.BK
BUNDESKRIMINALAMT

Cybercrime

Österreich

Jahresbericht 2015

Zum Online-Bericht

Inhalt

Vorwort

Liebe Leserinnen, liebe Leser,

wir sehen uns als Sicherheitsbehörde immer öfter mit internationalen Tätern und Tätergruppierungen konfrontiert, die mit immer neuen Ideen und hochtechnischer Ausrüstung ihr Unwesen im Internet treiben. Daher ist es eine zentrale Aufgabe des Bundeskriminalamtes dieser Entwicklung entgegenzutreten, gegen diese Kriminellen zu ermitteln und die Nutzerinnen und Nutzer vor deren Machenschaften zu schützen. Zur Verwirklichung dieses Vorhabens sind zwei Faktoren von größter Wichtigkeit.

Zum einen sind gut ausgebildete und modern ausgerüstete Polizistinnen und Polizisten unabdingbar, um die Ermittlungen zu führen. Zum anderen sind internationale Abkommen und Kooperationen immer wichtiger, um die Spur der Täter im Internet effektiv verfolgen zu können. Dies gilt für alle Bedrohungslagen, die mit dem weltweiten Netz verbunden sind. Sei es Hacking, der Diebstahl von Identitäten oder die Betrugs- und Finanzmittelkriminalität.

Um die Täter und deren Methoden effektiv zu bekämpfen, wurden 2015 von den Strafverfolgungsbehörden große Anstrengungen unternommen. Aufgrund der wachsenden Anforderungen an die Ermittlungsmethoden und die Beweismittelsicherung wurde der Ausbau von Hard- und Software fortgesetzt. Außerdem wird laufend in die Aus- und Weiterbildung der Mitarbeiterinnen und Mitarbeiter sowohl in den Landeskriminalämtern als auch im Cybercrime-Competence-Center im Bundeskriminalamt investiert.

Der vorliegende Cybercrime-Report skizziert die Entwicklung der Cybercrime-Delikte im Jahr 2015. Darüber hinaus werden aktuelle Entwicklungen und Phänomene beschrieben und die darauf ausgerichtete Arbeit der Polizei sowie einzelne Projekte und Schwerpunkte vorgestellt.

Wir hoffen, dass dieser Lagebericht nicht nur einen guten Überblick über die derzeitige Lage in Österreich gibt, sondern auch im Sinne der Prävention, die immer wichtiger wird, einen Anstoß zum besseren Selbstschutz gibt. Bedanken möchten wir uns an dieser Stelle bei allen Organisationen, Behörden, Vertretungen, aber auch Einzelpersonen, die in diesem Sinne gemeinsam mit uns zusammenarbeiten und so Österreich gemeinsam sicherer machen.

Mag. Wolfgang Sobotka
Bundesminister für Inneres

General Franz Lang
Direktor des Bundeskriminalamtes

Dr. Michael Fischer
Stellvertretender Direktor des Bundeskriminalamtes

Einleitung

Der Cybercrime-Report 2015 bietet einen Überblick der Entwicklungen und Maßnahmen im Bereich der Cyber-Kriminalitätsbekämpfung unter der Führung des Bundeskriminalamtes (BK). Dieser Report soll sowohl innerbehördlich als auch über die Behördengrenzen hinaus einen zusätzlichen Informations- und Präventionsbeitrag leisten. Da technische Fachbegriffe verwendet werden, sind die Definitionen der wichtigsten Begriffe im Glossar zu finden.

Der Bericht gliedert sich in sechs Teile: Der allgemeine Teil beschreibt die Delikte und die rechtlichen Voraussetzungen. Weiters ist die Anzeigenentwicklung im Bereich Cybercrime angeführt. Als Quelle dient die Polizeiliche Kriminalstatistik Österreich (PKS).

Der zweite Teil skizziert den Aufbau der Polizei und des C4 für die Kriminalitätsbekämpfung als auch die internationale Zusammenarbeit. Die beiden darauffolgenden Kapitel beschreiben Projekte des C4 und Schwerpunkte des BK. Im Kapitel „Wissenswertes“ werden Analysemethoden und im Kapitel „Prävention und Information“ die Maßnahmen und konkrete Tipps der Kriminalprävention aufgezeigt.

Zusammenfassung

Daten und Fakten

Im Bereich Cyber-Kriminalität ist die Zahl der Anzeigen um 11,6 Prozent auf 10.010 Fälle angestiegen. Das sind um 1.047 mehr als 2014. Die Aufklärungsquote lag 2015 bei 41,5 Prozent, mit nur 0,7 Prozentpunkten über jener von 2014, was sowohl auf die zunehmende Technisierung der Tätergruppen als auch auf deren vermehrten Gebrauch von Verschlüsselungs- und Anonymisierungstechniken hinweisen könnte.
Bei den Cybercrime-Delikten im engeren Sinn wurde 2015 ein Rückgang der Anzeigen um 3,3 Prozent verzeichnet, während die Zahl der Anzeigen wegen Internetbetrugs um 12,6 Prozent gestiegen ist.

Trends

Auch das Jahr 2015 folgt im Zehn-Jahresvergleich einem deutlichen Trend nach oben, wobei sich die Anzahl der Anzeigen der letzten vier Jahre auf hohem Niveau eingependelt hat. Die Technisierung des Alltags, die zunehmende Nutzung von Computern in Form von Mobile Devices verschiedenster Art und der Ausbau der Netzverbindungen bieten potenziellen Tätern eine stetig wachsende Angriffsfläche.
Insbesondere ist das vermehrte Auftreten von Ransomware und DDos-Attacken, Englisch für Distributed Denial-of-Service, zu beobachten. Während 2014 eher Klein- und Mittelunternehmen Ziel der Angriffe waren, sind mittlerweile auch große Betriebe und Privatpersonen stark betroffen. Die Bedrohungslage kann somit als ansteigend eingestuft werden.

Polizeiliche Maßnahmen

Das Cybercrime-Competence-Center C4 im Bundeskriminalamt fungiert national und international als Zentralstelle zur Bekämpfung von Cyber-Kriminalität in Österreich. Vergleichbare Dienststellen dazu gibt es auch in allen Landeskriminalämtern, in denen ebenfalls kriminalpolizeilich und technisch ausgebildete Expertinnen und Experten mit der Bekämpfung von Cybercrime und auf dem Gebiet der IT-Forensik ihre Aufgaben erfüllen.
Aufgrund des unaufhaltsamen technologischen Fortschrittes und der Digitalisierung des Alltags ergibt sich ein erhöhter Bedarf an hochqualifizierten Cybercrime-Ermittlungsexperten und IT-Forensikern. Für diese soll zukünftig ein maßgeschneidertes Ausbildungssystem vom BMI zur Verfügung gestellt werden.
Der internationale Aspekt im Bereich Cybercrime und die sich daraus ergebenden Möglichkeiten der Tätervernetzung sind mitverantwortlich für den kontinuierlichen Anstieg von Cyber-Attacken. 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.
Die laufenden Präventionsmaßnahmen und die damit verbundene Information aller Bevölkerungsschichten über die Gefahren von Cybercrime sowie der unmittelbare Kontakt mit den Bürgern sind wesentliche Faktoren um Schäden durch Cybercrime in Österreich vorzubeugen.

Ausblick

Für die Zukunft ist absehbar, dass Cyber-Delikte immer mehr mit klassischen Delikten verschmelzen und zunehmend als Mittel für unterschiedlichste Straftaten wie beispielsweise Erpressung, Betrug, Mobbing usw. verwendet werden. Dies ergibt sich unter anderem aus der ständigen Perfektionierung der Angriffsmethoden und aus dem nahezu grenzenlosen Betätigungsfeld der Cyber-Kriminellen, da sie ihre Aktivitäten unabhängig sowohl von der eigenen Örtlichkeit als auch der des potenziellen Opfers starten können. Die erforderliche technische Unterstützung wird dabei häufig von kriminellen Dienstleistern, Cybercrime as a Service, zum Beispiel im Darknet angeboten. Cyber-Kriminalität wird dadurch auch in den nächsten Jahren ein boomendes Kriminalitätsfeld bleiben.

Allgemeines über Cybercrime

Eine allgemein gültige Definition des Begriffs Computerkriminalität oder Cyber-Kriminalität (engl. Cybercrime) gibt es nicht. Üblicherweise versteht man darunter alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IKT) oder gegen diese begangen werden. Im polizeilichen Bereich wird darüber hinaus zwischen Cybercrime im engeren Sinn und Cybercrime im weiteren Sinn unterschieden.

Cybercrime im engeren Sinne:

Bezeichnet Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden. (z. B. Datenbeschädigung, Hacking, DDoS-Attacken).

Delikte die jedenfalls zu „Cybercrime im engeren Sinne" gehören, sind beispielsweise

- § 118a Strafgesetzbuch (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 sowie
- § 225a StGB: Datenfälschung.

Cybercrime im weiteren Sinne:

Unter Cybercrime im weiteren Sinne versteht man Straftaten, bei denen die Informations- und Kommunikationstechnik zur Planung, Vorbereitung und Ausführung für herkömmliche Kriminaldelikte eingesetzt wird, wie z. B. Betrugsdelikte, Kinderpornografie, Cyber-Grooming oder Cyber-Mobbing.

Ein typisches Merkmal von Cyber-Delikten ist deren Virtualität. Die Straftat wird mithilfe von Programmen und Computersystemen begangen und findet scheinbar nicht in der Realität statt. Dadurch sinkt vielfach die Hemmschwelle zur Begehung solcher Taten. Ein weiteres Merkmal stellt der internationale Aspekt der Delikte dar. Täter, Tatmittel und Opfer können sich in unterschiedlichen Ländern, ja sogar auf unterschiedlichen Kontinenten befinden. Ländergrenzen sind bedeutungslos. Diese Tatsache und auch die mit der ständigen Weiterentwicklung der Technik einhergehenden neuen Möglichkeiten der Tatbegehung begünstigen das Entstehen neuer Modi Operandi, wie z. B. Ransomware, Hacking, Phishing oder DDoS-Attacken. Gleichfalls bieten sich für die Täter durch Anonymisierungsdienste, Kryptografie und durch Nutzung des Darknets immer mehr Möglichkeiten sich der Strafverfolgung zu entziehen.

Rechtliche Aspekte

Cybercrime als Querschnittsmaterie kann in Kombination mit einer Vielzahl von anderen Straftaten, wie z. B. Betrug oder Erpressung in Erscheinung treten. Im österreichischen Strafrecht finden sich diese Bedrohungen vor allem im Bereich der Vermögensdelikte sowie im Bereich der strafbaren Handlungen gegen die Privatsphäre wieder.

Cybercrime tritt als weltweites Phänomen in immer vielfältigeren Erscheinungsformen auf und stellt den nationalen Gesetzgeber vor die Herausforderung, diesen Entwicklungen Rechnung tragen zu müssen. In den letzten Jahren hat das Phänomen des Cyber-Mobbings, die persönliche Belästigung via Computersystem, vor allem im Zusammenhang mit dem Selbstmord von Jugendlichen, auf tragische Weise Bekanntheit erlangt. Mit dem Strafrechtsänderungsgesetz 2015 (seit 1. Jänner 2016 in Kraft) und dem damit neu eingeführten § 107c StGB (Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems) wurden auch diese Handlungen unter Strafe gestellt. Gleichzeitig wurde der Tatbestand des § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem) verständlicher formuliert und die Errichtung von Bot-Netzen sowie Angriffe auf kritische Infrastruktur unter Strafe gestellt.

Zahlen und Fakten

Nach einem leichten Rückgang im Jahr 2014 auf knapp unter 9.000 Anzeigen sind die Zahlen im Jahr 2015 wieder gestiegen. Die Zunahme beträgt 11,6 Prozent bzw. 1.047 Anzeigen auf 10.010 Fälle. Wurden vor zehn Jahren in Österreich nur rund 3.200 Anzeigen erstattet, so hat sich seit 2012 die Zahl der Anzeigen auf rund 10.000 eingependelt.

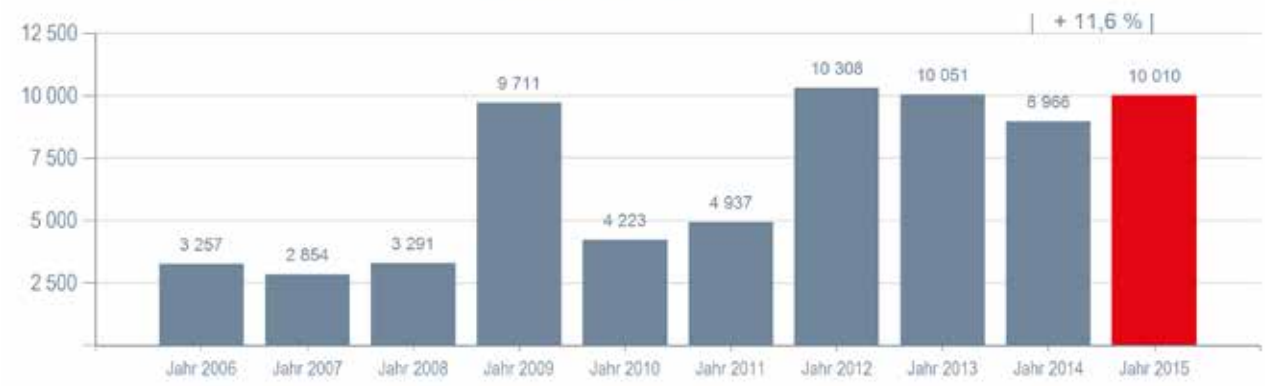

Abbildung 1: Anzeigen Cybercrime 2006 bis 2015

Die Aufklärungsquote lag 2015 bei 41,5 Prozent und damit um 0,7 Prozentpunkte über der von 2014, aber noch immer unter jener der Vorjahre. Die Ursachen liegen unter anderem in der stetig steigenden Technisierung der Tätergruppierungen und deren zunehmenden Möglichkeiten durch Nutzung von Verschlüsselungs- und Anonymisierungstechniken. Darüber hinaus spielt das Darknet eine immer größere Rolle.

Cybercrime	Angezeigte Fälle	Geklärte Fälle	Aufklärungsquote
Jahr 2006	3 257	2 312	71,0 %
Jahr 2007	2 854	1 940	68,0 %
Jahr 2008	3 291	2 458	74,7 %
Jahr 2009	9 711	8 794	90,6 %
Jahr 2010	4 223	2 336	55,3 %
Jahr 2011	4 937	2 370	48,0 %
Jahr 2012	10 308	2 807	27,2 %
Jahr 2013	10 051	4 544	45,2 %
Jahr 2014	8 966	3 660	40,8 %
Jahr 2015	10 010	4 157	41,5 %
Veränderung	11,6 %	13,6 %	0,7 %-Punkte

Abbildung 2: Entwicklung der Anzahl der angezeigten und geklärten Fälle sowie der Aufklärungsquote von 2006 bis 2015

Die Zahl der Anzeigen wegen Internetbetrugs ist um 12,6 Prozent von 6.635 Anzeigen auf 7.473 gestiegen.

Abbildung 3: Anzeigen Internetbetrugs 2006 bis 2015

Die Cybercrime-Delikte im engeren Sinne sind um 3,3 Prozent gesunken. Ein auffallender Rückgang ist beim widerrechtlichen Zugriff auf ein Computersystem, auch unter Hacking bekannt, zu verzeichnen. Die Zahl der angezeigten Angriffe ist von 677 im Jahr 2014 auf 387 Anzeigen im Jahr 2015 und somit über 42 Prozent gesunken. Besonders zugenommen haben die Fälle von betrügerischem Datenmissbrauch: Hier stieg die Zahl um 60,1 Prozent: von 404 im Jahr 2014 auf 647 im Vorjahr. Die Ursache liegt in einem verstärkten Einsatz von Malware wie zum Beispiel Trojaner-Schadsoftware.

Angezeigte Fälle	Jän-Dez 2014	Jän-Dez 2015	Veränderung
§ 118a StGB	677	387	-42,8 %
§ 119a StGB	17	19	11,8 %
§ 126a StGB - Vergehen	138	142	2,9 %
§ 126a/V StGB - Verbrechen	2	2	0,0 %
§ 126b StGB - Vergehen	118	127	7,6 %
§ 126b/V StGB - Verbrechen	22	37	68,2 %
§ 126c StGB	249	186	-25,3 %
§ 148a StGB - Vergehen	404	647	60,1 %
§ 148a/V StGB - Verbrechen	6	13	116,7 %
§ 225a StGB	121	136	12,4 %
Cybercrime im engeren Sinn	1 754	1 696	-3,3 %

Abbildung 4: Cybercrime-Delikte im engeren Sinne 2014 im Vergleich zu 2015

Cyberdelikte in Österreich

Money Mules
Nach wie vor sind zahlreiche E-Mails im Umlauf, in denen den Empfängern „gutes Geld für mühelose Arbeit" angeboten wird. Als Verdienst wird den Adressatinnen und Adressaten ein Einkommen von bis zu 8.000 Euro in Aussicht gestellt. Ihre Tätigkeit besteht darin, ein von den Tätern auf ihr Konto überwiesenes Geld in der Höhe zwischen 2.000 und 8.000 Euro in bar zu beheben. Danach muss das Geld nach Abzug von 20 Prozent Provision über einen Bezahldienstanbieter wie z. B. Western Union, MoneyGram, usw. an den „Betrieb" gesandt werden. Diese Vorgangsweise ist typisch für Geldwäscherei und dient zur Verschleierung der Zahlungsströme von illegal erworbenen Vermögensbestandteilen. Wer sich auf einen solchen „Nebenverdienst" einlässt wird als „Money Mule" bezeichnet und macht sich neben diversen Finanzvergehen auch der Geldwäscherei nach § 165 StGB strafbar.

Ransomware
2015 stieg in Österreich die Zahl der Vorfälle mit sogenannter „Ransomware". Unter dieser versteht man einen Sammelbegriff für Schadsoftware, die speziell dafür entwickelt wird, elektronische Daten und Systeme zu verschlüsseln, sodass diese nicht mehr verwendet werden können. Für die Entschlüsselung wird dann von den Tätern in weiterer Folge Lösegeld (engl. ransom) verlangt, meistens in Form des virtuellen Zahlungsmittels Bitcoin oder durch Prepaid-Karten. Beide Zahlungsformen sind anonym und erschweren dadurch die Strafverfolgung. Die Verbreitung der Verschlüsselungssoftware erfolgt insbesondere über präparierte E-Mails, durch Sicherheitslücken in Webbrowsern oder unbemerkt durch Downloads aus dem Internet (drive-dy-download). Betroffen sind sowohl Privatpersonen als auch Unternehmen, Behörden und sonstige Organisationen.

Die verschiedenen Varianten dieser Erpresser-Software werden überwiegend als manipulierte Anhänge oder Weblinks getarnt, z. B. als Verständigungs-E-Mails unterschiedlicher Zustelldienste oder Bewerbungsschreiben an Unternehmen. Um eine Überprüfung der tatsächlichen Dateiendung von im Anhang befindlichen Schreiben erst gar nicht zuzulassen, ergehen spezifische Job-Anfragen an Firmen, in denen vorgegeben wird, dass die Übermittlung der Bewerbungsmappe nicht möglich war. Diese sollte nunmehr von einer „Dropbox" des Bewerbers heruntergeladen werden. Der dafür in der Bewerbungs-E-Mail übermittelte Link lässt vorerst keinen Hinweis auf die Dateiendung zu. Auch nach dem Download der Datei ist es schwer zu erkennen, dass es sich um eine ausführbare Datei handelt, da einerseits das Icon auf den entsprechenden vorgegaukelten Dateityp geändert wurde und andererseits vom Betriebssystem die tatsächliche Endung je nach Systemeinstellung erst gar nicht angezeigt wird.

Diese Schadsoftware verwendet dabei meistens mehrere Verschlüsselungsdurchläufe mit sehr langen zufälligen Passwörtern und löscht danach die ursprünglichen Dateien. Im Anschluss an diese Vorbereitungshandlungen werden eigene Startseiten auf den befallenen Computern installiert, in denen auf die Verschlüsselung und Löschung der Daten hingewiesen wird.

Üblicherweise soll zur Freischaltung der gesperrten Daten oder Funktionen eine Art Lösegeld gezahlt werden, meist in Form der digitalen Währung Bitcoin. Allerdings kann die Zahlung eines Lösegeldes nicht garantieren, dass die Kriminellen auch tatsächlich die Kontrolle über vertrauliche Daten oder wichtige Funktionen zurückgeben. In vielen Fällen sind Daten, die in die Hände der Angreifer fallen, unwiederbringlich verloren. Neben den allgemeinen Sicherheitshinweisen zum Verhalten im Internet kann in solchen Fällen nur ein funktionierendes, fortlaufend durchgeführtes Backup auf externe bzw. abgekoppelte Systeme helfen.

Cyber-Kriminalitätsbekämpfung

Cybercrime Competence Center (C⁴)

Das im Bundeskriminalamt angesiedelte C⁴ ist nationale und internationale Zentralstelle zur Bekämpfung von Cyber-Kriminalität in Österreich. Die Aufgaben des C⁴ umfassen folgende Zuständigkeiten:

- Durchführung, Leitung und Koordinierung von Ermittlungen bei Cybercrime im engeren Sinn
- Unterstützung bei Ermittlungen zur Aufklärung von Cybercrime-Delikten im weiteren Sinn
- IT-Forensik wie z. B. Sicherung, Aufbereitung und Auswertung von elektronischen Beweismitteln
- Entwicklung und Bereitstellung von neuen technischen Lösungen.
- Analyse und Bewertung neuer Technologien
- Betrieb einer Meldestelle als 24/7 Kontaktstelle zu anderen spezialisierten Polizeieinheiten, wie dem Europäischen Cybercrime Center (EC3) bei Europol und dem Interpol Digital Cyber Center (IDCC). Das C⁴ ist als Kontaktstelle im Rahmen des internationalen „G8-Abkommens für dringliche Unterstützung bei Cybercrime-Fällen und der Sicherung von elektronischen Beweismitteln“ eingerichtet.
- Ansprechstelle für Anfragen aus der Wirtschaft und der Bevölkerung in Cybercrime-Angelegenheiten
- Schnittstelle zum Bereich Cybersecurity
- Fachaufsicht über den Assistenzbereich Cybercrime in den Landeskriminalämtern
- Internationale polizeiliche Kooperation in Cybercrime-Angelegenheiten

Das C⁴ beschäftigte im Jahr 2015 insgesamt 37 Mitarbeiterinnen und Mitarbeiter aus Verwaltung, Exekutive und Technik und ist in folgende Bereiche unterteilt:

- Zentrale Aufgaben
- IT-Beweissicherung
- Ermittlungen
- 24/7 Meldestelle

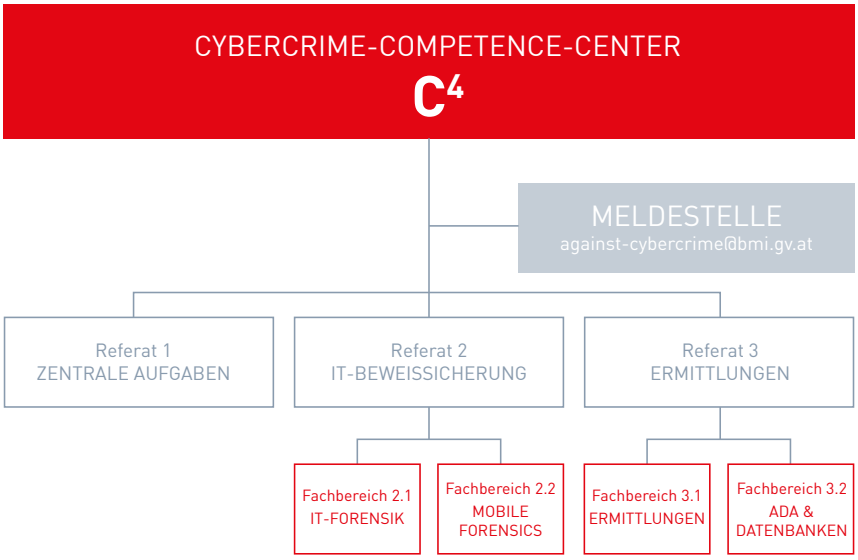

Abbildung 6: Organigramm des C⁴

Im Rahmen des technischen Supports werden C4-intern mittlerweile ca. 90 Client-Computer, 41 Serversysteme sowie 15 verschiedene Netzwerke administriert und betreut. Zusätzlich werden Infrastrukturen für nachgeordnete Dienststellen sowie Staatsanwaltschaften zur Verfügung gestellt, die ebenfalls im C4 konzeptioniert und umgesetzt wurden. Die Techniker des C4 leisteten in etwa 20 komplexen Fällen technische Unterstützung bei Auswertungen und Ermittlungen.

Im Bereich der IT-Beweissicherung wurden 2015 über 136 Terabyte (TB) an elektronischen Beweisen gesichert. Der Fachbereich „Mobile Forensik" hat knapp 1.200 Mobilgeräte und mehr als hundert Kraftfahrzeuge bzw. deren Fahrzeugelektronik und Datenspeicher ausgewertet.

Im Referat Ermittlungen sind neben zahlreichen aktuellen Fällen auch Phänomene wie die neue Schadsoftwarekategorie Ransomware, Polizeitrojaner, Phreaking usw. bearbeitet worden.

Die rund um die Uhr erreichbare Meldestelle wurde im letzten Jahr mit weit über 10.000 Mitteilungen aus der Bevölkerung sowie von in- und ausländischen Dienststellen konfrontiert. In dringenden Fällen, wie bei Suizidankündigungen über das Internet, kann durch den C4-Journaldienst die Einleitung von Maßnahmen zur technischen Unterstützung anderer Dienststellen wie Datensicherung, Handy und Navigationssystemauswertung veranlasst werden.

Kontakt zur Meldestelle: against-cybercrime@bmi.gv.at

Zusätzlich organisierte das C4 im November 2015 die zweite IT-B-Fachtagung in Wien. Ziel dieser Fachtagung ist es, den mit IT-Beweismittelsicherung und Cybercrime-Ermittlungen befassten Beamtinnen und Beamten in den Landeskriminalämtern und Bezirken mit einen Überblick über den aktuellen Stand der Entwicklungen auf diesen Gebieten zu bieten.

Internationale Zusammenarbeit

Gerade im Bereich der Internetkriminalität ist die internationale Zusammenarbeit unumgänglich. 2015 wurden zahlreiche Projekte umgesetzt, Fachtagungen und Kongresse besucht und ausgetragen:

- Auf internationalem Parkett waren Mitarbeiter des C4 bei wichtigen Konferenzen im Bereich Cybercrime vertreten, wie beispielsweise der „Europol Interpol Cybercrime Conference" in Den Haag.
- In der bei Europol angesiedelten European Cybercrime Training and Education Group (ECTEG) wurde 2015 der österreichische Vertreter des C4 zum stellvertretenden Vorsitzenden gewählt.

  Weiteres übernahm das C4 den stellvertretenden Vorsitz in einem von Europol initiierten Projekt mit dem Ziel, ein EU-weites Cybercrime-Ausbildungsmodell zu entwickeln und zu einzuführen. Hier werden neue Akzente gesetzt, indem ein neuer Prozess für die EU-weite nachhaltige Bereitstellung von „State-of-the art"-Cybercrime-Trainings erarbeitet wird. Zusätzlich stellt das C4 hier die Expertenvertreter für das Kernprojektteam.
- Das C4 war auch an den vorbereitenden Arbeiten für die Evaluierung der österreichischen Cybercrime Bekämpfungsdienststellen durch eine Expertengruppe der EU, der sogenannten GENVAL Evaluierung, maßgeblich beteiligt. Die Ergebnisse der Evaluierung sind für 2017 geplant.

Das C4 zeichnet sich als österreichisches Cybercrime-Kompetenzzentrum auch für die Mitwirkung an internationalen Gremien und Konferenzen aus.

- Vertreter des C4 nahmen 2015 unter anderem auch am „Quarto Congresso de Investigacao Criminal" in Portugal teil. Bei dieser Fachtagung waren über 1.000 Teilnehmerinnen und Teilnehmer aus Wissenschaft und Forschung sowie aus Polizeiorganisationen anwesend.

- Darüber hinaus wurde im November 2015 das 5. internationale Fachsymposium „Neue Technologien“ erstmalig in Wien veranstaltet und vom C4 ausgerichtet. Diese Tagung ist eine Kooperation zwischen dem Bundeskriminalamt (BKA) Wiesbaden, den Landeskriminalämtern Bayern und Baden Württemberg, der FedPol Schweiz und dem österreichischen Bundeskriminalamt. 2015 stand das Symposium unter dem Motto „Smart World - Smart Media - Smart Police“. Zahlreiche internationale Top-Experten referierten über verschiedene Möglichkeiten, wie diese neuen Technologien künftig für die Verbrechensbekämpfung effizient genutzt werden können. Die zweitägige Veranstaltung war international besucht und hatte jeden Tag über mehr als 200 Teilnehmerinnen und Teilnehmer.

Diese internationale Vernetzung trägt erheblich zum Erfolg der Polizeiarbeit bei.

Operation gegen DDoS-Erpresser

In den Jahren 2014 und 2015 zeigte sich eine Tätergruppe namens DD4BC weltweit für zahlreiche erpresserische E-Mails und DDoS-Angriffe verantwortlich. Dabei sandten die Täter E-Mails an Online-Unternehmen, in denen sie aufforderten, einen bestimmten Betrag mit dem virtuellen Zahlungsmittel Bitcoin zu entrichten. Widrigenfalls wurde damit gedroht, den Zugriff auf Webseiten der Unternehmen mittels DDoS-Angriffen zu blockieren. Im Anschluss an ihre E-Mails untermauerten die Kriminellen die Drohungen jeweils mit einer etwa einstündigen DDoS-Attacke.

Im Frühjahr 2015 trat diese Form der Online-Erpressung auch in Österreich verstärkt auf. Fünf namhafte Online-Unternehmen mit Sitz im Inland erstatteten Anzeige beim Bundeskriminalamt. Das C4 nahm daraufhin die Ermittlungen auf und stellte internationale Kontakte her. Rasch stellte sich heraus, dass die Gruppe DD4BC auch in anderen Ländern aktiv war, weshalb das C4 eine gemeinsame Ermittlung mit Europol initiierte. An der Joint Cybercrime Action Taskforce (J-CAT) beteiligten sich neben Österreich auch Europol, Interpol, Großbritannien, Deutschland, Frankreich, Rumänien, Bosnien und Herzegowina, Australien, die USA und Japan. Neben der Ermittlungsarbeit wurde auch eine Warnmeldung veröffentlicht und die Bevölkerung über diese Erpressungsform umgehend informiert.

Als Folge intensiver Ermittlungen fand unter dem Operationsnamen „Pleiades“ am 15. und 16. Dezember 2015 in Banja Luka/Bosnien eine internationale Polizeiaktion statt. Dabei konnten insgesamt sieben verdächtige Personen festgenommen werden, darunter auch der Haupttäter. Zudem wurden etwa 600 Gigabyte elektronisches Datenmaterial sichergestellt, sowie 59 E-Mail-Accounts und 251 Bitcoin-Wallets ausgeforscht. Insgesamt waren mindestens 310 Unternehmen betroffen.

Projekte im C4

Fahrzeugforensik

Dieses EU-teilgeförderte Projekt ist Teil des Internal-Security-Fund-Programmes (ISF) der Europäischen Kommission (EK) und dient der Errichtung und Schaffung einer zentralen Servicestelle zur kriminalpolizeilichen Beweismittelsicherung von Daten aus Kraftfahrzeugen, der Fahrzeugforensik. Bestandteil des Projektes sind Maßnahmen zur Aufklärung verschiedenster Straftaten, insbesondere aber zur Bekämpfung der grenzüberschreitenden organisierten Kriminalität sowie Maßnahmen zur Bekämpfung krimineller Netzwerke.

Durch den Einzug von Netzwerktechnologien und Internetdiensten innerhalb der Fahrzeuge dient das Projekt auch der Prävention und Eindämmung der Cyber-Kriminalität sowie dem besseren Schutz der Bürgerinnen und Bürger als auch Unternehmen im Cyberspace. Der Aufbau von Kapazitäten bei Strafverfolgung und Justiz sowie die Verbesserung der Interventionsmöglichkeiten bei Cyber-Angriffen stellen Synergieeffekte dar.

Electronic Visual Analysis (E.V.A)

Ziel dieses Projektes ist die Entwicklung einer computergestützten polizeilichen Methode zur forensischen Auswertung im Bereich der kriminalpolizeilichen Ermittlungsarbeit bei Kinderpornographie.

Die Ermittler in diesem Deliktsumfeld werden mit einer immer stärker wachsenden Menge an strafrechtlich relevanten Mediendateien wie Fotos oder Videos konfrontiert. So ist die Anzahl der jährlich zu bearbeitenden Fälle mit mehreren Hunderttausend Bildern und Videos pro Sicherstellung ständig im Steigen. Diese enorme Menge an Dateien müssen nicht nur forensisch behandelt und klassifiziert, sondern auch fallübergreifend inhaltlich ausgewertet werden, um Serientatbestände zu erkennen und eine funktionierende Täter-Opfer-Erkennung zu gewährleisten.

Dieses Projekt wird mittels des österreichischen Sicherheitsforschungsförderprogramms KIRAS unter der Programmverantwortung des Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT) und in Partnerschaft mit zwei österreichischen Universitäten implementiert.

www.kiras.at

Aufbau einer IT-Forensik in Kroatien

Im Juli 2014 wurde in Kooperation mit der Cyber-Einheit des spanischen Innenministeriums ein 15 Monate laufendes, EU-finanziertes Projekt in Kroatien gestartet. Die Aufgabe der österreichischen Expertengruppe bestand darin, das Ivan Vucetic Center des kroatischen Innenministeriums beim Aufbau eines IT-Forensik Centers zu beraten.

Das Zentrum für Kriminaltechnik, Forschung und Expertise „Ivan Vucetic“ ist vollwertiges Mitglied des „European Network of Forensic Science Institute“ (ENFSI) und wird als herausragende Institution für forensische Wissenschaft in den Bereichen Schusswaffen, Daktyloskopie, DNA, Chemie und Toxikologie angesehen.

Zur Erweiterung des Aufgabenspektrums IT-Forensik wurde das C4 ausgewählt, um mit seiner Expertise bei Aufbau, Organisation, Ausbildung und Ausstattung des IT-Forensik-Bereiches zu beraten und unterstützen. Zu den Ergebnissen zählen:

- Schaffung eines Langzeittraining-Programmes für IT-Forensik
- Entwicklung eines „Training of Trainers" Programmes
- Erstellung eines Trainingshandbuches mit konkreten Übungsbeispielen
- Trainingseinheit für zwei kroatischen Forensik Experten durch zehn Wochen Einsatz im C4

http://www.enfsi.eu

Maßnahmen im BK

Drogenhandel im Darknet

Der illegale Drogenhandel im Darknet gewinnt zunehmend an Bedeutung. Das unter österreichischer Führung mit deutscher Partnerschaft laufende EU-geförderte Projekt „Joint investigation to combat drug trafficking via the virtual market (Darknet) within and also into the EU" zeigt seine Stärken in der dem neuen Modus operandi angepassten Bekämpfungsstrategie. Diese zeigt sich in der speziellen Teamzusammenstellung: Drogenermittler arbeiten eng mit IT-Expertinnen und Experten zusammen.

Die Drogenermittler bringen ihr Fachwissen bezüglich Suchtmittel und Täterverhalten ein, die IT-Expertinnen und -Experten gewährleisten eine professionelle Datensicherung zur Anklageerhebung, verfolgen Flüsse virtuellen Geldes, wie Bitcoins, und lassen aktuelles Wissen auf dem Gebiet Cybercrime in laufende Ermittlungen einfließen.

Neben den operativen Schwerpunkten des Projektes ist es auch dessen Aufgabe, internationale Kontakte zu erweitern und vor allem für Bewusstseinsbildung zu sorgen. Ein Verständnis für die vorliegende Problematik ist vor allem einer effektiven Zusammenarbeit zwischen Polizei und Justiz dienlich. Während der nun 18-monatigen Projektlaufzeit wurden eine internationale Konferenz mit allen EU-Staaten, Beitrittskandidaten und Drittländern, Europol, Eurojust, Interpol, der Europäischen Drogenbeobachtungsstelle und den Vereinten Nationen (UNODC) abgehalten. Ergänzend dazu fanden neun operative Meetings in den verschiedensten Ländern statt, bei denen aktuelle Ermittlungsfälle besprochen und auf deren Basis Festnahmen und Sicherstellungen durchgeführt wurden. Im Zuge der Projektaktivitäten wurden bislang 37 Staaten aktiv eingebunden.

Obwohl statistische Daten erst mit Projektende erwartet werden, zeigen derzeitige Ermittlungen, dass die Dimension von Aktivitäten, Umsätzen und gehandelten Drogen beachtlich ist: So wurden in einem Ermittlungsfall im Laufe eines Jahres 14.000 Bestellungen und 6.000 Konsumentinnen und Konsumenten registriert. Innerhalb von 16 Monaten wurden 4,4 Millionen Euro umgesetzt. Dass es sich bei den im Darknet operierenden Kriminellen keinesfalls nur um „kleine Fische" handelt, zeigen die Strafausmaße gerichtlicher Verurteilungen. In einem der jüngsten Ermittlungsfälle wurden Freiheitsstrafen von vier und fünfeinhalb Jahren verhängt.

Ermittlungen gegen Kinderpornografie

Bereits im Jahr 1998 wurde im BK die Meldestelle für Kinderpornografie und Kindersextourismus eingerichtet, an die Bürgerinnen und Bürger auch anonym Hinweise richten können. Alleine im Jahr 2015 gingen hier 2.742 Hinweise ein, wobei 310 Meldungen auch einen Österreichbezug aufwiesen.

Im letzten Jahr gab es zahlreiche erfolgreiche Amtshandlungen, bei denen sexuelle Missbräuche an Kindern geklärt und umfangreiches Beweismaterial sichergestellt werden konnte.

- Österreich war beispielsweise an der internationalen Operation „Pacifier" in Zusammenarbeit mit Europol beteiligt. Hintergrund waren Ermittlungen wegen des Besitzes und der Verbreitung pornografischer Darstellungen Minderjähriger. Es konnten 50 IP-Adressen aus Österreich ausgewertet und unzählige kinderpornografische Dateien sichergestellt werden.
- Im Fall eines deutschen Staatsangehörigen mit österreichischem Wohnsitz erging ein Hinweis an die Meldestelle, dass über eine Social-Media-Plattform durch einen unbekannten Täter pornografische Darstellungen Minderjähriger hochgeladen wurden. In Zusammenarbeit mit den US-Behörden konnte der Mann nach umfangreichen Ermittlungen ausgeforscht werden. Bei einer Hausdurchsuchung und Auswertung der sichergestellten Datenträger wurde festgestellt, dass der Verdächtige Kontakt zu einem Mittäter auf den Philippinen hatte. Außerdem wurde er auch von den deutschen Behörden wegen des sexuellen Missbrauchs von Unmündigen per Haftbefehl gesucht.

SOKO Mozart

Im Jahr 2013 wurde im BK die Sonderkommission Mozart eingerichtet. Ihr gelang es eine vorwiegend russischsprachige Gruppierung auszuforschen, die seit 2011 Online-Banking-Nutzer in Österreich schädigte. Computer der Opfer wurden mit Schadsoftware infiziert. Die Kriminellen buchten von den Konten der Opfer Beträge zwischen 1.000 und 15.000 Euro ab. Es waren organisierte Täter am Werk, die weltweit agierten und arbeitsteilig vorgingen: So gab es Tätergruppen, die auf das Programmieren der Schadsoftware spezialisiert waren. Andere wiederum befassten sich mit dem Aufbau von Bot-Netzen. Eine weitere Gruppierung war mit Geldwäscherei beschäftigt. Aufgrund der internationalen Komponente der Ermittlungen wurde über Initiative von Österreich unter Führung der Staatsanwaltschaft Wien ein Joint Investigation Team (JIT) gegründet. Dieses bestand aus den Ländern Belgien, Finnland, Großbritannien, Norwegen und der Niederlande. Die Leitung des Ermittlungsteams übernahm Österreich, der Support erfolgte durch Eurojust und Europol. Es handelt sich um das bislang größte JIT Europas.

Aufgrund der Vielzahl der an diesen Verbrechen beteiligten Täter wurden vom Ermittlungsteam „Maintargets", primäre Ziele, ausgewählt. Jedes Teilnehmerland spezialisierte sich im Laufe der Ermittlungen auf eine oder mehrere dieser Ziele. Die Spuren zu den Identitäten der Täter sowie die Spuren zu deren Straftaten wurden zu einem Großteil von Österreich aus identifiziert und an Europol sowie an die Ermittlungspartner übermittelt.

Im Laufe der Ermittlungen kam es zu zahlreichen operativen Einsätzen wie zum Beispiel in den Niederlanden, in der Ukraine, in Lettland und in den USA. Österreich selbst konzentrierte sich auf die kriminelle Organisation, die mit der Geldwäscherei beschäftigt war. Die Täter schufen mindestens 40 Scheinfirmen im Internet und warben weltweit über diese Scheinfirmen Tausende meist nichtsahnende Personen an. Diese Personen waren im Glauben, für eine tatsächlich existierende Firma Tätigkeiten in Heimarbeit zu leisten. Zumeist wurden auf deren private Girokonten Gelder überwiesen, die abzuheben und über Geldüberweisungsdienste weiterzuleiten waren. Dass diese Gelder aus Online-Banking-Betrügereien stammten, erfuhren die Ahnungslosen erst, als sie von der Polizei zu den Sachverhalten befragt wurden. Ebenfalls wurden Tausende Personen dazu gebracht, Pakete zu empfangen und weiterzuleiten. In diesen Paketen befanden sich Waren, die mit gestohlenen Kreditkartendaten eingekauft wurden.

Die österreichischen Ermittler konnten sowohl die gesamte Struktur als auch den Kopf der Gruppierung identifizieren. Über Rechtshilfe wurden Mitte Juni 2015 in fünf verschiedenen Städten der Ukraine neun Hausdurchsuchungen gegen sieben verschiedene Personen durchgeführt. Es konnten mehr als 13 Terabyte Datenmaterial sichergestellt und ausgewertet werden. Die verdächtigen Personen zeigten sich sofort geständig. Der Schaden, den diese Gruppe weltweit angerichtet hat, wird auf ca. 50 Millionen Euro geschätzt.

Wissenswertes

Automatisierte Malware-Analyse

War es früher relativ einfach Malware zu analysieren, stellt die zunehmende Professionalisierung der Hersteller zunehmend höhere Anforderungen an IT-Foresniker der Polizei. Der Begriff Malware umfasst sämtliche Computerprogramme, die entwickelt wurden, um schädliche und unerwünschte Funktionen auf Computersystemen durchzuführen. Dazu zählen unter anderem Viren, Würmer, Trojaner und die derzeit sehr häufig auftretenden Varianten von Ransomware wie z. B. Cryptolocker. Gemäß Schätzungen kommen derzeit etwa 20.000 neue Schadprogramme pro Tag hinzu, von denen lediglich ein Bruchteil zeitnah von Antiviren-Programmen erkannt werden kann.

Wurde Schadsoftware lange über E-Mails verteilt, werden nun immer öfter nur noch Links zu infizierten Seiten oder zu schädlichen Dateien in der Cloud verteilt, um Virenscanner und Schutzmechanismen zu umgehen. Häufig erfolgt die Infektion durch Drive-by-Downloads oder das Ausnutzen veröffentlichter Sicherheitslücken von Anwendersoftware.

Moderne Malware baut nach dem Start in den meisten Fällen Verbindungen zu anderen infizierten Rechnern oder zentralen Steuerungssystemen, wie Command and Control Servern, auf und verbindet Hunderte bis mehrere Tausend betroffene Computersysteme zu komplexen BotNets. Diese können dann zum Beispiel zur Ausführung von Denial-of-Service-Attacken genutzt werden, indem die verfügbare Bandbreite aller Computer gebündelt wird. Die Kommunikation zwischen den Endgeräten erfolgte früher unverschlüsselt und konnte leicht zurückverfolgt werden. Moderne Systeme setzen jedoch auf Verschlüsselung und Kommunikation über das Darknet, wodurch die Analyse erschwert wird.

Im C4 wurde daher eine automatisierte Malware-Analyse-Plattform eingerichtet, die eine Voranalyse aktueller Bedrohungen ermöglicht. Die Ausführung der Schadsoftware erfolgt dabei in einer isolierten Umgebung. Durch sogenannte „Anti-Sandbox-Technologien“ kann moderne Malware erkennen, dass sie in einem Analysesystem ausgeführt wird. Deshalb werden im C4 „echte“ Computer und keine virtualisierten Umgebungen eingesetzt. Vor der eigentlichen Analyse erfolgt ein Abgleich mit Datenbanken, in denen bereits analysierte Malware und deren Identifizierungsmerkmale („Hashes“, „Mutexes“ etc.) gespeichert sind. Ist die Schadsoftware noch nicht bekannt, startet die Analyse. Neben der Dokumentation welche Prozesse gestartet werden, ob neue Dateien am System abgelegt werden, ob Änderungen an der Registry durchgeführt werden und ob sensible Benutzerdaten abgefangen werden, wird noch eine Vielzahl anderer Parameter überprüft. Besonderes Augenmerk wird dabei auf den Netzwerkverkehr gelegt, der über den gesamten Zeitraum der Ausführung mitgeschnitten wird. Sollte die Kommunikation verschlüsselt erfolgen, wird versucht, diese über verschiedene Techniken trotzdem lesbar zu machen.

Nach Abschluss der Analyse wird die physische Maschine wieder in einen „sauberen“ Zustand zurückgesetzt, um für die nächste Analyse wieder eine virenfreie Umgebung zu gewährleisten.

Die Ergebnisse der Auswertung stehen danach sowohl dem Forensik- als auch dem Ermittlungsbereich in mehreren Formaten zur Verfügung.

Für die Zukunft ist geplant, die Analyse-Software weiter auszubauen und sowohl an die laufend neuen Anforderungen als auch an Erkenntnisse und gewonnenen Erfahrungen anzupassen.

Beweissicherung und Analyse

Da IT-Medien in Kriminalfällen immer öfter eine Rolle spielen, ist deren Auswertung durch IT-Forensiker des C4 erforderlich. Amtshandlungen wie die Flüchtlingstragödie auf der Ostautobahn sowie die terroristischen

Aktivitäten innerhalb Europas sorgten 2015 für entsprechende Herausforderungen innerhalb der elektronischen Beweismittelsicherung. Die Geräte mussten dabei großteils unter schwierigsten Bedingungen zerlegt und ausgewertet werden, um ein verwendbares Ergebnis zu erzielen.

Smartphones und Tablet-PCs sowie Smart-Watches oder Minicomputer wie Raspberry Pi gewinnen immer mehr an Bedeutung für kriminalpolizeiliche Ermittlungen. Während die Geräte immer kleiner werden, steigt hingegen deren Kapazität. Auch im Jahr 2015 wurden bei Amtshandlungen Datenmengen im dreistelligen Terabyte-Bereich sichergestellt und ausgewertet.

2015 wurde besonders auf die Sicherung und Auswertung von Audio-, Video- und Bildmaterial sowie von Fahrzeugen Augenmerk gelegt. Durch eine bessere Aufbereitung und Auswertung von Bild- und Tonmaterial konnten bei der Aufklärung schwerer Verbrechen immer wieder wesentliche Beiträge geleistet werden, die letztendlich zur Ausforschung der Täter führten.

Bei beiden Bereichen handelt es sich um Zweige der Digitalforensik. Besonders im Bereich der Fahrzeugforensik wurde Ausrüstung gekauft, die entscheidend zum Ermittlungserfolg beitrug.

Neben Erfahrung und Know-how ist eine adäquate Ausstattung maßgeblich für eine erfolgreiche Datensicherung und Auswertung. Vor allem die großen Datenmengen können mit herkömmlichen forensischen Mitteln kaum noch bewältigt werden. 2015 kamen neue Suchtechnologien zum Einsatz, die mittels mathematischen Verfahren dabei helfen beweisrelevante Daten zu finden.

Die Bearbeitungsprozesse und Auswertezeiten haben sich stark verändert: Während der Auslesevorgang bei einem Mobiltelefon im Jahr 2007 noch bei rund 15 Minuten lag, nimmt ein zeitgemäßes Smartphone eine Auslesezeit von bis zu einem ganzen Tag in Anspruch. Dabei handelt es sich lediglich um die Sicherung der Beweismittel. Der eigentliche Bearbeitungsprozess hängt von vielen weiteren Faktoren wie dem Zustand des Endgerätes, der Kompatibilität, der manuellen Sicherung etc. ab. Zeitintensiv gestaltet sich auch die Analyse von Schadprogrammen auf Android-Geräten sowie die Auswertung von Navigationsgeräten, da diese zumeist nicht von den kommerziellen Auswerteprodukten unterstützt und manuell mit hohem Aufwand untersucht werden müssen.

Prävention und Information

Das World Wide Web bietet Kriminellen unzählige Möglichkeiten, unvorsichtige Menschen zu ihren Opfern zu machen. Meistens bringen die Täter ihre Opfer durch Vortäuschung falscher Tatsachen dazu, Geld oder sensible Daten herauszulocken oder sexuelle Handlungen durchzuführen. Die Beamtinnen und Beamten der Kriminalprävention stehen auch in diesem Bereich beratend zur Verfügung und setzen den Schwerpunkt auf verhaltensorientierte Maßnahmen.

Vor allem durch Informationen über PC-Sicherheit, Passwortsicherheit und sicheres Internetsurfen kann Schaden vermieden werden. Bei speziellen Fragen zum Thema Computerkriminalität können sich Bürgerinnen und Bürger sowie Unternehmen direkt an eine der Kriminalpräventionsstellen in ganz Österreich wenden. Diese stehen kostenlos und neutral unter der Nummer 059 133 für eine kompetente Beratung zur Verfügung.

Tipps der Kriminalprävention gibt es auch auf der Facebookseite und Homepage des BK sowie in der Polizei App, die gratis zum Download für Apple, Android und Windows Systeme zu Verfügung steht.

Die Facebook Seite des Bundeskriminalamtes hält bei 45.573 „Likes", die Polizei App wurde 198.833 Mal heruntergeladen.

www.facebook.com/bundeskriminalamt
www.bundeskriminalamt.at
http://www.bmi.gv.at/cms/BMI/sicherheitsapp/

Ältere Menschen erhalten in der Seniorenbroschüre „Sicher in den besten Jahren" Information über „Sicher im Internet".

Die Expertinnen und Experten des Bundeskriminalamts beteiligen sich an Veranstaltungen wie zum Beispiel bei jenen des Kuratoriums Sicheres Österreich (KSÖ) und der Wirtschaftskammer Österreich (WKO) und unterstützen Initiativen wie „SaferInternet" und den „Internetombudsmann", um das Verständnis für die Gefahren, die mit der Verwendung des Internets und der sozialen Medien verbunden sind, zu verbessern.

www.wko.at
https://kuratorium-sicheres-oesterreich.at/
www.saferinternet.at
www.internetombudsmann.at

Jugendpräventionsprojekte

Besondere Aufmerksamkeit bei der Präventionsarbeit wird auf die Arbeit mit Jugendlichen gelegt, die mit dem Internet und mit sozialen Medien aufwächst. Im Vordergrund steht das Projekt „Click & Check", das österreichweit sehr erfolgreich umgesetzt wird. Um eine möglichst hohe Nachhaltigkeit zu gewährleisten, werden Eltern und Unterrichtende in das Projekt einbezogen. Eigens geschulte Polizeibeamtinnen und -beamte klären Jugendliche in den Schulen über Happy Slapping, Cyberbullying und Cybermobbing auf, um unter Einbeziehung kurzer Videofilme das Unrechtsbewusstsein von Jugendlichen zu fördern und Gesetzesinformationen zu vermitteln. Im Jahr 2015 wurden österreichweit 52.155 Kinder und Jugendliche über den richtigen, sicheren Umgang mit Handy und PC sensibilisiert und informiert.

Weiterhin wurde im Jahr 2015 die Informationskampagne „Jugend OK!" fortgesetzt. Dabei steht das Thema „Cyber-Grooming" Vordergrund. 12.772 Jugendliche konnten mittels Informationskarten zu den Gefahren im Umgang mit modernen Kommunikationsmitteln informiert werden.

Um eine möglichst umfassende Aufklärungsarbeit auf dem Gebiet der Computerkriminalität gewährleisten zu können, muss die Ausbildung der auf diesem Gebiet tätigen Präventionsbeamtinnen und Präventionsbeamten laufend auf dem aktuellen Stand gehalten werden. Im Jahr 2015 nahmen 47 Beamtinnen und Beamte am Weiterbildungsseminar zur Internetkriminalität teil. Die etwa 330 Vortragenden des Projektes „Click & Check" wurden 2015 mit 25 Bediensteten verstärkt.

www.clickundcheck.at

Präventionstipps „Sicher im Netz"

1. Schutz des PC
An oberster Stelle steht eine gute Sicherheitsausstattung für Ihren Computer. Um den PC vor schädlichen Dateien zu schützen, sollten vor der ersten Nutzung des Internets ein Anti- Viren-Programm und eine Firewall installiert werden. Für diese Schutzprogramme, das Betriebssystem und den Internet-Browser werden regelmäßig Updates angeboten, die auch automatisiert abgerufen werden können. Es wird empfohlen, diese Updates umgehend zu installieren. Das gilt auch für auf dem PC installierte Anwendungsprogramme. Da Schadsoftware zunehmend über externe Datenträger wie CDs oder USB-Sticks verbreitet wird, sollten diese vor der Nutzung auf Viren geprüft werden.

2. E-Mails und Chat
Öffnen Sie nur E-Mails, die von vertrauenswürdigen Absendern stammen. Dubiose Mails von Unbekannten möglichst sofort löschen. Schadprogramme verbergen sich oft in Grafiken oder E-Mail-Anhängen. Verdächtige Dateien sollten Sie auf keinen Fall öffnen! Vorsicht auch vor angeblichen E-Mails von Kreditinstituten: Banken bitten Kunden nie per E-Mail, vertrauliche Daten bekannt zu geben. Auch in Communitys empfangene E-Mail-Anhänge sollten mit einem Schutzprogramm überprüft werden. Riskant können auch Chat-Nachrichten von Unbekannten sein: Kriminelle versenden oft Links zu Webseiten mit Viren. Das Aufrufen dieser Seiten installiert Ihnen möglicherweise eine Schadsoftware (Malware).

3. Software
Achten Sie darauf, welche Software oder Zusatzprogramme („Plug-Ins") Sie installieren. Eine Gefahr sind Schadprogramme, die in Gratis-Downloads oder Raubkopien von dubiosen Anbietern versteckt sind. Gesundes Misstrauen hilft: Wenn Zweifel an der Seriosität bestehen, besser auf Download und Installation einer Software verzichten.

4. Tauschbörsen
Wer im Internet mit Unbekannten Dateien tauscht, riskiert eine Infektion seines PCs mit Schadprogrammen. Zudem ist der Tausch von urheberrechtlich geschützten Musik-, Film- oder Software-Kopien strafbar und kann gegebenenfalls neben Geld- und Freiheitsstrafen zu Schadenersatzansprüchen der Rechteinhaber führen.

5. Online-Shopping
Zeichen für die Seriosität eines Online-Shops sind ein Impressum mit Nennung und Anschrift der Firma, des Geschäftsführers oder einer Umsatzsteuer-Identifikationsnummer (UID- Nummer) sowie klare Geschäftsbedingungen (AGB). Kunden sollten auch die Datenschutzerklärung lesen. Manche Shops werden von unabhängigen Experten geprüft und erhalten ein Zertifikat oder Siegel. Auch der Kunde kann Kontrolle ausüben: Auf vielen Shopping-, Preisvergleich- und Auktionsseiten werden Händler beurteilt. Gute Bewertungen können ein Hinweis auf seriöse Geschäftspraktiken sein. In jedem Fall ist jedoch eine Portion gesundes Misstrauen angebracht – vor allem auf Webseiten mit Angeboten weit unter dem tatsächlichen Wert. Weiterführende Informationen sowie „nicht zu empfehlende Webseiten" bieten die verschiedenen nationalen und internationalen Konsumentenschutzorganisationen
(www.europakonsument.at).

6. Bezahlung im Web
Beim Kauf von Waren im Internet ist allgemein Vorsicht geboten, insbesondere bei Vorauszahlung. Zur Bezahlung sollten Konto- oder Kreditkartendaten über eine verschlüsselte Verbindung übertragen werden, erkennbar an den Buchstaben „https" in der Adresszeile der Webseite und einem Schloss- oder Schlüssel-Symbol im Internet-Browser. Sichere Webseiten sind auch an einer grün hinterlegten Adresszeile oder an einem grün hinterlegten Zertifikatszeichen erkennbar, wenn sich der Betreiber einer unabhängigen Prüfung unterzogen hat. Zahlungen können per Lastschrift, Kreditkarte oder Rechnung erfolgen. Es gibt auch seriöse Bezahldienste bei denen die Bankdaten einmalig hinterlegt werden. Vorkasse per Überweisung ist zwar weit verbreitet, gilt aber generell als sehr viel riskanter.

7. Online-Banking
Beim Online-Banking sollte man die offizielle Adresse der Bank immer direkt eingeben oder über eigene Lesezeichen, so genannte Favoriten, aufrufen. Maßgeblich ist die Adresse, die die Bank in ihren offiziellen Unterlagen angibt. Die Verbindung zum Bankcomputer muss wie bei Bezahlvorgängen verschlüsselt sein (erkennbar an den Buchstaben „https" in der Adresse der Webseite). Für Überweisungen und andere Kundenaufträge sind Transaktionsnummern (TANs) nötig. In den Anfängen des Online-Bankings konnten die Nutzer einen solchen Code aus einer Liste frei wählen. Sicherer ist das iTAN-Verfahren, bei dem die Codes nummeriert sind. Ein Zufallsgenerator der Bank bestimmt, welche TAN eingegeben werden muss. Noch weniger Chancen haben Kriminelle beim mTAN-Verfahren: Die TAN wird dem Kunden aufs Handy geschickt und ist nur kurzzeitig gültig. Weitere Schutzverfahren sind eTAN und HBCI, bei denen der Kunde als Zusatzgeräte einen TAN-Generator oder ein Kartenlesegerät nutzt. PC-Nutzer sollten ihre Bank fragen und das modernste verfügbare Verfahren wählen.

Vorsicht gilt, falls mehrere Transaktionsnummern auf einmal abgefragt werden: Dann ist Phishing im Spiel. Phishing ist eine Art von Diebstahl persönlicher Daten über das Internet. Über E-Mails oder betrügerische Webseiten wird versucht, persönliche Daten oder Informationen wie Kreditkartennummern, Kennwörter, Kontodaten usw. abzufragen.
In diesem Fall informieren Sie bitte sofort Ihr Bankinstitut.

8. Private Infos, Fotos und Passwörter
Die meisten Menschen würden im Alltag kaum Unbekannten ihr Privatleben offenbaren. Dies gilt besonders im Umgang mit privaten Fotos und persönlichen Daten, wie z. B. Telefonnummern oder Wohnadressen. Einmal veröffentlicht, können Fotos zum Beispiel für Mobbing, Erpressung oder andere Deliktemissbraucht werden. Auch im Web haben es die Nutzer in der Hand, den Zugang zu privaten Infos zu beschränken. Nur gute Bekannte sollten in entsprechenden Foren und Communitys Zugriff auf Fotos oder Kontaktdaten erhalten. Je weniger von der eigenen Privatsphäre frei zugänglich ist, desto weniger Angriffsfläche wird potenziellen Tätern und anderen unbefugten Nutzern geboten. Seien Sie bei der Weitergabe Ihrer E-Mail-Adresse oder bei der Eintragung Ihrer Daten in Internetformulare vorsichtig. Gehen Sie immer davon aus, dass Ihre Daten weitergegeben und missbraucht werden können.

Bei vielen Online-Services müssen sich die Nutzer registrieren. Meist werden Benutzername und Passwort festgelegt. Soweit möglich, verwenden Sie nicht das gleiche Passwort für mehrere Dienste – etwa E-Mail-Konto, Online-Shops und Communitys. Je länger ein Passwort ist, desto schwerer ist es zu knacken. Es sollte mindestens acht Zeichen lang sein und aus einer zufälligen Reihenfolge von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Ein solches könnte leicht erstellt werden, indem sich der Benutzer einen Satz überlegt und von jedem Wort den ersten Buchstaben sowie alle Zahlen und Sonderzeichen verwendet. (zum Beispiel der Satz: „Ich bin am 1. Jänner 1970 geboren." ergäbe das Passwort: Iba1.J1970g.) Speichern Sie keine Passwörter (PIN, TAN...) auf dem PC. Mitarbeiter von Banken werden Sie nie nach Zugangsdaten fragen. Anfragen per E-Mail kommen in der Regel ausschließlich von Betrügern.

9. Angebote als Waren- oder Finanzagenten
Angebote im Internet oder per E-Mail als Waren- oder Geldvermittler zu arbeiten, sind konsequent abzulehnen. Der Vermittler dient den Tätern zur Verschleierung ihrer Identität. Web-Nutzer, die sich auf dubiose Angebote einlassen und Waren oder Gelder weiterleiten, betreiben Beihilfe zum Betrug oder zur Geldwäsche und müssen mit strafrechtlichen Folgen und Schadenersatzansprüchen rechnen.

10. Apps und Abofallen
Seien Sie sich bewusst, dass Apps Kosten verursachen sowie sensible Nutzerdaten übertragen können. Dies kann oftmals passieren, ohne dass diese für die Funktion der Apps notwendig sind. Installieren Sie daher nur Apps über die offiziellen App-Shops, da diese überprüft bzw. bei Problemen mittels Fernlöschung von Ihrem Handy entfernt werden. Seien Sie besonders bei kostenlosen Apps vorsichtig.

Achtung geboten ist zudem bei Online-Diensten, bei denen eine Registrierung erforderlich ist. Neben der breiten Masse der seriösen Werbeangebote gibt es auch Fallen, bei denen versteckt Bestellungen oder Abo-Verträge abgeschlossen werden. Die Nutzer werden dabei nicht ausreichend über die Vertragsbedingungen und Preise informiert. Oft wird dies erst im Nachhinein bemerkt, wenn Rechnungen bzw. Inkassoschreiben eingehen. Hilfestellung hierbei bietet einerseits die „Watchlist-Internet" des Internetombudsmannes, andererseits fungiert dieser auch als außergerichtliche Schlichtungsstelle in Streitfragen. Im Internet zu finden unter www.ombudsmann.at

Für die Meldung verdächtiger Sachverhalte im Internet steht die Internetmeldestelle im Bundeskriminalamt against-cybercrime@bmi.gv.at zur Verfügung.

Weitere Information sind auf jeder Polizeiinspektion sowie auf der Homepage www.bmi.gv.at/praevention und per BMI-SicherheitsApp erhältlich.

Die Spezialisten der Kriminalprävention stehen kostenlos und österreichweit unter der Telefonnummer 059133 zur Verfügung.

Ausblick

Das Internet hat sich im Laufe der Jahre immer mehr zu einem Experimentier- und Aktionsfeld verschiedenster krimineller Aktivitäten und Gruppen entwickelt, wobei nicht nur ein starkes Ansteigen der Delikte mit IT-Bezug sondern auch eine stetige Perfektionierung der Angriffsmethoden zu beobachten ist.

„Smarte" Kriminelle sind heutzutage Cyber-Kriminelle mit einem grenzenlosen Betätigungsfeld, die von überall in der Welt ihre Aktivitäten starten können, ohne mit ihren Opfern in eine besondere Nahebeziehung treten zu müssen. Nationale Grenzen, Anonymisierung und Verschlüsselung helfen ihnen dabei, sich einer etwaigen Strafverfolgung zu entziehen.

Technisches Wissen – wie in der Vergangenheit notwendig – brauchen Täter heute kaum noch, gibt es doch kriminelle Dienstleister, die sie bei ihren Aktivitäten unterstützen. Dieser neue Trend wird als „Crime-as-a-service" beschrieben. Daneben agieren Tätergruppen, die mit größter Professionalität und exzellentem technischen Know-how komplexe Angriffe auf Unternehmen und Institutionen durchführen. Die dabei möglichen Schäden sprengen die Dimensionen herkömmlicher Straftaten bei weitem, wie ein Angriff auf die Zentralbank von Bangladesch mit einer beabsichtigten Schadensumme von fast einer Milliarde US-Dollar belegt.

Cybercrime bleibt ein boomendes Kriminalitätsfeld. Besonders der leichte Zugang zu Schadprogrammen via Darknet und deren Anwenderfreundlichkeit verstärken diesen Trend. Diese Entwicklung ist aus polizeilicher Sicht besonders alarmierend. Die Errichtung des C4 im BK sowie die rasche und zeitlich begrenzte Errichtung von speziellen Ermittlungsgruppen waren wichtige Schritte, um auf diese Entwicklungen zu reagieren. Dennoch sind für die Zukunft noch weitere Anstrengungen notwendig. Insbesondere aufgrund der ständig steigenden Zahl an unterschiedlichen Hard- und Softwareprodukten sowie deren allumfassender Vernetzung.

Cybercrime ist die wohl internationalste und mobilste Kriminalitätsform überhaupt. Binnen Sekunden können Täter sowohl den Handlungsort als auch den Standort ihrer virtuellen Infrastruktur in andere Länder oder sogar Kontinente verlagern. Im Bereich der Strafverfolgung ist daher eine weitere Verstärkung der internationalen Kooperation angesagt. Darüber hinaus muss eine weltweit vergleichbare Strafbarkeit für Cyberdelikte existieren, damit es für Cyber-Kriminelle zukünftig keine sicheren Häfen mehr gibt. Eine internationale Vernetzung zwischen spezialisierten zentralen Kontaktstellen im polizeilichen Bereich ist in vielen Staaten bereits Realität, nicht zuletzt durch das Engagement von Organisationen wie Interpol und Europol.

Summary

Facts and Figures

In 2015 complaints have increased by 11.6 percent to 10,010 reported cases in the field of cybercrime. The detection rate was at 41.5 percent in 2015, with only 0.7 percentage points above the one of 2014, which could indicate both the expanding professionalisation of criminal groups as well as their greater use of encryption and anonymisation techniques.

While core cybercrime offenses recorded a decline in filed complaints by 3.3 percent, the complaints related to internet fraud increased by 12.6 percent in the corresponding time frame.

Trends

Also 2015 follows the significant ten-year upward trend whereby the number of filed complaints has stabilised at a high level over the past four years. The on-going digitalisation of everyday life, the increasing use of computers in the form of mobile devices of different types and the expansion of high-speed network connections offer potential offenders an ever growing attack surface.

In particular an increased occurrence of ransomware and DDoS attacks (Distributed Denial of Service) could be observed. During 2014 mainly small and medium enterprises were target of attacks, while now also large companies and individuals are affected. Consequently, this has to be acknowledged as a rising threat.

Counter-measures by the police

The Cybercrime-Competence-Center C4 acts nationally and internationally as the central unit to combat cybercrime in Austria. Comparable services are also established in all Provincial CIDs, in which professionally as well as technically trained experts fulfil their duties on the fight against cybercrime and in the field of computer forensics.

Because of the unstoppable technological progress and the connectivity and digitalisation of objects for everyday use, there is also an increasing demand for highly skilled cybercrime investigation experts and IT forensics experts. To meet this requirement, a customized training system will be provided by the Ministry of the Interior.
The international aspect of cybercrime and the resulting possibilities this provides to offenders strongly contributes to the continuous rise of cyber-attacks. The involvement of the relevant authorities in Austria to international bodies and projects ensures that the various law enforcement agencies have both a continuing strong global network and presence.

The on-going preventive measures and related information given to the general population on the dangers of cybercrime as well as the direct contact with the citizens are key factors to limit and prevent damage caused by cybercrime in Austria.

Outlook

For the future, it is foreseeable that cyber offenses will increasingly merge with traditional offenses and are ever more used as a means for various crimes such as extortion, fraud, harassment etc.. The increase also stems in part from the constantly perfecting methods of attack, the almost limitless fields of activity, and the non-locality of both the potential victims and cybercriminals.
With criminal service providers (Cybercrime as a Service) offering their technical assistance within e.g. the so called darknet, it has to be expected that cybercrime will remain a booming crime field in the upcoming years.

Glossar

Antivirenprogramm: (auch Virenscanner oder Virenschutz genannt) nennt man eine Software, die bekannte Malware wie Computerviren, Computerwürmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt. Die Mehrzahl dieser Programme identifiziert Schadcodes anhand von Signaturen, die dem Hersteller der Software bekannt sein müssen.

Backdoor: ist eine verbreitete Schadfunktion, die üblicherweise durch Viren, Würmer oder Trojanische Pferde eingebracht und installiert wird. Es ermöglicht Dritten einen unbefugten Zugang („Hintertür") zum Computer, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft genutzt, um den kompromittierten Computer als Spamverteiler oder für Denial-of-Service-Angriffe zu missbrauchen.

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" oder „Portemonnaie") 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.

BotNet: Unter einem BotNet oder Bot-Netz (die Kurzform von Roboter-Netzwerk) versteht man einen Verbund von fernsteuerbaren Computersystemen, auf die meist widerrechtlich Zugang verschafft wurde. Die Kontrolle über die einzelnen Systeme wird durch Würmer bzw. Trojanische Pferde erlangt, die dann auf Anweisungen des kontrollierenden Servers warten. Diese Netzwerke können für Spam-Verbreitung, (Distributed) Denial-of-Service-Attacken usw. verwendet werden, zum Teil ohne dass die betroffenen Computersystem-Benutzer etwas davon bemerken.

Bot: Ist ein Überbegriff für ein Programm das vorwiegend verwendet wird, um verschiedene Aufgaben automatisiert durchzuführen. Die Bot-Software nutzt für die Ausführung ihrer Aufgaben die Hardwareressourcen und Internetanbindung des Systems, auf dem sie ausgeführt wird. In der Regel auch als übernommener Rechner bezeichnet, der in ein BotNet eingebunden wurde.

Bot-Herder: Verwaltet und kontrolliert ein BotNet das aus fernsteuerbaren Computersystemen besteht und das bereit ist, beispielsweise DDos-Angriffe zu starten.
Browser: Webbrowser (engl. für „Durchstöberer", „Blätterer") sind spezielle Computerprogramme zum Betrachten von Webseiten im World Wide Web.

C&C-Server: Command and Control Server zumeist übernommen oder unter falscher Identität angemietet, wird er verwendet um Kommandos an das Bot-Netz zu übertragen und den Systemen auf welchen die Bot-Software aufgeführt wird Aufgaben zu übermitteln.

Computervirus: Ein Computervirus ist eine nicht selbstständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt.

Computerwurm: ähnelt einem Computervirus, verbreitet sich aber direkt über Netzwerke wie dem Internet und versucht, in andere Computer einzudringen. Es verbreitet sich zum Beispiel durch das Versenden infizierter E-Mails (selbstständig durch eine SMTP-Engine oder durch ein E-Mail-Programm), durch IRC-, Peer-to-Peer- und Instant-Messaging-MMS.

Cryptolocker: siehe Ransomware

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 Computernamens 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. DDoS: Der zur Blockade führende Angriff wird nicht nur von einem einzelnen Rechner ausgeführt, sondern von mehreren gleichzeitig. Dadurch wird sowohl der Angriff verstärkt als auch die Einleitung der Gegenmaßnahmen erschwert, da diese auf mehrere Quellen angewendet werden müssen.

Exploit (Zero-Day-Exploit): Ein Exploit (englisch to exploit - ausnutzen) ist eine Software oder eine Sequenz von Befehlen, die spezifische Schwächen beziehungsweise Fehlfunktionen eines anderen Computerprogramms ausnutzt. Ein Exploit, das vor oder am selben Tag erscheint, an dem die Sicherheitslücke (Zero-Day-Lücke) allgemein bekannt wird, nennt man Zero-Day-Exploit (0-Day-Exploit). Die Gefährlichkeit dieser Exploits rührt daher, dass zu diesem Zeitpunkt kaum ein Hersteller bzw. Entwickler in der Lage ist, die Sicherheitslücke sinnvoll und umfassend mittels eines Patchs zu schließen.

Firewall: (von engl. „die Brandwand") ist eine Netzwerksicherheitskomponente, die Datenverbindungen anhand eines definierten Regelwerks erlaubt oder verbietet. Das Ziel einer Firewall ist, den Datenverkehr zwischen Netzwerksegmenten abzusichern, indem es unerwünschte Arten der Netzwerkkommunikation verbietet.

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.

Happy Slapping: Unter Happy Slapping versteht man einen körperlichen Angriff auf Personen des näheren Umfelds oder willkürlich ausgewählte Passanten, der durch Veröffentlichung mitgefilmten Materials das Opfer erniedrigen soll.

IMEI: Die International Mobile Equipment Identity (IMEI) ist eine eindeutige 15-stellige Seriennummer, anhand derer jedes GSM- oder UMTS-Endgerät (Mobilstation) eindeutig identifiziert werden kann.

IMSI: Die International Mobile Subscriber Identity (IMSI) dient in GSM- und UMTS-Mobilfunknetzen der eindeutigen Identifizierung von Netzteilnehmern (interne Teilnehmerkennung). Neben weiteren Daten wird die IMSI auf einer speziellen Chipkarte, der so genannten SIM (Subscriber Identity Module), gespeichert. Die IMSI-Nummer wird weltweit einmalig pro SIM-Karte von den Mobilfunknetz Betreibern vergeben. Dabei hat die IMSI normalerweise nichts mit der Telefonnummer der SIM-Karte zu tun. Die IMSI hat immer 15 Zeichen.

Inhaltsdaten: Bezeichnet laut Telekommunikationsgesetz den Inhalt übertragener Nachrichten ohne entsprechende Metadaten.

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. Allen am Internet teilnehmenden Rechnern wird eine IP-Adresse zugeteilt.

Malware: (engl. Malicious "boshaft" und Software) bezeichnet Computerprogramme, die vom Benutzer unerwünschte (schädliche) Funktionen ausführen.

Man-in-the-middle: Der Angreifer steht dabei entweder physikalisch oder – heute meist – logisch zwischen den beiden Kommunikationspartnern und hat dabei mit seinem System komplette Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren. Das Besondere des Angreifers besteht darin, dass er den Kommunikationspartnern das jeweilige Gegenüber vortäuschen kann, ohne dass sie es merken.

Metadaten: Bezeichnet im Gegensatz zu dem Inhalt einer Kommunikation Daten, die die übertragenen (Inhalts-) Daten oder die Art bzw. den Zeitpunkt der Kommunikation beschreiben.

Money Mule: Als Money Mule werden Personen bezeichnet, die von kriminellen Organisationen hauptsächlich zu Zwecken der Geldwäsche eingesetzt werden. Sie sind dafür verantwortlich, Geldbeträge weiterzuleiten, entweder per Überweisung, Botendienst, Post oder ähnlichem. Der Money-Mule erhält für seinen Dienst meist einen fixierten Anteil an dem weitergeleiteten Betrag als Vergütung. Oft wissen die Money-Mules nichts über die Quelle und den Zweck ihrer Tätigkeit, da sie in dem Glauben gelassen werden nur einem „normalen" Nebenjob nachzugehen. Personen, die sich auf derartige Angebote einlassen und Waren oder Gelder aus illegalen Quellen weiterleiten, betreiben Beihilfe (zu Betrug, Geldwäsche, ...) und müssen mit strafrechtlichen Folgen und Schadenersatzansprüchen rechnen.

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.

Pharming: Bezeichnet eine Form von Cyber-Attacken, bei denen der Angreifer versucht, legitimen Netzwerkverkehr zu einer gefälschten Seite umzuleiten. Dies geschieht entweder durch Manipulation der lokalen Namensauflösung oder durch Ausnutzung von Sicherheitslücken bei entfernten DNS-Servern. Namensauflösung ist die Umwandlung von Hostnamen (Beispiel: bmi.gv.at) in die dazugehörende IP-Adresse, über die die eigentliche Kommunikation stattfindet.

Phishing: (engl. fishing = abfischen) 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.

Phreaking: (engl. phone freak = Telefonfreak) bezeichnet das in der Regel illegale Manipulieren von Telefonsystemen. Dabei ging es früher hauptsächlich um die kostenlose Benutzung analoger Telefonleitungen (Bluebox) oder das Nutzen spezieller kostenfreier Rufnummern für Telefontechniker, die über die Verbindungen zu beliebigen Gegenstellen hergestellt werden konnten. Seit der Einführung digitaler Telefonsysteme wird der Begriff aufgrund seiner Bekanntheit oft synonym weiter verwendet.

Port: Bezogen auf Computer-Hardware kann ein Port eine interne oder externe Schnittstelle darstellen, die zur Kommunikation von Hardware mit dem Rechnersystem dient. An externen Schnittstellen werden dabei Geräte in einem vorhandenen Steckplatz oder über eine Kabelverbindung betrieben. Die können zum Beispiel parallele/serielle Schnittstellen für die Verbindung von Laufwerken oder USB-Ports sein. Interne Schnittstellen werden über den sogenannten Input/Output-Bus (I/O-Bus) und Port-Adressen angesprochen. Die Kommunikation erfolgt durch den Hardware-Treiber, der einen Datentransfer ermöglicht, indem ein Zugriff auf die Hardware-Adresse ermöglicht wird. Dies können zum Beispiel Netzwerkkarten sein, mit denen das Betriebssystem kommunizieren muss, nachdem diese mit einer externen Schnittstelle verbunden wurden.

Ransomware: Die Kategorie der sogenannten „Ransomware" bezeichnet bösartige Software, die 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 solchen Situationen jedoch nicht gesichert, dass der Zugriff nach Bezahlung tatsächlich wieder möglich ist.

Rechnernetze: Zusammenschluss mehrerer Rechner, der die Kommunikation über standardisierte Protokolle ermöglicht. Die Übertragung der Daten findet dabei entweder über Kupferkabel, Glasfaserkabel oder Funk statt und wird über Netzwerkkomponenten wie Switches, Router, Hubs, Bridges oder Access-Points abgewickelt.

Netzwerkprotokolle: Sind Kommunikationsprotokolle die den Austausch von Daten zwischen Computersystemen ermöglichen. Ein Protokoll ist eine Sammlung von Regeln und Formaten, die allen Kommunikationspartnern bekannt sein müssen und deshalb durch internationale Organisationen standardisiert sind.

Proxy: (von engl. „proxy representative" = Stellvertreter) arbeitet als Vermittler, der auf der einen Seite Anfragen entgegen nimmt, um dann über seine eigene IP-Adresse eine Verbindung zur anderen Seite herzustellen. Er übernimmt somit stellvertretend für den anfragenden Klienten/Kunden die Kommunikation mit dem Ziel oder leitet einfach die Anfragen unter seinem Namen an das Ziel weiter, ohne die Kommunikation selbst zu führen.

Scamming: Unter Scamming versteht man gutgläubige Opfer zur Geldzahlung zu bewegen, nachdem diese mit Erbschaften, lukrativen Nebenjobs oder Lotteriegewinnen per E-Mail oder Chats angelockt wurden.

Schadprogramme: Schadprogramme sind Computerprogramme die unerwünschte und meist schädliche Funktionen am befallenen Computersystem ausführen. Sie können dabei nur dem Ausspähen des entfernten Systems dienen, offensichtliche Fehlfunktionen hervorrufen oder das System durch Löschen oder Verschlüsseln von Dateien unbrauchbar machen. Ein weiteres Ziel kann das Hinzufügen zu einem Rechnerverbund (BotNet) sein, der anschließend zum Beispiel zum Versand von Spam verwendet werden kann. Schadsoftware kann sich in vielen Fällen selbstständig verbreiten.

Server: Der Begriff Server (engl. to serve = bedienen) bezeichnet entweder eine Software (Programm) im Rahmen des Client-Server-Konzepts oder eine Hardware (Computer), auf der diese Software (Programm) im Rahmen dieses Konzepts abläuft.

Skimming: Skimming ist eine Form des Betrugs, bei dem illegal die Daten von Kredit- und Bankkarten ausgespäht werden. Dabei werden die Daten durch Manipulation von Geldautomaten ausgelesen und auf leere Karten (Rohlinge) kopiert.

Skriptkiddie: Ein Skriptkiddie (von „Skript" und „Kid") ist jemand, der leicht bedienbare, vorgefertigte Programme benutzt, um unerlaubt in fremde Computer- und Netzwerksysteme einzudringen oder durch absichtlich verbreitete Viren, Würmer oder Trojaner Schaden anzurichten. Die Bezeichnung hat Anklänge von unreifem Verhalten und Vandalismus.

Spam: Unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten, die dem Empfänger unverlangt zugestellt werden und massenhaft versandt wurden oder werbenden Inhalt haben. Dieser Vorgang wird Spamming oder Spammen genannt, der Täter Spammer.

Spyware: Damit bezeichnet man Programme die Informationen über die Tätigkeiten des Benutzers sammeln und an Dritte weiterleiten. Ihre Verbreitung erfolgt meist durch Trojaner.

Stammdaten: Darunter versteht man alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind. Dies sind: Familienname und Vorname, akademischer Grad, Wohnadresse, Teilnehmernummer und sonstige Kontaktinformation für die Nachricht, Information über Art und Inhalt des Vertragsverhältnisses und Bonität.

Standortdaten: Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben, sind Standortdaten.

Steganografie: Die Steganografie ist die Wissenschaft der verborgenen Speicherung oder Übermittlung von Informationen.

TAN (M-Tan, E-TAN, I-TAN): Eine Transaktionsnummer (TAN) ist ein Einmalpasswort das im Online-Banking verwendet wird.
- Ein M(obiler)-TAN wird über SMS versandt.
- Der E-TAN ist ein kleines elektronisches Kontrollgerät, dass die (TAN) Eingabe ersetzt. Während der Kunde bisher eine Liste mit Transaktionsnummern hatte, werden über eTAN die Transaktionsnummern in Echtzeit immer wieder neu generiert. Während der Eingabe der Daten bei der Online-Transaktion generiert die Internet-Seite der Bank eine Kontrollnummer, die der Kunde in seine eTAN-Box eingibt. Die eTAN-Box erstellt darauf eine Antwort-Nummer, mit der der Kunde die Transaktion durchführen kann.
- I-TAN oder indizierter TAN: der Kunde wird hier von der Bank aufgefordert eine bestimmte, durch eine Positionsnummer (Index) gekennzeichnete TAN aus seiner Liste einzugeben.

Trojaner: (Trojanisches Pferd) ist eine Kombination eines (manchmal nur scheinbar) nützlichen Wirtsprogramms mit einem versteckt arbeitenden, bösartigen Teil, oft Spyware oder ein Backdoor (Hintertür). Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogramms für seine Installation durch den Benutzer.

Verkehrsdaten: Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden.

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.

VoIP: Unter VoIP (Voice over Internet Protocol) versteht man das Telefonieren über das Internet. Die Sprachdaten werden dabei in digitale Form umgewandelt, in kleinen Datenpaketen über das Internet verschickt und beim Empfänger wieder zusammengesetzt.

Zombie: Beschreibt ein infiziertes Computersystem, das einen Teil eines BotNets bildet und durch C&C-Server kontrolliert wird.

Zugangsdaten: Sind jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind.

Weitere Publikationen 2016

Sicherheit 2015
Geldwäsche 2015
Schlepperkriminalität 2015
Verfassungsschutz 2015
Kulturgutbericht 2015
Präventionsbericht 2015
Menschenhandel 2015
Suchtmittelbericht 2015
Sicherheitsbericht 2015

Kontakt

Bundeskriminalamt
Meldestelle „Against Cybercrime"
Josef-Holaubek-Platz 1, 1090 Wien
Telefax: +43-(0)1-24836-985025
E-Mail: against-cybercrime@bmi.gv.at
Homepage: www.bundeskriminalamt.at
Facebook: www.facebook.com/bundeskriminalamt

Editorial

Bundeskriminalamt
Büro für Presse- und Öffentlichkeitsarbeit
Josef-Holaubek-Platz 1, 1090 Wien
Tel.: +43 (0) 1 24836-985004
E-Mail: BMI-II-BK-1-5-PRESSE@bmi.gv.at

Grafik und Design: ©Bundeskriminalamt/Armin Halm
Druck: Digitaldruckerei des BMI
Herrengasse 7, 1010 Wien
Erscheinungsdatum: November2016

Österreich

Cybersicherheit

Jahresbericht 2015