

Lagebericht Cybercrime 2018

Entwicklungen, Phänomene und Schwerpunkte



Lagebericht Cybercrime 2018

Wien 2019

Impressum

MedieninhaberIn, VerlegerIn und HerausgeberIn:
Bundesministerium für Inneres, Bundeskriminalamt
Josef-Holaubek-Platz 1, 1090 Wien
+43 1 24836 985925
www.bundeskriminalamt.at

Fotonachweis: ©BMI, Bundeskriminalamt und Adobe Stock
Druck: Digitaldruckerei des BMI
Wien 2019

Inhalt

Vorwort.....	5
1 Einleitung.....	6
2 Cybercrime Bekämpfung in Österreich.....	8
2.1 Kategorisierung des Begriffs „Cybercrime“.....	9
2.2 Merkmale von Cyberdelikten.....	10
2.3 Organisationsstruktur zur Strafverfolgung von Cybercrime.....	10
3 Rechtliche Aspekte und Rahmen.....	14
4 Jahresrückblick.....	16
4.1 Zahlen und Fakten im Überblick.....	17
5 Schwerpunkte des vergangenen Jahres.....	20
5.1 Data Leaks.....	21
5.2 “Distributed Denial of Service”-Angriffe (DDoS-Angriffe).....	21
5.3 Ransomware (Erpressungstrojaner).....	22
5.4 Internetbetrug.....	22
5.5 Kryptowährungen.....	23
5.6 Smart Contracts und Altcoins.....	24
5.7 Behördenwallets.....	24
5.7 Darknet.....	26
5.7 Kampf gegen die Verbreitung von kinderpornografischem Material.....	27
6 Ausbildung.....	29
6.1 BezIT-Ermitterschulung.....	30
6.2 Ausbildungscampus Cybercrime.....	31
6.3 Europäische Ausbildungsprogramme – ECTEG und CEPOL.....	31
6.4 INTERPOL Digital Security Challenge.....	32

7 Prävention	33
7.1 Sicherheitshinweise für den Alltag	34
7.2 Tipps zu Cloud-Services	35
8 Zusammenfassung	37
8.1 Daten und Fakten	38
8.2 Trends und Fazit	38
9 Summary	41
9.1 Facts and Figures	42
9.2 Trends and Conclusion	42
10 Glossar	41

Vorwort

Liebe Leserinnen und Leser!

Seit Bestehen des World Wide Web nutzen Kriminelle das Internet dazu, strafbare Handlungen zu begehen. Dazu benötigen die Täterinnen und Täter keine hochtechnische Ausrüstung, schon mit schlichtem IT-Equipment wie beispielsweise Smartphones können sie im Internet Straftaten begehen. Es ist eine zentrale Aufgabe des Bundeskriminalamts, die Entwicklung in diesem Bereich aufzuzeigen, gegen die Täter zu ermitteln und die Internetnutzerinnen und -nutzer mithilfe der gewonnenen Erkenntnisse zu schützen.

Es sind gut ausgebildete und modern ausgerüstete Polizistinnen und Polizisten nötig, um entsprechende Ermittlungen führen zu können. Darüber hinaus sind Polizeibehörden und deren Ermittler von internationalen Abkommen und Kooperationen abhängig, um die Täterinnen und Täter ausforschen zu können. Im Besonderen betrifft es Taten, bei denen das Internet anonymisiert genutzt wird und Kryptowährungen als Zahlungsmittel verwendet werden. Beispiele dafür sind Erpressungen durch Ransomware, Betrugsdelikte oder der Drogenhandel im Darknet. Es gibt kaum noch Delikte, die ohne Nutzung von Informationstechnologie begangen werden beziehungsweise nicht damit bewiesen werden können.

Der vorliegende Report skizziert die Entwicklung der internationalen Kriminalitätsform „Cybercrime“ im Jahr 2018. Beachtet werden aktuelle Entwicklungen und Phänomene, weiters wird über die Schwerpunkte der zur zielgerichteten Bekämpfung der Kriminalität ausgerichteten Tätigkeit der Polizei informiert.

Wir danken den Mitarbeiterinnen und Mitarbeitern für ihre wertvolle Arbeit bei der Bekämpfung der Internetkriminalität. Es bedarf gerade in diesem Kriminalitätsbereich einer intensiven Zusammenarbeit zwischen den nationalen Behörden und internationalen Partnern. Sie alle leisten einen wertvollen Beitrag, um Österreich sicherer zu machen.



Bundesminister
Dr. Wolfgang Peschorn



Direktor
Franz Lang

Dr. Wolfgang Peschorn
Bundesminister für Inneres

General Franz Lang
Direktor des Bundeskriminalamtes

1

Einleitung



Der vorliegende Cybercrime-Report 2018 soll eine kurze, fachlich fundierte Übersicht zur Bekämpfung von Cybercrime im Jahr 2018 bieten. Der Jahresbericht zeigt die Entwicklungen und Maßnahmen im Bereich der Cybercrime-Bekämpfung unter der Führung des Bundeskriminalamtes (BK) auf. Dieser Report soll sowohl innerbehördlich als auch über die Behördengrenzen hinaus einen Informations- und Präventionsbeitrag leisten.

Um die Täter und deren Methoden effektiv zu bekämpfen, wurden 2018 von den Strafverfolgungsbehörden große Anstrengungen unternommen. Aufgrund der wachsenden Anforderungen an die digitale Beweismittelsicherung und Ermittlungsmethoden wurde neben internationalen Kooperationen, Beratungen und Vorträgen ein besonderes Augenmerk auf die Aus- und Weiterbildung der Mitarbeiterinnen und Mitarbeiter gelegt.

Der Bericht beschreibt die Aufbau- und Ablauforganisation zur Bekämpfung von Cybercrime in Österreich und widmet sich der nationalen und internationalen Zusammenarbeit mit den Landeskriminalämtern und ausgebildeten IT-Ermittlern in den Polizeiinspektionen.

Neue rechtliche Voraussetzungen nach der Datenschutzgrundverordnung (DSGVO) stellen eine besondere Herausforderung für Unternehmen und Behörden in der Kriminalitätsbekämpfung dar und werden im Bericht kurz skizziert.

Der Jahresrückblick beschreibt Veränderungen im Vergleich zum Vorjahr und interpretiert die Anzeigenentwicklung aus der Kriminalstatistik. Diese Kennzahlen geben einen Aufschluss über die notwendigen Strategieanpassungen. Das anschließende Kapitel erklärt die festgestellten Schwerpunkte der Phänomene und Entwicklungen aus dem Blickwinkel des Cybercrime Competence Centers (C4) und bildet zudem die zugehörigen Sichtweisen aus den Fachbereichen zur Bekämpfung der Drogen- und Wirtschaftskriminalität sowie der Verbreitung von kinderpornografischem Material ab. Dabei werden die umgesetzten und geplanten Maßnahmen mit beispielhaften Erfolgen in der vor allem internationalen Zusammenarbeit des vergangenen Jahres erläutert.

Die Darstellung besonderer Weiterbildungsmaßnahmen erfolgt aufgrund ihrer Bedeutung für die nächsten Jahre in einem eigenen Kapitel.

Auch wenn es die Intention des Berichtes ist, vorrangig einen Überblick zum vergangenen Jahr zu geben, wird die Gelegenheit der Publikation genutzt, auch kriminalpräventive Sicherheitshinweise und allgemeine Handlungsempfehlungen in Erinnerung zu rufen.

Da die Verwendung einschlägiger technischer Fachbegriffe bei dieser Thematik unvermeidbar ist, lassen sich die wichtigsten Erklärungen im Glossar finden.

Bei den in diesem Bericht verwendeten personenspezifischen Bezeichnungen gilt die gewählte Form (generisches Masculinum) für beide Geschlechter.

2

Cybercrime Bekämpfung in Österreich



2.1 Kategorisierung des Begriffs „Cybercrime“

Die Bekämpfung von Cyber-Kriminalität ist eine der kriminalpolizeilichen Kernaufgaben der Sicherheitsbehörden und ist als Querschnittsmaterie zu sehen, die einen breiten Ansatz erfordert. Das Budapester Übereinkommen des Europarates vom 23. November 2001 ist die erste internationale Vereinbarung über Straftaten, die durch das Internet oder sonstige Computernetzwerke begangen werden. Mit eingeschlossen sind computerbezogener Betrug, Kinderpornografie und Verstöße gegen die Sicherheit von elektronischen Netzen. Das Abkommen stellt somit die internationale Bestrebung dar, einheitliche rechtliche Regelungen zur Bekämpfung der Cyber-Kriminalität und der nötigen internationalen Zusammenarbeit zu etablieren. Hauptzweck ist neben der Verfolgung einer gemeinsamen Strafrechtspolitik zum Schutz der Gesellschaft vor Straftaten, die mit Hilfe von Computern begangen wurden (cybercrimes), insbesondere die Schaffung entsprechender gesetzlicher Regelungen, aber auch die Förderung internationaler Zusammenarbeit im Bereich von Cyber-Kriminalität.

Die Anzahl von Sachverhalten, die als Delikte von Cybercrime im engeren Sinn angezeigt werden, ist rückläufig, da mit Angriffen auf Informations- und Kommunikationstechnologien meist nur Teilbereiche von komplexen Tathandlungen abgedeckt sind. Grundsätzlich stehen bei einem Großteil der Cybercrime-Fälle Delikte mit Bereicherungs- oder Nötigungsvorsatz im Vordergrund.

Cybercrime im engeren Sinne (IKT als Angriffsziel)

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 (z.B. Datenbeschädigung, Hacking, DDoS Angriffe).

Delikte, die zu „Cybercrime im engeren Sinne“ zählen, sind folgende Paragraphen:

- § 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
- § 148a StGB Betrügerischer Datenverarbeitungsmissbrauch
- § 225a StGB Datenfälschung

Cybercrime im weiteren Sinne (IKT als Tatmittel)

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 z.B. Betrugsdelikte, Drogenhandel im Darknet, pornographische Darstellungen Minderjähriger im Internet, Cybergrooming oder Cybermobbing.

2.2 Merkmale von Cyberdelikten

Ein typisches Merkmal von Cyberdelikten ist deren Begehung in der digitalen Welt. Die geringe Hemmschwelle der Täter wird dadurch begünstigt, dass die Straftaten in einem vertrauten Umfeld (z.B. von zu Hause aus oder einem Internetcafé) begangen werden, und eine große räumliche Distanz zu den Opfern besteht.

Ein weiteres Merkmal stellt der internationale Aspekt der Delikte dar. Täter, Tatmittel und Opfer können sich in unterschiedlichen Ländern, oft auf unterschiedlichen Kontinenten mit unterschiedlichen Rechtssystemen befinden. Herkömmliche Ländergrenzen sind praktisch bedeutungslos.

Zudem führt die ständige Weiterentwicklung der Technik zu neuen Sicherheitslücken in aktuellen Produkten und zu neuen Begehungsformen (Modi Operandi) in den altbekannten Angriffsarten, wie Ransomware, Hacking, Phishing oder DDoS Angriffe.

Anonymisierungsdienste, Verschlüsselungstechnologien, Zahlungen mittels Kryptowährungen und die Nutzung des Darknets erschweren zudem die Strafverfolgung.

2.3 Organisationsstruktur zur Strafverfolgung von Cybercrime

Cybercrime Competence Center (C4)

Das im Bundeskriminalamt angesiedelte Cybercrime Competence Center (C4) ist der nationale und internationale Kontaktpunkt zur Bekämpfung von Cyberkriminalität in Österreich. Der Kern setzt sich aus fachlich hochspezialisierten Experten aus den Bereichen der elektronischen Beweismittelsicherung und digitalen Ermittlungen zusammen. In Cybercrime-Angelegenheiten fungiert das C4 als internationale Drehscheibe, als Schnittstelle zum Cyber Security Center (CSC) des BVT sowie als nationale Cybercrime-Meldestelle für die Bevölkerung und die Wirtschaft. Die Meldestelle des C4 dient dem Europäischen Cybercrime Center (EC3) bei Europol, dem Interpol Digital Crime

Center (IDCC) und auch allen nationalen und internationalen Polizeidienststellen und Fachgremien als Informations- und Kontaktstelle.

Der Fokus auf die Aktualität der Ereignisse und die internationalen polizeilichen Kooperationen ermöglichen die frühzeitige Erkennung von neuen Phänomenen, die analysiert und bewertet werden müssen. In der Folge werden durch das C4 zeitnah technische Eigenlösungen entwickelt und für einschlägige Ermittlungsbereiche bereitgestellt. So gelangen im Jahr 2018 dem Bundeskriminalamt beachtenswerte Durchbrüche bei Sicherstellungen von Kryptowährungen.

Das C4 leitet und koordiniert eigene Ermittlungen zur Aufklärung von Cybercrime-Delikten im engeren Sinn, doch durch den enormen Anstieg des Arbeitsaufwandes dehnt sich das Aufgabenspektrum zusehends in jene Fachbereiche, die von Cybercrime im weiteren Sinne betroffen sind, aus. Die stark steigende Verlagerung klassischer Straftaten in den digitalen Raum spiegelt sich sowohl in der Kriminalstatistik, als auch in den täglichen Aufgaben der IT-Forensik wider, die für die Sicherungen, Aufbereitungen und Auswertungen von elektronischen Beweismitteln verantwortlich ist.

Technisch hochkomplexe Aufklärungsarbeit bei Cybercrime-Delikten kann meist nur nach richtigem Ersteinschreiten bei Amtshandlungen erfolgen. Daher wird der Fokus gemeinsam mit den Landeskriminalämtern zunehmend auf vereinheitlichte Prozesse und technische Lösungen gelegt. Aufgrund des stetigen Anstiegs von Cybercrime führt das C4 seit längerer Zeit Schulungen für Bezirks-IT-Ermittler (BezIT) durch. Die Inhalte wurden 2018 aktualisiert und erweitert. Diese besonders geschulten Ermittler sollen die Kollegen in den Polizeidienststellen bei der Anzeigenaufnahme sowie bei der möglichen Sicherstellung von Beweismitteln unterstützen.

Zuständigkeiten bei der Aufnahme und Bearbeitung von Cybercrime Delikten

In Österreich ist jedes Organ des öffentlichen Sicherheitsdienstes sowohl zur Gefahrenabwehr im Sinne des Sicherheitspolizeigesetzes als auch zur Strafrechtspflege im Sinne der Strafprozessordnung verpflichtet. Je nach örtlicher beziehungsweise sachlicher Zuständigkeit hat deshalb auch jede Polizeidienststelle schon bei der Anzeigenerstattung an der Bekämpfung von Computerkriminalität mitzuwirken.

Die Unterstützung der Kolleginnen und Kollegen auf den Polizeiinspektionen kann durch besonders geschulte BezIT-Ermittler, bei allgemeinen und technischen Fragen zu Cybercrime Ermittlungen auch schon bei der Erstaufnahme einer Anzeige erfolgen, insbesondere wenn die Beweissicherung digitaler Medien oder deren Inhalte abzuklären ist.

Ein nachahmenswertes Erfolgsmodell wurde in Niederösterreich seit einigen Jahren durch das Bezirkspolizeikommando (BPK) im Bezirk Gänserndorf umgesetzt. Seit einigen

Jahren werden an bestimmten Wochentagen fixe Zeiten für Servicedienste von digitalen Ermittlungen eingeteilt. So ist gewährleistet, dass Anzeigen über Cybercrime relevante Sachverhalte durch besonders qualifizierte Beamte entgegengenommen werden und sofortige Ermittlungen eingeleitet werden können. Bei Gefahr im Verzug oder wenn zusätzliche technische Expertise erforderlich ist, können die Landeskriminalämter und das C4 hinzugezogen werden. In allen anderen Fällen wird die Anzeigenaufnahme und Einvernahme auf einer Polizeiinspektion durchgeführt, wonach der Akt anschließend zur weiteren Bearbeitung an die zuständige Dienststelle beziehungsweise den zuständigen Sachbearbeiter übermittelt wird.

Diese Vorgangsweise garantiert eine optimale Bearbeitung von Sachverhalten, eine zeitnahe Reaktion bei Fällen von Cybercrime im engeren Sinn unter direkter Fachaufsicht und eine Qualitätskontrolle durch das Landeskriminalamt. Denn von der forensischen Sicherstellung, Auswertung, Datenbereitstellung, Sichtung bis hin zur Übergabe an die Staatsanwaltschaften und Gerichte muss jede Manipulation an einem digitalen Beweismittel sowie jede Weitergabe zum Zwecke der Nachvollziehbarkeit dokumentiert werden.

Die Landeskriminalämter führen für gewöhnlich forensische Aufgaben durch und sind in den Bundesländern für die Bekämpfung von Cybercrime im engeren Sinne zuständig. Jedoch ist eine auffallend hohe Verlagerung der Tätigkeiten in der Ermittlungsunterstützung und bei der Wissensvermittlung für fremde Fachbereiche erkennbar, da bei fast allen Erhebungen nunmehr auch das Internet zu berücksichtigen ist, was entsprechendes technisches Know-how erfordert.

Sind eine besondere technische Ausrüstung, internationale Ermittlungskooperationen oder akademisches Fachwissen erforderlich, kann die Übernahme oder Unterstützung des Falles durch die Spezialisten des C4 im Bundeskriminalamt erfolgen.

Die nationalen und internationalen Kooperationen des C4 auf strategischer und operativer Ebene umfassen:

- **Das Bundeskanzleramt**

Die Österreichische Strategie für Cybersicherheit (ÖSCS) regelt unter anderem die „Schaffung einer Struktur zur Koordination auf der operativen Ebene“. Diese soll sowohl periodische, als auch anlassbezogene Lagebilder für Cyber-Sicherheit liefern und im Krisenfall auf der operativen Ebene über weitere Maßnahmen beraten.

- **Das Bundesministerium für Europa, Integration und Äußeres**

Neben der Gesamtkoordination der österreichischen Europa- und Außenpolitik erfolgen auch Koordinationssitzungen im Bereich der Cybersicherheit und Cyberkriminalität, insbesondere bei OSZE, Europarat und UNO.

- **Die Europäische Union (Europol, CEPOL, OLAF)**

Im Bereich der Europäischen Union werden österreichische Sicherheitsinteressen in einem größeren institutionellen Rahmen verfolgt. Das C4 arbeitet hier vor allem bei der Analyse und Aufarbeitung von transnationalen, operativen Fällen und der Umsetzung strategischer Interessen, wie der Wissensvermittlung mit den Agenturen Europol (EC3), CEPOL und OLAF sowie ECTEG zusammen, deren Handlungsfähigkeit auch mit kooperierenden Drittstaaten weiter gestärkt werden sollte.

- **Den „Inneren Kreis der operativen Koordinierungsstrukturen“ (IKDOK)**

IKDOK ist ein staatliches Gremium, dem das Cyber Security Center (CSC im Bundesministerium für Inneres) vorsteht. Dazu zählen das Cybercrime Competence Center, das Cyber Defense Center (CDC), das Abwehramt, das Heeres-Nachrichtenamt und das milCERT (alle BMLV), das Bundesministerium für Äußeres, Europa und Integration (BMEIA) sowie das govCERT (Bundeskanzleramt – BKA).

3

Rechtliche Aspekte und Rahmen

§§ 118 bis 124 StGB

Missbräuchliches Abfangen von Daten

Wer in der Absicht, sich oder einem anderen Unbefugten von einem Computersystem übermittelten und nicht für ihn bestimmten Daten zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen einen Vermögensvorteil zuzufügen, eine Vorrichtung, die an dem Computersystem angeschlossen ist, abzufangen oder sonst empfangsbereit gemacht wurde, benützt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

3.1 DSGVO und WHOIS

Mit 25. Mai 2018 trat die neue Datenschutz-Grundverordnung (DSGVO) beziehungsweise für Österreich das Datenschutzgesetz (DSG) in Kraft. Eine der Auswirkungen ist die erhebliche Einschränkung beim Zugriff auf die Daten von registrierten Domänen. Eine „WHOIS“-Abfrage im Internet führte vormals direkt zum Inhaber der Domäne und/oder zu einer technisch zuständigen Kontaktperson. Diese personenbezogenen Auskünfte können für weiterführende Ermittlungen relevant sein und waren bisher öffentlich zugänglich. Die rechtliche Einschränkung der Abfrage dieser Daten als Folge der DSGVO stellt die Sicherheitsbehörden vor erhebliche Ermittlungshürden.

Die besondere Tragweite des Problems begründet sich darin, dass Domännennamen essentielle Grundbausteine des Internets sind und somit häufig bei digitalen Ermittlungen von Bedeutung sind.

In vielen technischen und rechtlichen Gremien, wie zum Beispiel der Dachorganisation der Domänenverwaltung ICANN, wird international schon seit Monaten nach Lösungsmöglichkeiten gesucht, erfolgsversprechende Konzepte wurden jedoch noch nicht in Aussicht gestellt.



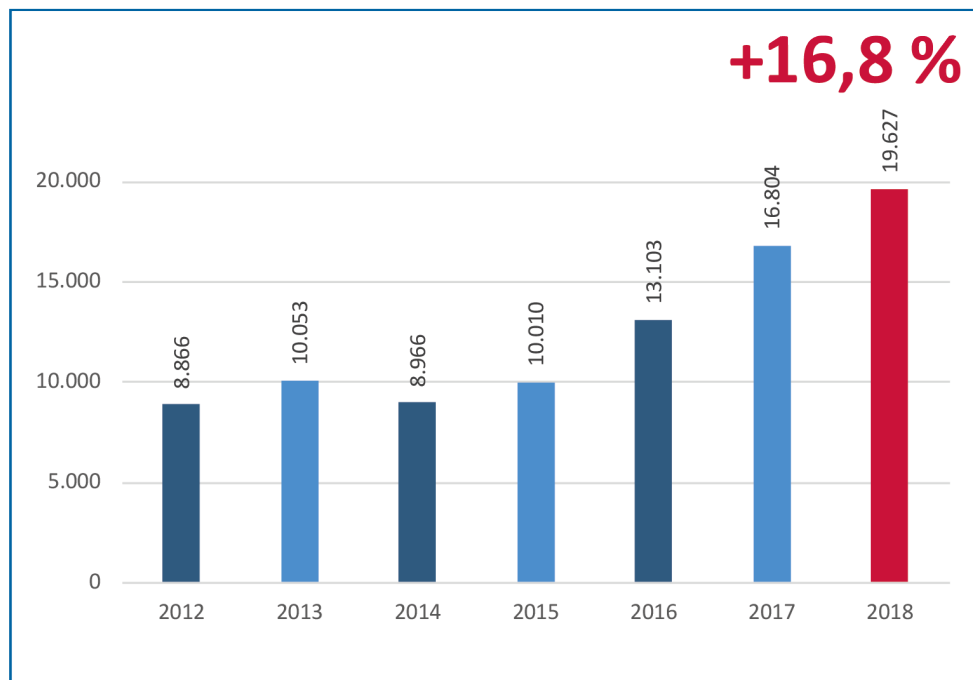
4

Jahresrückblick

4.1 Zahlen und Fakten im Überblick

Mit Verlautbarung der Polizeilichen Kriminalstatistik (PKS) wird die analysierte Kriminalitätsentwicklung des vergangenen Jahres auch im Bereich der Internetkriminalität präsentiert.

„Die Kriminalität verlagert sich weiter zunehmend ins Internet.“



Grafik 1: Anzahl der gesamten internetbasierten Straftaten (Vollendung und Versuch) in Österreich von 2012 bis 2018.

Die Zahl der Straftaten im Bereich der internetbasierten Kriminalität betrug 2018 insgesamt 19.627, das ist eine Steigerung im Vergleich zum Vorjahr um 16,8 Prozent. Die Anzahl der geklärten Straftaten konnte um 13,3 Prozent gesteigert werden, von 6.470 (2017) auf 7.332 (2018).

Bei der Betrachtung der angezeigten Fälle von Cybercrime im weiteren Sinne konnten, bis auf dem Gebiet der Urkundenfälschungen (§§ 223 und 224 StGB), massive Anstiege, vor allem bei Erpressungen durch Ransomware (§§ 144 und 145 StGB) und bei pornographischen Darstellungen Minderjähriger im Internet (§ 207a StGB) verzeichnet werden. Betrugsformen im Internet folgten dem stetig steigenden Trend der vergangenen Jahre.

Generell stieg laut der PKS im Jahr 2018 im Bereich der Internetkriminalität die Anzahl der Tatverdächtigen auf 7.980 an, was im Vergleich zum Vorjahr einen Anstieg von 7,1 Prozent bedeutet. Anhand der Geschlechterverteilung ist zu erkennen, dass 70,1 Prozent (5.591) der Tatverdächtigen männlich waren und 29,9 Prozent (2.389) weiblich. Die Altersverteilung der möglichen Straftäter zeigt, dass der Großteil (3.547) zwischen

25 und 39 Jahre alt ist, gefolgt von den über 40-jährigen (1.896) und von den 21- bis 24-jährigen (1.110).

Insgesamt sind im Bereich der Internetkriminalität die höchsten Steigerungsraten zu verzeichnen. Dies scheint vor allem durch die weitere Verlagerung klassischer Deliktformen in die digitale Welt begründet zu sein. Die zunehmende Digitalisierung bietet der Gesellschaft sehr viele Vorteile, eröffnet den Tätern aber auch neuartige und vielseitige Begehungsformen.

Tabelle 1: Anzeigen Internetkriminalität – Jahresvergleich 2017 und 2018

Angezeigte Straftaten	Jänner-Dezember 2017	Jänner- Dezember 2018	Veränderung
Internetbetrug	11 761	13 328	13,3%
§ 146 StGB	9 943	11 417	14,8%
§ 147 StGB	1 186	1 248	5,2%
§ 148 StGB	632	663	4,9%
sonstige Kriminalität im Internet	1 497	3 229	115,7%
§ 144 StGB	474	1 599	237,3%
§ 145 StGB	29	92	217,2%
§ 207a StGB	733	1 161	58,4%
§ 207b StGB	1	1	0,0%
§ 208a StGB	106	108	1,9%
§ 218 StGB	6	10	66,7%
§ 223 StGB	28	24	-14,3%
§ 224 StGB	34	7	-79,4%
§ 229 StGB		1	
§ 231 StGB	6	15	150,0%
§ 232 StGB	9	35	288,9%
§ 3d VerbotsG	2		
§ 3g VerbotsG	69	176	155,1%

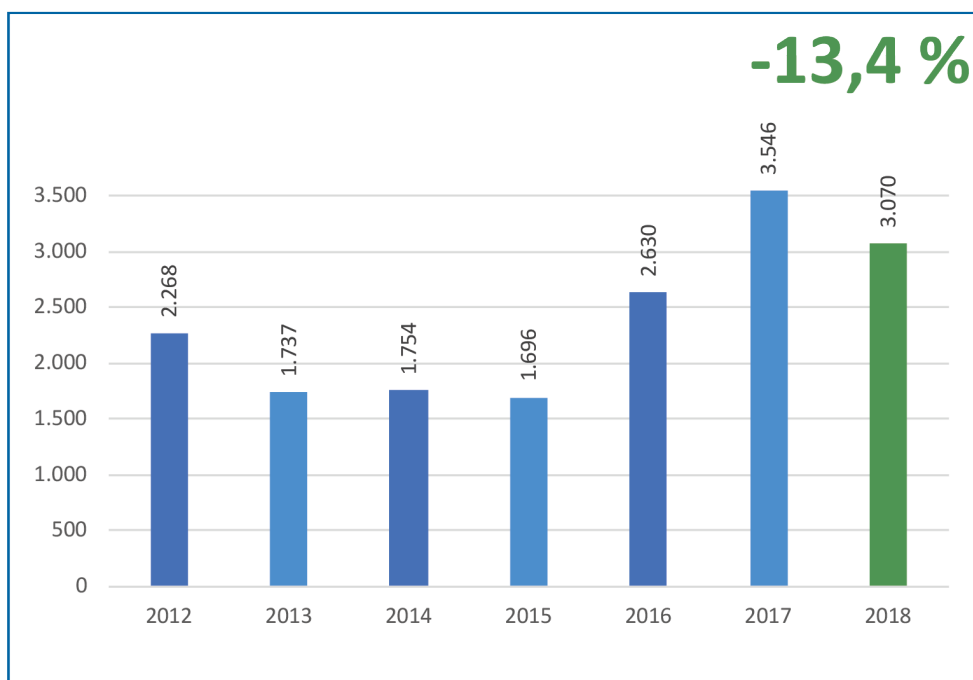
Die nachstehenden Tabellen zeigt, dass bei 3.546 Delikten, welche dem Begriff „Cybercrime im engeren Sinn“ zugerechnet werden, gegenüber dem Vorjahr ein Rückgang von 13,4 Prozent zu verzeichnen ist. Die Aufklärungsquote stieg dabei im gleichen Zeitraum um 3,9 Prozentpunkte. Es kann davon ausgegangen werden, dass dies auf gezielte operative Maßnahmen (z.B. durch Ransomware-Bekämpfung mittels SOKO Clavis) sowie auf erfolgreiche Präventionsarbeit zurückzuführen ist. Neue Kriminalitätsformen, speziell im Zusammenhang mit den Angriffsdienstleistungen der Darknet Marktplätze (Cybercrime as a Service), lassen jedoch auf einen zukünftigen Anstieg schließen.

Angezeigte Straftaten	Jänner-Dezember 2017	Jänner-Dezember 2018	Veränderung
§ 107c StGB	359	308	-14,2%
§ 118a StGB	363	403	11,0%
§ 119 StGB	16	11	-31,3%
§ 119a StGB	41	45	9,8%
§ 126a StGB	1 186	415	-65,0%
§ 126b StGB	105	102	-2,9%
§ 126c StGB	189	201	6,3%
§ 148a StGB	1 056	1 415	34,0%
§ 225a StGB	231	170	-26,4%
Cybercrime im engeren Sinn	3 546	3 070	-13,4%

Tabelle 2: Angezeigte Straftaten – Jahresvergleich 2017 und 2018

Cybercrime im engeren Sinn	Gesamt	Versucht	Vollendet	Auklärungs- quote
2017	3 546	264	3 282	28,2 %
2018	3 070	436	2 634	32,1 %
Veränderung zum VJ	-13,4 %	65,2 %	-19,7 %	3,9 %-Punkte

Tabelle 3: Anzeigen und Aufklärungsquoten Cybercrime im engeren Sinn – Jahresvergleich 2017 und 2018



Grafik 2: Cybercrime im engeren Sinn – Anzeigenvergleich 2012 bis 2018

5

Schwerpunkte des vergangenen Jahres



5.1 Data Leaks

E-Mail Adressen mit den dazugehörigen Passwörtern von gehackten Firmen und Portalbetreibern werden zunehmend nicht nur in Untergrundforen des Darknets, sondern auch frei erhältlich im Internet angeboten. Ebenfalls werden bereits installierte Apps, die Schadsoftware beinhalten, für Daten- und Identitätsmissbrauch genutzt. Große Sammlungen an geleakten Daten der letzten Jahre wurden aus unterschiedlichen Quellen zusammengetragen und wieder in gebündelter Form angeboten. Die missbräuchlich gewonnenen Daten stammen meist aus Angriffen auf verschiedene Geräte und Anwendungen. Auch schlecht gesicherte Webportale oder Mitarbeiter- und Kundenplattformen von Unternehmen bieten Angriffspunkte für Hacker.

Aufgrund von Ermittlungsergebnissen und nach Hinweisen aus internationalen Kooperationen konnten zahlreiche Datensätze potentiellen Opfern zugeordnet werden. Als präventive Schutzmaßnahme konnten die nationale C4 Meldestelle und Ermittlungsbeamte des C4 im Jahre 2018 annähernd 100.000 Betroffene benachrichtigen und dadurch eine Vielzahl an potentiell Geschädigten vorwarnen.

5.2 “Distributed Denial of Service”-Angriffe (DDoS-Angriffe)

Österreich hatte vom 1. Juli bis 31. Dezember 2018 zum dritten Mal den Vorsitz im Rat der Europäischen Union inne. Aufgrund der Erfahrungen anderer Länder während der Ratspräsidentschaft wurde von den Ermittlungsbehörden bereits im Vorfeld ein besonderes Augenmerk auf die Bekämpfung sogenannter DDoS Angriffe gelegt. Das C4 beteiligte sich zu diesem Zweck bei internationalen EMPACT Projekten (European Multidisciplinary Platform Against Criminal Threats) und auch an operativen Einsätzen bei der Joint Cybercrime Action Taskforce (J-CAT) bei Europol, die im Zusammenhang mit der Bekämpfung von DDoS Angriffen stehen. Bereits im April 2018 konnte unter der Koordinierung von J-CAT mit der operativen Aktion „Power Off“ einer der größten Dienstanbieter für DDoS Angriffe (webstresser.org) vom Netz genommen werden. Unter anderem gelang es aufgrund dieser erfolgreichen internationalen Amtshandlung, den Anstieg an DDoS Angriffen während der Ratspräsidentschaft gering zu halten. Ein starker Anstieg, wie bei vorangegangenen Ratspräsidentschaften anderer Länder, konnte somit erfolgreich vermieden werden.

5.3 Ransomware (Erpressungstrojaner)

2018 konnte die erfolgreiche Arbeit der SOKO Clavis zur Bekämpfung von Ransomware fortgesetzt werden. Während 2017 mit den Erpressungstrojanern NotPetya und Wanna-Cry weltweit hunderttausende PCs verschlüsselt wurden, pendelten sich die Fallzahlen im Jahr 2018 auf ein durchschnittliches Maß ein. Den Ermittlern der SOKO Clavis gelang es, mehrere Beschuldigte und Verdächtige zu großen Ransomware-Varianten, welche teilweise für mehr als hundert Millionen Euro Schadenssumme verantwortlich waren, auszuforschen.

International gesehen, scheinen laut Europolbericht 2018 in den meisten Mitgliedsstaaten die Angriffe eher ungezielt zu erfolgen. Dies könnte vor allem auf die breite Streuung von „Ransomware as a Service“ (RaaS) zurückzuführen sein.

Neben dem Einsatz von leicht zu beschaffenden Tools aus dem Darknet haben sich manche Cyber-Kriminelle zunehmend Expertenwissen angeeignet und sehr ausgereifte Tools eingesetzt, um in Netzwerke einzudringen oder sich dort auszubreiten (lateral movement). Diese Angriffe richteten sich häufiger gegen branchenspezifische Unternehmensgruppen (insbesondere kleine und mittlere Unternehmen) als gegen Einzelpersonen.

5.4 Internetbetrug

Der Internetbetrug umfasst eine Vielzahl von Modi Operandi, die von der vorgetäuschten Warenlieferung, BEC (Business E-Mail Compromise) bis zum Gewinnversprechen reichen. Das Medium Internet wird als Werkzeug zur Begehung der Tat eingesetzt. Dabei bietet es für Täter aufgrund der Anonymität und der weltweiten Vernetzung die Möglichkeit einer relativ einfachen Kontaktaufnahme mit einer großen Anzahl von Opfern.

Grundsätzlich gilt es, Betrugshandlungen im Internet durch eine rechtzeitige Erkennung im Vorfeld zu verhindern. Repressive Handlungen und Maßnahmen nach der Tat sind durch notwendige internationale Ermittlungen häufig erschwert. Das Bundeskriminalamt setzt daher neben der Präventionsarbeit auch auf eine intensive Zusammenarbeit zwischen Wirtschaft und Polizei, um Internetbetrug effektiv bekämpfen zu können.

Während im gesamten Jahr 2018, auch durch erfolgreiche Anstrengungen der Cybercrime Ermittler, die Delikte Cybercrime im engeren Sinn nur geringfügig angestiegen sind beziehungsweise teilweise sogar rückläufig waren, mussten sehr große Zunahmen bei klassischen Delikten, wie Betrug oder Erpressung unter Nutzung von Informationstechnologien, verzeichnet werden. So wurde festgestellt, dass Delikte mit digitalen Ermittlungsansätzen die Behörden in den Fachbereichen vor eine besondere Herausforderung hinsichtlich der Personalressourcen stellten. Dazu gehörten insbesondere die Versendung von Massen-

E-Mails mit gleichlautenden erpresserischen Inhalten, zahlreiche Betrugsversuche wie beispielsweise Tech Support Scam („Microsoft Betrug“), „Finanz-Online Betrug“ sowie der allgemeine Anlagebetrug unter Verwendung von Kryptowährungen.

Der abstrahierte Begriff des Internetbetrugs hatte im Jahr 2018 mit einem Zuwachs von 13,3 Prozent und in absoluten Zahlen mit 13.328 Anzeigen einen neuen Höchststand erreicht. Auf den gesamten Bereich Cybercrime gerechnet, stellt der Internetbetrug somit 68 Prozent der Anzeigen in diesem Deliktsbereich dar. Bei der Aufklärungsquote im Bereich Cybercrime im Jahr 2018 ist mit 37,2 Prozent ein nur durchschnittliches Ergebnis erzielt worden. Wie auch in den vergangenen Jahren wird dies auf die Verschleierungsmöglichkeiten der Täter im Internet und deren Professionalisierung zurückgeführt. Zusätzlich ist gerade im Bereich des Internetbetrugs von Massendelikten auszugehen. Die spezialisierten Tätergruppierungen gehen arbeitsteilig, technisch versiert und dementsprechend überlegt vor.

In diesem Deliktsfeld wird durch den zuständigen Fachbereich der Abteilung 7 des Bundeskriminalamtes besonders im Bereich Bestellbetrug ein Schwerpunkt gesetzt. Dabei stehen betrügerische Bestellungen über das Internet bei österreichischen Onlinehändlern im Fokus. Im letzten Jahr wurde diesbezüglich unter der Leitung Österreichs gemeinsam mit Europol die „E-Commerce Action Week“ abgehalten. Aufgrund des gemeinsamen Zieles, den Bestellbetrug in Europa zu bekämpfen, nahmen 23 Europol-Mitgliedsstaaten an dieser großangelegten Aktion teil. Dabei wurden 95 Festnahmen (vier davon in Österreich) und mehr als 200 Hausdurchsuchungen durchgeführt. Ermittlungen brachten mehr als 20.000 betrügerische Bestellungen (mehr als 2.700 in Österreich) mit einem geschätzten Gesamtwert von mehr als einer Million Euro zu Tage. Neben den repressiven Maßnahmen setzte Europol im Anschluss daran auf präventives Vorgehen mithilfe von Medienarbeit und eine gemeinsame Bewusstseinsbildungskampagne mit Informationsmaterial in 14 Sprachen, die auch in Österreich umgesetzt wurde.

Es wird immer klarer, dass für die Aufklärung von derartigen Betrugs- und Erpressungsarten mit klassisch-herkömmlichen Ermittlungsansätzen nicht mehr das Auslangen gefunden werden kann. Die Durchführung der Ermittlungen wird deshalb vermehrt von technisch erfahrenen Spezialisten oder mithilfe von Ermittlungsassistenzen durch das C4 beziehungsweise der Landeskriminalämter vorgenommen.

5.5 Kryptowährungen

Obwohl Kryptowährungen wie Bitcoin & Co noch im letzten Jahr herbe Kursverluste hinnehmen mussten, ist ein steigender Trend bei legalen, als auch illegalen Bezahlvorgängen zu beobachten. Insbesondere im Cybercrime-Bereich haben sich „Cryptos“ durchgesetzt. Mittlerweile wird auch mit weniger bekannten Kryptowährungen bezahlt,

Bitcoin rangiert allerdings noch immer an erster Stelle. Gerade bei den ansteigenden Fallzahlen in Zusammenhang mit Massenerpresser-E-Mails ist diese Entwicklung zu beobachten, da seit kurzer Zeit Sextortion-E-Mails als lukrative Einnahmequelle von Cyberkriminellen entdeckt wurden.

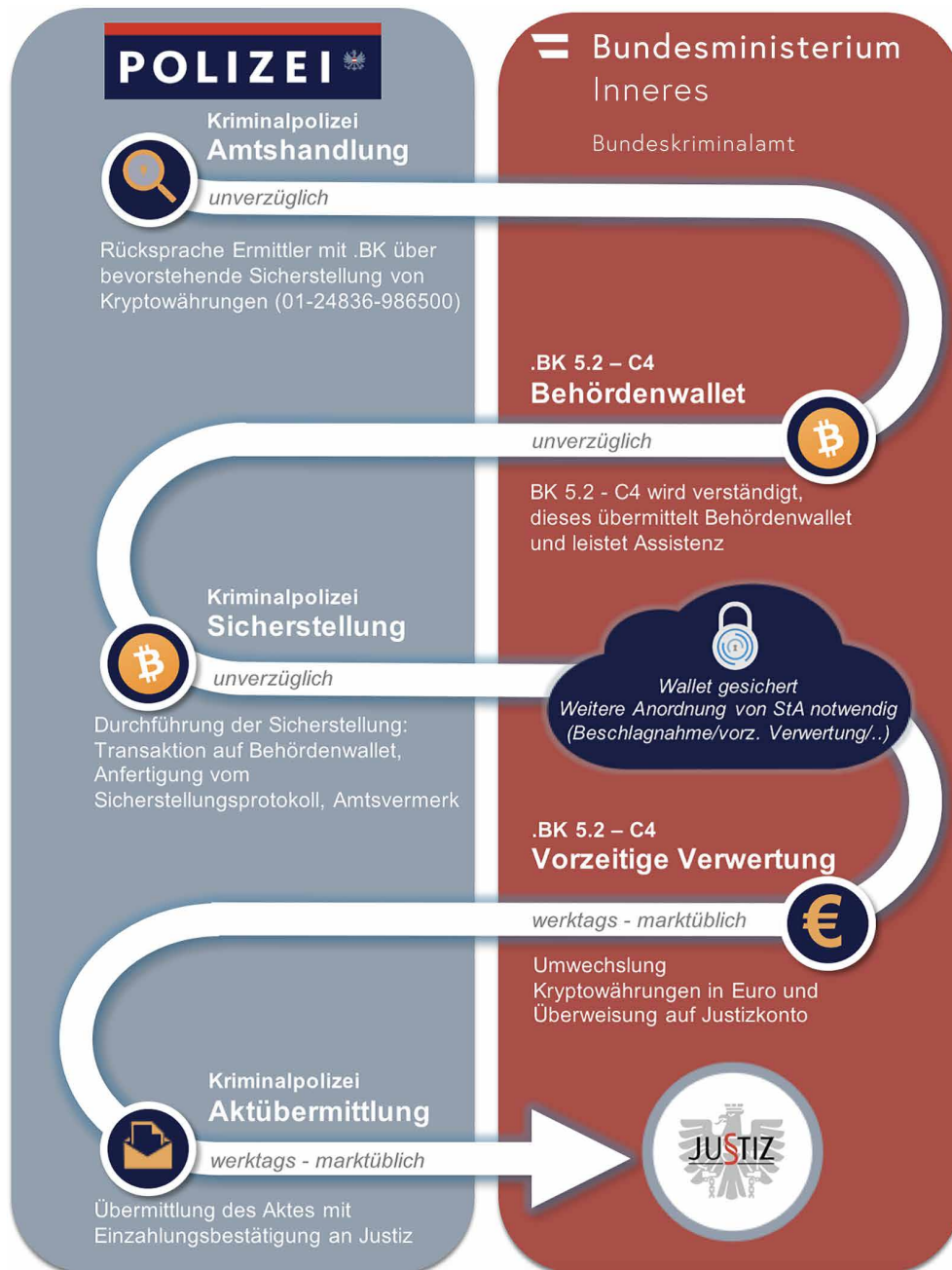
5.6 Smart Contracts und Altcoins

Bei der Ermittlung gegen einen im Darknet agierenden Verkäufer von Suchtmitteln wurde das C4 erstmalig mit einer speziellen Form von Kryptowährungstransaktionen, den sogenannten „Smart Contracts“, konfrontiert. Dabei handelt es sich um Computerprotokolle, die Verträge abbilden, überprüfen oder die Verhandlung und Abwicklung eines (Kauf-) Vertrages technisch unterstützen.

Generell stößt das C4 in Ermittlungen im Zusammenhang mit Smart Contracts zunehmend auf Straftaten, bei denen sogenannte Altcoins verwendet werden. Als solches werden im einschlägigen Sprachgebrauch jene Kryptowährungen bezeichnet, die nicht Bitcoins sind.

5.7 Behördenwallets

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



Grafik 3: Ablauf von Sicherstellungen

Die sichergestellten Kryptowährungen werden vom Gericht meist für verfallen erklärt, wobei in der Folge das C4 im Bundeskriminalamt in der Lage ist, auch die Verwertung durchzuführen und die Geldsummen an die jeweiligen Gerichte zu überweisen.

5.8 Darknet

Das „dunkle Netz“ hat seinen schlechten Ruf dadurch erlangt, dass es auch als Plattform für illegalen Waffen- und Drogenhandel, Hackerdienste und andere kriminelle Machenschaften genutzt wird.

Kriminelle Aktivitäten verlagern sich immer stärker ins Darknet, da es einen hohen Grad an Anonymität bietet. Darüber hinaus ist auch bei den Tätern eine immer stärkere Diversifizierung erkennbar. Das Angebot der Leistungen („Crime as a service“) im Darknet steigt kontinuierlich. Da der finanzielle Gewinn im Vordergrund steht, aber die Finanztransaktionen einer immer strengeren Kontrolle unterworfen werden, weichen die Täter auf virtuelle Währungen aus, die derzeit praktisch keiner Kontrolle unterliegen, vollkommen anonym gehandelt werden können und im digitalen Netz nur schwer nachvollziehbar sind.

Suchtgifthandel im Darknet

Der Onlinehandel mit verbotenen Substanzen hat sich in Österreich 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. Angefangen von der Kontaktaufnahme über die Verkaufsverhandlungen bis hin zur Bezahlung wird alles über verschlüsselte Netzwerke abgewickelt. Ermittlungen zeigen bislang, dass der Online Drogenhandel den Straßenhandel nicht verdrängt. Vielmehr wird der Handel auf Online Plattformen genutzt, um illegale Suchtmittel höherer Qualität zu erwerben und im Straßenverkauf gewinnbringend weiterzuverkaufen. Somit wird der klassische Straßenhandel durch den Internethandel nicht nur erweitert sondern auch ergänzt.

Seit September 2016 werden im internationalen Briefzentrum Frankfurt am Main Schwerpunktkontrollen bei den zu exportierenden Briefsendungen durch den deutschen Zoll durchgeführt. Dabei wurden durch das Zollfahndungsamt Frankfurt am Main bisher insgesamt 10.132 Briefsendungen sichergestellt, welche insgesamt 802.708 Gramm Suchtmittel zum Inhalt hatten. Adressiert waren die Briefsendungen an Empfänger in 90 verschiedenen Nationen. Dabei belegt Österreich seit Beginn der Kontrollen, gemessen an der Anzahl der Empfänger, mit 1.562 Postsendungen den zweiten Platz hinter den USA und liegt vor Destinationen wie Großbritannien, Frankreich oder Australien. Die für Österreich bestimmten Postsendungen enthielten insgesamt 138.136,34 Gramm Suchtgift. In Österreich werden im Zuge von Kontrollen durch die Zollverwaltung regelmäßig Postsendungen mit Suchtmitteln sichergestellt. Insgesamt wurden im Zeitraum von

18. Jänner 2016 bis 31. Dezember 2018 4.620 Briefsendungen mit Suchtmitteln in den österreichischen Postzentren beschlagnahmt. Diese Briefsendungen enthielten insgesamt 112.457,24 Gramm Suchtgift.

Die Folgeermittlungen zu den bisherigen Sicherstellungen ergaben, dass das Suchtgift der aufgegriffenen Briefsendungen ausschließlich über Darknet-Marktplätze bestellt wurde. Eine zunehmende Gefahr des Online-Handels zeigt sich auch durch den Postversand von designten Derivaten, wie z.B. Carfentanyl oder der Substanz U-47700. Diese Substanzen können schon beim Einatmen oder bloßen Hautkontakt zu beträchtlichen Gesundheitsschäden und bis hin zum Tod führen.

Eine große Anzahl der im Darknet verkauften illegalen Suchtmittel wird in den Niederlanden hergestellt und über diverse Vertriebskanäle auf dem Postweg nach Österreich versandt.

Aber nicht nur Konsumenten, sondern auch Darknet Suchtmittelhändler haben sich in Österreich etabliert. Im Laufe des Jahres 2018 konnten durch das Bundeskriminalamt im Büro Suchtmittelkriminalität die Betreiber von vier großen Darknet-Shops für Suchtmittel ausgeforscht und samt Mittätern festgenommen werden. Dabei wurden große Mengen Kokain, Ecstasy-Tabletten sowie Benzodiazepine sichergestellt.

5.9 Kampf gegen die Verbreitung von kinderpornografischem Material

In Österreich ist der Besitz pornografischer Darstellungen Minderjähriger, ebenso strafbar wie der wissentliche Zugriff auf kinderpornografisches Material im Internet. Seit 1. Jänner 2012 werden auch das sogenannte „Cybergrooming“, also die Anbahnung sexueller Kontakte zu Unmündigen über das Internet und die „Betrachtung pornografischer Darbietungen Minderjähriger“ (live mittels Web-Cam) strafrechtlich geahndet.

Eine eigene Meldestelle (E-Mail: meldestelle@interpol.at) nimmt Hinweise entgegen, wenn auf einer Webseite oder in einer Newsgruppe Texte oder Bilder entdeckt werden, die kinderpornografische Inhalte enthalten oder wenn auf einer Internetseite Sextourismus mit Kindern angeboten wird.

Im Bereich des Tatbestandes „Pornographische Darstellung Minderjähriger“ kam es im Jahresvergleich 2017/2018 zu einem sprunghaften Anstieg von 58,4 Prozent der angezeigten Straftaten. Das resultiert unter anderem daraus, dass die verschiedenen Anbieter von sozialen Medien in den USA beziehungsweise Kanada den Kampf gegen die Verbreitung von kinderpornografischem Material massiv verstärkt haben. So werden die einzelnen Dienste auf kinderpornografische Dateien überprüft und gegebenenfalls

der betroffene Account gesperrt. Damit einhergehend erfolgt eine entsprechende Verdachtsmeldung an das jeweilige Land, dem der Verursacher schließlich zugeordnet werden kann.

Eine weitere Problematik in diesem Bereich stellt das sogenannte „Liken“ und Weiterleiten von Videos dar, welche vor allem via Facebook verbreitet werden und sexuelle Handlungen von Minderjährigen mit Tieren zeigen. Derartige Darstellungen werden gedankenlos als vermeintliche „Spaßvideos“ an andere User weitergeleitet, ohne sich darüber im Klaren zu sein, dass der Besitz und die Verbreitung solcher Darstellungen ebenfalls strafbar sind. Daher wird in diesem Zusammenhang nochmals eindringlich davor gewarnt, derartige Videos mit anderen Usern zu teilen oder diese zu „Liken“. Ein solches Verhalten hat die Ausforschung des jeweiligen Account-Inhabers und eine entsprechende Anzeige bei der Staatsanwaltschaft zur Folge.

International wird nunmehr der englische Begriff „online sexual child exploitation“ statt Kinderpornografie genutzt. In diesem Bericht wird der Verständlichkeit halber noch der Begriff Kinderpornografie verwendet. Hintergedanke bei der neuen Namensgebung ist es, den Missbrauch in den Vordergrund zu stellen, da Pornografie dies nicht zwangsläufig abdeckt. Es ist daher wichtig zu betonen, dass rechtlich bei jeder neuerlichen Betrachtung das Kind erneut in die Opferrolle gebracht wird.

6 Ausbildung



6.1 Bezirks-IT-Ermitterschulung

Eine wichtige Grundlage zur Bekämpfung von Cybercrime ist die fundierte Ausbildung von BezIT-Ermittlern aus dem Exekutivdienst. Für die Umsetzung der Ausbildungsstrategie stellten Fachexperten aus dem C4 und den LKA AB6 ITB zuvor das umfangreiche Schulungskonzept zusammen und unterrichteten die Kollegen drei Wochen lang im Pilotkurs zu Themen, wie IT-Grundlagen, Täterstrukturen, Kryptowährungen, OSINT und Darknet. Neben Kriminologie und Kriminalistik wurden auch Module der Kriminaltechnik und -taktik vorgetragen. Insbesondere gute Kenntnisse im Bereich der Hardware- und Netzwerkgrundlagen, der mobilen Forensik sowie der wichtigsten forensischen Sicherstellungsprozesse sollen dazu beitragen, die Qualität der Ermittlungen und die Aufklärungsquoten nachhaltig weiter zu steigern.

Die Vorträge erfolgen vorrangig durch Polizisten, die im Bereich Cybercrime arbeiten. Dies stellt sicher, dass aktuelle Herausforderungen ebenfalls in die Ausbildung miteinfließen. Die gewonnenen Erfahrungen können so in eine praxisnahe Ausbildung eingearbeitet werden, um eine angestrebte kontinuierliche Verbesserung der Sicherung von Daten sowie bei der Fallbearbeitung zu erreichen. Die periodischen Schulungen werden quartalsweise durchgeführt. Die Planung dieser Ausbildung erfordert einen hohen Koordinationsaufwand, da die Vortragenden der Lehrtätigkeit zusätzlich zum eigentlichen Regelbetrieb nachgehen.

In der Aus- und Weiterbildung aller Polizisten (Säulen II und III) wurde das Thema Cybercrime in den Lehrplänen der Grundausbildungslehrgänge verstärkt berücksichtigt. Die im aktuellen Weiterbildungszyklus für Kriminalbeamte (KDFR - Kriminaldienst Fortbildungsrichtlinie) gesammelten Erfahrungen mit dem „Cybercrime-Tag“ werden in den nächsten Zyklus einfließen.

6.2 Ausbildungscampus Cybercrime

Im vergangenen Jahr wurde das Konzept „Ausbildungscampus Cybercrime“ fertig entwickelt und eingereicht. Dies ist erforderlich geworden, weil die in Frage kommenden Vortragenden bereits durch Schulungsmaßnahmen ausgelastet sind. Gleichzeitig ist hier, aufgrund der rasanten Entwicklungen in der Technik, eine enge Zusammenarbeit mit Wissenschaft und Forschung unumgänglich. Durch den gezielten permanenten Wissensaustausch zwischen Akademien und praktischen Erfahrungen aus der täglichen Ermittlungspraxis wird erwartet, dass mit den neuen Ausbildungen zu Spezialisten das erforderliche Niveau gehalten werden kann.

6.3 Europäische Ausbildungsprogramme – ECTEG und CEPOL

Auch auf europäischer Ebene wurde die Bedeutung einer fundierten Ausbildung der Strafverfolgungsbehörden zum Thema Cybercrime bereits früh erkannt. Das von der Europäischen Kommission unterstützte Projekt „Falcone“ (JAI/2001/Falcone/127 – ‘Training: Cybercrime Investigation – building a platform for the future’) empfahl unter anderem die Erstellung von europaweit einheitlichen Trainings für Cybercrime- Ermittler.

Einer der Gründe für die Einführung von standardisierten Trainings war es, die Anerkennung polizeilicher Arbeit vor Gerichten eines anderen Staates zu erleichtern. 2007 gründete EUROPOL die „Europol Working Group on the Harmonisation of Cybercrime Investigation Training“. Ihre Aufgabe war es primär, Erfahrung und Wissen bereitzustellen, um bei der Erstellung und Harmonisierung der Cybercrime-Ausbildung zu unterstützen. Im Jahr 2009 wurde der Name in „European Cybercrime Training and Education Group“ (ECTEG – <https://www-ecteg.eu/>) geändert. Es wurden Qualitätsstandards zur Aufbereitung und Vermittlung spezieller Wissensinhalte definiert und es wurde aber auch auf Rahmenbedingungen, wie beispielsweise Qualifikationen von Trainern oder die Ausstattung von Schulungsräumen Rücksicht genommen. Darauf basierend wurden zahlreiche Kurse konzipiert und den europäischen Strafverfolgungsbehörden zur Verfügung gestellt. Aufgrund der formalrechtlichen Rahmenbedingungen für Expertengruppen, wie früher ECTEG eine war, stellten sich Aktualisierung und Erweiterung des Kursangebotes als große Herausforderungen dar. Daher wurde ECTEG Ende 2016 als Verein neu gegründet. Die Mitglieder setzten sich aus Strafverfolgungsbehörden und Einrichtungen aus Wissenschaft und Forschung zusammen. Mittlerweile ist die Mitwirkung nicht mehr nur auf Europa beschränkt. Durch die Förderung der Europäischen Kommission und in enger Zusammenarbeit mit den European Cybercrime Center (EC3) von EUROPOL und CEPOL (der Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung) werden die bestehenden Ausbildungsmodule laufend aktualisiert und neue entworfen.

Bei der Erstellung neuer Ausbildungsmodule wird zunehmend der Einsatz von E-Learning gefördert. Diese Form der zentralen, elektronischen Wissensvermittlung erfordert zwar hohen Aufwand bei der Konzeption und Erstellung, kann aber im laufenden Betrieb mit bedeutend geringerem Ressourceneinsatz einer großen Zahl von Lernenden zur Verfügung gestellt werden. Es darf aber nicht außer Acht gelassen werden, dass diese regelmäßig aktualisiert und durch praktische Übungen und Präsenzs Schulungen ergänzt werden müssen.

Im C4 werden nicht nur eigene Schulungen gestaltet, es erfolgt auch eine Beteiligung an der Entwicklung von Fortbildungsmodulen. Im nationalen Bereich konnten beispielsweise auf der Intranet-Plattform „SIAC Campus“ zwei Teile der BezIT-Ermittlerausbildung zur Verfügung gestellt werden. Außerdem werden internationale E-Learning Module, die für Strafverfolgungsbehörden im kriminalpolizeilichen Bereich zum digitalen Themenkomplex zur Verfügung stehen, an die nationalen Gegebenheiten angepasst.

6.4 INTERPOL Digital Security Challenge

Von 19. bis 21. Februar 2018 fand, durch die Unterstützung des C4, die „INTERPOL Digital Security Challenge“ erstmalig in Europa statt. Zu diesem dreitägigen internationalen Trainingsevent mit Wettbewerbs-Charakter wurden alle Cybercrime-Experten der INTERPOL-Mitgliedsländer eingeladen. 52 Ermittler und IT-Forensiker aus 28 Ländern besuchten die Schulung und stellten sich einem fairen Wettstreit. Erfreulich darf die beachtenswerte Leistung des Gewinnerteams hervorgehoben werden, in welchem auch ein Mitglied des C4 vertreten war.

7

Prävention



Sicherheit kann in Fällen von Cybercrime nur in Kooperation mit der Bevölkerung und durch die Förderung des Sicherheitsbewusstseins der Bürger gewährleistet werden. Die Präventionsmaßnahmen des C4 waren vielfältig. Dazu zählten laufende Informationserstellung über Sicherheitslagen im In- und Ausland und deren Verteilung, anlassbezogene Gefahrenhinweise in Form von Newslettern bis hin zur Benachrichtigung Betroffener, deren Daten durch Daten-Leaks veröffentlicht wurden. Zudem beantwortete das C4 täglich zahlreiche Anfragen zu Cybercrime-Delikten von Bürgern, die an die Meldestelle ergingen.

Ebenfalls beteiligte sich das C4 mit Vorträgen und Informationsständen an zahlreichen Präventionsveranstaltungen. Auch im Jahr 2018 wurde im Rahmen von GEMEINSAM. SICHER die Zusammenarbeit mit der Wirtschaftskammer (WKO) weitergeführt (eDay, Beratertag, etc.).

Unvernunft bei der Handhabung, Freizügigkeit mit persönlichen Daten und Unachtsamkeit auf Endgeräten mit einer Internetanbindung führen alljährlich zu hohen Opferzahlen. Im Regelfall scheinen hohe Schadenssummen unwiederbringlich an die Täter verloren.

7.1 Sicherheitshinweise für den Alltag

Es handelt sich hier nur um eine exemplarische und keinesfalls vollständige Aufzählung:

- Brechen Sie unverzüglich den Kontakt ab, wenn Ihnen das Gegenüber verdächtig erscheint.
- Wenn Sie Erpresser-E-Mails erhalten, beantworten Sie diese nicht, bezahlen Sie auf keinen Fall und kommen Sie keinen sonstigen Anforderungen nach.
- Wählen Sie sichere Privatsphäre-Einstellungen in sozialen Netzwerken. Je weniger von Ihrem Profil öffentlich einsehbar ist, desto geringer ist die Wahrscheinlichkeit, in das Visier von Erpressern oder anderen Tätern zu geraten.
- Öffnen Sie keine E-Mail Anhänge oder Links in E-Mails von unbekannten Absendern.

- Unterziehen Sie eingehende E-Mails immer einer Plausibilitätsüberprüfung (beispielsweise mit Fragen wie: Erwarte ich diese E-Mail? Passt der Absender zum Inhalt? Kann es überhaupt sein, dass in dieser E-Mail meine Kontaktdaten angefragt werden? etc.).
- Im Falle einer bereits geleisteten Zahlung, beispielsweise bei einem Internetbetrug, erstatten Sie eine Anzeige auf einer Polizeiinspektion. Nehmen Sie dafür alle relevanten Dokumente und Beweismittel mit beziehungsweise stellen Sie diese dem aufnehmenden Beamten in geeigneter Weise zur Verfügung.
- Falls Sie einen Bildschirm oder Fernseher mit integrierter Kamera haben, kleben Sie diese zu oder decken sie ab, wenn Sie diese nicht in Gebrauch haben.
- Achten Sie auf Ihre persönlichen Accounts. Alte E-Mail Adressen werden bei Nichtnutzung durch den Betreiber oft wieder frei gegeben, von Tätern übernommen und dann missbräuchlich verwendet.
- Nutzen Sie niemals dieselben Passwörter für verschiedene Accounts. Sollte ein Täter auf irgendeine Weise ein Passwort erlangt haben, hätte er Zugriff auf weitere Accounts und könnte dadurch einen enorm hohen Schaden anrichten.
- Führen Sie regelmäßige Updates und Patches Ihrer Endgeräte (Router, Smartphones, PCs, etc.) durch.
- Verwenden Sie eine Firewall und einen aktuellen Virenschutz.

7.2 Tipps zu Cloud-Services

Da die Datendienste von Cloud-Services oftmals in Anspruch genommen werden, sollte man sich bewusst sein, dass man seine Informationen Dritten anvertraut. Deshalb sollten vorab folgende Fragen geklärt sein: Welche Informationen geben Sie weiter bzw. werden in der Cloud gespeichert? Wie wertvoll oder vertraulich sind diese Daten? Wie vertrauenswürdig ist der Cloud-Service Anbieter hinsichtlich Schutz der Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten? Auf den ersten Blick sehen alle Anbieter vertrauenswürdig aus, tatsächlich aber können einige riskant werden. So machte eine Sicherheitslücke in einer Smart Keyboard App (eine Applikation um die Texteingabe zu vereinfachen) vor einiger Zeit alle Eingaben von Millionen Nutzern öffentlich einsehbar,

darunter auch Benutzernamen und Passwörter für andere Online-Dienste. Sicherheitsrichtlinien und -standards sollten deshalb auch beim Einsatz von Cloud-Services gelten. Die Nutzung ungeprüfter Dienste oder Apps, z.B. für Notizen, den Austausch von Dateien oder das Konvertieren von PDF-Dateien, stellen ein hohes Risiko dar. Deren Verwendung kann die Vertraulichkeit verletzen und zu Datenverlust führen. Seien Sie besonders vorsichtig, wenn es um sensible Daten geht!

8

Zusammenfassung



8.1 Daten und Fakten

In der Kategorie Internetkriminalität sind die Anzeigen von 2017 auf 2018 von 16.804 auf 19.627 gemeldete Fälle angestiegen. Die Aufklärungsquote lag 2018 mit 37,4 Prozent, um 1,1 Prozentpunkte niedriger als im Vorjahr. Die immensen Steigerungen sind überwiegend auf den ausufernden Internetbetrug zurückzuführen. Der Rückgang in der Aufklärungsquote weist mitunter auf den Gebrauch von Verschlüsselungs- und Anonymisierungstechniken sowie datenschutzrechtliche Maßnahmen, wie die Umsetzung der neuen DSGVO insbesondere im Zusammenhang mit dem "WHOIS"-Protokoll, hin.

Bei den Cybercrime-Delikten im engeren Sinn wurde 2018 ein Rückgang der Anzeigen um 13,4 Prozent verzeichnet, während die Anzeigen von Internetbetrug um 13,3 Prozent gestiegen sind.

Die Deliktszahlen 2018 zeigen, dass der Trend weiter deutlich ansteigt. Die zunehmende Technisierung des Alltags, der mangelhafte Umgang mit Daten, die Verwendung IT-gestützter Kommunikationsformen und sozialer Medien, fehlerhafte Produkte und Applikationen, welche Sicherheitslücken darstellen, bieten potentiellen Tätern eine stetig wachsende Angriffsfläche.

8.2 Trends und Fazit

Während in den Vorjahren eher die undifferenzierte Masse der User attackiert wurde, gerieten auch wieder Klein- und Mittelunternehmen sowie Privatpersonen mit gezielten, aufwendigeren Angriffen in den Fokus der Täter. Die Bedrohungslage kann somit als steigend eingestuft werden. Insbesondere war das vermehrte Auftreten von Ransomware- und DDoS-Angriffe zu beobachten.

Die digitale Revolution bringt neben dem Mehr an persönlicher Freiheit und Selbstbestimmung auch höhere Gefahren für den Einzelnen sowie Risiken für die Gesellschaft.

Das erfordert das sicherheitsorientierte Überdenken von Schulungen und Maßnahmen zur Bewusstseinsbildung innerhalb der Bevölkerung und der Sicherheitsbehörden, die einerseits den sozialen Erfordernissen, andererseits auch den technologischen Weiterentwicklungen entsprechen sollten. Die richtige Nutzung von sozialen Netzwerken und elektronischen Kommunikationsformen erfordern den sicheren Umgang mit Daten jedes einzelnen Nutzers. Im eigenen privaten Bereich, wie auch in der Berufswelt, sind zur Abwehr von Attacken auch private Informationen gegen Social-Engineering und Erpressungsversuche zu schützen. Das Sicherheitsbewusstsein der Bevölkerung wäre weiterhin durch geeignete Präventionsarbeit zu heben.

Die Analysen der Aufgaben und Abläufe zeigen, dass entscheidende Ermittlungstätigkeiten vor allem durch technisches Fachpersonal durchgeführt werden müssen. Die Entwicklung von Cybercrime macht deutlich, dass weiterhin gezielte Rekrutierungsmaßnahmen und personelle Verstärkungen für die Assistenzdienste in den Landeskriminalämtern und im BK erforderlich sein werden. Die Schulungsmaßnahmen werden bestmöglich an die sich verändernde Kriminalitätsentwicklung angepasst. Dabei sind jedoch bei den benötigten (akademischen) Experten die demografische Entwicklung mit dem Fachkräftemangel sowie die Einkommensunterschiede zwischen dem privaten Sektor und dem Bund als möglichen Arbeitgeber, mit zu berücksichtigen. Die maßgeschneiderte Ausbildungsoffensive von Polizisten für die richtige Kategorisierung der Ereignisse, Anzeigenaufnahme und einfache Beweismittelsicherungen führt zu einem zusätzlichen Bedarf an BezIT-Ermittlern. Das Landeskriminalamt agiert bei Delikten mit Bezug zu Informationstechnologien oft federführend und wird zunehmend eingebunden. Für eine effizientere Aufklärung von international auftretenden Massendelikten und die zentralisierte Ermittlung bei Sonderfällen wird eine weitere Spezialisierung im BK als dringend notwendig erachtet.

Die Weichen zu einer aktiven Eindämmung von Cybercrime müssen rechtzeitig gestellt werden, da mit einem eigenständigen Rückgang von Internetkriminalität nicht gerechnet werden kann. Begründet werden kann dies mit der Zunahme von vernetzten Endgeräten, IoT (Internet of Things) und dem Risiko des Einsatzes von sehr mächtigen Machine Learning Algorithmen, welche sowohl zukünftige Angriffsflächen als auch Tatmittel und, damit verbunden, Angriffsdienstleistungen aus dem Darknet als Cybercrime as a Service (CaaS) wahrscheinlicher machen. Denn es ist ebenso anzunehmen, dass die verwendeten Tools mit der bereits festgestellten Perfektionierung der Angriffsmethoden und dem Wissenserwerb von Kriminellen raffinierter werden und die einhergehenden Probleme und Risiken mit den Angriffen weiterhin steigen werden. Dies ergibt sich unter anderem aus dem nahezu grenzenlosen Betätigungsfeld der Cyber-Kriminellen, da sie ihre Aktivitäten ortsunabhängig starten. Es kann deshalb der Schluss gezogen werden, dass mit dem erwarteten Anstieg des Ausbreiten der Angriffe in schnelleren Wellen, mit einer größeren Anzahl an Geschädigten und höheren Schadenssummen erfolgen wird.

Der internationale Aspekt im Bereich Cybercrime und die sich daraus ergebenden Möglichkeiten der Tätervernetzung sind mitverantwortlich für den kontinuierlichen Anstieg von Cyber-Angriffen. Durch die Beteiligung der in Österreich relevanten Behörden an internationalen Gremien und Projekten ist gewährleistet, dass auch unter den verschiedenen Strafverfolgungsbehörden eine fortwährende starke globale Vernetzung stattfindet.

Der Zuwachs der im vergangenen Jahr durchgeführten Angriffe über Sicherheitslücken in Endgeräten und fehlerhaften Applikationen ließe für die Zukunft erwarten, dass die industriellen Anbieter von Soft- und Hardware beziehungsweise Online Dienstleistungen

mehr in Sicherheitsvorkehrungen und Updates investieren, um ihre Kunden auch bei sachgemäßer Verwendung von Endgeräten ausreichend schützen zu können.

Die rechtlichen Vorgaben zur Bekämpfung neuer Phänomene der Internetkriminalität sollten aus kriminalpolizeilicher Sicht so geformt sein, dass internationale Strafverfolgungsstrategien nicht beeinträchtigt und operative Maßnahmen weiterhin ermöglicht werden.

9 Summary



9.1 Facts and Figures

The number of reported cybercrime offenses expanded from 16,804 in 2017 to 19,627 in 2018. 37.4 per cent of the cases were solved, down 1.1 per cent from the previous year. Rampant online fraud accounted for most of this increase. The lower percentage of solved cases could be attributed to the use of encryption and anonymisation tools, the lack of data retention in Austria, and data privacy rules such as the implementation of the new General Data Protection Regulation (GDPR), especially with regard to the WHOIS protocol.

In the category of pure cybercrime (attacks on data and computer systems), police reports declined by 13.4 per cent in 2018, while reported online fraud cases went up by 13.3 per cent.

The 2018 figures show an ongoing and significant uptrend in cybercrime. The popularisation of technology in everyday life, careless sharing of data, new messaging services, social media and insufficiently protected devices and apps are becoming an ever-bigger target for potential offenders.

9.2 Trends and Conclusion

While offenders tended to attack users indiscriminately in the past, they more recently started to target small and medium businesses as well as private individuals in more sophisticated attacks. This is a sign that the threat is growing. In particular, more ransomware and distributed denial of service (DDoS) attacks were observed.

A greater degree of personal freedom and self-determination are among the advantages of the digital revolution, but it also carries new risks for individuals and society at large.

To address this issue, there needs to be a security-focused review of educational measures for the population and law enforcement authorities, which ideally keep abreast of social requirements and technological developments. Users should learn how to correctly use social networks and new forms of communication in order to keep their data safe. As in the past, adequate programmes should be offered to raise awareness of these dangers and prevent private and professional information from being misused for social engineering and blackmail attempts.

Due to the high case numbers, the legal framework should be adapted to counteract the increasing difficulty in investigating crime and to bring the penalties for cybercrime in line with current requirements.

Analyses of tasks and processes show that crucial investigation work has to be primarily conducted by technical specialists. As cybercrime advances, it is vital to keep up targeted recruiting programmes and strengthen staff numbers of auxiliary services at the Provincial CIDs and Criminal Intelligence Service Austria. Training schemes are adapted as much as possible to changing crime trends, even though the availability of college-educated experts is hampered by the demographic shift, a lack of skilled labour and the income gap between the private and the public sectors. Additional district IT investigators are needed for customised training programmes to make police officers proficient in correctly categorising incidents, taking statements, writing reports and collecting evidence. The provincial CID unit often leads the way in handling IT-related offences and is increasingly included in investigations. In order to solve widespread international offences and to centralise investigations into special cases, a further specialisation of units at Criminal Intelligence Service Austria is of the essence.

Measures to proactively curb cybercrime must be initiated in a timely manner, as online crime is not expected to subside on its own. This is in part due to the Internet of Things (IoT) and powerful machine learning (ML) algorithms, which are both a potential security leak and a probable tool for offenders, who may offer Cybercrime as a Service (CaaS) in the Darknet. Criminals are also expected to keep refining their already perfected tools, leading to greater problems and risks in the wake of attacks. Moreover, the Internet allows cybercriminals to operate virtually without limits, which means that future attacks could occur in quick succession and on a broader scale, resulting in higher losses and a larger number of victims.

The international aspect of cybercrime and the opportunities for offenders to connect are part of the reason why cyberattacks are continually on the rise. Nevertheless, Austria's competent authorities participate in international panels and projects, ensuring that law enforcement authorities across the globe continue to build their own strong networks.

Considering the increase in attacks through security loopholes in end devices and through bugs in applications, it is reasonable to assume that software and hardware makers and online service providers will invest more in security and updates so as to protect their customers, even if they do not use the devices as intended.

From the standpoint of criminal investigators, legislation for combating new crime trends on the Internet should not interfere with international law enforcement strategies and should continue to allow operational measures.

10 Glossar



Anonymisierungsdienst

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

Antivirenprogramm

Ein Antivirenprogramm (synonym mit Virenschanner 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 (z.B. Tablets oder Smartphones) verwendet.

BEC (Business E-Mail Compromise)

Angreifer kompromittieren bei einem BEC den E-Mail 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 Briefftasche, 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.

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 (Clearweb) an, welche unverschlüsselt vorliegen, indexiert sind und meist über eine URL aufgerufen werden können. Um in das Darknet beziehungsweise Tor Netzwerk zu gelangen, benötigt man beispielsweise einen speziellen Browser, etwa den Tor-Browser. Daten werden im Darknet anonym und verschlüsselt über verschiedene Server geschickt. Das Darknet war ursprünglich für Personen/Journalisten 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 zur Kinderpornografie und weit darüber hinaus.

DDoS-Angriffe

DDoS-Angriffe beziehungsweise „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 Cyberattacks), 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 (z.B. aus 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.

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, E-Mails 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.

Spam

Als Spam bezeichnet man elektronische, unerwünschte Nachrichten, die massenhaft und ungezielt 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.

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 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 (z.B. <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 (englisch 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 Domains 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.

