencies, which are currently making criminal police work more difficult or even impossible.

An update of the cybercrime strategy is planned, covering IT investigations and seizing of digital evidence. Improvements to processes, including the technology used, are continually taking place in order to meet the ever-increasing technical challenges.

11 Glossar

Anonymisierungsdienst

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

Antivirenprogramm

Ein Antivirenprogramm (synonym mit Virenscanner oder Virenschutz) ist eine Software, die bekannte Schadsoftware wie beispielsweise Computerviren (siehe Viren) 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.

Business Email Compromise (BEC)

Angreifer kompromittieren bei einem BEC den Email Schriftverkehr eines Unternehmens mit dem Ziel, einen Mitarbeiter der Firma zu einer Geldtransaktion auf das Bankkonto der Täterschaft 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 Unternehmensmitarbeiter durchzuführen und es ist ratsam im Schriftverkehr mit Handelspartnern vorsichtig zu sein. Bei unklaren oder eigenartigen Sachlagen über eine andere Technologie (Telefon) sind die Sachverhalte zu überprüfen.

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.

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.

Chip Off-Verfahren

Dieses Verfahren dient zum Auslöten von elektronischen Bauteilen und das Auslesen von allenfalls enthaltenen Informationen.

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 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 pornografischen Darstellungen Minderjähriger 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 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 (siehe 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 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.

Love Scam

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

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 sich aktiv an Geldwäsche beteiligt. Die Anwerbung erfolgt oft über Email.

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 sogenannte Network Address Translation (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 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 heißt, 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.

OSINT

Open Source Intelligence (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, Emails oder andere Messenger-Nachrichten an persönliche Daten zu gelangen. Phishing steht häufig in Zusammenhang mit zumindest versuchten Betrugshandlungen und Identitätsmissbrauch.

Ransomware

Als Ransomware wird Schadsoftware bezeichnet, die den Zugriff auf Daten und elektronische Systeme einschränkt oder verhindert. Diese Ressourcen werden erst wieder nach Bezahlung eines Lösegeldes („ransom“) freigegeben.

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.

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.

Trojanisches Pferd (Trojaner)

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

URL

Ein URL (Uniform Resource Locator) 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 selbst verbreiten 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 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.