.BK
BUNDESKRIMINALAMT

entschlüsseln

LAGEBERICHT CYBERCRIME 2017

INHALT

VORWORT

Liebe Leserinnen und Leser!

Die Bekämpfung der Cyberkriminalität hat für das Innenministerium eine hohe Priorität und erfordert gemeinsame Anstrengungen bezüglich Training, technischer Ausstattung und internationaler Vernetzung. Denn sowohl im niederschwelligen als auch im Intensivtäter-Bereich nimmt diese Kriminalitätsform zu und fordert die Polizei. Ermittlungsmaßnahmen werden durch neue, sich aus dem technologischen Fortschritt ergebende modi operandi erschwert, beispielsweise Drohnenangriffe, Verlagerung der Kommunikation der Täter und krimineller Organisationen in das Darknet und Verwendung von verschlüsselter Kommunikation. Die Digitalisierung verstärkt die Möglichkeit der Anonymisierung, Verschleierung von Geldflüssen und ein arbeitsteiliges Vorgehen. In immer kürzeren Intervallen treten neue Kriminalitätsphänomene auf.

Die Weiterentwicklung des Cybercrime-Competence-Centers im Bundeskriminalamt zu einer modernen Hightech-Einheit hat daher oberste Priorität. Ergänzt wird dieser Ausbau durch Aus- und Fortbildungsmaßnahmen in den Landeskriminalämtern und den Polizeiinspektionen, um die Wissensweitergabe auch in der Polizeibasis zu verankern.

Die dritte Säule ist die Sicherstellung der Nachhaltigkeit durch Prävention. Zahlreiche Informations- und Präventionsmaßnahmen sollen die Awareness sowohl bei den Internet-Usern als auch bei den Betreibern heben und so zu nachhaltigen Erfolgen führen.

Herbert Kickl
Bundesminister für Inneres

General Franz Lang
Direktor des Bundeskriminalamtes

Dr. Michael Fischer
Stellvertretender Direktor des Bundeskriminalamtes

EINLEITUNG

Althergebrachte Prinzipien und bewährte Prozesse des Zusammenlebens werden auch in interaktiven Arbeitswelten durch die Dynamik der technologischen Weiterentwicklungen rasant verändert. Dies erfordert laufende Anpassungen und oftmals eine Neuorientierung in der Strafverfolgung und präventiven Aufklärung.

Das Cybercrime-Competence-Center (C4) im Bundeskriminalamt stellt sich gemeinsam mit den Landeskriminalämtern und den Bezirks-IT-Ermittlern dem Paradigmenwechsel mit sehr hohem persönlichem Einsatz. Dazu wird gut ausgebildetes Personal mit profundem Fachwissen und kriminalpolizeilichem Geschick mit modernster technischer Infrastruktur benötigt.

Das C4 fügt sich mit dem wichtigen internationalen Schwerpunkt der Kriminalitätsbekämpfung in den nationalen strategischen Rahmen des Bundeskanzleramtes ein und reagiert höchst flexibel mit der benötigten Erweiterung technischer Einrichtungen, der Anpassung interorganisationaler Abläufe und mit Bereitstellung fachlich hoch spezialisierter Experten.

Manche Problemstellungen können durch mangelnde Modernität oder fehlende Investitionsbereitschaft in IKT-Sicherheit, speziell in Österreich mit seinen vorwiegend Klein- und Mittelständischen Unternehmensstrukturen (KMU), verstärkt wahrgenommen werden. Durch den langjährigen Vertrauensaufbau zu heimischen Unternehmen und in Kooperation mit der Wirtschaftskammer (WKO) konnte die Bewusstseinsbildung für den präventiven Schutz vor Cybercrime weiter erfolgreich ausgebaut werden. Dazu wurden Informationen zu derzeitige Bedrohungslagen, sichere Datensicherungs-Konzepte und aktuelles Patch-Management verbreitet.

Bei einem internationalen Krisenfall durch eine Ransomware zeigte sich, dass das C4 in die operative Koordinierungsstruktur des Bundeskanzleramtes (BKA), als Bestandteil des Inneren Kreises der operativen Koordinierungsstrukturen (IKDOK) in das Cyber Krisenmanagement (CKM) hervorragend eingebunden war und durch schnelle Reaktionszeiten und Aufklärungsarbeiten im europäischen Vergleich nur eine geringfügige Anzahl von Unternehmen betroffen war. Die Analysen und Aufbereitungen des C4 führten im Rahmen der Sonderkommission (Soko) Clavis in Kooperation mit Europol und Virenschutzanbietern zur weltweit einzigen erfolgreichen Entschlüsselung dieser Schadsoftware.

Die in organisationsübergreifenden Teams der Soko Kfz und der Arbeitsgruppe (AG) Motorrad fest verankerte Fahrzeugforensik des C4, konnte 2017 wesentliche Beiträge für die Ermittlungsarbeit leisten und Präventions- und Informationsmaßnahmen umsetzen. Der österreichweite Rückgang des Kfz-Diebstahls um 11,2 Prozentpunkte als auch die erhebliche Verringerung von Motorraddiebstählen um 51 Prozentpunkte wurde durch die Fahrzeugforensik entscheidend mitverantwortet.

Das sich ausdehnende Phänomen Cybercrime erfordert die Zusammenarbeit und den Informationsaustausch mit internationalen Behörden und Organisationen, aber auch umsetzbare Vorschläge zu legislativen Vorhaben. Eine zentrale Herausforderung werden die Auswirkungen der derzeitigen Beschlussfassung des Netz- und Informationssicherheitsgesetzes (EU-NIS Richtlinie) und die Einführung der Datenschutzgrundverordnung (DSGVO) sein. Das Ziel der Verbesserung der operativen Koordinierungsstruktur wird in Folge weitere Anpassungen der Ermittlungsmöglichkeiten des C4 erfordern.

Trotz des enorm steigenden Arbeitsanfalls und der zunehmenden technischen Komplexität, konnte auch in diesem Jahr die Aufklärungsquote bei Cybercrime-Delikten erheblich gesteigert werden.

ÜBER DAS CYBERCRIME-COMPETENCE-CENTER (C⁴)

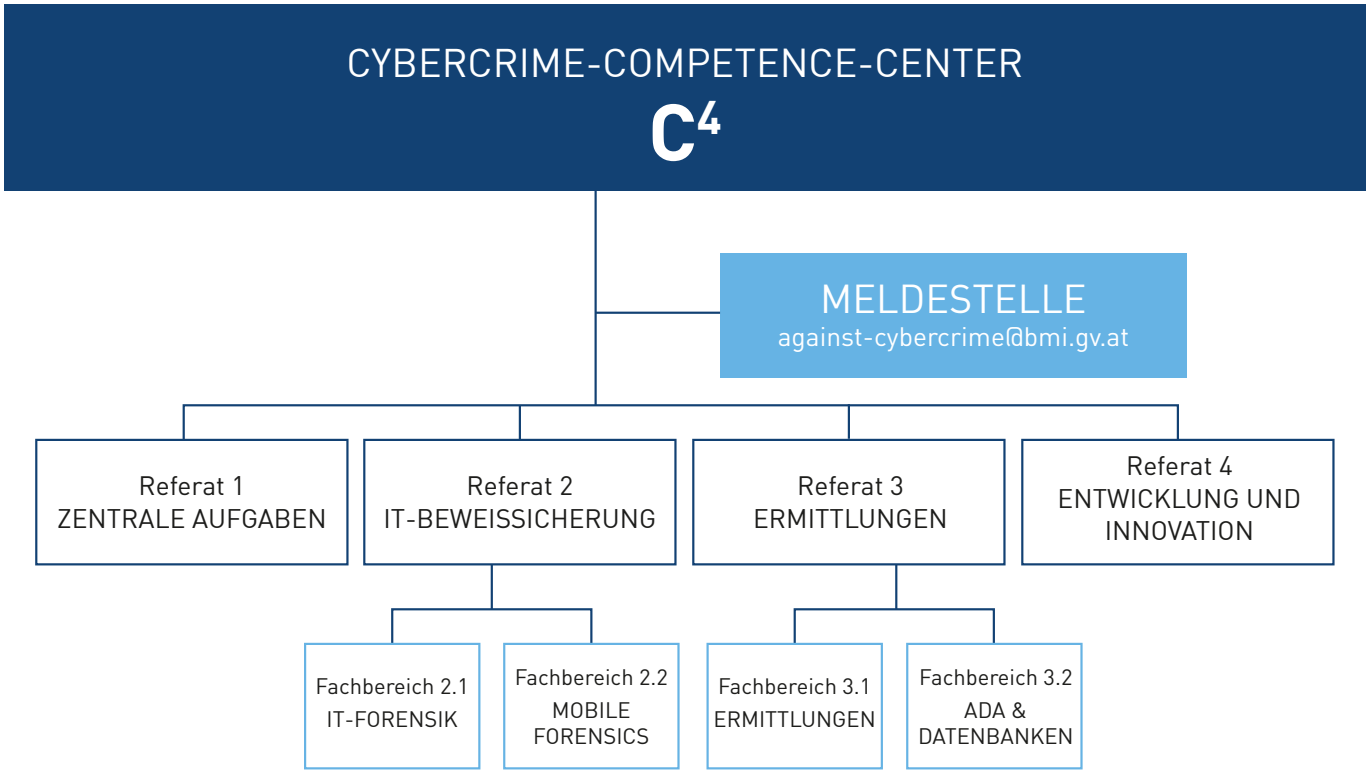

Abbildung 1: Organigramm des C⁴ (Quelle: BK)

Das C⁴ wurde 2011 zur Bekämpfung von Computerkriminalität als eigene Einheit innerhalb der Abteilung Kriminalpolizeiliche Assistenzdienste des BK etabliert. Es ist nationale und internationale Koordinierungs- und Meldestelle für Ermittlungen im Zusammenhang mit Cybercrime im engeren Sinn und für die elektronische Beweismittelsicherung und deren Auswertung zuständig. Darüber hinaus ist im C⁴ die Meldestelle als Ansprechstelle für die Bevölkerung und zu den Unternehmen etabliert, wodurch im Schadensfall eine rasche Unterstützung erfolgen kann und neue Phänomene frühzeitig erkannt werden. Das C⁴ fungiert aber auch intern für alle heimischen und globalen Polizeidienststellen als wichtige Drehscheibe sowie Koordinationspunkt und gliedert sich mit ihren Schnittstellen zum Cyber Security Center (CSC) des Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) als wesentlicher Bestandteil in die Strategie des BKA ein. Im Krisenfall erfolgt so die Unterstützung des IKDOK .

Das C⁴ passt sich den Aufgaben auch aufbauorganisatorisch laufend an: so wurde 2017 das Referat Entwicklung und Innovation neu etabliert und der Fachbereich Mobile Forensik um das Aufgabengebiet der Fahrzeugforensik erweitert. Die Änderungen der Aufbauorganisation im C⁴ wurden somit im Sinne der vereinbarten BMI-Strategie entsprechend umgesetzt. Das definierte Wirkungsziel der Kernaufgaben ist die konsequente und zielgerichtete Kriminalitätsbekämpfung, die enorme materielle Schäden abwenden und das Vertrauen der Bevölkerung stärken soll. Diese Zielerreichung sollte mit der Stärkung der Cybercrime-Ermittlungen und durch die Bekämpfung der Internetkriminalität erfolgen.

DIE REFERATE IM ÜBERBLICK

Das C⁴ besteht aus vier Referaten:

- Das Referat für zentrale Aufgaben verstärkt die administrativen Tätigkeiten der Abteilung vor allem bei nationalen und internationalen Gremienarbeiten, öffentlichen Veranstaltungen, im Berichtswesen, wissenschaftlichen Kooperationen und der Koordination bei Aus- und Fortbildungsmaßnahmen für die IT-Ermittlungen und die IT-Forensik. Außerdem sind hier die Beschaffung, Bereitstellung und Aufrechterhaltung der C⁴ internen Infrastruktur angesiedelt.

- Das Referat der IT-Beweissicherungen ist mit der Leitung, Koordination und Durchführung von nationalen und internationalen Datensicherungseinsätzen betraut. Des Weiteren werden forensische Sicherungen in IT-Infrastrukturen von Servern, Rechnern, elektronischen Medien, mobilen Endgeräten und Kraftfahrzeugen durchgeführt.

- Das Referat der IT-Ermittlungen leitet und koordiniert nationale und internationale Ermittlungen zur zielgerichteten Aufklärung von Cybercrime-Delikten in bi- oder multilateraler Zusammenarbeit mit Europol und Interpol (INCRP). Der Fachbereich „ADA und Datenbanken“, Automatischer Daten Abgleich (ADA), führt im Anlassfall neben Ermittlungsfällen und Projektunterstützungen auch die Koordination und Durchführung des automationsunterstützten Datenabgleichs durch. Das Referat ist auch in der Lage technisch sehr komplexe Ermittlungen auszuführen wie zum Beispiel Blockchain-Analysen.

- Das neu gegründete Referat für Entwicklung und Innovation befasst sich wissenschaftlich mit neuen Technologien und deren Folgenabschätzung bei kriminellen Straftaten oder deren Potentiale für die Aufklärung. Ebenso werden durch Innovationen konkret anwendbare Lösungen für die Kriminalitätsbekämpfung ausgearbeitet.

MELDESTELLEN

INTERNETKRIMINALITÄT

Die Meldestelle zur Bekämpfung der Internetkriminalität ist seit knapp sieben Jahren im C⁴ etabliert und ist im 24/7 Betrieb rund um die Uhr erreichbar. Mit über 10.000 schriftlichen Anfragen und Mitteilungen von Bürgern, Unternehmen sowie nationalen und internationalen Polizeidienststellen wurde die Meldestelle im Jahr 2017 konfrontiert. In diesem Zeitraum nahm das Team mehr als 1.000 telefonische Hinweise und Meldungen entgegen.

In ihrer zentralen Funktion als Schnittstelle innerhalb polizeiinterner Strukturen sowie als Meldestelle für Bevölkerung und Wirtschaft agiert die Meldestelle sowohl als Koordinierungs- als auch Informationszentrum im Bereich Cybercrime. Dies umfasst auch pro aktive, präventive Maßnahmen in Form von Warnmeldungen und Newslettern, die von speziell geschulten Mitarbeitern erstellt werden. Die deutlich erkennbare Sensibilisierung und Bewusstseinsbildung zum Thema Cybercrime erfolgte einerseits durch die fortlaufende Kooperation mit unterschiedlichen Institutionen aus dem Bereich der Wirtschaft und Vereinen, wie beispielsweise der WKO oder der Initiative „Watchlist". Andererseits führen Erstanalysen der eingehenden Meldungen zu schnellen Informationsweitergaben aktueller Phänomene, um akute Bedrohungslagen zeitnahe abzuschwächen. Für diese Aufgaben ist ein technischer Journaldienstbetrieb eingerichtet, der in dringenden Fällen organisationsübergreifende Sofortmaßnahmen einleiten kann.

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

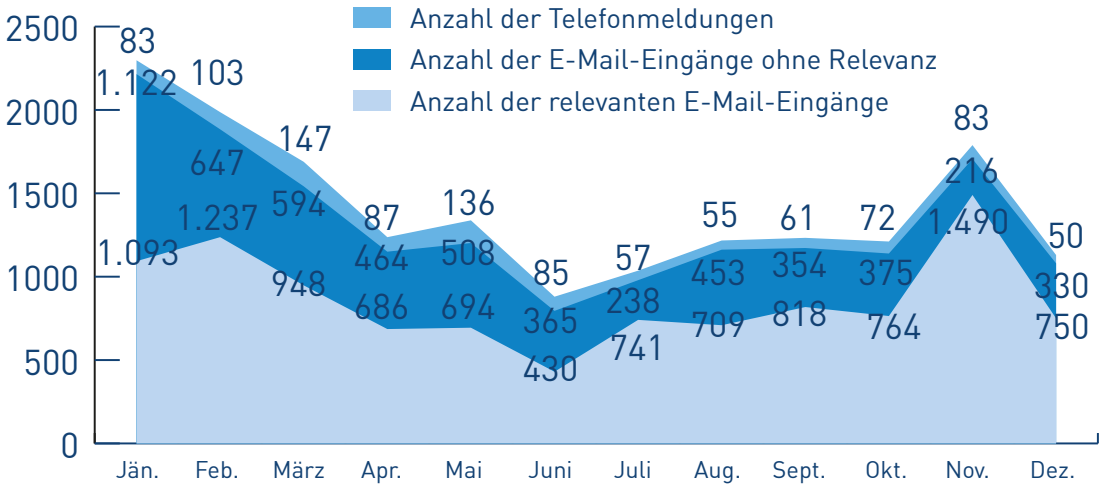

Abbildung 2: Eingänge in die Meldestelle des C⁴ 2017 (Quelle: BK)

KINDERPORNOGRAFIE UND KINDERSEXTOURISMUS

2017 gingen 1.698 Hinweise in der Meldestelle ein, wobei 499 Meldungen einen Österreichbezug aufwiesen. Darüber hinaus führte die Meldestelle zahlreiche erfolgreiche Amtshandlungen, bei denen sexuelle Missbräuche an Kindern geklärt und umfangreiches Beweismaterial sichergestellt werden konnte.

Beispielhaft darf eine Operation angeführt werden, die gemeinsam mit dem Bundeskrimimalamt (BKA) Wiesbaden bearbeitet wurde. Im Zuge von Ermittlungen in Deutschland war man auf das Darknet-Forum "Elysium" gestoßen. Zunächst wurden nach umfangreichen Ermittlungen der 39-jährige Administrator der Plattform sowie zwei Missbrauchstäter in Deutschland identifiziert. Das von den Ermittlern sichergestellte Bildmaterial ließ darauf schließen, dass es noch einen weiteren Täter geben musste. Die deutschen Ermittler fanden heraus, dass die Aufnahmen in Österreich gemacht worden waren, woraufhin das deutsche BKA mit dem österreichischen BK in Kontakt trat. Es wurden Informationen sowie Videosequenzen zur Verfügung gestellt, auf denen zwei männliche Täter sowie die zwei Opfer, ein Bub und ein Mädchen, zu sehen waren. Nach genauer Analyse konnte ein tatort-spezifischer Bezug hergestellt werden. Die Beamten kontaktieren die in der Nähe des Tatortes befindlichen Schulen, in denen eine Lehrerin das siebenjährige Mädchen erkannte. Die Überprüfung der Daten ergab, dass das Mädchen mit ihrem fünfjährigen Bruder und ihrem 28-jährigen Vater in einer Wohnung in Wien Favoriten lebte. Der 28-jährige wurde als mutmaßlicher Täter identifiziert. Er soll sich nicht nur an seinen Kindern vergangen und sich dabei gefilmt haben, sondern auch weiteren Männern den Missbrauch ermöglicht haben. Durch das Geständnis des 28-Jährigen ergab sich kurze Zeit später die Festnahme eines 40-jährigen Wieners, der ebenso die beiden Kinder seit vielen Jahren missbraucht und Missbrauchsmaterial ins Netz gestellt haben soll.

Meldestelle Kinderpornographie und Sextourismus mit Kindern
Telefax: +43-(0)1-24836-951310
E-Mail: meldestelle@interpol.at

RECHTLICHE ASPEKTE

Das gesamte Ausmaß des Begriffs Cybercrime lässt sich nur schwer fassen. In der Alltagssprache werden dazu alle Straftaten gezählt, die unter Verwendung von Informations- und Kommunikationstechnik (IKT) oder gegen diese verübt werden. Die Polizei unterscheidet dabei zwischen Cybercrime im engeren und Cybercrime im weiteren Sinne.

Als Cybercrime im engeren Sinne werden alle Straftaten bezeichnet, bei denen es sich um direkte Angriffe auf Daten oder Computersysteme handelt. Darunter fallen beispielsweise Datenbeschädigung, Hacking oder Distributed-Denial-of-Service (DDoS) Attacken, die eine Dienstblockade darstellt.

Cybercrime im weiteren Sinne erfasst jene Delikte, bei denen die Informations- und Kommunikationstechnik in der Planungsphase, Vorbereitung und zur Ausführung herkömmlicher Straftaten begangen werden, wie etwa Betrugsdelikte, Kindesmissbrauchsmaterial, Cyber-Grooming, Cyber-Mobbing oder Cyber-Bullying. Dabei kann es sich um jede Form von Kriminalität handeln.

Durch das hochdynamische Feld der Informationstechnologie sowie durch die zunehmende Digitalisierung und beschleunigte Durchdringung sämtlicher Lebensbereiche wird der Gesetzgeber dauerhaft vor neue Herausforderungen gestellt. Zum Schutz von Jugendlichen wurde mit einer Anpassung des § 207a/5 Strafgesetzbuch (StGB) auf deren geändertes Onlineverhalten reagiert. Dabei wird das sexuelle Selbstbestimmungsrecht von jungen Menschen gewahrt und es findet eine zielgerechte Ahndung der missbräuchlichen Verbreitung von Sexting im Bereich Cyber-Mobbing statt. Bereits im Jahr 2016 wurde durch den § 107c StGB der neue Tatbestand des Cyber-Mobbings eingeführt.

ZAHLEN – DATEN – FAKTEN

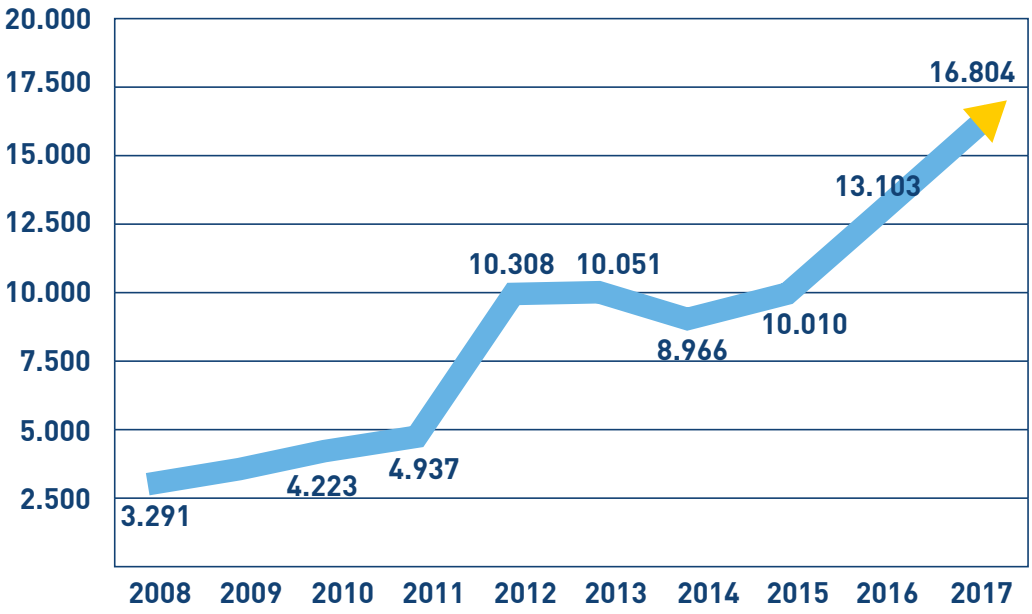

Abbildung 3: Entwicklung von Cybercrime in den Jahren 2008 bis 2017 (Quelle: BK/Polizeiliche Kriminalstatistik)

Seit 2014 sind kontinuierliche Anstiege im Bereich Cybercrime zu verzeichnen: 2017 wurden 16.804 Anzeigen der Polizei gemeldet. Mit einer Zunahme von 28,2 Prozentpunkten gegenüber dem Vorjahr wird der Trend der letzten Jahre fortgesetzt.

Angezeigte Fälle	Jän-Dez 2016	Jän-Dez 2017	Veränderung
§ 107c StGB		359	
§ 118a StGB	457	363	-20,6 %
§ 119 StGB		16	
§ 119a StGB	42	41	-2,4 %
§ 126a StGB - Vergehen	656	1 184	80,5 %
§ 126a/V StGB - Verbrechen	3	2	-33,3 %
§ 126b StGB - Vergehen	249	98	-60,6 %
§ 126b/V StGB - Verbrechen	33	7	-78,8 %
§ 126c StGB	234	189	-19,2 %
§ 148a StGB - Vergehen	816	1 055	29,3 %
§ 148a/V StGB - Verbrechen	1	1	0,0 %
§ 225a StGB	139	231	66,2 %
Cybercrime im engeren Sinn	**2 630**	**3 546**	**34,8 %**
§ 207a StGB - Vergehen	646	689	6,7 %
§ 207a/V StGB - Verbrechen	35	44	25,7 %
§ 208a StGB	80	106	32,5 %
Internetbetrug	9 672	11 761	21,6 %
Sonstige Straftaten im Internet	40	658	1545,0 %
Cybercrime im weiteren Sinn	**10 473**	**13 258**	**26,6 %**
Cybercrime Gesamt	**13 103**	**16 804**	**28,2 %**

Abbildung 4: Angezeigte Fälle Cybercrime im engeren und im weiteren Sinn (Quelle: BK/Polizeiliche Kriminalstatistik)

Die Zahl der Tatbestände von Cybercrime im engeren Sinne ist österreichweit von 2.630 im Jahr 2016 auf 3.546 im Jahr 2017 angestiegen. Das entspricht einem Anstieg um 34,8 Prozentpunkte gegenüber dem Vorjahr. Einen überdurchschnittlichen Anstieg der Anzeigen verzeichneten 2017 der § 126a StGB Datenbeschädigung mit 1.184 angezeigten Fällen (80,5 Prozent), der § 225a StGB Datenfälschung mit 231 angezeigten Fällen (66,2 Prozent) und der § 148a StGB Betrügerischer Datenverarbeitungsmissbrauch mit 1.055 angezeigten Fällen (29,3 Prozent).

Bei Cybercrime im weiteren Sinne konnte in allen Bereichen der angezeigten Fälle ein Anstieg festgestellt werden. Dieser betrug im Jahr 2017 26,5 Prozentpunkte. Im Vergleich zum Vorjahr stiegen die angezeigten Fälle im Bereich des § 208a StGB Anbahnung von Sexualkontakten zu Unmündigen um 32,5 Prozentpunkte an.

Aufklärungsquoten	Jän-Dez 2016	Jän-Dez 2017	Veränderung
§ 107c StGB		76,3 %	76,3 % Pt
§ 118a StGB	21,4 %	29,2 %	7,8 % Pt
§ 119 StGB		87,5 %	87,5 % Pt
§ 119a StGB	16,7 %	22,0 %	5,3 % Pt
§ 126a StGB - Vergehen	8,5 %	6,5 %	-2,0 % Pt
§ 126a/V StGB - Verbrechen	0,0 %	0,0 %	0,0 % Pt
§ 126b StGB - Vergehen	1,2 %	5,1 %	3,9 % Pt
§ 126b/V StGB - Verbrechen	0,0 %	14,3 %	14,3 % Pt
§ 126c StGB	17,9 %	15,9 %	-2,0 % Pt
§ 148a StGB - Vergehen	17,6 %	26,0 %	8,4 % Pt
§ 148a/V StGB - Verbrechen	0,0 %	0,0 %	0,0 % Pt
§ 225a StGB	88,5 %	91,3 %	2,8 % Pt
Cybercrime im engeren Sinn	**18,0 %**	**28,2 %**	**10,2 % Pt**
§ 207a StGB - Vergehen	89,2 %	88,7 %	-0,5 % Pt
§ 207a/V StGB - Verbrechen	74,3 %	88,6 %	14,3 % Pt
§ 208a StGB	72,5 %	69,8 %	-2,7 % Pt
Internetbetrug	40,4 %	39,0 %	-1,4 % Pt
Sonstige Straftaten im Internet	75,0 %	23,3 %	-51,7 % Pt
Cybercrime im weiteren Sinn	**43,9 %**	**41,3 %**	**-2,6 % Pt**
Cybercrime Gesamt	**38,7 %**	**38,5 %**	**-0,2 % Pt**

Abbildung 5: Veränderung der Aufklärungsquote in Bezug auf Cybercrime im engeren und im weiteren Sinn (Quelle: BK/Polizeiliche Kriminalstatistik)

2017 konnte die Aufklärungsquote im Bereich Cybercrime im engeren Sinn um 10,2 Prozent gesteigert werden. Der Erfolg lässt darauf schließen, dass die getroffenen Maßnahmen zum Umbau des C^4 zu einer modernen High-Tech-Crime Unit des BK ihre Wirkung zeigen.

CYBERCRIME SCHWERPUNKTE 2017

RANSOMWARE

Durch die Schadsoftware Petya/NotPetya und WannaCry wurden 2017 weltweit mehrere hunderttausend Computer infiziert. Diese Schadsoftware „Ransomware" verschlüsselt die Daten der infizierten Computersysteme. Nach der Verschlüsselung der Daten fordern die Täter von den Opfern eine vorab bestimmte Summe zur Entschlüsselung der Daten (meist ca. 300 Euro) in der Kryptowährung Bitcoin. Trotz Bezahlung des Lösegeldes werden in der Regel die Daten der Opfer aber nicht entschlüsselt.

Insbesondere auf Grund der epidemischen Ausbreitung und der daraus resultierenden Folgeschäden nannten Fachexperten Petya/NotPetya und WannaCry als die weltweit bedrohlichsten Cyber-Attacken in der Geschichte der Cyberkriminalität. Im C⁴ des österreichischen BK verzeichnete die zur Bekämpfung von Ransomware eingerichtete Soko CLAVIS in den Monaten Februar und März 2017 eine sprunghafte Steigerung der Anzeigen.

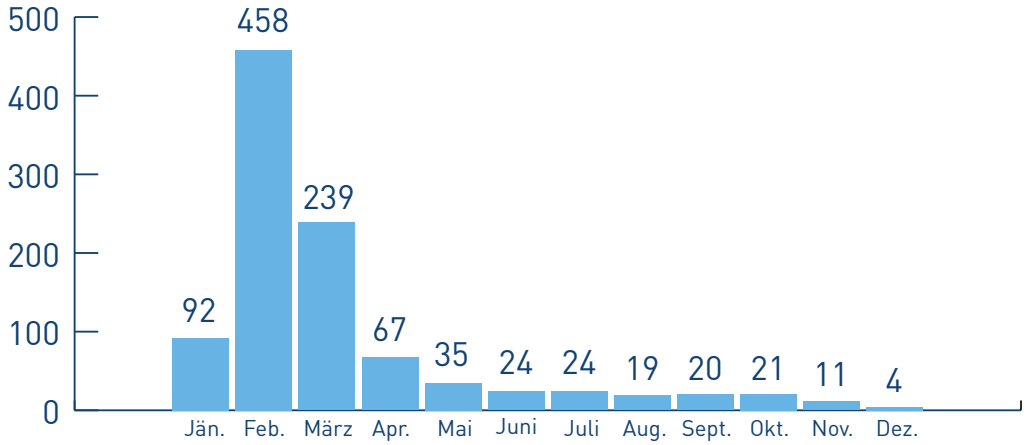

Abbildung 6: Angezeigte Fälle von Ransomware in Österreich 2017 (Quelle: BK)

Im weiteren Jahresverlauf sanken die angezeigten Fälle von Ransomware und es änderten sich auch die Angriffsvektoren.

REMOTE DESKTOP PROTOKOLL ALS ANGRIFFSVEKTOR

Seit Ende 2017 haben sich die Angriffsvektoren in Bezug auf Ransomware geändert. Waren bis dahin Phishing-Mails mit Links zur Schadsoftware oder Dateianhänge hauptsächlich als Initiatoren für die Verschlüsselung der Daten verantwortlich, erfolgen die Angriffe nun oft über die RDP Schnittstelle (Remote Desktop Protokoll). Solche mangelhaften oder mit einfachen Passwörtern abgesicherten Schnittstellen, sind das Angriffsziel der Täter. RDP Schnittstellen werden zum Fernsteuern bzw. zur Fernwartung eines entfernten Computers und Darstellen dessen Bildschirminhaltes benötigt. Dabei werden die Zugangsdaten mit sogenannten „Brute Force Attacken" geknackt um in die Systeme der Opfer einzudringen und die Daten zu verschlüsseln. Geldforderungen erfolgen nun nicht mehr pauschal sondern individuell abgestimmt nach vorheriger Abschätzung der finanziellen Möglichkeiten der Opfer durch die Täter.

KRYPTOWÄHRUNGEN UND MINING

Mit dem medialen Aufsehen der großen Ransomware-Wellen 2017 Petya/NotPetya und WannaCry fanden Kryptowährungen vermehrt Einzug in die Berichterstattung. Während Kryptowährungen bis 2017 nur in gewissen Teilbereichen ihre Verwendung fanden und deshalb auch nur einer geringen Anzahl von Menschen bekannt waren, stieg der Bedarf an Kryptowährungen und deren Verbreitung im Verlauf des Jahres 2017 massiv an. Insbesondere der Wertzuwachs von Bitcoin machte den Einsatz von Kryptowährungen für kriminelle Handlungen immer beliebter. Kryptowährungen wurden nicht nur immer häufiger für die Begehung klassischer Delikte zum Beispiel Betrugshandlungen mit Bitcoin-Bons und Phishing-Versuche zur illegalen Aneignung von Zugangsdaten verwendet. 2017 wurden im Zusammenhang mit Kryptowährungen auch völlig neue kriminelle Phänomene wahrgenommen wie beispielsweise die Verwendung fremder Rechenleistung zum „Minen".

Das neue Phänomen Cryptojacking begann sich Ende 2017 abzuzeichnen, wobei sich Cryptojacking dabei aus „Crypto" für Mining-Programme und „Hijacking" für das Kapern fremder Rechenleistung zusammensetzt. Heimliches Crypto-Mining erfolgt auf fremde Kosten und liegt aufgrund der steigenden Verbreitung der Crimeware im Trend von Cyberkriminellen. Geld verdient beim illegalen Crypto-Mining nur der Kriminelle. Unabhängig von der Art des betriebenen Minings läuft dieses auf Standardhardware ohne spezielle Optimierungen und Wissen äußerst ineffizient. Betrachtet man das unrentable Kosten- Nutzen-Verhältnis, so muss ein Standardrechner ganze sechs Stunden Mining betreiben, um nur einen einzigen Cent zu erwirtschaften. Dabei fällt etwa das Zwanzigfache an Stromkosten an. Zusätzlich sind die Konsequenzen für das Ökosystem beträchtlich, da für das Schaffen virtueller Werte große Mengen an realem Strom verbraucht werden. Deshalb zeichnet sich bereits ab, dass Kriminelle zunehmend Geräte aus dem Internet der Dinge etwa Router, Drucker, Webcams und andere Geräte mit Internetanschluss unter ihre Kontrolle bringen. Die kriminelle Handlung ist nur dann rentabel, wenn das Mining ohne nennenswerte eigene Ausgaben erfolgen kann und die Kosten auf viele andere Geschädigte verteilt werden können.

Das legal betriebene Crypto-Mining kann deshalb unter Einbezug von Investitions- und Betriebskosten als unwirtschaftlich betrachtet werden. Dies sollte in diesem Zusammenhang auch bei neuen Formen des Wirtschaftsbetrugs berücksichtigt werden. Nicht nur Kleinkriminelle betreiben illegales Crypto-Mining, auch die organisierte Kriminalität hat dieses lukrative Geschäftsmodell mit beträchtlichen Schadenshöhen bereits entdeckt.

ZIELGERICHTETE MASSNAHMEN

SPEZIALISIERUNGEN UND PERSONELLE MASSNAHMEN

Der immer häufigeren Verwendung von Kryptowährungen bei kriminellen Handlungen wurde durch eine Spezialisierung von Mitarbeitern des C^4 begegnet. Die Eigenentwicklung besonderer Tools unterstützt bei den notwendigen kriminalpolizeilichen Nachforschungen. Durch behördeneigene Wallets konnten nach Auftrag der Justiz auch Vermögenswerte dieser Währungsform sichergestellt werden.

AUS- UND FORTBILDUNG

Wie bei jeder anderen Kriminalitätsform ist auch bei Cybercrime nicht nur Erfahrung, sondern auch eine geeignete Ausbildung eine wichtige Grundlage der täglichen Arbeit. Daher wurde für diesen Bereich ein durchgängiges Schulungskonzept erarbeitet.

Dieses Gesamtkonzept basiert auf drei Säulen und drei Ebenen.

Abbildung 7: Ausbildungskonzept C^4 (Quelle: BK)

Die erste Säule definiert drei Ebenen von speziell für die Bekämpfung von Cybercrime geschulten Polizisten. Speziell bei diesen Delikten setzen bereits die Entgegennahme der Anzeige und die ersten Ermittlungsschritte technisches Grundverständnis voraus. Daher ist es erforderlich, dass zu jedem Zeitpunkt entsprechendes Wissen in den Bezirken vorhanden ist. Dies soll damit erreicht werden, dass in jedem Bezirk im Schnitt drei Bezirks-IT-Ermittler ausgebildet werden. Diese können bei Bedarf auf die zweite Ebene, Cybercrime-Experten sowohl auf Landesebene als auch im BK, zugreifen. Da ein allgemeines Wissen, sei es noch so fundiert, für manche Herausforderungen nicht ausreicht, gibt es in den beiden letztgenannten Bereichen die Möglichkeit, sich auf

benötigte Themenbereiche zu spezialisieren. Auf dem Weg zur Umsetzung dieses Konzeptes wurde 2017 ein wichtiger Schritt gesetzt. Die Inhalte und Rahmenbedingungen für die Bezirks-IT-Ermittler Ausbildung wurden aktualisiert und erweitert, sodass im Jahr 2018 mit den neuen Schulungen begonnen werden konnte.

Zumindest ebenso wichtig wie die Ausbildung eines Pools von Fachleuten ist es, jedem Polizisten grundlegendes Wissen zu diesem Themenbereich zu vermitteln. Dies kann nur über die polizeiliche Grundausbildung, die Ausbildung zum dienstführenden Beamten, Kriminalbeamten und leitenden Beamten erfolgen. Auch hier stößt das Thema Cybercrime auf hohe Akzeptanz. So wird die Aufnahme entsprechender Lehrinhalte bei jeder Adaptierung des Lehrplanes berücksichtigt.

Aber auch die bereits im aktiven Dienst stehenden Polizisten sind auf dieses Wissen angewiesen. Hier ist der im Konzept gewählte Ansatz die Aufnahme einschlägiger Themen in die laufende Fortbildung. Im Jahr 2017 wurde in einem ersten Schritt die Fortbildung der Kriminalbeamten um einen „Cybercrime-Tag" verlängert. An diesem werden, angepasst an die jeweiligen Teilnehmer, Grundlagen und Besonderheiten dieser Kriminalitätsform sowie aktuelle Entwicklungen vermittelt.

Durch die schrittweise Umsetzung des Konzeptes und seine laufende Anpassung werden den Ermittlern die notwendigen Werkzeuge zur erfolgreichen Bekämpfung von Cybercrime in die Hände gegeben.

EINRICHTUNG EINES WISSENSCHAFTLICHEN BEREICHS

Mit 1. November 2017 wurde im C^4 das Referat für Entwicklung und Innovation eingerichtet, um neueste Entwicklungen aus Wissenschaft und Forschung für die polizeiliche Anwendung zu erschließen, zukünftig den Missbrauch von Technologien vorausschauend zu erkennen, Risiken zu bewerten und auf deren Einsatz durch Kriminelle u verhindern.

Das Referat erfüllt dabei Aufgaben auf speziellen cyberrelevanten Gebieten wie zum Beispiel:

- Forschung und Bewertung von Phänomenen im Bereich der IT-Kommunikation insbesondere im Internet einschließlich der automatischen maschinengestützten Kommunikation (Internet of Things).
- Wissenschaftliche Entwicklung von Konzepten und Werkzeugen zur Kriminalitätsbekämpfung, Abwehr und Aufklärung mittels High-Tech Ansätze sowie Künstlicher Intelligenz und Methoden der Datenanalyse.
- Bewertung neuer Entwicklungen und Technologien sowie Aufbau und Betrieb einer IT-spezifischen wissenschaftlichen Wissensdatenbank.
- Wissenschaftliche Entwicklung, Aufbau und Betrieb eines Echtzeit-Lagebildes zu kriminellen Aktivitäten und Bedrohungen im Cyberraum.
- Vernetzung mit jeglichen Forschungseinrichtungen sowie Ziel- und Bedarfsdefinitionen für die Sicherheitsforschung im Cyberbereich.
- Sachverständigentätigkeit im Bereich der Informations- und Kommunikationstechnik.

BEWEISSICHERUNG UND ANALYSE

IT und Speichermedien stellten auch 2017 einen unverzichtbaren Bestandteil im Bereich strafrechtlicher Ermittlungen dar. So konnte auch dieses Jahr wieder ein deutlicher Anstieg an forensischen Auswertungen verzeichnet werden. Die elektronische Beweismittelsicherung im C⁴ sowie in den LKA gewinnt damit weiterhin an Bedeutung.

Aufgrund der technischen Entwicklung wird die Auswertung dieser Medien aber immer schwieriger. Herstellerspezifische verschlossene Systeme mit ausgeprägten Verschlüsselungsverfahren stellen die elektronische Beweissicherung fortwährend vor große Herausforderungen. Insbesondere im Bereich der mobilen Forensik werden Datensicherungen und Auswertungen immer schwieriger. Mit der Fertigstellung einer eigenentwickelten technischen Lösung zum Öffnen versperrter Geräte konnte 2017 ein kleiner, aber wichtiger Vorstoß in diesem Bereich erzielt werden. Auch die Kooperation mit privaten Institutionen unterstützt dabei maßgeblich Ermittlungserfolge zu erreichen.

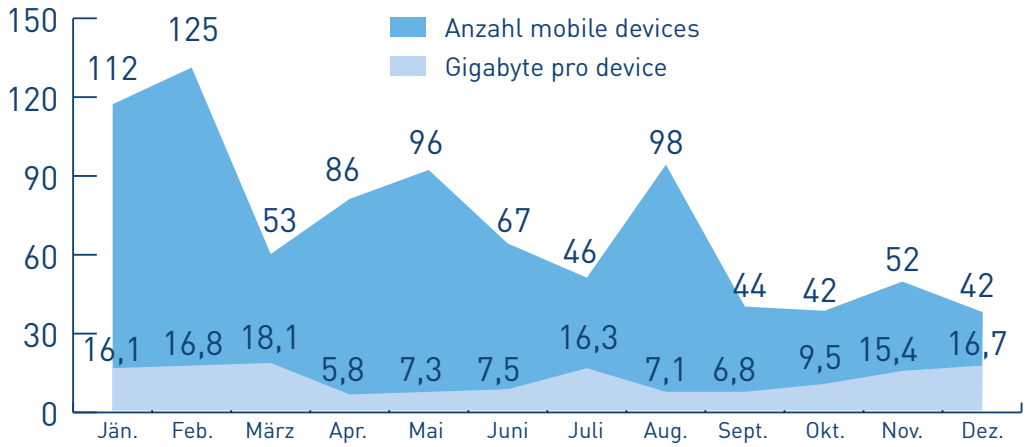

Abbildung 8: Auswertungen mobiler Endgeräte 2017 (Quelle: BK)

Daten werden vermehrt auf verschlüsselten Medien oder direkt im Internet in der sogenannten Cloud gespeichert. Im Bereich der herkömmlichen Datenverarbeitung zeigen diese beiden Trends der Auslagerung einen starken Zuwachs, wodurch sich zum einen, neue Abhängigkeiten und neue Gefahren, aber auch die Chancen der professionelleren und sicheren Betreuung von IT-Systemen ergeben können.

Unter Kriminellen erfreute sich das Darknet im Jahr 2017 weiter steigender Beliebtheit. Dies erforderte bei der forensischen Sicherung von Daten ein völliges Umdenken und lässt der sogenannten „Live-Forensik" eine immer höher werdende Bedeutung zukommen. Erschwernisse ergeben sich aber nicht nur aus technischer sondern meist auch aus rechtlicher Sicht. Rechtliche Grundlagen insbesondere bei grenzüberschreitenden Amtshandlungen stellen die Datensicherer vor immer größeren Herausforderungen.

Die Thematik Big Data hat auch 2017 weiter an Bedeutung zugenommen. Zahlreiche Amtshandlungen im Bereich von Wirtschaft und Korruption aber auch im Bereich der Gewaltdelikte ließen im letzten Jahr beschlagnahmte Daten im dreistelligen Terrabyte-Bereich aufkommen. Derartige Datenmengen für das Gericht verwertbar zu machen, stellt nicht nur die Datensicherung, sondern auch deren Auswertung vor große Herausforderungen. Die obligatorische Einhaltung forensischer Standards erfordert auch akribische Genauigkeit bei der Durchsicht von gewaltigen Datenmengen. Dazu wurde in Zusammenarbeit mit den zuständigen Fachabteilungen im BK sowie in den Landeskriminalämtern an der Weiterentwicklung und der Einführung von Such- und Analysetools gearbeitet. Diese sollen künftig eine Erleichterung und vor allem eine wesentlich effizientere Abarbeitung von Massendaten ermöglichen.

Wie schon die Jahre zuvor wurden auch 2017 die Leistungen der Fahrzeugforensik in steigendem Ausmaß in Anspruch genommen. Ähnlich wie in der mobilen Forensik entstehen durch verschlossene Geräte sowie durch die Vernetzung von Fahrzeugen untereinander und neu zu schaffender Infrastrukturen auch viele zusätzliche Problemfelder. So konnte im letzten Jahr festgestellt werden, dass vermehrt Motorräder mittels elektronischer Werkzeuge manipuliert und gestohlen wurden. Die Fahrzeugforensik des C⁴ wurde als wichtige Säule durch

konkrete Unterstützung der Ermittlungsarbeiten, forensische Schwerpunktkontrollen und Intensivierung der Zusammenarbeit mit ausländischen Dienststellen etabliert. Des Weiteren wurde eine Fülle von präventiven Maßnahmen getroffen, die auch aktive Medienarbeit oder die Teilnahme bei Veranstaltungen von Händlern, Motorradclubs und Fachmessen umfassten.

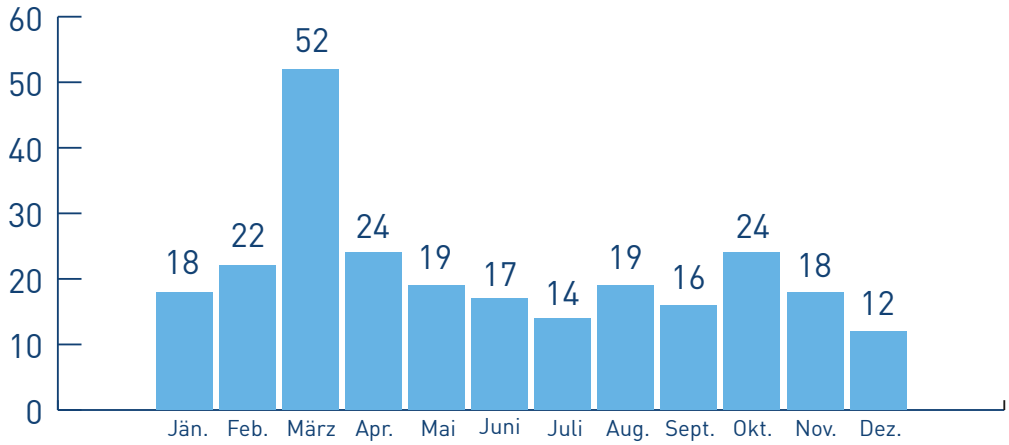

Abbildung 9: Anzahl der ausgewerteten Fahrzeuge (Quelle: BK)

Der Fortschritt im Bereich der Automobilindustrie, insbesondere im Rahmen des autonomen Fahrens sowie autonomer Verkehrsleitsysteme ergibt neue Sicherheitslücken, die in weiterer Folge Gegenstand von Ermittlungen werden und damit zunehmend forensische Datensicherungen erforderlich machen. Die steigende Verbreitung und Einsatz von Drohnen sowohl im privaten als auch kommerziellen Bereich geht mit neuen Kriminalitätsformen und neuen Bedrohungen einher. Durch die steigende missbräuchliche Verwendung von Drohnen als Tatmittel sind neue Ermittlungsmethoden und Best Practices zur forensisch korrekten digitalen Beweismittelsicherung erforderlich. Dies unterstreicht die Wichtigkeit und Notwendigkeit des gemeinsamen Wirkens und des Informationsaustausches der Dienststellen inner- und außerhalb des BMI.

Um den neuen Herausforderungen zu begegnen wurden die Prozesse und das benötigte Know how analysiert damit gezielte Änderungen in der Aufbauorganisation vorgenommen werden konnten. Die Mitarbeiter des C^4 und der LKA nahmen kontinuierlich an spezifischen Fachschulungen und Arbeitsgruppen teil. Ebenso wurden seitens des C^4 mehrere Fachtagungen und Schulungsveranstaltungen durchgeführt. So werden gefährliche Wissenskonzentrationen vermieden und die Wissensvermittlung durch Fachexperten auf das gesamte Bundesgebiet ermöglicht.

PROJEKTE

„IO-THREATS“

Das nationale Projekt „IO-Threats“ setzt sich mit Internet of Things (IoT) und damit einhergehenden Bedrohungen auseinander. Ziel ist es auf diesem hochaktuellen und noch kaum erfassten Themen- und Problemfeld forensisch und polizeilich tätig zu werden. Dabei werden potenzielle Angriffsszenarien auf den österreichischen Smart-Home-Markt beleuchtet. Gleichzeitig findet eine Bewertung der Rechtslage statt, die darauf ausgerichtet ist, konkrete polizeiliche Maßnahmen nach Projektabschluss zu etablieren.

Das Projekt läuft von September 2017 bis März 2019. Projektteilnehmer sind neben dem C^4 das Joanneum Research, eine außeruniversitäre Forschungseinrichtung der Uni Graz, Austrian Center for Law Enforcement Sciences (ALES), ein Unternehmen sowie das Polizei- und Justizforschungszentrum der Universität Wien.

UPLOAD-PLATTFORM

Insbesondere terroristische Anschläge wie jener auf den Weihnachtsmarkt in Berlin, aber auch die Amokfahrt in Graz stellen die Sicherheitsbehörden bei den Ermittlungen vor neue Herausforderungen. Dabei spielt vor allem die Identifizierung der Täter sowie das Auffinden und die Sicherung von Beweisen eine große Rolle. An vielen öffentlichen Plätzen sind heute Videosysteme installiert, die im Ernstfall für kriminalpolizeiliche Auswertungen herangezogen werden können. In der Regel arbeiten diese Systeme aber nicht flächendeckend, sodass unter Umständen genau die relevanten Plätze nicht umfasst oder nicht eindeutig einsehbar sind. Oft ist auch die Qualität dieser Aufnahmen so mangelhaft, dass sich relevante Informationen darauf nicht erkennen lassen.
Derartige Situationen erfordern es, schnell eine Übersicht über die Geschehnisse zu bekommen um mögliche weitere Gefahren zu verhindern. Aus diesem Grund müssen alle Informationen herangezogen werden, die Aufschluss über den Ablauf der Geschehnisse liefern. Die Entwicklung der mobilen Technik bei Smartphones bietet heute die Möglichkeit, Bild-, Video- und Tonaufzeichnungen zu erstellen und diese auch gleich in sozialen Medien an Freunde und Bekannte weiterzuleiten. Diese Möglichkeit hat unsere Kommunikationskultur entsprechend geprägt. Ereignisse werden heute, leider oft auch zum Nachteil der Beteiligten, bildlich festgehalten und danach meist im Internet verbreitet.

Da genau dieses Bildmaterial relevante Informationen für Ermittlungen beinhalten kann, soll nach dem Vorbild der bayrischen Polizei der Bevölkerung die Möglichkeit geboten werden, der Behörde derartiges Bildmaterial zur Verfügung zu stellen. Dazu steht künftig ein Web-Portal zur Verfügung, das genau diese Möglichkeit bieten kann. Dieses Webportal wird bei Großschadenslagen aktiviert und der Link zu dieser Upload-Plattform in diversen Medien publiziert. Jeder Zeuge erhält dadurch die Möglichkeit relevantes Bildmaterial den Ermittlungsbehörden zu übermitteln.

Eine eigens installierte Sichtungsgruppe nimmt die Daten dann in Augenschein, bewertet und klassifiziert diese. In weiterer Folge werden die relevanten Daten für Sofortmaßnahmen und für das Ermittlungsverfahren verwendet. Die erwartete Informationsmenge kann bei derartigen Fällen durch technische und organisatorische Vorbereitungen besser erhoben und nachvollzogen werden. Mit Hilfe der Bevölkerung können künftig nicht nur die Ermittlungen beschleunigt, sondern auch die Beweislage gegen Verdächtige entsprechend gefestigt werden.

PRÄVENTION DURCH INFORMATION

Noch besser als das Ausforschen von Tätern ist es Taten im Vorfeld zu verhindern. Gerade Straftaten, die mit dem Internet und genutzten Computersystemen zusammenhängen, können durch geeignete Präventivmaßnahmen verhindert werden.

Um auf die möglichen Gefahren des Internets aufmerksam zu machen, besteht die Aufgabe der Kriminalprävention darin, Informationen in Form von Beratungen an die Bevölkerung weiterzugeben. Ein besonderer Schwerpunkt wird auf Jugendliche und deren sensiblen Umgang mit neuen Medien gelegt. Auch Erwachsene, die bisher weder in der Schule noch im Beruf Ausbildung auf diesem Sektor erhalten haben, werden in Schulungen von den Präventionsbediensteten über mögliche Gefahren des Internets informiert.

Das Wissen über den Schutz von IT-Systemen, über aktuelle Bedrohungen bis zur richtigen Anwendung und Funktionsumfang diverser Endgeräte soll flächendeckend vermittelt werden, indem Polizeibedienstete zu diesen Themen ausgebildet werden. Diese Inhalte werden in Zukunft sowohl digital, als auch in Vorträgen und Beratungen zur Verfügung stehen.

Vor allem durch grundlegende Informationen zur PC Sicherheit, Passwortschutz und gefahrloses Internetsurfen können Schäden verhindert werden. Daher betreibt die Kriminalprävention im BK und in den Landespolizeidirektionen zielgruppenorientierte Öffentlichkeitsarbeit. Dies erfolgt durch Aufklärung

- in **sozialen Medien,**
- auf der **Homepage des BK**
- und durch die **Polizei App**
- die für Apple, Android und Windows Systeme gratis zum Download zur Verfügung steht.
- Die Broschüre „Sicher in den besten Jahren“ beinhaltet das Kapitel „Sicher im Internet“. Für die Zielgruppe der älteren Menschen finden sich dort Informationen zum richtigen Umgang mit dem Internet.

Zur **Broschüre**.

JUGENDPRÄVENTIONSPROJEKTE DER KRIMINALPRÄVENTION

Mit Beginn des Schuljahres 2017/2018 wurde das Gesamtkonzept der Kriminalprävention mit der Zielgruppe Jugendliche unter 18 Jahren und dem Namen „UNDER18“ ausgerollt. Das Programm setzt sich mit den Themenbereichen der Gewalt- und Suchtprävention auseinander und wird österreichweit von insgesamt 300 Präventionsbediensteten betreut.

Weiterführende Informationen zu **„UNDER18“**.

Für die Gewaltprävention im Kontext digitaler Medien wurde das bestehende Präventionsprogramm „Click & Check“ komplett überarbeitet und auf die Altersklasse von 10 bis 17-Jährige angepasst. Im Vorfeld der jeweiligen Präventionsprogramme stehen die Themenfelder der präventiven Rechtsinformation und die Jugendschutzbestimmungen. Darauf aufbauend werden mit dem Programm „Click & Check“ unter anderem die Themen Chats und Soziale Netzwerke, Cybermobbing, Grooming und Sexting gemeinsam mit den Jugendlichen erarbeitet. Um eine möglichst hohe Nachhaltigkeit zu gewährleisten, werden auch Eltern sowie Lehrpersonal in das Projekt miteinbezogen.
Ziel des Programmes „Click & Check“ ist die Förderung eines verantwortungsvollen Umganges mit digitalen Medien und die Erweiterung bzw. Verinnerlichung von Handlungsstrategien in sozialen Netzwerken. Im Jahr 2017 wurden österreichweit 57.386 Schüler und deren Eltern sowie Lehrpersonal im Rahmen von Präventionsveranstaltungen sensibilisiert und informiert.

GEMEINSAM.SICHER

Ziel der Initiative "GEMEINSAM.SICHER in Österreich" ist es, die Bevölkerung an der Gestaltung der öffentlichen Sicherheit in ihrer Gemeinde oder Stadt mitwirken zu lassen sowie den Dialog zwischen Bürgern, Stadtverwaltung und der Polizei zu intensivieren. Internationale Erfahrungen zeigen, dass so negative Entwicklungen verhindert und Probleme rascher geklärt werden, wodurch das Vertrauen in die Sicherheit steigt.

Einer der Schwerpunkte der Initiative waren 2017 die Themen Datensicherheit und Vorbeugung von Cybercrime. Dazu wurden mehrere Vereinbarungen zwischen Interessenvertretungen und verschiedenen Ministerien abgeschlossen.

„GEMEINSAM SICHER – fIT im Netz“ war eine Kooperation zwischen der IT-Security Experts Group, des Fachverbandes Unternehmensberatung und Informationstechnologie (UBIT), der WKO und dem BK.

„GEMEINSAM SICHER mit der Wirtschaft“ basiert auf der Zusammenarbeit zwischen der Dachorganisation der WKO und dem BMI. Einer der Gründe, warum diese Themen gerade in diesem Jahr verstärkt kommuniziert wurden, ist die Datenschutzgrundverordnung der EU, die mit Mai 2018 schlagend wurde. Darin werden unter anderem für weite Bereiche der Wirtschaft, Vereine und anderen Organisationen, Maßnahmen für Datensicherheit nach dem Stand der Technik vorgeschrieben. Neben der Einrichtung einer Zertifizierung zum „Certified Data & IT Security Expert“ wurden vor allem Veranstaltungen zur Bewusstseinsbildung durchgeführt. Als Zielgruppe wurden Multiplikatoren wie beispielsweise Unternehmensberater, Buchhalter und Gründungsberater ausgewählt, um möglichst viele Betroffene zu erreichen. Organisiert wurden die Vorträge und Schulungen in Form von “Roadshows“, die durch alle Bundesländer tourten. Darüber hinaus wurden in vielen Bundesländern Planspiele organisiert, in denen Firmen die Möglichkeit geboten wurde, sich auf mögliche Cybervorfälle vorzubereiten, um dadurch ihre persönliche Resilienz zu verbessern.

Aktuelle Informationen zu **„GEMEINSAM.SICHER“**.

CONCLUSIO UND AUSBLICK

RISIKOMINDERUNGSSTRATEGIEN UND MASSNAHMEN DES C4

Die Technologien, die bei der Internetkriminalität eingesetzt sind, werden sich weiterhin rasant ändern. Es gibt kaum eine Kriminalitätsform bei der Elektronik, IT und ihre Vernetzung keine Rolle mehr spielen. Sei es als Medium, wie das Darknet, als Beweismittel, wie zum Beispiel ein Smartphone, das als Tatmittel verwendet wurde, oder die Verwendung einer Schadsoftware, wie es bei „Ransomware" der Fall ist. Veranschaulicht wird das Tempo der Entwicklung durch das IoT, der Vernetzung der Glühbirne bis hin zum Kühlschrank. Abschreckende Beispiele einschlägig bekannter Sprachsteuerungen eines börsennotierten amerikanischen Online-versandhändlers zeigen klar auf, dass die Benutzerfreundlichkeit an erster Stelle und die Sicherheit an letzter steht. Diese wird üblicherweise erst dann nachgerüstet, wenn der Endbenutzer sie als gravierend mangelhaft empfindet.

Die Problematik des kontinuierlichen Anstiegs von Cybercrime Fällen wird durch die stark zunehmende Anzahl von vernetzten Geräten noch massiv verstärkt und bietet daher ein besonders attraktives Angriffsziel für Kriminelle. Um diese Entwicklung einzubremsen, ist ein Umdenken nicht nur bei den Anwendern, sondern auch bei den Herstellern erforderlich. Solange hier keine Änderungen eintreten, wird die Gefährdungslage bei IoT durch Cybercrime weiterhin steigen. IoT Geräte sollten deshalb nicht ungeschützt im Internet betrieben werden.

Auch der Einsatz von Künstlicher Intelligenz („Artificial Intelligence") erfasst immer mehr Bereiche des gesellschaftlichen und wirtschaftlichen Lebens. Das Missbrauchspotential von Künstlicher Intelligenz durch Cyber Kriminelle steigt, weshalb in der Zukunft auch mit automatisierten Angriffen durch Künstlicher Intelligenz Systeme gerechnet werden muss.

Blockchain-Technologien lassen unter anderem neue Kryptowährungen entstehen: Bitcoin, Ethereum und andere Krypotwährungen haben in den letzten Monaten die Schlagzeilen vieler Medien gefüllt. Doch neben den primär spekulativen Aspekten im Finanzbereich werden sie weiterhin einen maßgeblichen Anteil an kriminellen Geschäftsmodellen bilden. Solange keine strengen Kontrollen und Reglementierungen für Kryptowährungen umgesetzt werden, können sie von Kriminellen weiterhin sehr einfach für Betrug, Erpressung, Geldwäsche und zahlreiche andere Delikte eingesetzt werden. Die meisten Staaten sind sich dieser Problematik bewusst und beginnen bereits ihre ersten Initiativen gegen diese Entwicklung zu setzen.

Die Strafverfolgungsbehörden müssen immer mit dem raschen und stetigen Wandel der Technologien schritthalten, um den Anschluss nicht zu verlieren. Die aufgrund der EU-Richtlinie vorgegebenen Gesetzgebung und die koordinierte Umsetzung strategischer Vorgaben erfordern eine präzise Maßnahmenplanung mit Prozessanalysen und genauen Abgrenzungen in den sich überschneidenden Teilbereichen von Cybercrime und Cybersicherheit. Die geringe Infektionsrate bei einem Ransomware-Angriff im letzten Jahr zeigte klar auf, dass eine schnelle Reaktion der kooperierenden Behörden und Institutionen mit strukturellen Frühindikatoren, enorme Schadenshöhen für die heimische Wirtschaft verhindern kann und entsprechende finanzielle Investitionen auch im Sinne der Umweg Rentabilität betrachtet werden können.

Dazu sind aus der Mitarbeiterperspektive eine ausreichende Anzahl an hochspezialisierten Experten aus verschiedenen Fachgebieten, wie zum Beispiel IT- und Netzwerktechnik, Kryptowährungen, Datenforensik sowie ein hohes Maß an kriminalpolizeilichem Wissen erforderlich. Spezialisierungen mit Sonderausbildungen und Bündelungen von technischen Expertisen mit den Ressourcen im Bereich High-Tech-Crime führen zur Weiterentwicklung des notwendigen fachlichen Wissensaufbaus ohne gefährliche Wissenskonzentrationen zuzulassen. Darüber hinaus müssen aus einer Prozessperspektive die internationale polizeiliche Kooperation mit Interpol und Europol weiter ausgebaut und geeignete rechtliche Rahmenbedingungen möglichst rasch geschaffen werden.

Auch im kommenden Jahr wird in dieser dynamischen virtuellen Welt der Internettechnologien das C4 gefordert sein sich an die vereinbarten strategischen Ziele der internationalen Kriminalitätsbekämpfung auszurichten und mit interorganisationalen Kooperationsprozessen auf neuartig begangene Straftaten unverzüglich zu reagieren.

SUMMARY

Technologies used in the field of cybercrime will continue to change in rapid succession. There is hardly any crime that does not involve technology, either as a medium like the darknet, or as means of evidence like a smartphone when used as an instrument of crime or as a criminal tool like ransomware. Criminals take advantage of these technologies and use them for carrying out illegal activities. The distribution of voice assistants by large online resellers is driven by the aspect of usability, but demonstrates at the same time the lack of awareness for security and privacy issues regarding end-users. The increase in cybercrime cases is due to the rising degree of interconnectedness between devices through the Internet (IoT). Hence, it can be concluded that the enormous number of new gadgets are likely to become increasingly targets for criminal activities. The misuse of artificial intelligence (AI) for automated attacks can be seen as a potential threat to IT-systems. Articles about blockchain technologies and newly established crypto-currencies ruled the tech-focused magazines in 2017. A rise in crime-related business models can be expected in addition to the aspect of financial speculation. Other offence types besides fraud, extortion and money laundering are expected to prosper as a consequence of inadequate control mechanisms and a lack of regulations.

Law enforcement agencies need to keep abreast of the ongoing changes in a flexible way. EU strategic directives, which are transposed into national law, makes it necessary to analyze processes and to make coordinated and accurate action plans in the rapidly changing area of cybercrime. In 2017, Austria saw a comparatively low rate of ransomware attacks. The successful control of such attacks was achieved through the monitoring early indicators and the quick response of cooperating public authorities and their partner institutions. This approach saved the Austrian business community from enormous losses and goes to show that investments in security prove effective and pay off for governments on a long-term basis. On the personnel side an adequate number of experts from different specialized fields (e.g. network engineering, crypto-currencies, data forensics, etc.) are required. Providing the necessary training, specialization and pooling of resources is a major challenge to avoid excessive workload when it comes to analyzing criminal intelligence. The constant quest for improvement calls for a comprehensive approach, which includes operative work within international organizations like Europol and Interpol.

The C^4 is faced with a series of new offence types in th dynamic virtual world of he Internet and will be able to to make the necessary adaptations for achieving the strategic goals. Appropriate measures and operations will be implemented to join in the international fight against cybercrime.

GLOSSAR

Bitcoin – Bitcoin Wallet
Bitcoin (englisch für „digitale Münze") ist ein weltweit verwendbares dezentrales Zahlungssystem und der Name einer digitalen Geldeinheit. Überweisungen werden von einem Zusammenschluss von Rechnern über das Internet mithilfe einer speziellen Peer-to-Peer-Anwendung abgewickelt, sodass anders als im herkömmlichen Bankverkehr keine zentrale Abwicklungsstelle benötigt wird. Eigentumsnachweise an Bitcoin können in einer persönlichen digitalen Brieftasche, einem sogenannten Bitcoin Wallet, gespeichert werden. Das Wallet (englisch für „Geldbeutel") steht sinnbildlich für eine Art virtuellen Geldbeutel, der die Bitcoins eines Teilnehmers enthält. Da Bitcoins jedoch nur innerhalb der Block Chain (verteiltes Datenbankmanagementsystem) existieren und transferiert werden können, ist das Wallet eher vergleichbar mit einer Kreditkarte, die bestimmte Daten enthält, mit denen der Kunde Zahlungen tätigen kann, selbst aber kein Geld enthält.

CEO-Betrug
Dabei handelt es sich um eine Betrugsform, bei der unbekannte Täter einen oder mehrere Mitarbeiter eines Unternehmens über E-Mail und/oder Telefon kontaktieren und sich als Vertreter der Geschäftsführung ausgeben. Die so kontaktierten Mitarbeiter werden über streng vertrauliche Vorgänge informiert, welche zumeist eine Firmenübernahme einleiten sollen. Für diese Abwicklung würden Anzahlungen benötigt, die dieser Mitarbeiter in die Wege leiten soll. Die Gelder werden zumeist auf Konten bei Banken aus dem asiatischen Raum überwiesen. Durch ständige Hinweise auf die Dringlichkeit und Vertraulichkeit des Vorgangs sollen die Mitarbeiter unter Druck gesetzt und Nachfragen vermieden werden. Meist haben die Täter durch vorhergehende, aufwändige Recherchen umfangreiches Wissen über Aufbau, Personal und Zuständigkeiten in der betroffenen Firma.

Cyber-Grooming
Bezeichnet das Ansprechen von Personen im Internet mit dem Ziel der Anbahnung sexueller Kontakte und kann als Form der sexuellen Belästigung im Internet angesehen werden. Es führt nach dem Aufbau von Vertrauen meistens zu sexuellem Missbrauch oder der Anfertigung kinderpornografischen Materials.

DNS
Das Domain Name System (DNS) ist einer der wichtigsten Dienste im Internet. Seine Hauptaufgabe ist die Auflösung des Computernamen oder der URL einer Webseite in eine IP-Adresse.

DoS/ DDoS-Attacke
Engl. „Denial of Service" (= außer Betrieb setzen). Angriff auf die Verfügbarkeit der Ressourcen und Dienste eines IT-Systems mit dem Ziel, diese zu blockieren und somit regulären Benutzern keinen Zugriff mehr zu ermöglichen. Wird der zur Blockade führende Angriff nicht nur von einem einzelnen Rechner ausgeführt, sondern von vielen gleichzeitig, spricht man von einem „Distributed Denial of Service" oder DDoS-Angriff. Dadurch wird sowohl der Angriff verstärkt als auch die Einleitung der Gegenmaßnahmen erschwert, da diese auf mehrere Quellen angewendet werden müssen.

Hacking
Bezeichnet das, nicht unbedingt illegale Eindringen in Computersysteme, durch vorhergehende Analyse und Suche nach Schwachstellen. Ursprünglich bezieht sich der Begriff auf Computer- und Hardware Enthusiasten, mit einer stark ausgeprägten Hingabe zur Technik. In der Öffentlichkeit ist der Begriff negativ konnotiert und steht für die illegale Aktivität unbefugt Sicherheitslücken zum eigenen finanziellen Vorteil auszunutzen.

IP-Adresse
Eine IP-Adresse (Internet-Protocol-Adresse) dient zur eindeutigen Adressierung von Rechnern und anderen Geräten in einem IP-Netzwerk. Die IP-Adresse entspricht funktional der Rufnummer in einem Telefonnetz. Technisch gesehen ist die Nummer eine 32- oder 128-stellige Binärzahl. Das bekannteste Einsatzgebiet in dem IP-Adressen verwendet werden, ist das Internet.

Internet Protocol Version 6

Im Internet braucht jedes Gerät eine IP-Adresse. Dabei gibt es zwei verbreitete Versionen von IP-Adressen. Im Moment basiert der Großteil des Internetverkehrs noch auf Internet Protocol Version 4 (IPv4). Österreich hat derzeit eine IPv6 Adoptionsrate von 6.1 Prozent. Dabei könnte eine bereitere Nutzung von IPv6, dabei helfen, die IT-Forensik zu erleichtern. Es würde der rechtmäßige Zugriff der Strafverfolgungsbehörden auf sachdienliche Informationen in den Fällen gewährt werden, in denen dieser Zugriff aus Gründen der Sicherheit und Gerechtigkeit notwendig und verhältnismäßig ist. Deswegen gibt es bereits Bestrebungen die Einführung des neuen Protokolls (IPv6), das die Zuordnung einer einzigen IP-Adresse pro Nutzer ermöglicht, was für die Strafverfolgung und Ermittlungen im Bereich Cybercrime mit klaren Vorteilen verbunden ist, zu forcieren. Dabei wird neben politischen Maßnahmen auch auf freiwillige Vereinbarungen zur Beschleunigung der Einführung von IPv6 mit den Internetdienstanbietern (ISPs) gesetzt.

Krypto-Mining

Mining, englisch für schürfen, bezeichnet die Tätigkeit der Ausstellung von Transaktionsbestätigungen und Transaktionsdokumentation sowie der Erzeugung völlig neuer Einheiten bei Krypto-Währungen mit Hilfe aufwendiger mathematischer Rechenfunktionen. Für Kriminelle eröffnet sich hier die Möglichkeit fremde Rechenkapazität für sich gewinnbringend einzusetzen. Dabei kommt es immer wieder zu massiven Krypto-Mining-Kampagnen, dabei versuchen die Täter sich Zugriff auf viele fremde Rechner zu verschaffen und sie für sich arbeiten zu lassen. Für den Täter steigt mit der eingesetzten Rechenleistung die Wahrscheinlichkeit einen Block auf der Blockchain als erster zu minen und eine entsprechende monetäre Belohnung dafür zu erhalten. Der Stromverbrauch solcher Mining-Pools kann dabei immens sein.

Malware

Bezeichnet Computerprogramme, welche vom Benutzer unerwünschte schädliche Funktionen ausführen.

Peer to Peer (P2P)

In einem Peer to Peer-Netz sind alle Computer gleichberechtigt und können sowohl Dienste in Anspruch nehmen als auch Dienste zur Verfügung stellen. Die Computer können als Arbeitsstationen genutzt werden, aber auch Aufgaben im Netz übernehmen.

Phishing

Ist eine Form des Trickbetrugs im Internet. Dabei wird vor allem per E-Mail versucht, den Empfänger irrezuführen und zur Herausgabe von Zugangsdaten und Passwörtern zu bewegen. Dies bezieht sich in den meisten Fällen auf Online-Banking und andere Bezahlsysteme.

Ransomware

Die Kategorie der sogenannten „Ransomware“ bezeichnet bösartige Software, welche zur Erpressung des Benutzers genutzt wird indem sie die Funktionalität seines Systems einschränkt und eine Geldzahlung fordert um die Einschränkungen aufzuheben. Bei Cryptolockern werden zum Beispiel sämtliche Daten auf lokalen Speichermedien sowie meist auch Netzlaufwerke, USB-Sticks, Speicherkarten etc. mit einem starken Algorithmus verschlüsselt sodass der User keinen Zugriff mehr darauf hat. Danach wird ein Geldbetrag gefordert nach dessen Bezahlung der Malwarebetreiber zusichert die Daten wieder zu entschlüsseln und den Zugriff freizugeben. Es ist in derartigen Situationen jedoch nicht gesichert, dass der Zugriff nach Bezahlung tatsächlich wieder möglich ist.

Remote Desktop Protokoll

Ursprünglich zur Fernwartung durch den zuständigen Systemadministrator vorgesehen,
tritt dieses Verfahren bei Sachverhalten hinsichtlich des wiederrechtlichen Zugriffs auf ein Computersystem verstärkt in Erscheinung. Die Motivation der Täter kann hier ganz unterschiedlich sein und reicht vom infizieren eines Computers mit Schadsoftware etwa Verschlüsselungstrojaner oder Crypto-Mining bis zum Cyber-Stalking bei dem das Opfer etwa mithilfe eine eventuell vorhandenen Webcam vom Täter beobachtet wird. Deswegen wird empfohlen Webcams sofern nicht im Moment in Verwendung abzustecken bzw. durch Anbringen eines Stickers abzudecken. Dies gilt auch für Geräte die durch Kinder und Jugendliche genutzt werden. Computerkriminelle bedienen sich zumeist unsicherer Passwörter und anderer Schwächen um Zugriff auf den PC via Fernwartung zu erhalten und verkaufen diese Zugänge dann an andere Tätergruppen weiter, die wieder ihre eigenen Motive für die Nutzung haben.

Spyware
Damit bezeichnet man Programme die Informationen über die Tätigkeiten des Benutzers sammeln und an Dritte weiterleiten. Ihre Verbreitung erfolgt meist durch Trojaner, als kostenlose Zugaben zu anderen Programmen oder als Zusatzfunktion zu kostenlosen Apps.

Trojaner
Ist eine Kombination eines manchmal nur scheinbar nützlichen Wirtsprogramms mit einem versteckt arbeitenden, bösartigen Teil, oft einer Software die Daten ohne Wissen des Computerbenutzers ausspioniert. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogramms für seine Installation durch den Benutzer.

Verschlüsselung
Bezeichnet einen Vorgang, bei dem ein Klartext durch einen Verschlüsselungsalgorithmus zusammen mit einem, in der Regel, geheimen Schlüssel in einen verschlüsselten Text umgewandelt wird. Man unterscheidet grundsätzlich zwischen:

Symmetrische Verschlüsselung: Für Ver- und Entschlüsselung wird ein und derselbe Schlüssel verwendet.

Asymmetrische Verschlüsselung: Für die Verschlüsselung wird ein Public-Key, öffentlicher Schlüssel verwendet und für die Entschlüsselung kommt ein Private-Key, geheimer Schlüssel zum Einsatz. Der Schlüssel zum Verschlüsseln der Nachricht ist also ein anderer als jener, der zur Entschlüsselung verwendet wird.

PUBLIKATIONEN, KONTAKT UND EDITORIAL

WEITERE PUBLIKATIONEN 2017

Kriminalstatistik
Schlepperei
Kulturgut
Kriminalprävention
Verfassungsschutz
Suchtmittelkriminalität
Menschenhandel
Geldwäscherei
Sicherheitsbericht

KONTAKT

Bundeskriminalamt
Meldestelle Cybercrime
Josef-Holaubek-Platz 1, 1090 Wien
Tel: +43 (0)1 24836-985025
E-Mail: against-cybercrime@bmi.gv.at

Sie haben Fragen zur Broschüre? Wir freuen uns auf Ihre E-Mail. Schreiben Sie uns: bk.presse@bmi.gv.at.

EDITORIAL

Bundeskriminalamt
Büro für Presse- und Öffentlichkeitsarbeit
Josef-Holaubek-Platz 1, 1090 Wien
Tel.: +43 (0) 1 24836-985004
E-Mail: bk.presse@bmi.gv.at

Grafik, Fotos und Design: ©BK/Halm

Hinweis
Die Broschüre wurde mit großer Sorgfalt und viel Engagement erstellt. Dennoch können sich Fehler eingeschlichen und unseren Korrekturlesungen standgehalten haben. Wir bitten um Verständnis.

www.bundeskriminalamt.at