CYBERCRIME

JAHRESBERICHT 2016

.BK

BUNDESKRIMINALAMT

Zur Online-Version

LIEBE LESERINNEN UND LESER!

Das Thema Cyber-Kriminalität ist eine zentrale Herausforderung der Zukunft sowohl für Wirtschaftsbetriebe, als auch die Bevölkerung im Allgemeinen und auch für die Strafverfolgungsbehörden. Diesem weltweiten Trend kann sich auch Österreich nicht entziehen. Das bestätigen die Zahlen dieses Reports: die Zahl der Anzeigen wegen Cybercrime ist um über 30 Prozent gestiegen. Die Schwierigkeit in der Bekämpfung liegt vor allem darin, dass nicht nur die Zahl der Delikte steigt, sondern die Täter immer raffinierter werden und die Strafverfolgung erschweren.

Das Bundesministerium für Inneres hat sich darauf eingestellt und seine Schwerpunkte auf die Bekämpfung der organisierten Cyber-Kriminalität fokussiert. Wir investieren laufend nicht nur in die Hardware – in die Technik und Ausstattung –, sondern auch in die „Software" – in die Aus- und Weiterbildung der Polizistinnen und Polizisten –, die täglich mit neuen Phänomenen und neuen technischen Errungenschaften konfrontiert werden.

Die Basis unseres polizeilichen Strebens ist und bleibt aber Präventionsarbeit, die wir auch 2016 weiter ausbauen konnten. Im Rahmen des Projekts „CyberKids" treten wir an Kinder ab acht Jahren heran und informieren sie über die Gefahren im Internet und sensibilisieren darauf, achtsam zu sein. Wir vermitteln den Grundschutz, um nicht in die Gefahr zu kommen, Opfer zu werden.

Darüber hinaus steht die Polizei in Österreich für Zusammenarbeit. Es freut uns, dass wir auch im abgelaufenen Jahr wieder zahlreiche Kooperationsprojekte mit der Wirtschaft und der Wissenschaft starten konnten. Diesen Weg werden wir auch zukünftig weitergehen.

Mag. Wolfgang Sobotka
Bundesminister für Inneres

General Franz Lang
Direktor des Bundeskriminalamtes

Dr. Michael Fischer
Stellvertretender Direktor des Bundeskriminalamtes

INHALT

EINLEITUNG 07

ZUSAMMENFASSUNG 08
DATEN UND FAKTEN **08**
MASSNAHMEN **08**
TRENDS **08**
AUSBLICK **09**

ALLGEMEINES 10
RECHTLICHE ASPEKTE **10**

ZAHLEN UND FAKTEN 11

CYBER-PHÄNOMENE 2016 14
RANSOMWARE – DIE DIGITALE ERPRESSUNG **14**
BITCOIN UND VIRTUELLE ZAHLUNGSMITTEL **15**
CYBERCRIME-AS-A-SERVICE (CCaaS) **15**
DISTRIBUTED-DENIAL-OF-SERVICE (DDoS) **16**
INTERNET OF THINGS (IoT) **16**

CYBER-KRIMINALITÄTSBEKÄMPFUNG IN ÖSTERREICH 18
CYBERCRIME-COMPETENCE-CENTER (C^4) **18**
LANDESKRIMINALÄMTER **19**
BEZIRKS-IT-ERMITTLER **19**
POLIZEIINSPEKTIONEN, STADT- UND BEZIRKSPOLIZEIKOMMANDEN **20**

BEWEISSICHERUNG UND ANALYSE 21
FAHRZEUGFORENSIK **21**
MOBILE FORENSIK **22**
VIDEO UND MULTIMEDIA FORENSIK **22**

IT-ERMITTLUNGEN 23
OPERATION „AVALANCHE“ **23**
SOKO CLAVIS **23**

MELDESTELLEN 24
CYBERCRIME **24**
KINDERPORNOGRAFIE UND KINDERSEXTOURISMUS **25**

INTERNATIONALE ZUSAMMENARBEIT 26

PROJEKTE 27
E.V.A **27**
FAHRZEUGFORENSIK **27**
MOBILE FORENSIK **27**
BITCRIME **27**

PRÄVENTION UND INFORMATION 28
KINDER UND JUGENDLICHE **28**

AUSBLICK 30

SUMMARY 31

GLOSSAR 33

EINLEITUNG

Der Cybercrime Report 2016 stellt Entwicklungen der Cyber-Kriminalitätsbekämpfung dar. Darüber hinaus gibt er einen Überblick über die, unter der Führung des Bundeskriminalamtes, gesetzten Maßnahmen. Zusätzlich soll ein Informations- und Präventionsbeitrag geleistet werden.

Nach einem kurzen Überblick über die rechtlichen Rahmenbedingungen folgen Zahlen und Fakten auf Basis der Polizeilichen Kriminalstatistik Österreich.

Der Darstellung einiger Phänomene und Entwicklungen, die sich 2016 besonders hervor getan haben und deren steigende zukünftige Bedeutung, folgt ein Überblick über das Cybercrime-Competence-Center (C^4) im Bundeskriminalamt sowie relevante Projekte.

Einen wichtigen Punkt in der Bekämpfung von Cybercrime nimmt die internationale Zusammenarbeit ein. Außerdem spielt die Bekämpfung der Cyber-Kriminalität auch in den Landeskriminalämtern eine wichtige Rolle. Dazu ist geschultes Personal erforderlich, das derzeit ausgebildet wird.

Weiters werden einige Präventionstipps, Informationen und ein Glossar mit den Definitionen der wichtigsten Begriffe angeboten.

ZUSAMMENFASSUNG

DATEN UND FAKTEN

In Österreich war im Jahr 2016 ein Anstieg der Zahl an Cybercrime-Anzeigen um rund 31 Prozent zu verzeichnen – von 10.010 im Jahr 2015 auf 13.103. Am stärksten gestiegen – mehr als 55 Prozent – ist die Zahl der Fälle, die besonderes technisches Know-how verlangen.

Die Ursachen sind vor allem

- die globale Streuung von Tätern, Tatmitteln (Servern, etc.), Opfern und Geldflüssen,
- die immer stärkere Nutzung des Darknets durch Kriminelle,
- die weltweit steigende Verbreitung von Schadsoftware,
- das mangelnde Gefahrenbewusstsein der Opfer sowie
- die Schwächen in den IT-Systemen – wie zum Beispiel fehlende Sicherheitsupdates.

MASSNAHMEN

Um dem massiven Anstieg von Ransomware entgegenzuwirken,wurde im Juni 2016 die Sonderkommission (Soko) Clavis ins Leben gerufen. In dieser werden alle Ransomware-Fälle von einem speziell zusammengesetzten Expertenteam österreichweit zentral bearbeitet.

Im Bereich der IT-Forensik wurden technologisch neue Fachgebiete auf- und ausgebaut wie insbesondere Fahrzeugforensik und Video- sowie Multimediaforensik. Zur Verbesserung der Ausbildung wurde 2016 mit der Erarbeitung von neuen Ausbildungsprogrammen insbesondere für die Bezirks-IT-Ermittler begonnen. Das Projekt „CyberKids" soll im Endausbau (2018) den Kindern der Altersgruppe von acht bis zwölf Jahren einen sicheren und gefahrlosen Umgang mit dem Internet ermöglichen.

TRENDS

Ransomware bleibt auch weiterhin ganz oben auf der Liste der kriminellen Trends. Hier ist eine zunehmende Spezialisierung auf bestimmte Ziele und Zielgruppen wie Personalabteilungen, Klein- und Mittelbetriebe, usw. feststellbar. Virtuelle Zahlungsmittel wie Bitcoins werden von Kriminellen immer häufiger dazu verwendet, ihre kriminellen Gewinne und Geldflüsse vor den Ermittlungsbehörden zu verschleiern. Das Darknet hat die Entstehung krimineller Dienstleister in Form von „Cybercrime as a Service" begünstigt und beschleunigt. Die Entwickler dieser kriminellen Tools ermöglichen damit etwa die Durchführung von technisch anspruchsvollen Cyber-Attacken für Jedermann.

Eine zunehmende Bedrohung stellt die Verlagerung der herkömmlichen Kriminalität, wie beispielsweise des Drogen- oder Waffenhandels, in das Internet und hier insbesondere in das Darknet dar.

AUSBLICK

Cybercrime ist ein globales Phänomen und kein Land kann sich von diesen weltweiten Entwicklungen abschirmen. Neue Technologien eröffnen dabei für Kriminelle weitere Angriffsziele. Von besonderer Bedeutung wird in diesem Zusammenhang das Internet der Dinge sein. Bis 2020 sollen rund 20 Milliarden Geräte auf diese Weise mit dem Internet verbunden sein. Heute sind es laut einer Schätzung des Marktforschers Gartner (www.gartner.com) bereits 4,9 Milliarden Geräte, die eine Verbindung mit dem Internet haben. Die meisten dieser Geräte sind dabei ungeschützt. Die DDoS-Attacken im Herbst 2016 mit dem „Mirai-Botnet" auf das US-Unternehmen „DynDNS" haben gezeigt, welches Gefahrenpotenzial uns durch das IoT (Internet of Things) – dem Internet der Dinge – erwartet.

Neue Technologien erfordern rechtliche Anpassungen. So müssen neue Tatbestände und neue Ermittlungsmethoden möglichst zeitnah Eingliederung in die Rechtsordnung finden und so formuliert sein, dass sie bei technologischen Änderungen weiter anwendbar bleiben.

Der technologische Fortschritt verlangt von den behördlichen Strukturen eine rasche und innovative Weiterentwicklung. Der Ausbau der bestehenden und der Aufbau neuer Bereiche auf Grund neuer Technologien sowie die Verfügbarkeit von fundiertem technischem Know-how sind die Herausforderungen, die dringend in Angriff genommen werden müssen. Um in Zukunft diese Herausforderungen meistern zu können, werden „state of the art" ausgerüstete und ausgebildete Cybercrime-Einheiten erforderlich sein.

ALLGEMEINES

Ein Anstieg von Cybercrime ist weiterhin weltweit zu verzeichnen, wobei die Angriffsszenarien technisch immer raffinierter werden. Der Fortschritt in der IT verändert auch die Art und Qualität der eingesetzten Tatmittel. Darüber hinaus begünstigen die Möglichkeiten der Anonymisierung, der Verschlüsselung und die unbegrenzte Verfügbarkeit des Internets die Verbreitung von Cybercrime massiv. Die weltweit stark steigenden Zahlen von Ransomware zeigen hier ein deutliches Bild. Die Entstehung krimineller Dienstleister in Form von „Cybercrime as a Service" wurde durch das Darknet massiv begünstigt und beschleunigt. Durch die Entwicklung und den Vertrieb von maßgeschneiderter Schadsoftware ist die Durchführung von Cybercrime-Attacken mittlerweile für jedermann möglich.

RECHTLICHE ASPEKTE

Eine allgemein gültige Definition des Begriffs 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 zwischen Cybercrime im engeren Sinn und Cybercrime im weiteren Sinn unterschieden.

Cybercrime im engeren Sinn beschreibt jene Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden (z.B. Datenbeschädigung, Hacking, DDoS-Attacken).

Unter Cybercrime im weiteren Sinn versteht man Straftaten, bei denen die Informations- und Kommunikationstechnik zur Planung, Vorbereitung und Ausführung für herkömmliche Kriminaldelikte eingesetzt werden, wie z.B. Betrugsdelikte, Kinderpornografie, Cyber-Grooming oder Cyber-Mobbing. Diese Straftaten können praktisch jede Form von Kriminalität annehmen.

Der rasante technische Wandel und immer neue Begehungsformen stellen dabei den Gesetzgeber in rechtlicher Hinsicht vor große Herausforderungen. Mit dem Strafrechtsänderungsgesetz 2015 (Bundesgesetzblatt I Nr. 112/2015) wurden unter anderem auch Cybercrime relevante Bestimmungen eingefügt oder ergänzt, wie z.B. die Definition der kritischen Infrastruktur im § 74 StGB oder die Neufassung von § 118a StGB, wodurch neben Hacking auch Bot-Netzwerke von der Strafbarkeit erfasst werden sollen. Mit dem § 107c StGB (Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems) werden auch diese Handlungen nunmehr unter Strafe gestellt.

ZAHLEN UND FAKTEN

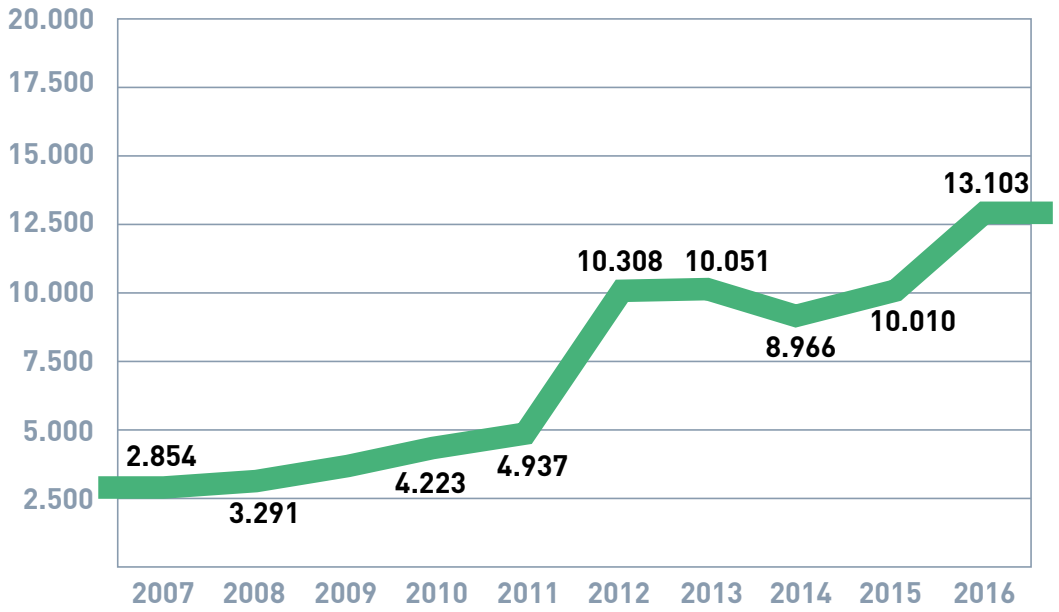


Abbildung 1: Die Entwicklung von Cybercrime in den Jahren 2007 - 2016

Angezeigte Fälle	Jän-Dez 2015	Jän-Dez 2016	Veränderung
§ 118a StGB	387	457	18,1 %
§ 119a StGB	19	42	121,1 %
§ 126a StGB - Vergehen	142	656	362,0 %
§ 126a/V StGB - Verbrechen	2	3	50,0 %
§ 126b StGB - Vergehen	127	249	96,1 %
§ 126b/V StGB - Verbrechen	37	33	-10,8 %
§ 126c StGB	186	234	25,8 %
§ 148a StGB - Vergehen	647	816	26,1 %
§ 148a/V StGB - Verbrechen	13	1	-92,3 %
§ 225a StGB	136	139	2,2 %
Cybercrime im engeren Sinn	**1 696**	**2 630**	**55,1 %**
§ 207a StGB - Vergehen	431	646	49,9 %
§ 207a/V StGB - Verbrechen	34	35	2,9 %
§ 208a StGB	52	80	53,8 %
Internetbetrug	7 473	9 672	29,4 %
Sonstige Straftaten im Internet	324	40	-87,7 %
Cybercrime im weiteren Sinn	**8 314**	**10 473**	**26,0 %**
Cybercrime Gesamt	**10 010**	**13 103**	**30,9 %**

Abbildung 2: Verhältnis der angezeigten Fälle in den Bereichen Cybercrime im engeren und Cybercrime im weiteren Sinn

2016 zeigt Cybercrime mit einem Gesamtanstieg der Zahl der Anzeigen von 30,9 Prozent in fast allen Bereichen eine weiterhin steigende Tendenz (2015: 10.010; 2016: 13.103), wobei die Zahl der Tatbestände von Cybercrime im engeren Sinne österreichweit von 1.696 im Jahr 2015 auf 2.630 und somit um 55,1 Prozent angestiegen ist.

Die Zahl der Tatbestände gemäß § 126a StGB mit einem Anstieg von rund 362 Prozent (+ 514 Fälle) und § 126b StGB mit einem Anstieg von 96,1 Prozent (+ 122 Fälle) sind überdurchschnittlich stark angestiegen. Der Grund für diese Zunahme der Zahl an Anzeigen liegt vor allem in der weltweit steigenden Verbreitung von Ransomware. Der Anstieg der Zahl der Fälle von Cybercrime im weiteren Sinn beträgt 26 Prozent, wobei vor allem der Internetbetrug mit einer Zunahme von rund 2.200 Fällen am stärksten gewachsen ist.

Im Jahr 2016 ist auch die Anzahl von Anzeigen wegen Hacking, dem unbefugten Eindringen in ein Computersystem (§118a StGB), mit einer Zunahme von 70 Fällen stark angestiegen (Plus von 18,1 Prozent).

Aufklärungsquoten	Jän-Dez 2015	Jän-Dez 2016	Veränderung
§ 118a StGB	16,8 %	21,4 %	4,6 % Pt
§ 119a StGB	15,8 %	16,7 %	0,9 % Pt
§ 126a StGB - Vergehen	35,2 %	8,5 %	-26,7 % Pt
§ 126a/V StGB - Verbrechen	50,0 %	0,0 %	-50,0 % Pt
§ 126b StGB - Vergehen	3,9 %	1,2 %	-2,7 % Pt
§ 126b/V StGB - Verbrechen	2,7 %	0,0 %	-2,7 % Pt
§ 126c StGB	19,4 %	17,9 %	-1,5 % Pt
§ 148a StGB - Vergehen	19,5 %	17,6 %	-1,9 % Pt
§ 148a/V StGB - Verbrechen	30,8 %	0,0 %	-30,8 % Pt
§ 225a StGB	90,4 %	88,5 %	-1,9 % Pt
Cybercrime im engeren Sinn	**24,4 %**	**18,0 %**	**-6,4 % Pt**
§ 207a StGB - Vergehen	88,4 %	89,2 %	0,8 % Pt
§ 207a/V StGB - Verbrechen	82,4 %	74,3 %	-8,1 % Pt
§ 208a StGB	57,7 %	72,5 %	14,8 % Pt
Internetbetrug	40,6 %	40,4 %	-0,2 % Pt
Sonstige Straftaten im Internet	83,3 %	75,0 %	-8,3 % Pt
Cybercrime im weiteren Sinn	**45,0 %**	**43,9 %**	**-1,1 % Pt**
Cybercrime Gesamt	**41,5 %**	**38,7 %**	**-2,8 % Pt**

Abbildung 3: Aufklärungsquote in Bezug auf Cybercrime im engeren und Cybercrime im weiteren Sinn

Die Aufklärungsquote bei Cybercrime im engeren Sinn ist um 6,4 Prozent auf 18 Prozent zurückgegangen, was vor allem auf die immer stärkere Nutzung des Darknets durch Kriminelle und die technisch immer anspruchsvoller werdenden Ermittlungen zurückzuführen ist. Insgesamt ist die Aufklärungsquote bei Cybercrime von 41,5 Prozent auf 38,7 Prozent zurückgegangen. Zu den im Bereich Cybercrime angezeigten Fällen 2016 konnten in 5.613 Fällen Tatverdächtige ermittelt werden, die sich in den folgenden Altersklassen wiederfinden.

Ermittelte Tatverdächtige Altersgruppen	Fremde	Inländer	Veränderung
0 - 9 Jahre		1	1
10 - 13 Jahre	7	59	66
14 - 17 Jahre	54	453	507
18 - 20 Jahre	145	284	429
21 - 24 Jahre	231	399	630
25 - 39 Jahre	1 357	1 152	2 509
über 40 Jahre	528	943	1 471
Gesamt	**2 322**	**3 291**	**5 613**

Abbildung 4: Verhältnis der Altersgruppen in Bezug auf Cybercrime zwischen Fremden und Inländern

Bei den Altersgruppen sind vor allem die 25- bis 39-Jährigen mit 2.509 Verdächtigen am stärksten vertreten. In der Gruppe der ab 40-Jährigen gab es 1.471 Verdächtige und in den Altersgruppen von 14 bis 24 Jahren sind 1.566 Verdächtige ermittelt worden, wobei in der Gruppe der besonders jungen Täter im Alter von 14 bis 17 Jahren 507 Verdächtige aufscheinen.

Von den im Zusammenhang mit Cybercrime ausgeforschten 5.613 Tatverdächtigen sind 3.291 Inländer und 2.322 Fremde. Sie stammen vor allem aus Deutschland (815), der Russischen Föderation (232), Nigeria (143), Serbien (111) und Bosnien-Herzegowina (106).

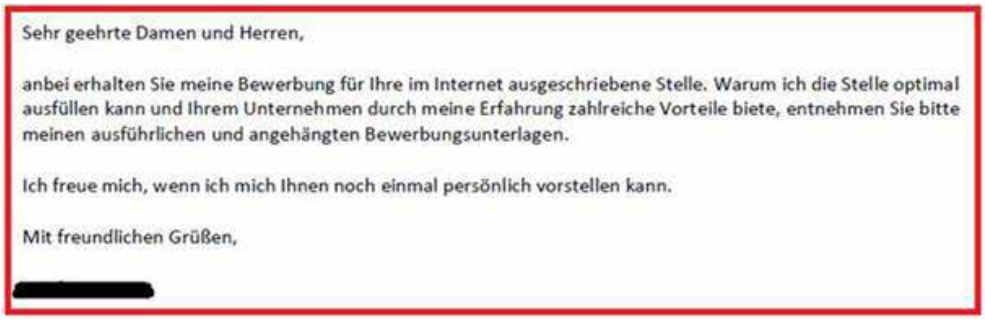
CYBER-PHÄNOMENE 2016

RANSOMWARE – DIE DIGITALE ERPRESSUNG

Ransomware ist ein 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 Lösegeld (englisch: ransom) erpresst, meistens in Form des virtuellen Zahlungsmittels „Bitcoin", das anonym ist und dadurch die Strafverfolgung erschwert. Die Verbreitung der Verschlüsselungssoftware erfolgt insbesondere über präparierte E-Mails, durch Sicherheitslücken in Applikationen oder durch unbewusstes Herunterladen aus dem Internet (drive-by-download). Betroffen sind sowohl Privatpersonen als auch Unternehmen, Behörden und sonstige Organisationen.

Anfang 2016 erfolgte die Verbreitung sehr oft via E-Mails mit Verständigungen über nicht erfolgreich durchgeführte Paketzustellungen. Der Empfänger wurde aufgefordert, um täglich anfallende Gebühren zu vermeiden, den Versandschein über einen Link in der E-Mail, laut angezeigtem Text von der Internet-Seite des mutmaßlichen Versenders, herunterzuladen. Tatsächlich verwies der Link jedoch auf einen anderen Server. Bei der heruntergeladenen Datei handelte es sich um Schadsoftware. Eine abgewandelte Version solcher E-Mails hatte angebliche Rechnungen von Mobilfunkunternehmen oder Energieanbietern zum Inhalt. Hier sollten die potenziellen Opfer oft durch überhöhte offene Beträge zum Herunterladen der Online-Rechnung verleitet werden. Auch in diesen Fällen handelte es sich um Schadsoftware.

Weite Verbreitung fanden auch gefälschte Bewerbungsschreiben: Dabei wurde in den meisten Fällen in einem kurzen Anschreiben mit unterschiedlichen Absendern wie z.B. julian.heyne@aon.at auf weiterführende Unterlagen Bezug genommen. Der Download selbst sollte zumeist von einer Dropbox erfolgen, manchmal war die Schadsoftware auch direkt an die E-Mail angehängt. Der E-Mail-Inhalt erschien glaubwürdig, die Gründe dafür, dass die Bewerbungsunterlagen nicht direkt beigelegt werden konnten, nachvollziehbar, was ein Erkennen des Gefahrenpotenzials enorm erschwerte.


Sehr geehrte Damen und Herren,

anbei erhalten Sie meine Bewerbung für Ihre im Internet ausgeschriebene Stelle. Warum ich die Stelle optimal ausfüllen kann und Ihrem Unternehmen durch meine Erfahrung zahlreiche Vorteile biete, entnehmen Sie bitte meinen ausführlichen und angehängten Bewerbungsunterlagen.

Ich freue mich, wenn ich mich Ihnen noch einmal persönlich vorstellen kann.

Mit freundlichen Grüßen,

[redacted]

Abbildung 5: Beispiel Ransomware

Ransomware macht vor niemandem halt. Besonders kleine und mittlere Unternehmen (KMU) sind in ihrem wirtschaftlichen Fortbestehen stark bedroht. Dabei kann keine Einschränkung auf bestimmte Sparten festgestellt werden. Betroffen waren 2016 Autohäuser, öffentliche und gemeinnützige Betriebe, Getränkehandel, Notare, Rechtsanwälte, usw.

Bei der Bekämpfung von Ransomware hat sich gezeigt, dass nur eine zentrale kriminalpolizeiliche Bearbeitung im Rahmen einer weitgehenden internationalen Kooperation zielführend ist. Aus diesem Grund wurde im Juni 2016 im C^4 die Soko Clavis eingerichtet. Ein hochqualifiziertes Expertenteam aus IT-Technikern, Kriminalbeamten und Bitcoin-Spezialisten hat im Berichtsjahr rund 480 Ransomware-Fälle zentral für ganz Österreich bearbeitet. Von den in Österreich auftretenden, über 30 verschiedenen Ransomware-Arten nahmen vor allem CryptOl0cker, CERBER und Locky die Spitzenreiterrolle ein.

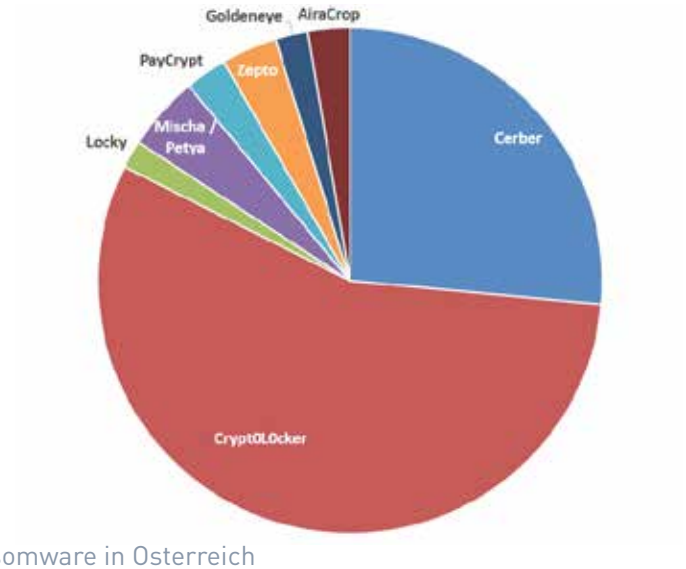


Abbildung 6: Arten von Ransomware in Osterreich

BITCOIN UND VIRTUELLE ZAHLUNGSMITTEL

Sowohl technisch als auch rechtlich stellt die Verwendung von Bitcoins und anderen virtuellen Währungen eine Herausforderung für die Bekämpfung von Cybercrime dar. Die Gewinne und Geldflüsse aus Drogenhandel, Erpressungen und anderen schweren Verbrechen werden bereits überwiegend auf diese Weise transferiert. Darüberhinaus bieten Dienstleister im Internet sogenannte „Bitcoin-Mixer" an, um jegliche Verfolgung der Finanzströme zu unterbinden. Die rechtliche Einordnung von Krypto-Währungen im europäischen Rechtssystem, die Sicherstellung von virtuellen Gewinnen und die Verfolgung der kriminellen Geldströme bedürfen Antworten, die auf internationaler Ebene gefunden werden müssen.

CYBERCRIME-AS-A-SERVICE (CCaaS)

Auch wenn es sich bei Cybercrime-as-a-Service nicht um ein Phänomen, sondern um ein Geschäftsmodell handelt, trägt es zur Steigerung der Computerkriminalität bei. Im Unterschied zu heute mussten die Kriminellen zu Beginn des Aufkommens von Cybercrime den gesamten Ablauf selbst übernehmen: Sie brauchten enormes Fachwissen, um die Schadsoftware zu allererst zu erstellen. Diese Software mussten sie in weiterer Folge an die potenziellen Opfer verteilen und abschließend noch die Geldspuren verwischen, um nicht auf diesem Weg ausgeforscht werden zu können. Da nicht jede oder jeder auf all diesen Gebieten Expertin oder Experte sein konnte, unterliefen den meisten Fehler und sie wurden festgenommen.

Heute haben es Kriminelle wesentlich leichter. Nahezu jeder einzelne Baustein dieser kriminellen Geschäftsmodelle kann im Darknet bestellt werden. Ähnlich einem Fahrzeug-Konfigurator der Autohersteller können die gewünschten Eigenschaften einer Schadsoftware ausgewählt und gekauft werden. Immer öfter gibt der Hersteller eine Geld-zurück-Garantie, falls sie nicht funktioniert oder blockiert wird. Auch die Verteilung der Software z. B. nach Regionen oder Sprachen und das Waschen des Geldes werden angeboten. Neben Schadsoftware werden im Darknet auch DDoS-Attacken gestaffelt nach Dauer und Bandbreite des Angriffes zum Kauf angeboten. Bezahlt wird mittels Kryptowährungen wie z.B. Bitcoin. Diese sind anonym und daher nur schwer einer Person zuzuordnen. Hinter Cybercrime-as-a-Service stehen meist weit verzweigte, arbeitsteilig agierende Organisationen, die sowohl die erforderlichen Spezialistinnen und Spezialisten als auch Handlanger beschäftigen und bei einem Ausfall schnell für Ersatz sorgen. Die Strukturen sind dabei jenen im Menschen- und Drogenhandel nicht unähnlich.

DISTRIBUTED-DENIAL-OF-SERVICE (DDoS) ATTACKEN

Im Gegensatz zu den weit gestreuten Wellen von Schadsoftware handelt es sich bei DDoS-Attacken um gezielte Angriffe. Sie ziehlen darauf ab, die Verfügbarkeit von Systemen und Ressourcen massiv einzuschränken. Wenn es sich dabei um einen Webshop handelt und dieser für die Kundschaft nicht mehr erreichbar ist, kann dies den Ruin für das betroffene Unternehmen bedeuten. Sollte ein staatlicher Service davon betroffen sein und es dadurch z. B. zu Fristverlusten kommen, können weite Teile der Wirtschaft und auch Privatpersonen geschädigt werden.

Die größte mediale Aufmerksamkeit in diesem Bereich erhielten 2016 wohl die Angriffe auf A1 und die Zentralanstalt für Meteorologie und Geodynamik (ZAMG). Darüber hinaus gab es zahlreiche mehr oder weniger erfolgreiche Angriffe auf Internetseiten von Unternehmen sowie öffentlichen Organisationen und Einrichtungen. In vielen Fällen folgten Drohungen, die Angriffe zu wiederholen, falls nicht eine bestimmte Summe bezahlt werden würde.

INTERNET OF THINGS (IoT)

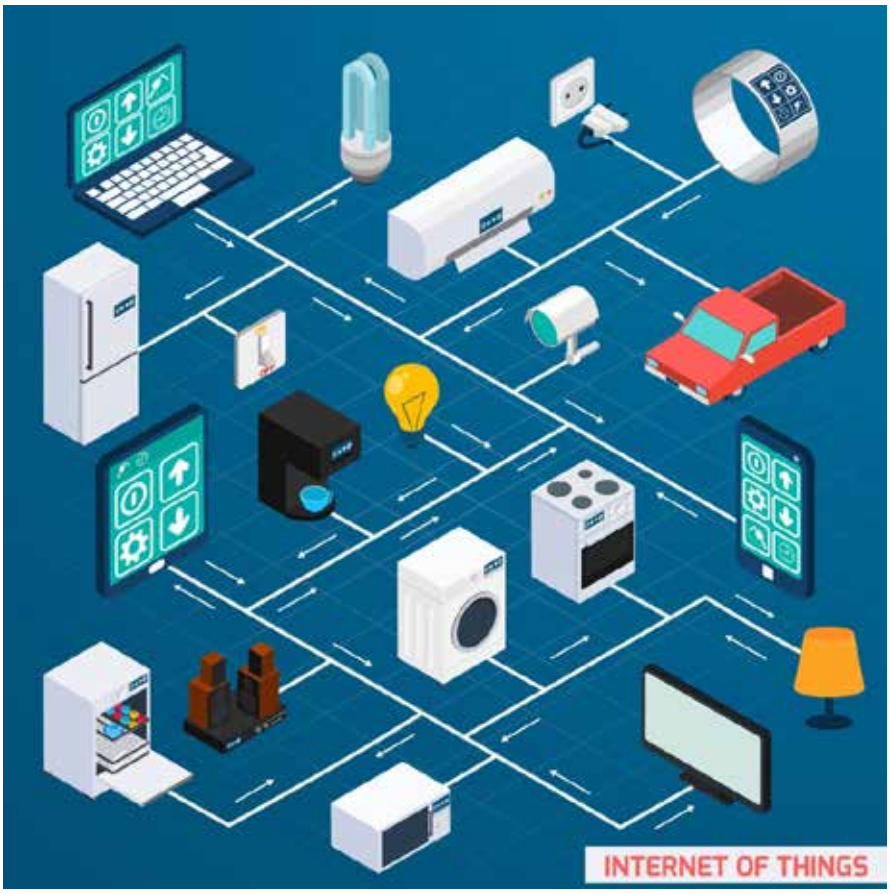


Abbildung 7: Internet of Things (© fotolia.com/macrovector)

IoT bezeichnet die Vernetzung von Gegenständen mit dem bzw. über das Internet, damit diese Geräte selbstständig kommunizieren und verschiedene Aufgaben für die Nutzerin und den Nutzer erledigen.

Die unzähligen internetfähigen Gegenstände und Elektrogeräte lassen sich in folgende Kategorien unterteilen:

- Smart-Home (Lichtregelung, Komfort-Heizung, Haus-Steuerungs-Systeme),
- E-Health (Fitness-Tracker, Wearables, Herzschrittmacher, etc.),
- M2M – Machine to Machine (Automatischer Datenaustausch zwischen Geräten, automatisierte Produktionsabläufe (Industrie 4.0), Wasserkraft-, Windkraft-, Sonnenkraft-, Fernheizanlagen u.v.m.),
- Car2X (Connected Car) und Verkehrsleiteinrichtungen
- sowie Sonstiges (z. B. Gimmicks, Gadgets, Amazon Echo, Babyfon, u. a.)

Das Internet of Things birgt aufgrund der Vernetzung auch eine Vielzahl an Missbrauchs- und Angriffsmöglichkeiten, wie den Aufbau von Bot-Netzwerken und den damit verbundenen DDoS-Attacken, Cryptolocker, Malware, Phishing, u.v.a.

Diese Geräte sind durchgehend online und jederzeit für Angriffe verfügbar. Dies ist oft gepaart mit schlechten Sicherheitsvorkehrungen und dem Fehlen von Sicherheitsupdates. Bei vielen Geräten hat der Besitzer nicht die Möglichkeit zur Absicherung, da von Seiten der Hersteller keine Änderungen am System vorgesehen sind. Die meisten Geräte haben fixe Wartungszugänge der Hersteller mit schlechter bzw. fehlender Verschlüsselung oder Standardpasswörter, die zu entschlüsseln keine Herausforderung darstellen. Ein weiterer Aspekt sind die oft überforderten Benutzer mit geringem IT-Wissen.

Aufgrund der massenhaften Verbreitung und der sich ständig erneuernden Trends wird es zunehmend schwieriger für den Endanwender, kriminelles Handeln im Hintergrund zu entdecken. Es ist in diesem Bereich von einer hohen Dunkelziffer auszugehen, da die Gefahr für den Angreifer entdeckt zu werden, gering ist. Ein unbefugter Zugriff wird oftmals nicht als solcher erkannt, sondern eher als ein Systemfehler vermutet.

Beispielsweise kann man in Elektronikgeschäften und vielen Supermärkten internetfähige Überwachungskameras kaufen. Viele davon senden Alarmmeldungen an das Smartphone des Besitzers und lassen sich über eine App steuern. Schließlich ist es bequem, von überall auf die aktuellen Überwachungsbilder zuzugreifen und die Kamera drehen oder zoomen zu können.

Für den Privathaushalt werden immer häufiger Produkte angeboten, die per App kontrolliert und gesteuert werden können.

Fast alle aktuellen Fernsehgeräte bieten die Möglichkeit, Filme, Dokumentationen oder Serien über das Internet zu „streamen“. Bei einigen kann man auch über die eingebaute Kamera Videotelefonate führen oder sie reagieren auf Gesten und gesprochene Kommandos.

Sprachsteuerungen lassen auch viele andere Funktionen zu wie etwa das Licht ein- ausschalten, den Sender am Fernseher wechseln, Heizung oder Klimaanlage steuern, die Vorhänge schließen und vieles mehr. Selbst die Haustüre lässt sich inzwischen mittels einer App am Smartphone auf- und zusperren (vorausgesetzt, es ist ein entsprechendes Schloss eingebaut).

Derartige Technologien bieten auch für Spielzeug neue und spannende Möglichkeiten. So können etwa Puppen, mit denen Kinder spielen, „verstehen“ und entsprechend reagieren oder antworten. Da Spracherkennung eine hohe Rechenleistung erfordert, geschieht dies in der Regel nicht in der Puppe. Vielmehr werden alle Geräusche in der Umgebung der Puppe an den Hersteller übertragen, dort ausgewertet, die Reaktion der Puppe ermittelt und dann die in Frage kommende Antwort zurückgesendet. Oder es wird über eine Spielekonsole mit dem entsprechenden Equipment der Spieler, inklusive dem dazugehörigen Raum in dem er sich befindet, gefilmt, um dessen Bewegungen für die entsprechenden Steuerungskommandos zu verifizieren.

Vorsicht ist bei Bestellungen von Geräten im Billigst-Segment (Stichwort: „China-Gadgets“) geboten, da hier die Gefahr besteht, dass bereits Hintertüren eingebaut sind.

Alle diese Funktionen sind sicher sehr praktisch, allerdings sollten sich die Interessenten oder Besitzer solcher Geräte über die Gefahren, die mit IoT einhergehen, bewusst sein und sich genau über mögliche Folgen informieren.

CYBER-KRIMINALITÄTSBEKÄMPFUNG IN ÖSTERREICH

Um mehr Sicherheit im virtuellen Raum zu gewährleisten, ist es notwendig, eine bundesweit umfassende Strategie zur Bekämpfung von Cybercrime zu verfolgen. Dazu ist notwendig, nicht nur auf zentraler Ebene, sondern auch auf Länder-, Bezirks- und Gemeindeebene, ausreichend Know-how zu transportieren. Die Bekämpfung der Internetkriminalität nimmt bei der Polizei einen Schwerpunkt ein:

- Einerseits österreichweit auf lokaler Ebene in den rund 900 Polizeiinspektionen und in über 100 Bezirks- und Stadtpolizeikommanden.
- Auf Länderebene sind technisch ausgebildete Expertinnen und Experten zur Durchführung beziehungsweise Unterstützung bei technischen Ermittlungs- und Beweissicherungsmaßnahmen tätig.
- Auf Bundesebene wird das Cybercrime-Competence-Center, kurz „C⁴", als zentrale Koordinierungs- und Meldestelle aufgebaut. Es setzt sich aus technisch und fachlich hochspezialisierten Expertinnen und Experten zusammen.

Wird eine Straftat mit IT-Bezug bei der Sicherheitsbehörde – in der Regel durch die Mitteilung eines Geschädigten bei einer Polizeiinspektion – bekannt, kann auf das Fachwissen der Bezirks-IT-Ermittler zurückgegriffen werden. Auf Ebene der Landeskriminalämter sind Fachbereiche zur Klärung solcher Straftaten eingerichtet. Diese fungieren als Bindeglied zum Cybercrime-Competence-Center im Bundeskriminalamt.

CYBERCRIME-COMPETENCE-CENTER (C⁴)

Im Rahmen des INNEN.SICHER-Projektes wurden Maßnahmen für eine effiziente Bekämpfung von Cybercrime erarbeitet. Ein wesentlicher Bestandteil dieser Maßnahmen war die Errichtung des Cybercrime-Competence-Centers (C⁴) 2011 im BK.

Das C⁴ ist als nationale und internationale Zentralstelle für die elektronische Beweismittelsicherung und -auswertung, Ermittlungen im Zusammenhang mit Cybercrime im engeren Sinn sowie die Koordinierung der Bekämpfung von Cybercrime zuständig.

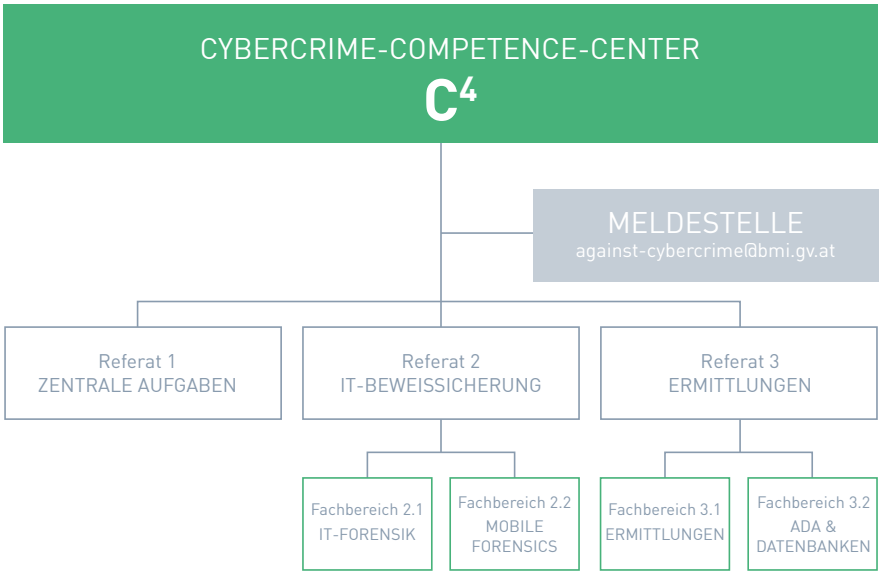


Abbildung 8: Organigramm C⁴

Organisatorisch gliedert sich das C^4 in drei Referate:

- Zentrale Aufgaben
- IT-Beweissicherung
- Ermittlungen

und die Meldestelle.

Zentrale Aufgaben: Zu den Hauptaufgaben dieses Referats zählen der Betrieb der technischen Infrastruktur, die Beobachtung von aktuellen technologischen Entwicklungen und der organisatorische und technische Support innerhalb des C^4. Darüber hinaus sind die internationale Zusammenarbeit, Präventionsmaßnahmen, die Abwicklung und Unterstützung von Projekten als auch die Ausbildung und Schulung wesentliche Schwerpunkte. Letzteres wird derzeit neu ausgearbeitet, um zu gewährleisten, dass die Polizistinnen und Polizisten über ein fundiertes Standardwissen verfügen und darüber hinaus Spezialausbildungen für bestimmte Bereiche erhalten. Ziel ist es, mit der Vielfalt und Dynamik der Cybercrime-Delikte entsprechend umgehen zu können. Dabei sollen alle Bereiche von der Grundausbildung bis zur laufenden Weiterbildung zielgruppengerecht abgedeckt werden.

IT-Beweissicherung: Im Fachbereich IT-Beweissicherung wird die Leitung, Koordination und Durchführung der Analyse, Datensicherung, -aufbereitung und -auswertung von elektronischen Beweismitteln wie Audio-, Video- und IT-Medien sowie mobilen Endgeräten durchgeführt. Das Referat ist auch nationale und internationale Ansprechstelle (NCRP) im Bereich der Analyse und Datensicherung von elektronischen Medien, wie IT-Medien und mobilen Endgeräten. Weiters wird die Leitung, Koordination und Durchführung von überregionalen Datensicherungseinsätzen übernommen.

Ermittlungen: Im Fachbereich Ermittlungen wird die Leitung, Koordinierung und Durchführung von nationalen und internationalen Ermittlungen zur Aufklärung von Cybercrime-Delikten im engeren Sinn gewährleistet. Es werden Analysen und Lagebilder im Cybercrime-Bereich erstellt sowie spezifische Präventionsmaßnahmen entwickelt. Aktuelle globale IT-Phänomene werden beobachtet und bei Hinweisen auf Täter oder Opfer in Österreich, Ermittlungsschritte und Präventionsmaßnahmen eingeleitet. Hierbei findet national eine enge Zusammenarbeit mit den Landeskriminalämtern, dem CSC (Cyber-Security-Center) des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung (BVT), dem Computer-Emergency-Response-Team (CERT) und anderen statt. International ist eine ständige Zusammenarbeit mit Interpol und Europol zur zielgerichteten Bekämpfung von Cybercrime-Delikten unumgänglich.

LANDESKRIMINALÄMTER

In den Landeskriminalämtern der Bundesländer sind fachlich ausgebildete Exekutivbedienstete tätig. Diese verfügen über eine spezielle polizeiliche Ausbildung und sind zusätzlich im IT-Bereich geschult. Sie servicieren die jeweiligen Ermittlungsbereiche bei digitalen, forensischen Sicherungen sowie deren Auswertungen und Aufbereitungen. Neben den forensischen Tätigkeiten umfasst deren Aufgabengebiet auch Ermittlungstätigkeiten im Cybercrime-Bereich auf nationaler Ebene. Aufbauend auf die Bezirks-IT-Ermittler-Ebene gewährleistet der Assistenzbereich 06 ein professionelles Einschreiten bei höherrangigen Strafrechtsdelikten mit entsprechendem IT-Bezug. Besonders bei internationalen Ermittlungen stellt der Assistenzbereich 06 durch seine Schnittstellenfunktion auf Bundesländerebene eine Hilfeleistung für das Cybercrime-Competence-Center im Bundeskriminalamt dar.

BEZIRKS-IT-ERMITTLER

In den Bundesländern gibt es mittlerweile das Modell der Bezirks-IT-Ermittler. Dabei handelt es sich um Polizeibeamtinnen und -beamte, die durch das jeweilige Landeskriminalamt eine Zusatzausbildung und eine Praxisschulung im Bereich Cybercrime erhalten haben. Sie unterstützen das jeweilige Landeskriminalamt bei der Datensicherung und Erstaufnahme von Cybercrime-Delikten auf lokaler Ebene und sind erste Ansprechstelle für die Mitarbeiterinnen und Mitarbeiter in den Polizeiinspektionen.

POLIZEIINSPEKTIONEN, STADT- UND BEZIRKSPOLIZEIKOMMANDEN

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

BEWEISSICHERUNG UND ANALYSE

Auch 2016 hat es sich bestätigt, dass IT-Medien immer mehr zum Werkzeug und Ziel für kriminelle Handlungen werden. Aus diesem Grund stellte die elektronische Beweismittelsicherung im C^4 und in den Landeskriminalämtern immer wieder eine wichtige Komponente innerhalb strafrechtlicher Ermittlungen dar. 2016 standen vor allem Sicherungen und Auswertungen nach terroristischen Aktivitäten in Europa im Mittelpunkt der elektronischen Beweismittelsicherung, gefolgt von Ermittlungen im Bereich der Wirtschaftskriminalität, körperlicher Gewalt und der organisierten Kriminalität. Deutlich ist dabei zu erkennen, dass der Trend zu Smartphones und Tablets nicht abreißt und daher für kriminalpolizeiliche Ermittlungen eine immer wichtigere Rolle spielt. Besonders die Kapazitäten dieser Geräte steigen kontinuierlich an, sodass diese mit der herkömmlichen IT vergleichbar werden. Parallel steigt die Tendenz, Daten zu verschlüsseln und gegen fremden Zugriff zu schützen. Darüber hinaus werden die Daten nicht mehr am Gerät selbst, sondern auf verteilten Systemen im Internet – der Cloud – gespeichert. Cloud-Dienste haben 2016 die elektronische Beweismittelsicherung besonders gefordert, da für ihre forensisch korrekte Sicherung herkömmliche technische Möglichkeiten keine Anwendung mehr finden können. Dafür mussten neue Herangehensweisen entwickelt und Prozeduren definiert werden, um die Beweiskraft der sichergestellten Daten zu sichern um weiterhin den nationalen und internationalen Anforderungen zu entsprechen. Neben den technischen Herausforderungen kommen auch immer wieder rechtliche hinzu, da der Umgang mit diesen elektronischen Beweismitteln von gesetzlichen Bestimmungen zum Teil noch nicht umfasst ist.

Ein deutlicher Anstieg konnte 2016 auch in der Multimedia-Forensik beobachtet werden: Es wurden über 100 Akte bearbeitet und durch Verbesserung von Bild- und Tonmaterial oftmals ein entscheidender Beitrag zur Aufklärung zahlreicher Verbrechen geleistet. Der Umgang mit elektronischen Beweismitteln bedarf eines speziellen Fachwisses und entsprechender Erfahrung. Dieses wurde in zahlreichen nationalen und internationalen Spezialausbildungen aufgebaut und erweitert. Weiters konnten im Rahmen des Cybercrime-Ausbildungskonzeptes bereits Module entworfen werden. Damit konnte ein Grundstock an Wissen definiert werden, das künftig jede Forensikerin und jeder Forensiker innerhalb der Behörde aufweisen soll.

FAHRZEUGFORENSIK

Abbildung 9: Vernetzte Autos (© fotolia.com/sydia productions)

In der Fahrzeugforensik hat Österreich in den letzten Jahren eine Vorreiterrolle gegenüber anderen europäischen Ländern übernommen. Die Fahrzeugtechnik und deren Elektronik entwickeln sich rasant weiter, weshalb die daraus gewonnenen digitalen Informationen immer mehr an Bedeutung gewinnen. Durch die zunehmende Vernetzung der Fahrzeuge werden diese zu einem wichtigen Bestandteil polizeilicher Ermittlungen.

Zu den Aufgaben der Fahrzeugforensik zählen die forensische Untersuchung von IT-Systemen und Datenspeichern in Fahrzeugen. Die Sicherung digitaler Beweismittel aus Bordsystemen und Steuergeräten dient unter anderem

dem Erkennen von Manipulationen in der Fahrzeugelektronik, der Rekonstruktion von Standorten oder der Ermittlung von Betriebszuständen zu einem bestimmten Zeitpunkt. Im Mittelpunkt steht die Klärung einer Straftat. So können zum Beispiel Informationen der Crash Data Records bzw. Event Data Records bei der Rekonstruktion von Unfällen von Bedeutung sein.

Die Mitarbeiterinnen und Mitarbeiter der Fahrzeugforensik unterstützen in erster Linie bei Ermittlungen von schweren Straftaten. Ein beträchtlicher Anteil ist im Bereich der organisierten Kriminalität zu finden. Die Expertinnen und Experten der Fahrzeugforensik sind national und international tätig und unterstützen nicht nur in Form von Labor- und Büroarbeit bei der Begutachtung von Beweismaterial, sondern auch am Tatort selbst oder durch Mitwirkung an operativen Einsätzen, wie zum Beispiel bei der Interpol-Taskforce „Paso del Estrecho" in der Hafenanlage von Algeciras/Spanien. Im Rahmen solcher Schwerpunktaktionen arbeiteten die Bereiche Kfz-Ermittlung und -Forensik eng zusammen.

MOBILE FORENSIK

Der Bereich Mobilkommunikationsforensik umfasst die Sicherung von Mobilgeräten wie Mobiltelefone, Tablets, Navigationsgeräte oder Smart-Watches. Dieser Bereich ist eine große Herausforderung, da nicht nur die Anzahl der verschiedenen Geräte und der User steigen, sondern auch die Anzahl und Vielfalt der Gadgets. Gerade diese Vielzahl an verschiedenen Herstellern, von denen praktisch jeder seine Geräte individuell aufbaut, führt zu einer enormen Zahl an Schnittstellen und Protokollen. Das wiederum stellt die Forensik bei der Auswertung dieser Geräte vor immer neue Aufgaben. Dieser Bereich ist aus der polizeilichen Ermittlungsarbeit nicht mehr wegzudenken, da durch die Auswertung mobiler Geräte Beweismittel gewonnen werden, die in allen Deliktsbereichen unentbehrlich geworden sind.

Ein Großteil der Auswertungen erfolgt in den Landeskriminalämtern. Wenn es sich um Bundesländer übergreifende Fälle oder einen internationalen Bezug handelt, wenn spezielle Ausrüstung oder Wissen erforderlich sind oder neuartige Geräte analysiert werden müssen, dann langen die Geräte im C^4 ein.

VIDEO UND MULTIMEDIA FORENSIK

Die Multimediaforensik beinhaltet forensische Techniken zur Überprüfung digitaler Mediendaten. Ein Aspekt ist die Frage des Ursprungs digitaler Mediendaten sowie die Erkennung von Manipulationen daran. Die Echtheit der Daten ist Grundvoraussetzung, um als Beweismittel dienen zu können. Eine Herausforderung sind die großen Datenmengen und die Vielfalt an Dateiformaten. Für jedes Format ist ein geeignetes Werkzeug zur Decodierung erforderlich. Eine zentrale Aufgabe ist die Suche nach nützlichen Daten. Dabei spielt neben der Dateigröße vor allem auch die Länge des Videomaterials eine Rolle. Das gewonnene Bildmaterial wird analysiert, verglichen und relevante Informationen für die weiteren Ermittlungen extrahiert. Dies kann etwa zur Identifizierung von Fahrzeugen oder Personen dienen.

Abbildung 10: Beispiel Bildverbesserung

Beispiel einer Bildverbesserung: Bei der Person links im Hintergrund sind vor der Bearbeitung die Aufschrift des T-Shirts und das Gesicht nur unscharf zu erkennen. Nach der Bearbeitung sind Gesicht und Aufschrift des Shirts deutlich erkennbar.

IT-ERMITTLUNGEN

OPERATION „AVALANCHE“

Im Zuge dieser Operation wurde nach vierjähriger Ermittlungstätigkeit Ende November 2016 ein Verwaltungssystem vom Internet genommen, das Bulletproof-Hostern ermöglichte, kriminelle Internetdienste anzubieten. Österreich war maßgeblich an den internationalen Ermittlungen und der Ausforschung der Täter beteiligt. Zusätzlich zur notwendigen Schwergewichtsbildung in Bezug auf die Bekämpfung von Ransomware waren wie auch in den Jahren zuvor, DDos-Angriffe in Verbindung mit Erpressungen, Malware-Verbreitung und Phishing-Attacken.

SOKO CLAVIS

2016 wurde der Schwerpunkt auf den Entwurf einer Strategie zur Bekämpfung der massiv angestiegenen Ransomwarefälle gelegt. Zu diesem Zweck wurde Mitte des Jahres eine Sonderkommision eingerichtet, die sich ausschließlich dieser Thematik widmet.

In der Soko werden alle Ransomware-Fälle zusammengefasst, bearbeitet und ermittelt. Diese Vorgangsweise ermöglicht eine weitgehende Klassifizierung der einzelnen Ransomware-Arten und Tätergruppierungen. Die dabei gewonnen Erkenntnisse werden im Rahmen von Arbeitsgruppen mit Europol und anderen Staaten abgeglichen. Durch die internationale Zusammenarbeit mit dem European Cybercrime Center (EC3) bei Europol und den betroffenen Staaten sind hier eine hohe Ermittlungskompetenz und eine breite Vernetzung von Expertinnen und Experten zur Bekämpfung von Ransomware verfügbar. Internationale Kooperationen und Ermittlungsgruppen bei Europol und Interpol stehen ständig miteinander in Kontakt und ermitteln gemeinsam, um die Täter auszuforschen.

Bei Europol wurde auf Initiative der Soko Clavis eine Arbeitsgruppe (J-CAT) zur Ausforschung der Tätergruppe CERBER initiiert und geleitet. Darüber hinaus gibt es bei Europol noch weitere Arbeitsgruppen zu den einzelnen Ransomware Arten, bei der die Experten der Soko vertreten sind, um an der Ausforschung der Täter mitzuwirken. Besonders wichtig ist die Partnerschaft im Projekt „www.Nomoreransom.org“. Auf dieser Homepage bieten zahlreiche Polizeieinheiten, Europol und große IT-Sicherheitsunternehmen wie Kaspersky Information und Hilfe für Betroffene an. Auf dieser Webseite werden auch zahlreiche Entschlüsselungstools zur Verfügung gestellt. Das C^4 ist seit Dezember 2016 Mitglied in dieser Initiative.

Abbildung 11: Website Nomore Ransome (© Europol)

Im Deliktsbereich Ransomware kann von einer hohen Dunkelziffer ausgegangen werden. Dies deshalb, weil viele betroffene Privatanwender keine Anzeigen erstatten. Auch viele Unternehmen verzichten zum Beispiel aufgrund eines vermuteten Reputationsverlustes auf die Erstattung einer Anzeige. In manchen Fällen sind auch notwendige Vorkehrungen vorhanden, die eine rasche Systemwiederherstellung möglich machen.

MELDESTELLEN

MELDESTELLE CYBERCRIME IM C4

Im C4 ist rund um die Uhr eine Meldestelle eingerichtet, die laufend Meldungen über aktuelle Cyber-Vorfälle aus der Bevölkerung, der Wirtschaft und dem polizeilichen Bereich erhält.

Durch die Vielzahl an eingehenden Informationen ist es möglich, Phänomene zu erkennen und Warnmeldungen mit entsprechenden Handlungsempfehlungen in Form eines Newsletters an ausgewählte Multiplikatoren zu versenden. 2016 wurden zehn Newsletter zu aktuellen Cyber-Phänomen versandt.

Die Mitarbeiterinnen und Mitarbeiter der Meldestelle informieren und beantworten Anfragen zum Thema Cybercrime von anderen Polizeidienststellen, Unternehmen, Bürgerinnen und Bürgern, usw. 2016 wurden mehr als 11.000 Mitteilungen und Hinweise aus der Bevölkerung sowie von in- und ausländischen Dienststellen und der Wirtschaft durch die Meldestelle bearbeitet.

Der Inhalt der Meldungen konzentrierte sich auf den Einsatz von Ransomware bzw. CEO-Betrug. Häufig wurden auch allgemeine Betrugsphänomene wie zum Beispiel der Scheckbetrug bei Vorreservierungen aus dem Ausland, die Zustellung von ungerechtfertigten Rechnungen bei Eintragungen in Wirtschaftsdatenbanken oder der Domänenregistrierung gemeldet. Die gemeldeten Fälle von Sextortion und ähnlichen Erpressungen sind 2016 im Vergleich zu den Vorjahren rückläufig.

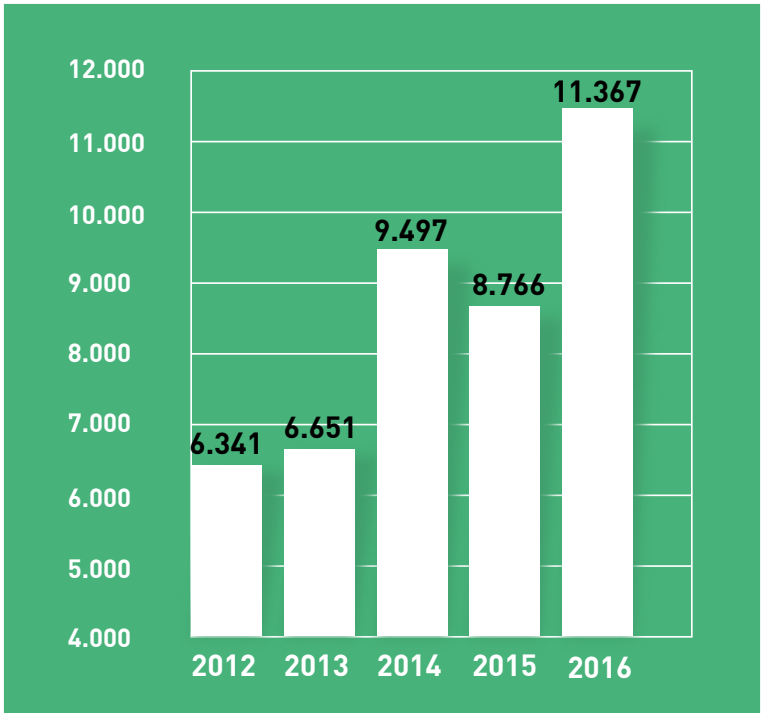


Abbildung 12: Anzahl der im C4 eingegangenen Meldungen

Besonders intensiviert wurde 2016 die Zusammenarbeit mit der Wirtschaft und Vereinen wie zum Beispiel der Wirtschaftskammer Österreich (WKO) oder der Initiative „Watchlist Internet", um über aktuelle Phänomene zu informieren. 2016 war festzustellen, dass mögliche Opfer aufgrund der allgemeinen Sensibilisierung vor- und umsichtiger geworden sind und sich bei Ungereimtheiten häufig Informationen durch die Meldestelle einholten.

MELDESTELLE KINDERPORNOGRAFIE UND KINDERSEXTOURISMUS

Die Zahl der Anzeigen wegen kinderpornografischer Darstellung Minderjähriger (§ 207a StGB) ist von 465 im Jahr 2015 auf 681 im Jahr 2016 angestiegen. Die Zahl der Anzeigen wegen Groomings (§ 208a StGB) ist von 52 Anzeigen auf 80 Anzeigen im Jahr 2016 angestiegen. Die Zahl der Hinweise, die in der Meldestelle Kinderpornografie und Kindersextourismus im BK eingegangen sind, war rückgängig (2015: 2.742 Hinweise, davon 310 mit Österreichbezug; 2016: 1.530 Hinweise, davon 347 mit Österreichbezug). Dieser Rückgang ist darauf zurückzuführen, dass das digitale Missbrauchsmaterial vermehrt in geschlossenen Foren bzw. im „Peer-to-Peer"-Bereich (P2P) verbreitet wird. Dieser ist der Öffentlichkeit großteils nicht zugänglich.

INTERNATIONALE ZUSAMMENARBEIT

Cybercrime ist eine internationale Kriminalitätsform. Dies charakterisiert sich darin, dass eine geographische Nahebeziehung von Täter und Opfer in der Regel nicht notwendig ist. Erschwerend kommt hinzu, dass die notwendige IT-Infrastruktur sich in einem dritten Land befinden kann. Dabei kann der Täter seine Aktivitäten sowie die verwendete Infrastruktur innerhalb kürzester Zeit weltweit verlagern. Diese Umstände erschweren die Ermittlungen und Strafverfolgung erheblich, weshalb eine rasche und zuverlässige internationale Zusammenarbeit aller beteiligten Behörden unbedingt erforderlich ist.

Im polizeilichen Bereich haben sich das Global Complex for Innovation von Interpol und das EC3 von Europol als wichtige und rasche Informationsdrehscheibe etabliert und bewährt. Mitarbeiterinnen und Mitarbeiter des C^4 sind daher auch in wichtigen Gremien wie zum Beispiel in der European Cybercrime Taskforce (EUCTF) oder dem European Multidisciplinary Program Against Criminal Threats (EMPACT) vertreten. Internationale Workshops und Schulungen sowie Hospitationen verbessern das Know-how und die internationale Vernetzung.

Die Spezialisten des C^4 haben die Führung in der Operation CERBER unter dem Schirm der Joint Cybercrime Action Taskforce (J-CAT) bei Europol übernommen. J-CAT steuert den Informationsaustausch und administriert die länderübergreifende Zusammenarbeit auf operativer Ebene. Diese Form der Zusammenarbeit ermöglicht rasche und effektive Ermittlungen über die Landesgrenzen hinweg.

Das C^4 ist mit seiner Meldestelle Teil des weltweiten G8-Netzwerks, das von zentralen Ansprechstellen bei dringlichen Cyber-Vorfällen eingerichtet wurde.

Wie in den Vorjahren nahm Österreich unter Leitung des BK auch 2016 an von Europol koordinierten internationalen Schwerpunktaktionen teil: Eine Schwerpunktaktion betraf die Buchung von Flügen mit rechtswidrig erlangten Kreditkartendaten im Internet. Die Ermittlungen zeigten, dass für den Bereich der illegalen Immigration als auch des Schmuggels kriminelle Flugbuchungen mit rechtswidrig erlangten Kreditkartendaten durchgeführt wurden. Neben Flug- und Zugbuchungen werden missbräuchlich erlangte Kreditkartendaten auch zur Bestellung von Waren im Internet verwendet. Bei der erstmalig durchgeführten Schwerpunktaktion im Oktober 2016 wurden neun Beschuldigte ausgeforscht, die Handys, Markenkleidung und Kfz-Ersatzteile im Internet bestellt hatten.

Eine weitere Aktion betraf die Bekämpfung der Herstellung und Verteilung von gefälschten Euro-Banknoten. Diese Kriminalitätsform verlagert sich zunehmend in das Darknet. Durch gemeinsame Ermittlungen mit den Niederlanden und Europol konnte eine Tätergruppe ausgeforscht werden.

PROJEKTE

E.V.A.

Mit dem KIRAS-Projekt E.V.A. (Electronic Visual Analysis) wurde im Oktober 2015 der Grundstein für eine künstliche-Intelligenz-unterstützte kriminalpolizeiliche Methodik zur forensischen Auswertung und Klassifikation von Multimediadaten gelegt und weiterentwickelt. In enger Kooperation mit dem BK wurden Prototypen für Hard- und Software entwickelt, die Aufgaben des maschinellen Bildverstehens und die automatisierte Verarbeitung großer Datenmengen ermöglichen. Zur effizienten kriminalpolizeilichen Nutzung dieses Computersystems im Bereich der Ermittlungen im Deliktsfeld Kinderpornographie wurde eine für den Ermittler optimierte Benutzeroberfläche mit zahlreichen Ermittlungsfeatures implementiert. Erste Zwischenergebnisse zeigen deutlich, dass die physische und psychische Belastung der Ermittlungsbeamten durch das E.V.A.-System deutlich reduziert werden kann. Das Projekt endet im Oktober 2017 und soll danach schrittweise in den Echtbetrieb übergeführt werden.

FAHREZEUGFORENSIK

Dem Projekt „Fahrzeugforensik – Forensische Untersuchung von IT-Systemen und Datenspeicher in Kraftfahrzeugen zur Klärung von Straftaten“ werden ebenfalls EU-Fördermittel durch den ISF-Fonds zur Verfügung gestellt. Dieses Projekt dient der Errichtung und Schaffung einer zentralen Servicestelle zur kriminalpolizeilichen Beweismittelsicherung von Daten aus der Fahrzeugforensik im BK. Durch diese Spezialisierung soll eine forensisch korrekte Beweismittelsicherung von Fahrzeugdaten ermöglicht werden, um weitere Ermittlungen und die Klärung von Straftaten zu erleichtern. 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 sowie Unternehmen im Cyberspace. Der Aufbau von Kapazitäten bei der Strafverfolgung und Justiz sowie die Verbesserung der Interventionsmöglichkeiten bei Cyber-Angriffen stellen Synergieeffekte dar.

BITCRIME

Das deutsch-österreichische Projekt „Bitcrime“ hat die Erforschung innovativer Lösungen zur Identifikation, Bekämpfung und Prävention der organisierten Finanzkriminalität mittels Kryptowährungen wie Bitcoins zum Inhalt. Die entwickelte Software wird bereits bei nationalen sowie internationalen Ermittlungsbehörden verwendet. Aufgrund der positiven Resonanz wird die Zusammenarbeit mit privaten und öffentlichen Forschungseinrichtungen zukünftig in weiteren Projekten rund um die Thematik von Kryptowährungen intensiviert.

PRÄVENTION UND INFORMATION

Um auf die 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 gelegt, da hier ein sensibler Umgang mit neuen Medien besonders wichtig ist. Aber auch Erwachsene, die keine schulische Ausbildung auf diesem Sektor erhalten haben, werden von den Präventionsbediensteten über die Gefahren des Internets informiert.

Vor allem durch grundlegende Informationen bezüglich PC- und Passwortsicherheit und sicheres Internetsurfen kann Schaden verhindert werden. Daher betreibt die Kriminalprävention im BK und in den Landespolizeidirektionen zielgruppenorientierte Öffentlichkeitsarbeit durch Aufklärung in sozialen Medien im Internet und der Polizei App, die gratis zum Download für Apple-, Android- und Windows -Systeme zu Verfügung steht.

SCHWERPUNKT KINDER UND JUGENDLICHE

- Besondere Aufmerksamkeit bei der Präventionsarbeit im IT-Bereich wird auf die Arbeit mit Jugendlichen gesetzt, da diese Zielgruppe mit dem Internet und mit sozialen Medien aufwächst. Im Vordergrund steht dabei das Projekt „Click & Check“, das österreichweit sehr erfolgreich umgesetzt wird. Um eine möglichst hohe Nachhaltigkeit zu gewährleisten, werden auch Eltern sowie Lehrerinnen und Lehrer in das Projekt miteinbezogen. Eigens geschulte Präventionsbedienstete klären dazu in den Schulen über „Happy Slapping“ und „Cyberbullying und -mobbing“ auf, um unter Einbeziehung kurzer Videofilme das Rechtsbewusstsein von Jugendlichen zu fördern und Gesetzesinformationen zu vermitteln. Im Jahr 2016 wurden österreichweit 56.920 Schülerinnen und Schüler, Eltern sowie Lehrerinnen und Lehrer über den richtigen, sicheren Umgang mit Handy und PC sensibilisiert und informiert.

- Schwerpunkt „Cyergrooming“: 2016 wurde die Informationskampagne „Jugend OK!“ fortgesetzt. Dabei stand das Thema „Cybergrooming“ im Vordergrund. Über 7.700 Jugendliche erhielten Karten mit Informationen zu Gefahren im Umgang mit modernen Kommunikationsmitteln.

- Um eine möglichst nachhaltige und flächendeckend einheitliche Umsetzung der Programminhalte zu gewährleisten, wurden die Präventionsmaßnahmen für Jugendliche neu konzipiert. Im Projekt „Under 18“ wurden die Programme überarbeitet und mit neuen Modulen erweitert, die von ca. 300 Präventionsbediensteten zur Umsetzung gelangen.

- Im März 2015 startete das vom EU-Fonds für die innere Sicherheit geförderte Präventionsprojekt „CyberKids“, das altersgruppengerechte Inhalte und Methoden zum verantwortungsvollen Umgang mit dem Internet für Kinder im Alter von acht bis zwölf Jahren beinhaltet.

Abbildung 13: Logo Cyberkids

Es wurde ein Ausbildungskonzept für die CyberKids-Landestrainer erstellt. Gemeinsam mit der Sicherheitsakademie des Bundesministeriums für Inneres wurde ein E-Learning-Modul entwickelt und einwöchige Präsenzschulungen durchgeführt. Die Schwerpunkte der Ausbildung waren Cybercrime und Cyber-Präventionsthemen, Entwicklungs- und Schulpsychologie, Didaktik, Methodik und Rhetorik. In die Schulung waren interne und externe Experten zur Qualitätssicherung mit einbezogen.

Im ersten Quartal 2017 startete das Programm „CyberKids" in den Volksschulen. Die Umsetzung erfolgt zuerst durch die Kinderpolizei in fünf Themenbereichen

- „Polizei – Schutz"
- „Gefühle – Vertrauen"
- „Chancen und Gefahren"
- „Persönliche Daten – Datenschutz"
- „Was ist das Internet?".

Schulkinder ab zehn Jahren werden von Experten der Kriminalprävention in Präventionsthemen geschult. In dieser Altersgruppe werden die Themen, die in der Volksschule behandelt wurden, vertieft und um weitere Themen (Apps, Chats, Sexting, Sextortion, Grooming, Cybermobbing) ergänzt.

AUSBLICK

Wenn bei Gesprächen über die weiteren Entwicklungen in der Cyberworld das Thema „Internet der Dinge" aufkommt, hört man oft das Argument „Bis der Kühlschrank selbst im Internet Lebensmittel nachbestellt, dauert es noch lange." Irgendwie dürfte dieses Beispiel in vielen Köpfen eng mit dem Begriff IoT verbunden sein. Dass dies nicht der einzige Aspekt in diesem Zusammenhang ist, und vor allem dass sich daraus ergebende Gefahrenpotenzial, wurde bereits im Kapitel IoT beleuchtet.

Mehrere renommierte Unternehmen haben Schätzungen veröffentlicht, wie viele Geräte in Zukunft an das Internet angeschlossen sein werden. Für das Jahr 2020 werden mehr als 20 Milliarden Geräte prognostiziert. Jedes davon stellt ein potenzielles Ziel für kriminelle Aktivitäten dar. In diesem Zusammenhang sind der kriminellen Phantasie keine Grenzen gesetzt. Aus dem beinahe exponentiellen Anstieg der Angriffsziele lässt sich ableiten, dass die weltweit zu beobachtende Steigerung bei Cybercrime anhalten wird.

Dabei werden Maßnahmen zur Verfolgung und Aufklärung der Straftaten alleine nicht ausreichen. Vielmehr sind auch die Anwender und Hersteller gefordert, Maßnahmen zu setzen, damit es Kriminellen erschwert wird, sich diesem riesigen Reservoir an potenziellen Werkzeugen und Zielen zu bedienen.

SUMMARY

FACTS AND FIGURES

In Austria the number of complaints involving cybercrime rose from 10,010 in 2015 to 13,103 in 2016, which is an increase by about 31 per cent. The number of cases requiring special technical knowhow has shown the biggest rise of over 55 percent.

The principal causes are

- the global spread of offenders, resources (servers, etc.), victims and money flows,
- the increasing use of the Darknet by criminals,
- the global spread of malicious software
- the lack of threat awareness
- the weaknesses of IT systems such as outstanding security updates

MEASURES

To counter the massive increase in ransomware, a special investigation team termed CLAVIS was set up in June 2016. It is composed of experts who centrally process all ransomware cases. In the field of IT forensics, new technological fields have been introduced and expanded, in particular vehicle forensics and multimedia forensics. In order to improve police training, new programs were launched in 2016, focussing on IT investigators in the field. The project „CyberKids" is aimed at empowering children of eight to twelve years to safely handle the Internet in its final phase (2018).

TRENDS

Ransomware continues to be at the top of criminal trends. There is an increasing emphasis on specific objectives and target groups such as personnel departments and small and medium-sized enterprises. Virtual currencies such as bitcoins are increasingly used by criminals to conceal their criminal proceeds and money flows from the investigative authorities. The Darknet has facilitated and accelerated the emergence of criminal service providers in the form of „cybercrime as a service". Criminal tools make it possible for virtually everyone to execute, for instance, technically sophisticated cyberattacks. An growing threat is the shifting of conventional crime such as drug or arms trade to the Internet, in particular to the Darknet.

OUTLOOK

Cybercrime is a global phenomenon and no country can shield itself from its global developments. New technologies open up new targets for criminals. The Internet of things will be of particular relevance in this context. By 2020, some 20 billion devices are expected to be connected to the Internet in this way. Already today, 4.9 billion devices have a connection with the Internet according to an estimate by market researcher Gartner (www.gartner.com). Most of these devices are unprotected against attacks. The DDoS attacks on the US company „DynDNS" in the autumn of 2016, using the „Mirai-Botnet", have gone to show the potential threat involved in the IOT - the Internet of Things.

New technologies require legal adjustments. New statutory definitions of criminal offences and new methods of investigation must, as soon as possible, be incorporated into the legal system and be formulated in such a way as to remain applicable whenever there are technological changes.

The rate of technological progress also requires rapid and innovative adjustments on the part of government authorities. The expansion of existing and the establishment of new fields of action to deal with new technologies as well as the availability of profound technical know-how are challenges to be tackled urgently. In order to be able to meet these challenges in future, cybercrime units with state-of-the-art equipment and training will be imperative.

GLOSSAR

Antivirenprogramm (auch Virenscanner oder Virenschutz): 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.

Bulletproof-Hoster: Sind Internetdienstanbieter die ihren Kunden anonyme Services im Internet zur Verfügung stellen.

Bot (auch Zombie genannt): 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 wird auch der übernommene Rechner so bezeichnet (als Kurzform von Roboter), der in ein BotNet eingebunden wurde.

Bot-Herder: Verwaltet und kontrolliert ein BotNet das aus fernsteuerbaren Computersystemen besteht und bereit ist, beispielsweise DDos Angriffe zu starten.

BotNet: Unter einem BotNet oder Bot-Netz (die Kurzform von Roboter-Netzwerk) versteht man einen Verbund von fernsteuerbaren Computersystemen, auf welche sich (meist widerrechtlich) Zugang verschafft wurde. Die Kontrolle über die Systeme wird durch Würmer bzw. Trojanische Pferde erlangt, die 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.

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

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 Mitarbeiter werden über (angeblich) streng vertrauliche Vorgänge informiert, die zumeist eine Firmenübernahme einleiten sollen. Für diese Abwicklung würden Anzahlungen benötigt, die dieser Mitarbeiter in die Wege leiten solle. Die Gelder werden zumeist auf Konten bei Banken aus dem asiatischen Raum überwiesen. Durch ständige Hinweise auf 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 erworben.

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. Der Virus 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. Wird der zur Blockade führende Angriff nicht nur von einem einzelnen Rechner ausgeführt, sondern von vielen gleichzeitig, spricht man von einem „Distributed (=verteilt) 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.

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 ausnutzen. 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 entsprechenden 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 manipulieren. Das Besondere des Angreifers besteht darin, dass er den Kommunikationspartnern das jeweilige Gegenüber vortäuschen kann, ohne dass sie es merken.

Metadaten: Liefern Zusatzinformationen zu gespeicherten Daten (z.B. Erstelldatum, Verfasser, Autor, etc.)

Mirai: Ist eine Schadsoftware für „Internet-of-Things"-Geräte, die unter speziellen Linux-Varianten laufen, mit deren Hilfe Botnetze aufgebaut werden können. Damit lassen sich beispielsweise gezielte Angriffe durch absichtliche Überlastungen von Netzen durch DoS oder DDoS-Attacken organisieren. Mirai befällt Internet-of-Things-Systeme und schaltet dann die infizierten Geräte mit anderen zu einem Botnet zusammen.

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.

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 Crypt0l0ckern 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.

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 z.B. 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: 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, als kostenlose Zugaben zu anderen Programmen (Browserleisten, ...) oder als Zusatzfunktion zu kostenlosen Apps.

Stammdaten: Darunter versteht man alle personenbezogenen Daten, die für die Begründung, 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.

TAN: Bedeutet Transaktionsnummer und ist ein Einmalpasswort das im Online-Banking verwendet wird. Ein M(obiler) -TAN besteht in der Einbindung des Übertragungskanals SMS.

Der E-TAN ist ein kleines elektronisches Kontrollgerät, der die (TAN) Eingabe ersetzt. Während der Kunde bisher eine Liste mit Transaktionsnummern hatte, werden über E-TAN 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 TAN-Box eingibt. Die TAN-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.

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 2017

Kriminalitätsentwicklung 2016
Schlepperkriminalität 2016
Kriminalprävention 2016
Verfassungsschutz 2016
Suchtmittelkriminalität 2016
Menschenhandel 2016
Geldwäscherei 2016
Sicherheitsbericht 2016

Kontakt
Bundeskriminalamt
Meldestelle Cybercrime
Josef-Holaubek-Platz 1, 1090 Wien
Tel: +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: bk.presse@bmi.gv.at

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

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.

.BK

BUNDESKRIMINALAMT