ZAHLEN, INITIATIVEN UND PROJEKTE 2014
TRENDS 2015

CYBERCRIME 2014

CYBERCRIME 2014

BUNDESKRIMINALAMT ÖSTERREICH

CYBERCRIME

2014

INHALT

VORWORT

Liebe Leserinnen und Leser,

Weltweit findet eine digitale Revolution statt, die sich rasant vollzieht. Die enorm hohe Geschwindigkeit bei der Weiterentwicklung digitaler Technologien erfordert eine ständige Anpassung der Sicherheitsmaßnahmen, um sich vor kriminellen Angriffen wirksam schützen zu können. Die Bekämpfung von Cyber-Kriminalität muss heutzutage schnell, strukturiert und auf dem Stand der Technik erfolgen. Daher ist die enge Zusammenarbeit von Institutionen wie Europol und Interpol sowie aller nationalen Ermittlungs- und Strafverfolgungsbehörden von größter Wichtigkeit. Nur so können wir den aktuellen Phänomenen bei der Bekämpfung von Internetkriminalität entgegenwirken. Das gilt auch für Bedrohungslagen wie zum Beispiel der Wirtschaftsspionage, Hacking oder der Betrugs- und Finanzmittelkriminalität, wo vor allem persönliche Daten wie E-Mail-Adressen oder Bank- und Kreditkartendaten für Cyber-Kriminelle ein reizvolles Gut darstellen.

Um die Cyber-Kriminalität effektiv zu bekämpfen, wurden im Jahr 2014 neuerlich große Anstrengungen unternommen. Aufgrund der wachsenden Anforderungen an die Ermittlungsmethoden und die Beweismittelsicherung wurde der Ausbau von Hard- und Software weiter fortgesetzt. Außerdem wurde 2014 neuerlich stark in die Aus- und Weiterbildung der Mitarbeiter sowohl in den Landeskriminalämtern als auch im Cybercrime-Competence-Center C^4 im Bundeskriminalamt investiert.

Cybercrime ist wesenstypisch eine internationale Kriminalitätsform. Aus diesem Grunde war das Jahr 2014 ebenso wie die vorangegangenen Jahre erneut geprägt von einer Vielzahl internationaler Kooperationsmaßnahmen, Fachtagungen sowie operativer länderübergreifender Ermittlungen. Gleiches gilt für die zahlreichen Präventions- und Forschungsprojekte, die laufend ausgebaut werden.

Ein Dankeschön gebührt an dieser Stelle allen zuständigen Mitarbeitern für Ihr Know-how, ihre Bereitschaft zur ständigen Weiterentwicklung und ihren Einsatz. Den Lesern dieses Berichts möchten wir mit dieser Broschüre einen Überblick über die Cyber-Kriminalitätsbekämpfung in Österreich geben. Wir hoffen auf diese Weise kompaktes Cybercrime-Wissen auf interessante Art und Weise gemäß dem Motto des Bundeskriminalamtes zur Verfügung zu stellen: „Wissen schützt!“

Mag.^{a} Johanna Mikl-Leitner
Bundesministerin für Inneres

General Franz Lang
Direktor des Bundeskriminalamtes

EINLEITUNG

Der vorliegende Cybercrime Report 2014 bildet überblicksartig die im Bereich der Cyber-Kriminalitätsbekämpfung unter der Führung des Bundeskriminalamtes vorgenommenen operativen Maßnahmen ab, die dazu dienen, den aktuellen Cyber-Bedrohungen wirkungsvoll zu begegnen. Weiters soll der Report auch einen Informations- und Präventionsbeitrag sowohl innerbehördlich als auch über die Behördengrenzen hinaus leisten.

Die Entwicklung neuer krimineller Begehungsformen im Deliktsfeld Cybercrime in Kombination mit den großen Anpassungserfordernissen cyberspezifischer Rechtsgrundlagen wird auch die Polizei in den kommenden Jahren sehr beschäftigen. Gilt es doch nationale wie auch internationale Bestimmungen zu harmonisieren, um den Ermittlungs- und Strafverfolgungsbehörden die für ihre Arbeit notwendigen zeitgemäßen Rechtsgrundlagen bereitstellen zu können. Diese wichtigen rechtlichen Schwerpunktthemen werden in den kommenden Jahren sowohl in Österreich als auch auf internationaler Ebene sehr große Herausforderungen für alle Beteiligten bereithalten. Damit einhergehend wurde die Notwendigkeit neuer, moderner Aus- und Fortbildungsmaßnahmen für die Bereitstellung hochqualifizierter Cybercrime-Ermittlungsexperten sowie IT-Forensiker erkannt. Deshalb wurden 2014 sowohl auf nationaler als auch auf europäischer Ebene große Anstrengungen unternommen, um eine neue moderne Fachausbildung für künftige Cybercrime-Experten innerhalb des BMI in naher Zukunft zu verwirklichen.

Cybercrime ist und bleibt ein äußerst dynamisches und hochinnovatives Kriminalitätsphänomen, das die Ermittlungsbehörden ständig vor neue Herausforderungen stellt. Kriminelle können praktisch rund um die Uhr gleichzeitig in den verschiedensten Regionen der Erde aktiv werden, während sich ihre Serverinfrastruktur in anderen Ländern befindet und sie sich an einem ganz anderen Ort aufhalten. Die Internationalität dieser Kriminalitätsform verbunden mit den Möglichkeiten von Verschlüsselung und Anonymisierung erklären die ständig steigende Zahl von Cyber-Angriffen.

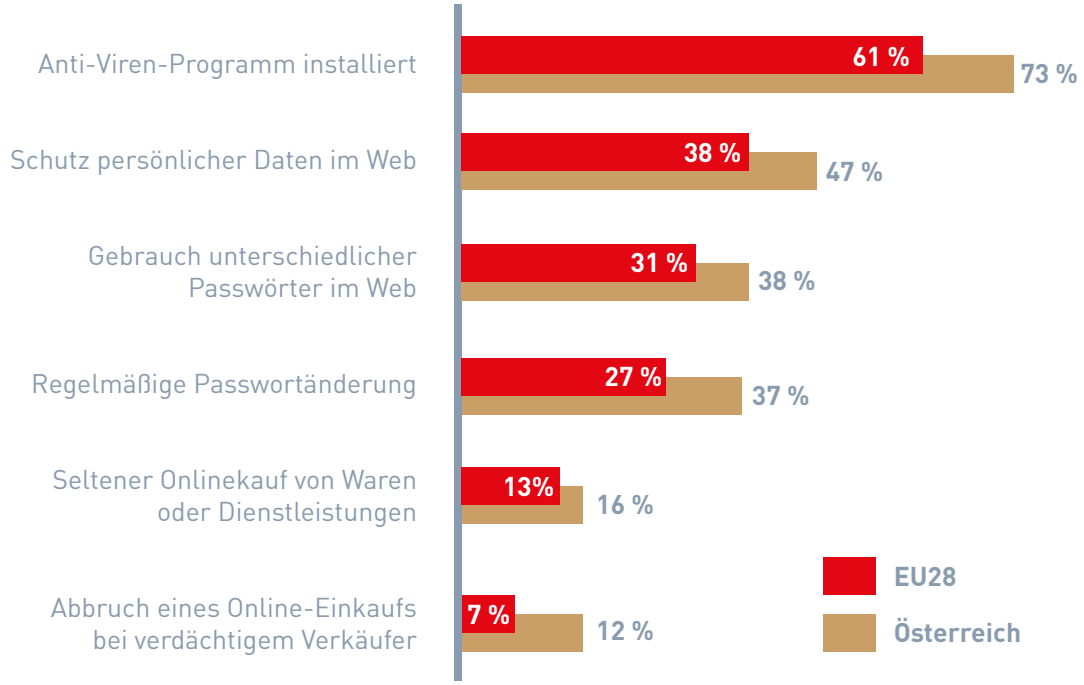


Abbildung 1: Umfrage zum Thema Sicherheitsbewusstsein im Bereich Computerkriminalität 2014, Quelle: Eurobarometer

Das Sicherheitsbewusstsein der Österreicherinnen und Österreicher ist höher als der europäische Durchschnitt.

ZUSAMMENFASSUNG DES CYBERCRIME REPORTS 2014

DATEN UND FAKTEN

Im Bereich der Cyber-Kriminalität sind die Anzeigen 2014 auf 8.966 (2013: 10.051 Anzeigen) gesunken, was einen Rückgang von 10,8 Prozent zum Vorjahr bedeutet. Hingegen stieg die Anzahl der reinen IT-Delikte (Cybercrime im engeren Sinn) 2014 leicht an. Darunter versteht man Straftaten, die mit Hilfe der Technologien des Internets begangen werden, wie zum Beispiel der widerrechtliche Zugriff auf ein Computersystem. Die Aufklärungsquote lag 2014 bei 40,8 Prozent und liegt damit 4,4 Prozentpunkte unter der von 2013. Dieser Rückgang ist unter anderem auf die Professionalisierung der international vernetzten Tätergruppen und den verstärkten Einsatz von Verschlüsselung und Anonymisierungstechniken zurückzuführen.

TRENDS

Auch wenn aktuell ein Rückgang der Cyber-Kriminalität zu verzeichnen ist, so ist im Zehn-Jahresvergleich doch ein deutlicher Trend nach oben ablesbar. Dies ist durch die zunehmende Verbreitung von Computern – speziell in Form von Smartphones und Tablets – dem Ausbau von Netzwerken und hier vor allem mobilen Breitbandverbindungen zu erklären. Da die Informations- und Kommunikationstechnologie dadurch zu einem ständigen Begleiter im Alltag geworden ist, entstehen laufend neue Kriminalitätsphänomene, wobei weiterhin von einem großen Dunkelfeld im Bereich Cybercrime auszugehen ist.

Nach wie vor sind eine Unmenge an Phishing- und Spam-Mails im Umlauf. Eine deutliche Steigerung gab es auch bei Meldungen über versuchte Betrugsfälle auf Online-Plattformen, bei Ein- und Verkäufen im Internet – zumeist bei Kfz- oder Immobilienangeboten. Der gängige Modus Operandi des Bestellens und Nichtbezahlens geht hier in Richtung der Vortäuschung von gefälschten Bezahlbestätigungen durch PayPal- und Amazon-Konten.

POLIZEILICHE MASSNAHMEN

Das im Bundeskriminalamt angesiedelte Cybercrime-Competence-Center C^4 ist die nationale und internationale Zentralstelle zur Bekämpfung von Cyber-Kriminalität in Österreich. Neben dem C^4 auf Bundesebene bestehen in allen Landeskriminalämtern vergleichbare Dienststellen. In diesen Organisationseinheiten sind kriminalpolizeilich und technisch ausgebildete Experten mit der Bekämpfung von Cybercrime und der IT-Forensik in den jeweiligen Bundesländern befasst. Für

die Bekämpfung von Cybercrime auf lokaler Ebene und zur Unterstützung der Kollegen in den Polizeiinspektionen wurden in den letzten Jahren rund 280 Bezirks-IT-Ermittler ausgebildet.

Bei der Bekämpfung von Cybercrime spielt auch Prävention eine wesentliche Rolle, hierbei ist auch der unmittelbare Kontakt mit der Bevölkerung von Bedeutung. Die Beamten in den Polizeiinspektionen, die Bezirks-IT- Ermittler, die Präventionsbeamten und die Experten in den Landeskriminalämtern sowie im Cybercrime-Competence-Center C^4 arbeiten im Rahmen von Beratungen und Vorträgen laufend daran, in Österreich ein angemessenes Schutzniveau zu etablieren.

AUSBLICK

Das Gefährdungs- und Schädigungspotenzial durch Cybercrime bleibt auch in Zukunft unverändert hoch. Neben den Zugangsdaten im Online-Banking werden alle Formen der digitalen Identität ausgespäht, vermarktet und in weiterer Folge missbräuchlich eingesetzt. Das Deliktsfeld Cybercrime entwickelt sich weiterhin dynamisch. Technologische Neuerungen werden von Kriminellen auf Schwachstellen und Eignung für kriminelle Aktivitäten untersucht und in der Folge auch entsprechend eingesetzt. Neue technische Sicherheitsmaßnahmen – auch in Form von Software-Updates, die bereits bekannte Fehler beheben sollen – werden schnell durch neue Schadsoftware überwunden oder es erfolgt eine Anpassung des Modus Operandi.

ZAHLEN UND DATEN IN ÖSTERREICH

Im Gegensatz zum stetigen Anstieg der Anzeigen in den Vorjahren, sind diese im Bereich der Cyber-Kriminalität in Österreich 2014 gesunken. Mit einem Rückgang von 10,8 Prozent sind die Anzeigen mit exakt 8.966 deutlich unter die 10.000er-Marke gesunken (2013: 10.051 Anzeigen). Hingegen stieg die Anzahl der reinen IT-Delikte (Cybercrime im engeren Sinn) 2014 leicht an.

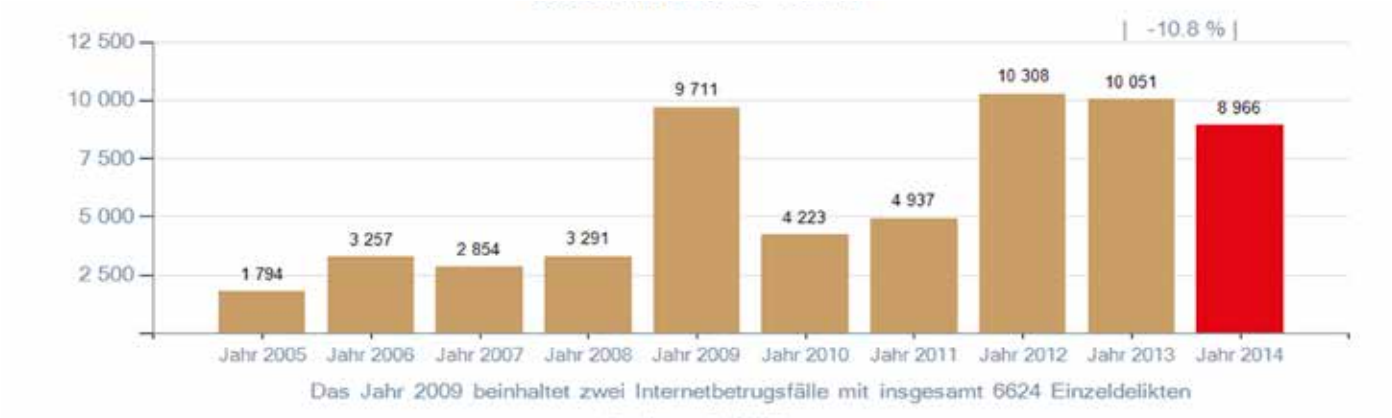


Abbildung 2: Anzeigen Cybercrime 2005 bis 2014, Quelle: Polizeiliche Kriminalstatistik Österreich (PKS)

Der Rückgang ist vor allem im weiter definierten Bereich von Cybercrime und hier vor allem beim Internetbetrug zu finden. Die Anzeigen wegen Internetbetrugs sind um 13,5 Prozent von 7.667 auf 6.635 Anzeigen gesunken, liegen aber dennoch mit 6.598 Anzeigen über dem Wert des Jahres 2012.

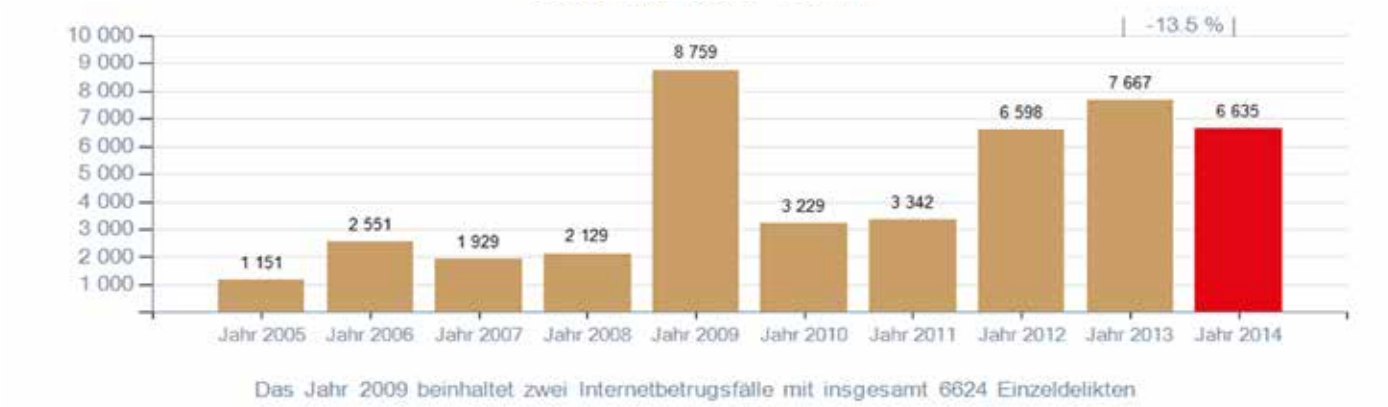


Abbildung 3: Anzeigen Internetbetrug 2005 bis 2014, Quelle: PKS

Wie in den letzten Jahren ist bei Cybercrime eine Verlagerung der einzelnen Delikte zu beobachten, was unter anderem auf das weitgehend zyklische Auftreten von unterschiedlichen Phishing- und Malware-Attacken zurückzuführen ist. So gingen Anzeigen wegen § 126b Strafgesetzbuch (StGB) „Störung der Funktionsfähigkeit eines Computersystems" von 470 Anzeigen im Jahr 2013 auf 118 Anzeigen im Jahr 2014 zurück, was einem Rückgang um etwa 74,9 Prozent entspricht. Deutlich gestiegen ist hingegen der § 118a StGB „Widerrechtlicher Zugriff auf ein Computersystem", das allgemein unter dem Begriff Hacking bekannt ist. Waren es 2013 noch 391 Anzeigen, so wurden im Jahr 2014 bereits 677 Fälle angezeigt, was einem Anstieg von über 73 Prozent entspricht.

Angezeigte Fälle	Jän-Dez 2013	Jän-Dez 2014	Veränderung
§ 118a StGB	391	677	73,1 %
§ 119a StGB	10	17	70,0 %
§ 126a StGB - Vergehen	196	138	-29,6 %
§ 126a/V StGB - Verbrechen	2	2	0,0 %
§ 126b StGB - Vergehen	470	118	-74,9 %
§ 126b/V StGB - Verbrechen	34	22	-35,3 %
§ 126c StGB	171	249	45,6 %
§ 148a StGB - Vergehen	421	404	-4,0 %
§ 148a/V StGB - Verbrechen	5	6	20,0 %
§ 225a StGB	37	121	227,0 %
Cybercrime im engeren Sinn	**1.737**	**1.754**	**1,0 %**

Tabelle: Cybercrime-Delikte im engeren Sinn im Vergleich 2013 und 2014, Quelle: PKS

Die Aufklärungsquote lag 2014 bei 40,8 Prozent und damit um 4,4 Prozentpunkte unter der von 2013. Dieser Rückgang ist unter anderem auf die immer stärkere Professionalisierung der international vernetzten Tätergruppen und den dadurch bedingten verstärkten Einsatz von Verschlüsselung und Anonymisierungstechniken zurückzuführen.

Auch wenn aktuell ein Rückgang der Cyber-Kriminalität zu verzeichnen ist, so ist im Zehn-Jahresvergleich doch ein deutlicher Trend nach oben ablesbar. Dies ist durch die zunehmende Verbreitung von Computern – speziell in Form von Smartphones und Tablets – dem Ausbau von Netzwerken und hier vor allem mobilen Breitbandverbindungen zu erklären. Da die Informations- und Kommunikationstechnologie dadurch zu einem ständigen Begleiter im Alltag geworden ist, entstehen laufend neue Kriminalitätsphänomene, wobei weiterhin von einem großen Dunkelfeld im Bereich Cybercrime auszugehen ist.

DIE HÄUFIGSTEN CYBER-ANGRIFFSFORMEN IN ÖSTERREICH

2014 konnte in Österreich eine Häufung von folgenden Angriffsformen beobachtet werden:

KRIMINELLE ALS MICROSOFT-MITARBEITER

Zur Vorgehensweise: Bei einem Microsoft-Windows-Kunden geht ein Telefonanruf ein. Der Anrufer stellt sich als Mitarbeiter von Microsoft vor. Er spricht zumeist in relativ schlechtem Englisch und gibt an, dass das Computersystem des Kunden mit Schadsoftware infiziert und deshalb gefährdet sei. Dadurch sei Microsoft auf den Kunden aufmerksam geworden. Der Mitarbeiter bietet an, die Viren und Trojaner vom Computer des Kunden kostenlos zu entfernen. Damit der vermeintliche „Microsoft Mitarbeiter" sich mit dem Gerät des Kunden verbinden kann, wird der Kunde aufgefordert ein „Remote-Zugriffs-Tool" für Fernwartungen herunterzuladen und zu installieren. Oftmals wird auf die kostenlose Software „Team Viewer" verwiesen. Nach Installation der Software und Bekanntgabe eines Zugriffs-Codes für das Remote-Tool an den angeblichen „Microsoft Mitarbeiter", kann dieser uneingeschränkt auf die Daten des Computersystems zugreifen. Während der angeblichen „Bereinigung" des Systems lenkt der „Microsoft Mitarbeiter" den Kunden immer wieder durch unwichtige Erklärungen ab und zeigt angebliche Fundstellen von Schadsoftware. Dazwischen bleibt der Bildschirm mehrfach schwarz, wodurch für den Kunden nicht ersichtlich ist, wo und nach welchen Daten der Eingreifer auf der Festplatte sucht. Nach erfolgter „Bereinigung des Systems" bzw. nachdem der Täter die für ihn relevanten Daten auf dem System zu sich übertragen hat, wird zumeist darauf verwiesen, dass eine Lizenz abgelaufen ist und diese bei sofortiger Erneuerung sehr günstig verlängert werden kann. Die angebotene Lizenz zum Preis von zehn bis 30 Euro für den weiteren Schutz des Systems soll dann vom Kunden sofort bezahlt werden. Dafür wird ein fertiges Formular zur Verfügung gestellt. In den meisten Fällen bittet dann der „Microsoft Mitarbeiter" den Kunden die Bezahlung durch die Eingabe von Kreditkartendaten oder Online-Banking durchzuführen, um dabei seine Bankdaten auszuspähen, sollte er die entsprechenden Daten nicht ohnedies schon durch einen vorherigen Zugriff auf das Computersystem des Kunden gefunden haben. In den meisten Fällen hat sich gezeigt, dass die angeblichen Abbuchungsbeträge in der Höhe von zum Beispiel 29 Euro schlussendlich auf dem Kreditkartenkonto mit 129 oder 229 Euro ausgewiesen und abgebucht wurden. Es kann zusätzlich davon ausgegangen werden, dass durch den vermeintlich hilfsbereiten „Microsoft Mitarbeiter" auch Schadsoftware installiert wurde, wodurch weiterhin sensible persönliche Daten in das Internet übermittelt werden oder ein uneingeschränkter Zugriff über die installierte Remote-Software für den Täter möglich ist. Meist kann der Computer nur mehr durch professionelle Hilfe wieder funktionsfähig gemacht werden. Das „Herauslocken von Zugriffsdaten" wird als „Social Engineering" bezeichnet.

RANSOMWARE - FINANZIELLE BEDROHUNG FÜR FIRMEN?

2014 wurden speziell im Bereich der Landespolizeidirektion (LPD) Tirol zahlreiche Fälle mit sogenannter Ransomware bekannt. Betroffen waren neben Privatpersonen auch einige kleinere Unternehmen. Die Zahl der betroffenen Computer dürfte tatsächlich weitaus höher liegen, da erfahrungsgemäß nur ein Bruchteil der betroffenen Personen bzw. Firmen Anzeigen erstatten.

Die verschiedenen Varianten dieser Erpresser-Software werden überwiegend als manipulierte E-Mail-Anhänge getarnt bzw. mit speziell präparierten Webseiten auf den Computer des Besuchers installiert (Drive-By-Download). Anschließend durchsuchen sie das infizierte System inklusive der internen und externen Datenträger und Netzwerkfreigaben und verschlüsseln auf dem Zielsystem vorhandene Dateien nach vorgegebenen Mustern, wie zum Beispiel Word- und Excel-Dateien, E-Mails, Datenbanken, etc. Die neueren Versionen dieser Schadsoftware verwenden dabei meistens zwei Verschlüsselungsdurchläufe mit sehr langen zufälligen Passwörtern und löschen danach die ursprünglichen Dateien mit speziellen „Wipe-Programmen", sodass ein Wiederherstellen auch für professionelle Datenretter unmöglich wird. Abschließend werden auf den befallenen Computern eigene Startseiten installiert, in denen auf die Verschlüsselung und Löschung (wipe) der Daten hingewiesen wird.

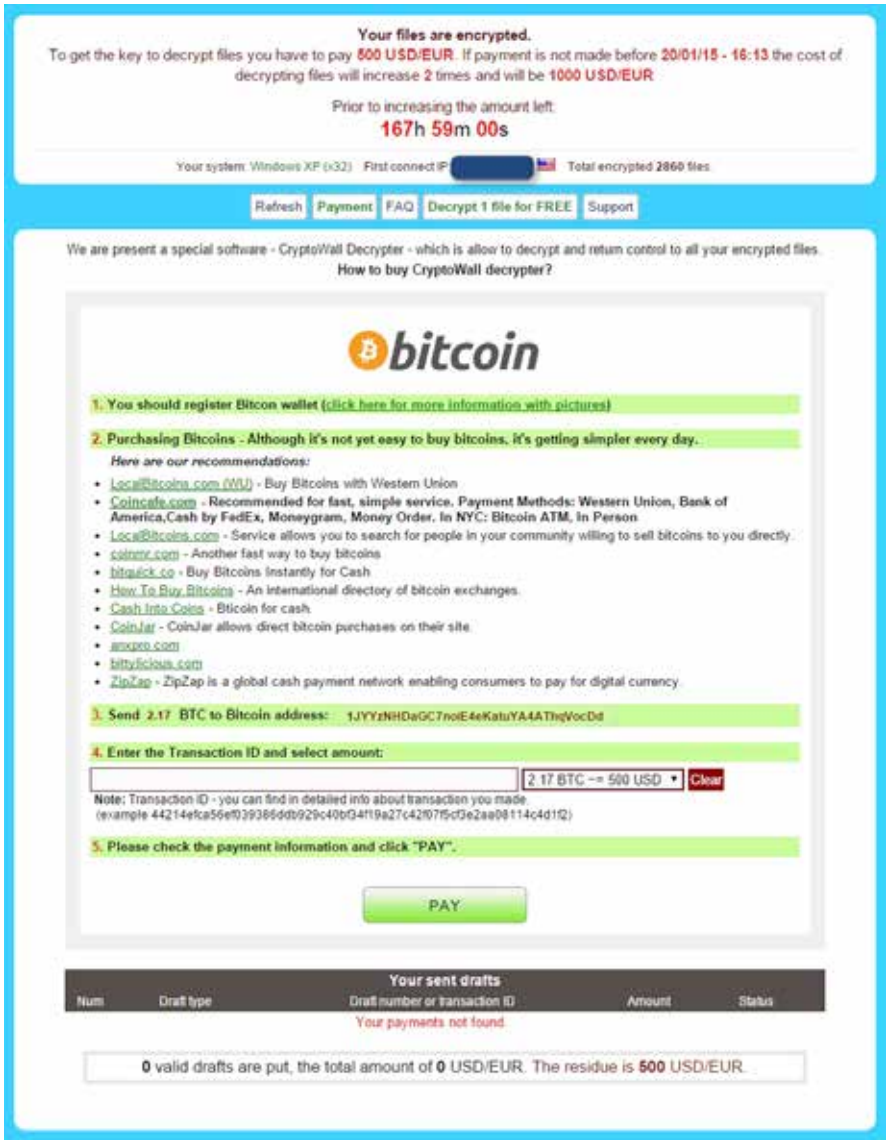


Abbildung 4: Crypto-Wall

Die Täter bieten an, die Verschlüsselung durch Zahlung eines Geldbetrags über verschlüsselte Kanäle aufzuheben. In den meisten Fällen können auch durch die Zahlung des Geldbetrages die verschlüsselten Daten nicht mehr hergestellt werden. Die Kommunikation zwischen den infizierten Systemen mit den „Befehlsservern" der Erpresser erfolgt dabei unter anderem über das Tor- bzw. das I2P-Netzwerk. Eine Rückverfolgung der Kommunikationswege ist nahezu ausgeschlossen. Die Schäden für die betroffenen Privatpersonen bzw. Unternehmen belaufen sich auf bis zu mehrere Zehntausend Euro. Nicht mehr vorhandene Kundendaten, fehlender Schriftverkehr und gelöschte Buchhaltung etc. können die Betroffenen oft an den Rand einer Insolvenz bringen.

Neben den allgemeinen Sicherheitshinweisen zum Verhalten im Internet kann in solchen Fällen nur ein funktionierendes, fortlaufend durchgeführtes Backup auf externe bzw. abgekoppelte Systeme helfen.

NOTFALL-E-MAILS

Bei diesem Cyber-Angriff werden die E-Mail-Accounts einer Person durch Hacking- oder Phishing-Attacken übernommen. Die Absicht der Täter ist es, an die Daten des E-Mail-Adressbuches ihrer Opfer zu gelangen und im nächsten Schritt an diese Kontakte eine „Notfall-E-Mail" zu senden. Hier wird üblicherweise auf eine finanzielle Notlage im Urlaub oder auf einer Reise im Ausland verwiesen. Sie geben an, dass ihnen Geld und oder Dokumente gestohlen wurden und bitten um eine Überweisung eines Geldbetrages für die sofortige Bezahlung der noch offenen Hotel- oder Flugrechnung, da ihnen sonst eine Heimreise nicht möglich ist. Die Rückzahlung des geborgten Geldbetrages wird sofort nach Rückkehr zugesagt. Die Überweisung soll meist über einen vom Täter vorgeschlagenen Money-Transfer-Dienst erfolgen, da hier eine Rückverfolgung des Geldflusses nahezu unmöglich ist. In den meisten der bekannten Fälle werden die Passwörter der übernommenen E-Mail-Accounts vom Täter geändert, so dass kein Zugriff mehr durch den eigentlich Berechtigten erfolgen kann. Danach werden die kompletten Kontaktdaten gelöscht und analog zur E-Mail-Adresse ein weiterer E-Mail-Account bei einem anderen Dienstanbieter erstellt. Der weitere E-Mail-Verkehr zwischen den Opfern und dem Täter findet nun über die neue E-Mail-Adresse statt, die alte Adresse dient zum Teil nur noch als Relay-Station. Große Free-E-Mail-Anbieter zeigen sich mittlerweile bereit, die „übernommenen" E-Mail-Accounts für den eigentlichen Inhaber wiederherzustellen. Voraussetzung dafür ist unter anderem, dass ein eindeutiger Besitz an den Daten und der Rechtmäßigkeit nachgewiesen werden kann, zum Beispiel durch Zusendung einer Kopie eines Reisepasses oder Personalausweises. Dazu dient insbesondere die doppelte Absicherung des Accounts zum Beispiel durch Passwort und hinterlegter Rückrufnummer.

BETRÜGEREIEN AUF VERKAUFSPLATTFORMEN

Im Juli 2014 erstattete eine österreichische Firma eine Anzeige, dass ihr Onlineportal gehackt worden sei. Es stellte sich heraus, dass das Online-Bezahlsystem gehackt und die eingehenden Beträge auf ein Konto der Täter umgeleitet wurden. Es entstand ein Schaden im fünfstelligen Euro-Bereich. Mehrere Tatverdächtige wurden ausgeforscht, zwei konnten festgenommen werden. Im Zuge der Ermittlungen wurde festgestellt, dass von diesen Personen nicht nur Webseiten gehackt, sondern auch „Willhaben.at-Betrügereien" durchgeführt wurden. Bisher konnten 15 Geschädigte aus dem gesamten Bundesgebiet identifiziert werden. Die Hacker gingen dabei arbeitsteilig vor: Das „Anbieten der Waren auf Willhaben.at" wurde von einer Tätergruppe durchgeführt, während die Kontoöffnung bzw. das Abheben der Geldbeträge von einer anderen Gruppe erfolgte. Die Aufteilung der erbeuteten Gelder erfolgte ebenfalls durch verschiedene Internetdienste. Die Tätergruppen kannten sich nicht persönlich und die Kommunikation erfolgte via Chat im Internet. Bei der Auswertung der sichergestellten Datenträger wurde festgestellt, dass durch die Tatverdächtigen auch von einer Vielzahl von Geschädigten die Bank- und Kreditkartendaten mittels Phishing erlangt und mit diesen Daten auch Waren von verschiedenen Online-Shops zum Weiterverkauf bestellt worden waren.

CYBER-KRIMINALITÄTSBEKÄMPFUNG IN ÖSTERREICH

CYBERCRIME-COMPEDENCE-CENTER C⁴

Das im Bundeskriminalamt angesiedelte Cybercrime-Competence-Center C⁴ ist die nationale und internationale Zentralstelle zur Bekämpfung von Cyber-Kriminalität in Österreich. Sie setzt sich zusammen aus den Bereichen

- Zentrale Aufgaben,
- IT-Beweissicherung,
- Ermittlungen und
- der Meldestelle

Zu den Aufgaben des Cybercrime-Competence-Centers C⁴ zählen:

- Durchführung, Leitung und Koordinierung von Cybercrime-Ermittlungen im engeren Sinn.
- Internationale polizeiliche Kooperation in Cybercrime-Angelegenheiten.
- IT-Forensik, wie zum Beispiel Sicherung, Aufbereitung und Auswertung von elektronischen Beweismitteln.
- Ermittlungen zur Aufklärung von Cybercrime-Delikten.
- Entwicklung und Bereitstellung von neuen technischen Lösungen.
- Analyse und Bewertung neuer Technologien.
- Durchführung des automationsunterstützten Datenabgleiches (Rasterfahndung).
- Betrieb einer Meldestelle als Kontaktstelle zu anderen spezialisierten Polizeieinheiten, wie dem Europäischen Cybercrime Center (EC3) bei Europol und dem Interpol Digital Cyber Center (IDCC).
- Ansprechstelle für Anfragen aus der Wirtschaft und der Bevölkerung in Cybercrime-Angelegenheiten.
- Schnittstelle zum Bereich Cybersecurity.
- Fachaufsicht über den Assistenzbereich 06 (AB 06) in den Landeskriminalämtern.

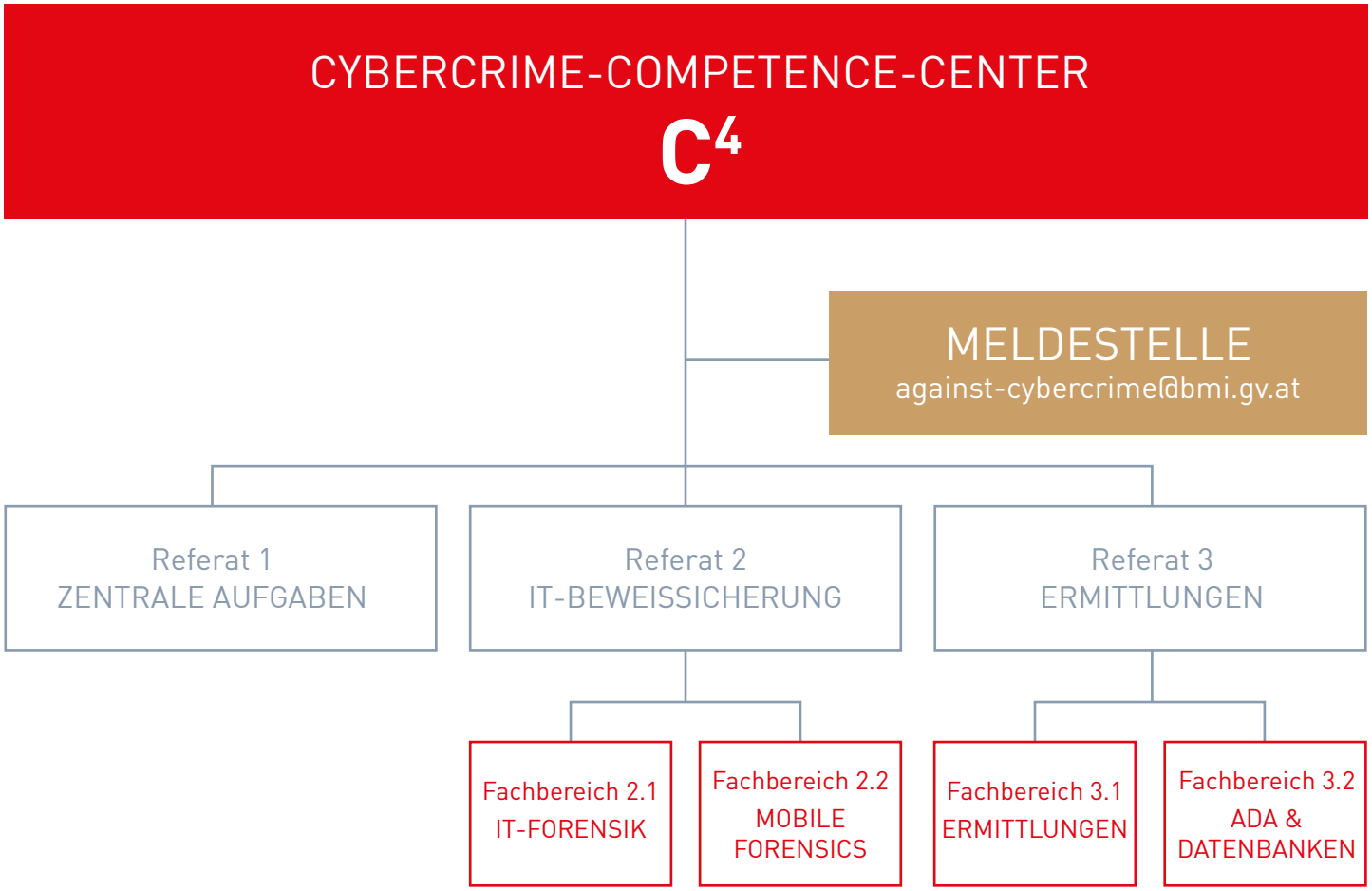


Abbildung 5: Organisation und Aufbau des C4

Im Rahmen des technischen Supports des Cybercrime-Competence-Centers C4 werden mittlerweile 80 Client-Computer und 25 Server sowie die Netzwerkinfrastruktur von acht unterschiedlichen Netzen administriert und betreut. Techniker des C4 leisteten in 15 komplexen Fällen, für die technisches Spezialwissen erforderlich war, erfolgreich Assistenz. Im Bereich der IT-Beweissicherung wurden 2014 in mehr als sechs Sonderkommissionen über 120 Terabyte (TB) an elektronischen Beweisen gesichert. Der Fachbereich Mobile Forensik hat 2014 knapp 1.200 Mobilgeräte ausgewertet. Im Referat Ermittlungen sind neben zahlreichen anderen Fällen auch Phänomene wie die Schadsoftware BlackShades, Polizeitrojaner, Telefon-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 kann durch den C4-Journaldienst beispielsweise die Einleitung von Maßnahmen zur technischen Unterstützung anderer Dienststellen, Datensicherung, Handy- und Navigationssystemauswertung veranlasst werden, beispielswiese bei Suizidankündigungen über das Internet.

Im Oktober 2014 wurde vom C4 erstmalig eine Fachtagung für IT-Forensiker und Bezirks-IT- Ermittler organisiert. Bei der Fachtagung wurden die Zuständigkeiten und Aufgaben des C4 einem breiten Publikum vorgestellt. Darüber hinaus wurden technische Themen vorgetragen. Von besonderem Interesse waren auch die geplanten Änderungen im Rahmen der laufenden Strafrechtsreform, die von Univ.-Prof. Dr. Susanne Reindl-Krauskopf vom Austrian Center for Law Enforcement Studies (ALES) dargestellt wurden. Ein Vertreter von Europol referierte über den internationalen Aspekt der kriminalpolizeilichen Zusammenarbeit und die Kooperation mit EC3.

Weitere Infos auf:
http://ales.univie.ac.at
https://www.europol.europa.eu/ec3

LANDESKRIMINALAMT UND BEZIRKS-IT-ERMITTLER

Neben dem Cybercrime-Competence-Center C^4 auf Bundesebene bestehen in allen Landeskriminalämtern mit dem Assistenzbereich 06 „IT-Beweissicherung“, dem C^4 vergleichbare Dienststellen. In diesen Organisationseinheiten sind kriminalpolizeilich und technisch ausgebildete Experten mit der Bekämpfung von Cybercrime und der IT-Forensik in den jeweiligen Bundesländern befasst.

Für die Bekämpfung von Cybercrime auf lokaler Ebene und zur Unterstützung der Kollegen in den Polizeiinspektionen wurden in den letzten Jahren rund 280 Bezirks-IT-Ermittler ausgebildet.

PROFESSIONALISIERUNG BEI DER BEKÄMPFUNG VON CYBER-KRIMINALITÄT

Die Professionalisierung beginnt bereits bei der Ausbildung der Polizisten und setzt sich in den Polizeiinspektionen den Stadt- und Bezirkspolizeikommanden fort.

2014 wurden auch wieder zahlreiche Spezialschulungen für die operativ tätigen Kriminalbeamten abgehalten und sechs Ausbildungskurse für Bezirks-IT-Ermittler durchgeführt. Die Aufgabe dieser Beamten besteht einerseits in der Unterstützung bei der IT-Beweissicherung. Andererseits bilden sie die Schnittstelle zwischen der täglichen Polizeiarbeit an der Basis und den Bereichen IT-Forensik und Cybercrime-Ermittlungen in den Landeskriminalämtern.

Laufende Kontakte und Zusammenarbeit unter anderem mit dem Bundesministerium für Justiz (BMJ), dem Bundesministerium für Finanzen (BMF) sowie anderer Behörden spiegeln die enge Verflochtenheit bei der Bekämpfung von Cybercrime wider.

Mitarbeiter der Landeskriminalämter (LKA, Assistenzbereich 06) haben an den Schulungen zu „Mobile Forensik“ teilgenommen. Von den LKAs wurden Spezialschulungen und Workshops ausgerichtet und Kurse in Fachhochschulen (zum Beispiel FH Hagenberg) genutzt. Gleichzeitig wurden auf Grund der Kriminaldienst-Fortbildungsrichtlinien (KDFR) Schulungen für andere Abteilungen und andere kriminalpolizeiliche Bereiche abgehalten.

Das LKA Vorarlberg (Assistenzbereich 06) hat in Folge des starken Zusammenhangs zwischen Betrugs- und Cyber-Kriminalitätsdelikten für die Bezirks-IT-Ermittler eine Ausbildung im Bereich Betrugsermittlung organisiert. Zusätzlich veranstaltete die Landespolizeidirektion (LPD) Vorarlberg die Fortbildungstage 2014, wo neben fachspezifischen Themen auch die aktuelle Kriminalitätsentwicklung im Internet mit den Schwerpunktthemen Betrug, Erpressung, Nötigung und Cybermobbing ergänzt um Ermittlungsansätze im IT-Bereich geschult wurden.

Im Februar 2014 wurden im Rahmen eines von der EU geförderten Projektes „EU Support to Law Enforcement“ Polizeieinheiten aus den unterschiedlichen Kantonen in Bosnien und Herzegowina geschult. Bei dieser einwöchigen Veranstaltung schulten Mitarbeiter des C⁴ zu dem Thema „IT Security in Law Enforcement Agencies“, um grundlegende als auch vertiefende Aspekte aktueller IT-Security-Standards und „best practices“ den Einheiten in Bosnien und Herzegowina zu vermitteln. Ziel dieses Workshops war es, die Teilnehmer mit Spezialwissen auszustatten, so dass ein Cyber-Kriminalitätslabor samt technischer Ausstattung mit hohen Sicherheitsanforderungen aufgebaut werden kann.

Techniker des Cybercrime-Competence-Centers C⁴ haben an einem speziellen Technik-Workshop in Baden-Württemberg teilgenommen. Bei dieser jährlichen Veranstaltung treffen sich Techniker aus dem Bereich IT-Ermittlung, -Forensik und Cyber-Kriminalität, um technische Lösungen und Probleme zu besprechen sowie Erfahrungen auszutauschen. Die vorgestellten Eigenentwicklungen stellen oftmals einen hohen Mehrwert für die Arbeit bei der Lösung von technischen Aufgaben dar.

Weitere Infos auf:
https://www.justiz.gv.at
https://www.bmf.gv.at
http://www.fh-ooe.at/campus-hagenberg
http://msb.gov.ba

MELDESTELLE „AGAINST CYBERCRIME“

Im Mai 2011 wurde als Ansprechstelle für die Bürger unter der E-Mailadresse against-cybercrime@bmi.gv.at die Meldestelle für Cyber-Kriminalität eingerichtet. Dort werden verdächtige Wahrnehmungen im Internet entgegengenommen. Im Jahr 2014 wurde in der Meldestelle ein 24/7-Betrieb eingerichtet, um zeitnahe wichtige und dringende Mitteilungen entgegenzunehmen und Sofortmaßnahmen veranlassen zu können. Die kontinuierliche Steigerung der gemeldeten Verdachtsfälle setzte sich auch im Berichtsjahr fort. So wurden in der Meldestelle des C^4 im Jahr 2014 9.497 E-Mails bearbeitet und über 900 telefonische Anfragen beauskunftet.

THEMENSCHWERPUNKTE

Nach wie vor liegt der Schwerpunkt der Anfragen auf Phishing- und Spam-Mails. Eine deutliche Steigerung gab es bei Meldungen über versuchte Betrugsfälle auf Online-Plattformen, bei Ein- und Verkäufen im Internet – zumeist bei Kfz- oder Immobilienangeboten. Der gängige Modus Operandi des Bestellens/Nichtbezahlens geht hier in Richtung der Vortäuschung von gefälschten Bezahlbestätigungen durch PayPal- und Amazon-Konten. Weiters konnte eine erhöhte Anzahl von Meldungen über sogenannte „Fake-Webshops“ und „B2B-Shops“ und damit zusammenhängende Betrugs- und Urheberrechtsverletzungen registriert werden. Neben den laufend auftretenden Deliktsformen war 2014 durch das massive Auftreten von Anrufen von angeblichen „Microsoft Mitarbeitern/Technikern“, der Verständigung von über 40.000 in Österreich betroffenen E-Mail-Accounts nach einem in Deutschland vorgefallenen „Datenklau“ sowie von schwerwiegenden Fällen von „Ransomware“ wie Crypto-Wall und Crypto-Locker geprägt.

Vermehrt musste auch Unterstützung für andere Dienststellen im Zusammenhang mit Vorfällen und Mitteilungen aus dem Internet geleistet werden, wie zum Beispiel die Ausforschung von IP-Adressen im Falle von Suizidankündigungen, der Meldung von Gewaltvideos im Internet, der Verständigung von Betroffenen bei inkriminierten Webseiten und Domänen und mehr.

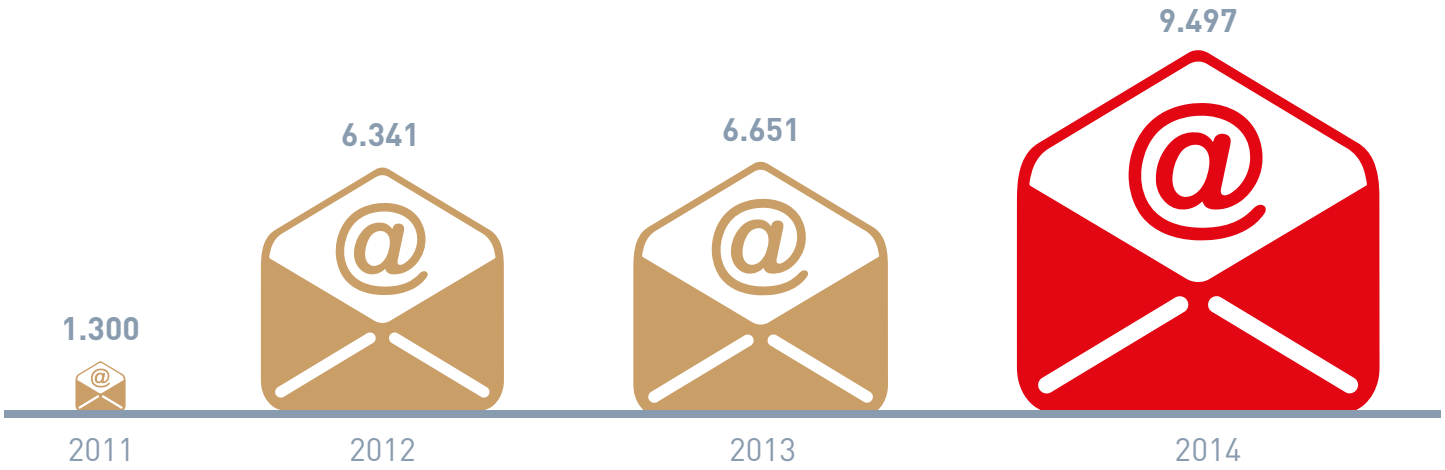


Abbildung 6: Anzahl der Hinweise an die Meldestelle against-cybercrime@bmi.gv.at seit ihres Bestehens im Jahr 2011

BEWEISSICHERUNG UND ANALYSE

Die Verwendung von IT-Medien ist mittlerweile in fast alle Kriminalitätsformen vorgedrungen. Waren es zu Beginn der elektronischen Beweismittelsicherung meist nur Stand-PCs und Laptops, geht der Trend nun zu immer kleineren und leistungsstärkeren mobilen Geräten. Daten von Smartphones und Tablets gewinnen dabei immer mehr an Bedeutung für kriminalpolizeiliche Ermittlungen. Wie bereits in den letzten Jahren war auch 2014 ein deutlicher Anstieg der Zahl von Auswertungen derartiger Geräte zu verzeichnen. Bei immer kleiner werdender physischer Größe steigt hingegen die Datenkapazität exponentiell nach oben. Im Vergleich zum Vorjahr stieg die Anzahl der Auswertungen erneut um rund 30 Prozent, wobei die Datenmenge eine nahezu hundertprozentige Steigerung ergab. Vor allem diese spielt im Rahmen der elektronischen Beweissicherung eine immer bedeutungsvollere Rolle. Mittlerweile erreichen einzelne Datensicherungen im Zuge von polizeilichen Ermittlungen einen dreistelligen Terabyte-Bereich. Sogenannte „Private-Cloud"-Lösungen ermöglichen es, die Speicherkapazitäten nahezu unendlich zu erweitern. Der rasante Preisverfall bei Datenträgern unterstützt diesen Trend und sorgt dafür, dass immer höhere Datenmengen bei polizeilichen Ermittlungen gesichert werden. Dies stellt nicht nur die Datensicherung sondern vor allem die weitere Auswertung vor extreme Herausforderungen. So wurden im Jahr 2014 durch das C^4 über 500 TB an Daten sichergestellt.

In Verbindung mit den großen Datenmengen wird auch die Speicherung von Daten in der sogenannten „Cloud" immer beliebter. Neben der privaten Cloud, die es ermöglicht, die Kapazitäten der eigenen Infrastruktur immer größer werden zu lassen, werden mit den sogenannten „Public Cloud"-Lösungen die Daten an externe Anbieter ausgelagert.

Um eine erfolgreiche Beweissicherung, -aufbereitung und -auswertung der auf den Speichermedien sichergestellten Daten gewährleisten zu können, ist spezielles Fachwissen und vor allem praktische Erfahrung notwendig. Dieses Know-how im Bereich der IT-Beweissicherung konnte auch 2014 wieder durch die Teilnahme an entsprechenden Spezialtrainings im In- und Ausland sichergestellt werden.

Neben entsprechender Erfahrung und Know-how ist auch eine adäquate Ausstattung für eine erfolgreiche Datensicherung und Auswertung maßgeblich. Vor allem die großen Datenmengen können mit herkömmlichen forensischen Mitteln kaum noch bewältigt werden. Suchtechnologien, die mittels mathematischen Verfahren dabei helfen sollen, die berühmte „Nadel im Heuhaufen" zu finden, wurden 2014 umfangreich getestet und werden auch 2015 für Auswertungen zur Verfügung stehen. Damit soll gewährleistet sein, dass die forensische Datensicherung innerhalb der Exekutive den Entwicklungen der nächsten Jahre standhält.

Allein durch den Assistenzbereich 06 IT-Beweissicherung im LKA Burgenland wurden mehr als 50 Fälle bearbeitet. Daraus ergab sich ein Gesamtdatenvolumen von 50 TB. Darüber hinaus wurden in Summe 120 Aktenvorgänge durch die Bezirks-IT-Ermittler bearbeitet. In der LPD Kärnten wurden mehr als 849 Delikte mit IT-Bezug, das heißt Cyber-Kriminalitätsdelikte im engeren und weiteren Sinn, gemeldet.

„BEST PRACTICES“ 2014

TEILNAHME AN INTERNATIONALEN OPERATIONEN

Im November 2014 beteiligte sich die österreichische Polizei im Rahmen einer weltweit angelegten Europol-Operation zur Bekämpfung der internationalen Kreditkartenkriminalität. Dabei standen betrügerisch erworbene Flugtickets im Fokus, die mittels widerrechtlich erlangter Kreditkartendaten im Internet bezahlt wurden. Bei den zweitägigen Kontrollen – auch am Standort Flughafen Wien-Schwechat – sowie an weiteren 80 Flughäfen in 45 Ländern wurden 118 Verdächtige festgenommen. Die Aktion erfolgte in Kooperation mit privaten Unternehmen. Sie zeigt, dass der Internetbetrug durch Zusammenarbeit erfolgreich bekämpft werden kann. Eine weitere internationale Zusammenarbeit der Strafverfolgungsbehörden im Bereich Zahlungskartenkriminalität fand im Rahmen der Operation „Archimedes“ statt.

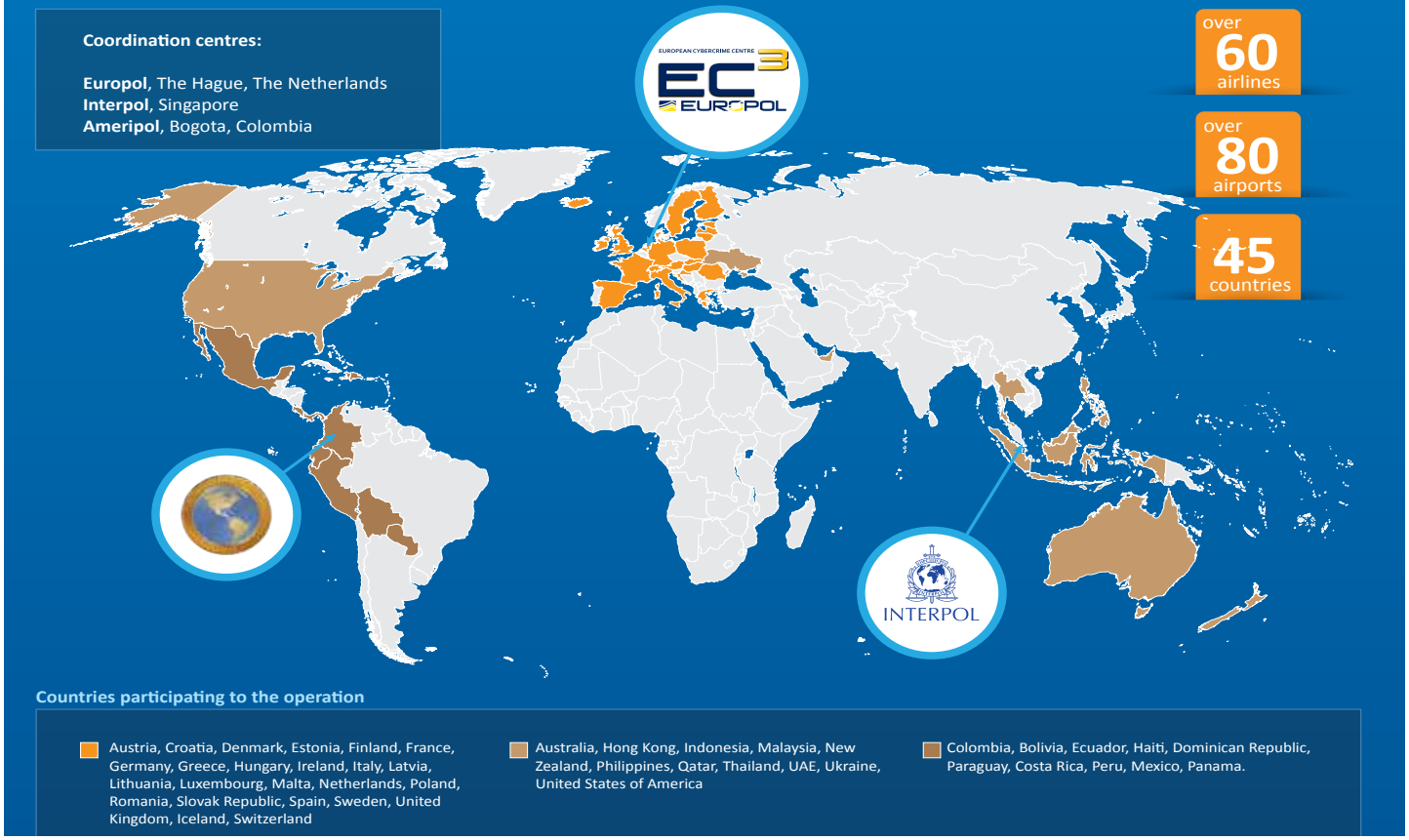
Mehr Infos auf:
https://www.europol.europa.eu/

Global action against online fraudsters in the airline sector

26 - 27 November 2014

Operation

The coordinated Global Airport Action targeted criminals suspected of fraudulently purchasing plane tickets online using stolen or fake credit card data.



Countries participating to the operation

- Austria, Croatia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Romania, Slovak Republic, Spain, Sweden, United Kingdom, Iceland, Switzerland
- Australia, Hong Kong, Indonesia, Malaysia, New Zealand, Philippines, Qatar, Thailand, UAE, Ukraine, United States of America
- Colombia, Bolivia, Ecuador, Haiti, Dominican Republic, Paraguay, Costa Rica, Peru, Mexico, Panama.

Abbildungen 7 und 8: Internationale Operation gegen Kreditkartenkriminalität, Quelle: Europol

ZUSAMMENARBEIT IM KAMPF GEGEN INTERNETBETRUG

Das Internet bietet den Tätern Anonymisierungsmöglichkeiten, eine größere Reichweite und eine schnelle Vorgehensweise unter Nutzung ständig wechselnder falscher Identitäten. Vielfach agieren die Täter aus dem Ausland und verschleiern ihre Spuren, wodurch eine Nachverfolgung für die Strafverfolgungsbehörden in Österreich deutlich erschwert wird. Die Aufklärungsarbeit erfordert neben der Tatortarbeit am Computer des Opfers auch die konsequente Verfolgung der Geldspur durch die Polizei. Das Ziel der Täter ist das Geld der Opfer. 2014 wurde daher die Zusammenarbeit der Spezialisten innerhalb der Polizei weiter ausgebaut. Experten aus den Bereichen Betrugsermittlung, der IT-Forensik und der Finanzermittlung verschränken ihr Wissen und eröffnen damit neue Ermittlungsansätze zur Ausforschung von Tatverdächtigen. Zusätzlich ist eine zuverlässige internationale Kooperation entscheidend, um die Gelder der Opfer zu sichern und die Täter im Ausland ausforschen zu können.

LEICHTSINNIGER UMGANG MIT PASSWÖRTERN

Vom 1. bis 20. März 2014 kam es in Kärnten zu einem Fall von Datenbeschädigung und widerrechtlichem Zugriff auf ein Computersystem, im Zuge dessen ein Schaden von über 20.000 Euro entstanden ist. Beim Beschuldigten und beim Opfer handelt es sich jeweils um große Firmen, die mit dem Handel von Lkw-Teilen, dem Verkauf und der Reparatur von Lkws in Kärnten marktbestimmend sind. Während des oben angeführten Zeitraumes verschaffte sich der anfangs noch unbekannte Beschuldigte über ein Warenwirtschaftssystem des Markenherstellers im Ausland durch Verwendung fremder Passwörter unberechtigten Zugriff auf die Preislisten des konkurrierenden Unternehmens und änderte diese. Der Zugriff erfolgte dabei unter Verwendung fremder oder alter zurückgesetzter Zugangsdaten. Ziel des Täters war es, das Vertrauen der Kundschaft in das konkurrierende Unternehmen zu schädigen und so selbst mit dem eigenen Unternehmen mehr Aufträge zu lukrieren und die Marktposition zu verbessern. Im Zuge der Ermittlungen im Unternehmen des Opfers sowie in Zusammenarbeit mit den IT-Administratoren des Lkw-Herstellers konnte letztendlich die IP-Adresse des Beschuldigten ermittelt werden. Im Zuge der Hausdurchsuchung konnten beim Inhaber der IP-Adresse maßgebliche Dokumente sichergestellt werden. Letztendlich wurden unter der Tastatur des Beschuldigten sogar rechtswidrig erlangte Passwörter aufgefunden, die den Beschuldigten zum Eingeständnis der Tat bewegten. Dieser Fall hat einmal mehr die Wichtigkeit im Umgang mit Passwörtern und deren Aufbewahrung gezeigt.

PRÄVENTION

Bei der Bekämpfung von Cybercrime spielt der unmittelbare Kontakt mit der Bevölkerung eine wesentliche Rolle. Die Beamten in den Polizeiinspektionen, die Bezirks-IT- Ermittler, die Präventionsbeamten und die Experten in den Landeskriminalämtern sowie im Cybercrime-Competence-Center C^4 arbeiten im Rahmen von Beratungen und Vorträgen daran, in Österreich ein angemessenes Schutzniveau zu etablieren.

So liegt ein Schwerpunkt der Kriminalpolizei in Vorarlberg neben der Präventionsarbeit bei der internen Sensibilisierung der Kollegenschaft. Bei Betrugshandlungen im Internet gilt es für die Polizeidienststellen an der Basis neben der Bearbeitung des Sachverhaltes auch an der Minimierung des Schadens mitzuwirken. So sind die Beamten den Opfern bei der Rückabwicklung von allfälligen Überweisungen und der Verhinderung der Auszahlung von Geldern an die Täter behilflich. Unterstützt werden die Kollegen durch aktuelle Informationen im Intranet der LPD Vorarlberg mit Anleitungen zum Erkennen und zur Bearbeitung von Cyber-Kriminalitätsdelikten und Lösungsansätzen zur kriminalpolizeilichen Ermittlung und Schadensminimierung. Ziel soll es sein, das Intranet als Informationsquelle für die tägliche Polizeiarbeit zu etablieren. Im Rahmen der Präventionsarbeit wurden Vorträge durch besonders geschulte Beamte der Polizeiinspektionen in Vorarlberg im Rahmen des Jugendpräventionsprojektes „Click & Check“ angeboten. Dieses Informationsangebot wurde vom LKA Vorarlberg durch Informationen zum Thema Jugendschutz, Gefahren im Netz sowie Recherchen im Netz ergänzt. Ein Fokus wurde auch darauf gelegt, die Bevölkerung in den Medien und sozialen Medien vor aktuellen Begehungsformen der Internetkriminalität zu warnen.

In allen Bundesländern wurden Geschädigten und Opfern entweder im Rahmen der Vernehmung bzw. bei einem anschließenden Gespräch Informationen über Schutzmaßnahmen für Computer und Mobiltelefone sowie Ratschläge zum richtigen Umgang mit dem Internet vermittelt.

KOOPERATIONEN

Für die Kriminalprävention stellt das Thema „IT-Sicherheit“ einen immer höheren Stellenwert der täglichen Arbeit dar. Durch verstärkte, kompetente und rasche Präventionsarbeit kann viel zur Sicherheit jedes Einzelnen im Internet beigetragen werden. Denn viele strafbare Handlungen, die im Zusammenhang mit Computern und Internet begangen werden, könnten bei entsprechender Aufmerksamkeit und adäquaten technischen Schutzvorkehrungen verhindert werden. Jeder sollte sich die Zeit nehmen, und sich über mögliche Gefahren und Schutzmaßnahmen im Netz zu infomieren. Einen wesentlichen Anteil am hohen Standard der Präventionsprojekte stellt die enge Kooperation mit der Wissenschaft, im speziellen mit der Fakultät für Informatik der Universität Wien, dar. In vielen Veröffentlichungen und Veranstaltungen liefert die Kriminalprävention

für Bürger, aber auch für Unternehmen konkrete Handlungsempfehlungen, die zu mehr Sicherheit im Umgang mit Datenverarbeitungssystemen beitragen. So beteiligen sich unter anderem die Experten des Bundeskriminalamts an Beiträgen bei Veranstaltungen, wie zum Beispiel bei jenen des Kuratoriums Sicheres Österreich (KSÖ) und der Wirtschaftskammer Österreich und unterstützen Initiativen wie „SaferInternet“ und den „Internetombudsmann“, um die Zielgruppen zu erreichen und das Bewusstsein für die Gefahren, die mit der Verwendung des Internets und der sozialen Medien verbunden sind, zu schärfen.

Die Abteilung Wirtschaftskriminalität im Bundeskriminalamt führte auch 2014 die Zusammenarbeit im Rahmen des Projektes „Unternehmen Sicherheit“ zwischen der Wirtschaftskammer Österreich (WKO) und dem BMI weiter. Dabei informiert die WKO ihre Mitglieder über aktuelle Betrugsphänomene auf Basis der Information durch das Bundeskriminalamt. Eine weitere Kooperation besteht mit dem „Österreichischen Institut für angewandte Telekommunikation“ (ÖIAT), das die Plattformen „Internetombudsmann“ und „Watchlist Internet“ betreibt. Darüber hinaus referieren die Experten regelmäßig in Fachvorträgen, Diskussionen und auf Kongressen über die Gefahren im Internet.

Weitere Infos unter:
https://kuratorium-sicheres-oesterreich.at
http://www.wko.at/sicherheit
http://www.ombudsmann.at
https://www.watchlist-internet.at

PERSÖNLICHE BERATUNG UND BERATUNG IM INTERNET

Im Vordergrund der Kriminalprävention steht der persönliche Kontakt mit der Bevölkerung. Bei speziellen Fragen zum Thema Computerkriminalität können sich Bürger und 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.
Auf der Webseite und auf den Social-Media-Seiten des Bundeskriminalamts gibt die Polizei laufend Tipps, wie man sich selbst und seinen Computer im Internet schützen kann und informiert über aktuelle Gefahren und Schutzmaßnahmen:

www.bundeskriminalamt.at
www.facebook.com/bundeskriminalamt

Zur Polizei-App

Die „Polizei-App“, die gratis zum Download für Apple, Android und Windows Systeme zur Verfügung steht, bringt unter anderem Präventionstipps auf das Smartphone. Außerdem wird in Zusammenarbeit mit der Universität Wien ein E-Learning Modul für Erwachsene entwickelt, mit dem man bequem von zu Hause den richtigen Umgang mit dem Internet und sozialen Medien lernen kann.

JUGENDPRÄVENTIONSPROJEKTE DER KRIMINALPRÄVENTION

Der Themenbereich der neuen Medien wurde auf Polizeiebene in zwei Projekten umgesetzt. Im Vordergrund steht dabei das Projekt „Click & Check“, das österreichweit erfolgreich umgesetzt wird. Um eine möglichst hohe Nachhaltigkeit sicherzustellen, werden Eltern, Lehrer und Schüler in das Projekt miteinbezogen. So wird gewährleistet, dass ein Bewusstsein für diese Gefahren bei erwachsenen Bezugspersonen geschaffen wird. Polizeibeamte klären Jugendliche in den Schulen über „Happy Slapping und „Cyberbullying oder -mobbing“ auf, um unter Einbeziehung kurzer Videofilme das Unrechtsbewusstsein von Jugendlichen zu fördern und Gesetzesinformationen zu vermitteln. Im Jahr 2014 wurden österreichweit über 44.100 Kinder und Jugendliche im Rahmen von „Click & Check“ über den richtigen, sicheren Umgang mit Handy und PC sensibilisiert und informiert.

Neben dem Jugendpräventionsprojekt „Click & Check“ standen auch 2014 die Gefahren von „Cyber-Grooming“ im Projekt „Jugend OK“ im Vordergrund. Bei Cyber-Grooming handelt es sich um eine besondere Form der sexuellen Belästigung: Mittels falschem Profil nehmen Täter über das Internet Kontakt zu Minderjährigen auf und versuchen, von ihnen selbsterstellte kinderpornografische Fotos (Nackt-Selfies) zu entlocken. Manchmal ersuchen sie auch um ein persönliches Treffen, mit dem Ziel, die Kinder oder Jugendlichen sexuell zu missbrauchen.

Im Aktionsmonat vom 15. November 2014 bis 15. Dezember 2014 wurden Jugendliche mittels Informationskarten auf die Gefahren von Handydiebstahl und Handymissbrauch aufmerksam gemacht. Eine Auflistung technischer Möglichkeiten zur Sicherung des Mobiltelefons in Form von vorinstallierten Programmen oder Apps war Inhalt einer weiteren, neuen Informationskarte. In diesem Zeitraum konnten 27.982 Jugendliche zu den Gefahren im Umgang mit modernen Kommunikationsmitteln informiert werden.

Weitere Infos auf:
www.clickundcheck.at

PROJEKTE IM JAHR 2014

DATA TRASH: PERSÖNLICHE DATEN AUF DEM FLOHMARKT

Unwissenheit und Vertrauen bei der Entsorgung privater Datenträger sind die Ursache, dass oft ganz persönliche und sensible Daten in falsche Hände geraten. Die einzig sichere Methode, ihre Daten unwiederbringlich zu vernichten, ist die physikalische Vernichtung unter persönlicher Anwesenheit. Wenn Sie eine Festplatte nicht überschreiben wollen oder können, sollten Sie die Festplatte beschädigen oder zerstören. Das gilt auch für Speichermedien wie CD/DVDs oder USB-Sticks. Dabei kann durchaus auch ein Bohrer oder Hammer hilfreich sein. Computer, Festplatten, USB-Sticks, Speicherkarten, CD/DVDs, Magnetbänder, Handys, usw. sind ideale Speichermedien. Aber was passiert mit ihnen, wenn sie nicht mehr benötigt werden? Mit Daten und Datenträgern wird leider oft sehr sorglos umgegangen. Daten können zwar gelöscht, aber in den meisten Fällen auch wieder rekonstruiert werden. Gelangen Daten in falsche Hände, sind sie nicht nur unerschöpfliche Informationsquellen und dadurch eine Gefahr für jeden Einzelnen, die Familie, die soziale Struktur und das öffentliche Leben, und können eine Grundlage krimineller Aktivitäten werden.

Im Zuge eines Projektes des Landeskriminalamtes Tirol wurden im Internet und auf Flohmärkten 60 gebrauchte Datenträger mit dem Ziel gekauft, die Datenträger zu sichten und den Inhalt bei Bedarf mit kostenloser Software zu rekonstruieren. In weiterer Folge wurden die Ergebnisse veröffentlicht, um auf diese Thematik hinzuweisen und für die Zukunft zu verhindern, dass auf diese Weise sensible Daten in falsche Hände gelangen. Das Ergebnis: Kein einziger der 60 Datenträger mit einem Gesamtdatenvolumen von rund 1,5 Terabyte war gelöscht oder formatiert. Es war also nicht notwendig, die Datenträger mit Programmen zu bearbeiten, um die eventuell gelöschten Daten wiederherzustellen. Auf den Datenträgern befanden sich „für jeden lesbar" teilweise hochsensible Daten: Persönliche Dokumente, E-Mails, Bilder, Kreditkarteninformationen, Bankdaten, Finanzierungsunterlagen, Bewerbungsschreiben, Kontoauszüge, Finanzsituation, Sparbücher, Informationen über sexuelle Interessen, ungelöschter Internetverlauf und damit Hinweise auf das User-Verhalten, Daten einer Schule aus Deutschland mit Aufzeichnungen über Schüler, Exekutionsdaten eines deutschen Gerichtes, Daten eines Vereines und einer politischen Repräsentantin aus Deutschland mit Protestschreiben, Mitgliederverzeichnis, Vereinsfinanzen, Protokolle über Sitzungen und Zerwürfnisse.

Resümee dieses Projektes: Daten kennen keine Grenzen – auch wenn sie nicht über das Internet versendet oder empfangen werden. Der Angriff auf persönliche und sensible Daten erfolgt meist viel unspektakulärer als angenommen. Grundsätzlich sollte sich daher jeder Nutzer eines PCs folgende Fragen stellen: Wem vertraue ich meine Datenträger oder Geräte (PC, Smartphone usw.) an, wenn sie defekt sind? Wie viele Datenträger habe ich und was ist darauf gespeichert? Und ... wo sind sie? Wie habe ich bisher meine Geräte und Datenträger entsorgt? Sperrmüll, Flohmarkt, Internet, Familie, Freunde?

KIRAS PROJEKT „SOCIAL MEDIA CRIME“

Im Rahmen des Projektes „Social Media Crime“ wurde eine umfangreiche Untersuchung zur wissenschaftlich fundierten Strukturierung von Social-Media-spezifischen Kriminalitätsformen durchgeführt. Mittels wissenschaftlicher Recherche und Erhebungen wurde eine Analyse einzelner Social-Media-Crime-Phänomene und -Aktivitäten erstellt, die nicht nur Aufschluss über Erscheinungsformen, sondern auch über Ursachen und Folgen sowie Opfer- und Tätercharakteristika gibt. Die Ergebnisse wurden auf Basis von kriminalpolizeilichen Anforderungen strukturiert und kategorisiert. Anhand dieser Einteilung werden Präventions- und Gegenmaßnahmen, die international bereits eingesetzt bzw. angedacht sind, aufgezeigt. Aufbauend auf diesen Erkenntnissen wurden konkrete Handlungsempfehlungen generiert, die kriminalpolizeiliches Vorgehen dabei unterstützen sollen, Social Media Crime langfristig zu reduzieren.

Projektpartner waren SYNYO GmbH, Austrian Center for Law Enforcement Studies (ALES) der Universität Wien und das Cybercrime-Competence-Center C^4.

Weitere Infos auf:
www.kiras.at

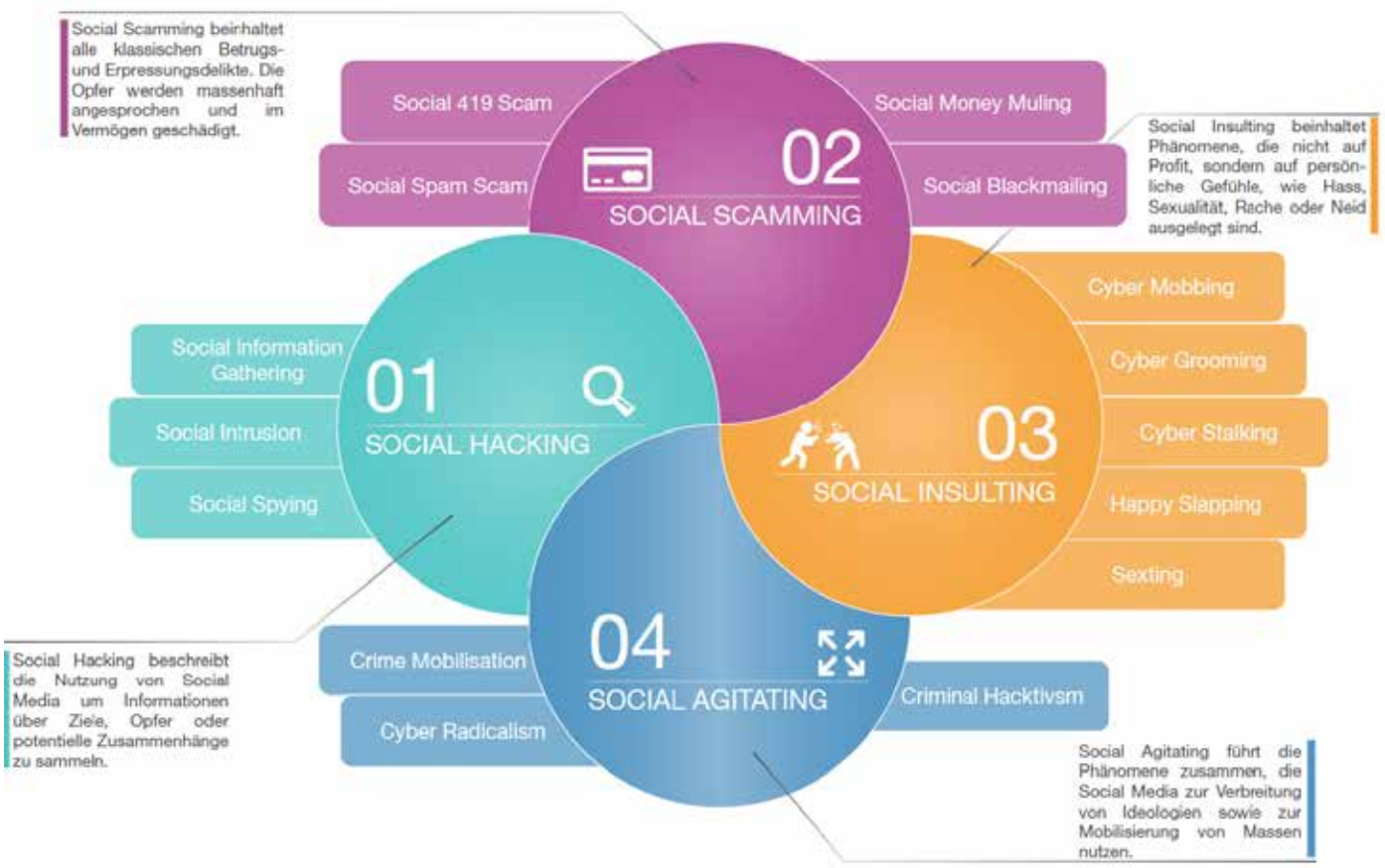


Abbildung 9: Social Media Crime Taxonomie

INTERNATIONALES

2014 wurden zahlreiche Projekte und Maßnahmen umgesetzt und die enge Zusammenarbeit mit Europol und dem Europäischen Cybercrime Center (EC3) forciert:

EUROPÄISCHE EBENE

Im Rahmen des EMPACT-Programms (European Multidisciplinary Platform Against Criminal Threats) war das Cybercrime-Competence-Center C^4 in der Sub-Priority Group Cyberattacks maßgeblich an den Umsetzungsarbeiten der acht Strategieziele sowie dem Operational Action Plan (OAP) 2014 beteiligt. Insbesondere auf das 6. Strategieziel, das die europaweite Einführung von Mindeststandards für die Ausbildung im Bereich Cybercrime-Ermittlungen und IT-Forensik betrifft, wurde besonderer Wert gelegt. Seit Mai 2014 ist die Funktion des ECTEG (European Cybercrime Training & Education Group) Vice Chair durch einen Mitarbeiter des C^4 besetzt, wodurch das Thema Ausbildung von Cybercrime- und IT-Forensik-Experten aus österreichischer Sicht auch auf europäischer Ebene besser transportiert wird.

Im Dezember 2014 konnte für den Operational Action Plan (OAP) 2015 das Maßnahmenpaket zur Erarbeitung eines IT-Governance-Models durch EC3, European Cybercrime Training and Education Group (ECTEG), Eurojust sowie Österreich als EMPACT-Mitgliedsstaat initiiert werden. Ziel ist es bis Sommer 2015 ein Dokument zu erarbeiten, das den Anforderungen einer EU-weiten IT-Governance aufzeigen soll. Im Zentrum steht die Erarbeitung von Maßnahmen, die eine nachhaltige EU-Finanzierung aller Ausbildungsmaßnahmen zur fortlaufenden Qualifizierung der „Law Enforcement"-Experten für Cybercrime und IT-Forensik der europäischen Mitgliedstaaten künftig sicherstellen soll.

Weitere Infos auf:
http://www.ecteg.eu/

JOINT CYBERCRIME ACTION TASKFORCE (J-CAT)

J-CAT wurde im September 2014 als Pilotprojekt des EC3 ins Leben gerufen. Ziele dieses Projektes sind vor allem ein rascher, intensiver Informationsaustausch sowie die effektive operative Zusammenarbeit. Neben zahlreichen EU-Mitgliedsstaaten beteiligen sich derzeit auch die USA, Kanada, Australien und Kolumbien an dieser Taskforce. J-CAT führt Ermittlungen

nicht selbständig, sondern koordiniert die internationale Zusammenarbeit auf direkte, unbürokratische Weise, dient als Informationsdrehscheibe und leistet erforderlichenfalls technischen Support. Um die österreichische Beteiligung möglichst effizient gestalten zu können, befasst sich ein Verbindungsbeamter des Bundeskriminalamtes in Den Haag (Niederlande) ausschließlich mit J-CAT.

Einer der aufsehenerregendsten Erfolge dieser länderübergreifenden Zusammenarbeit war die Operation „Onymous", bei der illegale Online-Marktplätze, insbesondere die „Silk Road 2.0" im Fokus der Ermittlungen standen. Im Zuge dieser internationalen Polizeiaktion wurden in 15 Ländern mehr als 100 Services vom Netz genommen, 17 Verdächtige verhaftet, 13 Hausdurchsuchungen durchgeführt, sowie Bitcoins und Bargeld im Wert von über eine Million US-Dollar, Drogen, Gold und Silber sichergestellt. Außerdem wurden 414 illegale Webseiten vom Netz genommen.

Weitere gemeinsame Operationen befassen sich derzeit mit

- Counter Antivirus Services,
- Bulletproof Hosting,
- bösartiger Software zum Angriff auf Banken,
- bösartigen Smartphone-Apps,
- komplexen Betrugshandlungen im Internet,
- der Bekämpfung von Bot-Netzen und
- Ermittlungen im Zusammenhang mit Geldwäsche im Internet.

INTERNATIONALE EBENE

Die Inbetriebnahme des neuen Interpol Standortes in Singapur im Oktober 2014 sowie der damit einhergehende Start der operativen Phase des „Interpol Digital Crime Centers" (IDCC) markieren einen weiteren Meilenstein bei der Bekämpfung von Internetkriminalität auf internationaler Ebene geht. Im IDCC sind Experten aus aller Welt in den Bereichen Innovation, Forschung und digitale Sicherheit tätig und widmen sich verstärkt dem Thema Cybercrime. Auch Österreich hat einen Vertreter entsandt: der die Funktion des Assistent Directors for International Partnerships and Development bekleidet.
Weitere Infos auf: http://www.interpol.int

AUSBLICK

Das Gefährdungs- und Schädigungspotenzial durch Cybercrime ist unverändert hoch. Neben Zugangsdaten im Bereich des Online-Bankings werden alle Formen der digitalen Identität ausgespäht, vermarktet und in weiterer Folge missbräuchlich eingesetzt.

Das Deliktsfeld Cybercrime entwickelt sich weiterhin dynamisch, technologische Neuerungen werden von Kriminellen auf Schwachstellen und Eignung für kriminelle Aktivitäten untersucht und in der Folge auch entsprechend eingesetzt. Neue technische Sicherheitsmaßnahmen – auch in Form von Software-Updates, die bereits bekannte Fehler beheben sollen – werden schnell durch neue Schadsoftware überwunden oder es erfolgt eine Anpassung des Modus Operandi. Diese Dynamik lässt sich am Beispiel des Phishings, dem „Fischen" nach Passwörtern, beim Online-Banking, in sozialen Plattformen, bei E-Commerce Portalen sowie bei kontaktlosen Bezahlsystemen eindrucksvoll darstellen. Gerade in diesem Bereich ist auch in den nächsten Jahren mit weiterhin steigenden Fällen vor allem vor dem Hintergrund zu rechnen, dass die Täter schon jetzt über das entsprechende technische Wissen verfügen, Sicherungssysteme für mobile Anwendungen anzugreifen. Die unreflektierte Markteinführung neuer Technologien zum Wohle der Kunden bietet dafür ausreichend Potenztial.

Die Anpassungs- und Innovationsfähigkeit der Täter im Bereich Cybercrime erklärt sich anhand der Täterstrukturen, die sich verändert haben. Es agieren nicht mehr wenige hochspezialisierte Einzeltäter, wie in manchem Hollywoodfilm suggeriert, sondern überwiegend kriminelle Organisationen, die zumeist auf internationaler Ebene arbeitsteilig und interdisziplinär zusammenwirken und so die nationalen rechtsstaatlichen Möglichkeiten zur Strafverfolgung überfordern.

Die immer weiter voranschreitende Auslagerung von Rechen- und Speicherkapazität – praktisch „Global on Demand" – an diverse Anbieter zu Lasten der eigenen Kontrolle über IT-Sicherheit aber zu Gunsten des eigenen Budgets, bilden die beste Grundlage, um das Gefährdungs- und Schädigungspotenzial des Phänomens Cybercrime auch weiterhin hoch erscheinen zu lassen.

SUMMARY OF THE CYBERCRIME REPORT 2014

FACTS AND FIGURES

In 2014 cybercrime reports have decreased from 10.051 in 2013 to 8.966, which is a 10.8 reduction as compared to last year. By contrast, the number of IT offences (cybercrime in the narrow sense) has slightly increased in 2014. They include criminal acts involving Internet technologies such as illegal accessing a computer system. The detection rate was 40.8 percent in 2014, which is 4.4 percentage points below the 2013 rate. This decline is partly due to the professionalization of internationally operating criminal networks and to the increased use of encryption and anonymisation techniques.

TRENDS

While cybercrime is currently on the decline, the review of a ten-year-period clearly shows an upward trend. This can be explained by the large-scale expansion of computers - specifically smart phones and tablet computers – and data networks, in particular mobile broadband connections. The fact that information and communication technology has become an integral part of everyday life has brought about new crime phenomena and in the field of cybercrime it can be assumed that there is a large portion of unrecorded cases.

As before, a plethora of phishing and spam e-mails are in circulation. A significant increase of crime reports has been recorded in respect of attempted fraud on online platforms and in connection with sales and purchase transactions on the Internet – chiefly involving motor vehicle and real property offers. The usual modus operandi is ordering items and forging payment confirmations of Paypal and Amazon accounts.

CONTERACTION BY THE POLICE

The Cybercrime Competence Center C4 is the national and international contact point for combatting cybercrime in the Austrian Criminal Intelligence Service. On a regional level similar services have been established. In the regional units technically trained criminal investigators deal with IT forensics and the fight against cybercrime. In addition, around 280 district IT investigators have been trained in recent years with a view to support the staff in the police stations in suppressing cybercrime at a local level. Prevention is of vital importance for an efficient cybercrime control. So as to involve the population our officials in the police

stations, the district IT investigators, specialized prevention officials and CID experts working in the regional CIDs and in the Cybercrime Competence Center C4 provide counselling and give presentations on a continuous basis in an attempt to establish an adequate level of protection in Austria.

OUTLOOK

Cybercrime continues to pose a serious threat in terms of hazards and losses. In addition to access data for online banking all forms of digital identities are scouted, marketed and subsequently abused. Cybercrime is a highly dynamic offense area. Technological innovations are examined by criminals for vulnerability and suitability for criminal activities and they are subsequently used, where appropriate. Technical security measures such as software updates fixing known bugs are soon frustrated by new malicious software or newly adopted modi operandi.

GLOSSAR

Account Hijacking: Die Übernahme eines fremden Accounts (engl. „hijacking“: entführen, überfallen, berauben) z. B. von E-Mail-Accounts oder anderen Konten in einem Computersystem.

Antivirenprogramm (auch Virenscanner oder Virenschutz genannt): Software, die bekannte Computerviren, Computerwürmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt. Die Mehrzahl dieser Programme identifiziert Schadcode anhand von Signaturen, ohne die die Schadsoftware oftmals unerkannt bleiben kann.

Backdoor: 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-Attacken zu missbrauchen.

BotNet (Bot-Netz): (Kurzform von Roboter Netzwerk) Fernsteuerbares Netzwerk im Internet von Computersystemen, das aus untereinander kommunizierenden Bots besteht. Diese Kontrolle wird durch Würmer bzw. Trojanische Pferde erreicht, die den Computer infizieren und dann auf Anweisungen warten. Diese Netzwerke können für Spam-Verbreitung, (Distributed-) Denial-of-Service-Attacken usw. verwendet werden, zum Teil ohne dass die betroffenen Computersystembenutzer etwas davon bemerken. Zur Steuerung dieser Roboterarmee im Netzwerk werden sogenannte Command & Control-Server (C&C–Server) eingesetzt.

Bot: Überbegriff für ein Programm das vorwiegend verwendet wird, um Aufgaben automatisiert durchzuführen. In der Regel auch als übernommener Rechner bezeichnet, der in ein BotNet eingebunden wurde.

Browser: Webbrowser (engl. für „Durchstöberer“, „Blätterer“) sind spezielle Computerprogramme zum Betrachten von Webseiten im World Wide Web.

Brute Force Attacke: Es handelt sich hierbei um eine Methode um Passwörter oder Schlüssel zu „erraten„. Es werden dabei nacheinander alle möglichen Zeichenkombinationen ausprobiert bis das gesuchte Kennwort gefunden wird. Je länger das verwendete Passwort ist, desto länger dauert dieser Vorgang. Deshalb wird oft mit Wortlisten gearbeitet, um die Anzahl der Kombinationen, die ausprobiert werden, einzuschränken.

B2B (Business-to-Business): Anbieter von Waren, die sich primär oder ausschließlich an Geschäftskunden richten (und nicht an Privatpersonen).

Cloud-Services bzw. Cloud-Computing: Metapher für das Internet selbst. Es bezeichnet das Speichern oder den Zugriff auf Daten und Anwendungen (Programme) über das Internet an Stelle der Nutzung von lokalen Ressourcen wie Festplattenspeicher, Rechenleistung, etc. im PC selbst oder einem lokalen Netzwerk.

Command and Control-Server (C&C-Server): Zumeist übernommene oder unter falscher Identität angemietete Computer zur Steuerung der Bots.

Code Injection: Generelle Bezeichnung für Angriffe, wo Programmcode in eine (Web-)Anwendung (automatisch) eingegeben wird. Dieser Angriff nutzt die schwache Handhabung einer Anwendung aus (Sicherheitseinstellungen, Schwachstellen bei der Programmierung hinsichtlich der Überprüfung von Dateneingabe und -ausgabe). Bekannt ist die sogenannte SQL-Injektion, bei der in die Datenbankanwendung ein Programmcode eingegeben wird, der bei Abarbeitung im Datenbankprogramm den unberechtigten Zugriff ermöglicht (durch Manipulation der Abfrage-Semantik der Datenbank).

Computervirus: 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: Ein Computerwurm ähnelt einem Computervirus, verbreitet sich aber direkt über Netzwerke wie dem Internet und versucht in andere Computer einzudringen. Er 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.

Cross Site Scripting (XSS): Cross Site Scripting bezeichnet eine Angriffsmethode auf Webseiten. Es wird dabei eine Sicherheitslücke in der Webapplikation ausgenutzt und z. B. über eine Benutzereingabe eigener HTML-Code eingeschleust, wodurch Nutzerdaten gestohlen oder Seiteninhalte manipuliert werden können.

Crypto-Locker: siehe Ransomware

Crypto-Wall: siehe Ransomware

Cyber-Grooming: Anbahnung von Sexualkontakten zu Unmündigen via Internet (z. B. in sozialen Netzwerken, etc.).

Darknet: Sammlung von Verfahren und Technologien, die einen anonymen Datenaustausch und Kommunikation im Internet ermöglichen. Es wird auch als „Untergrund-Internet“ bezeichnet und wird unter anderem für die Verbreitung von illegalen Inhalten angewendet.

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

DoS/DDoS-Attacke: Angriff auf die Verfügbarkeit der Ressourcen und Dienste eines IT-Systems mit dem Ziel, dieses zu blockieren und somit regulären Benutzern keinen Zugriff mehr zu ermöglichen. DoS ist die Abkürzung von „Denial of Service“ („außer Betrieb“). Bei der DDoS-Attacke („Distributed Denial of Service“) wird der zur Blockade führende Angriff nicht nur von einem Computer 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.

Drive-by-Download: Unbeabsichtigter/unbemerkter Download von Schadsoftware während des Betrachtens einer Webseite (Drive-by: „im Vorbeifahren“). Realisiert werden derartige Drive-by-Downloads meist über eigens dafür präparierte Webseiten.

Exploit (Zero-Day-Exploit): Ein Exploit (englisch to exploit - ausnutzen) ist eine Software oder eine Sequenz von Befehlen, die spezifische Schwächen bzw. 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 Patches zu schließen.

Fake-Webshop: Webseiten die im Internet Waren anbieten, die Bestellungen nach der Zahlung allerdings nicht ausliefern und den Kunden somit um den Bestellwert betrügen.

Firewall: Netzwerksicherheitskomponente, die Datenverbindungen anhand eines definierten Regelwerks erlaubt oder verbietet. Das Ziel einer Firewall ist, den Datenverkehr zwischen Netzwerksegmenten mit verschiedenen Vertrauensstufen abzusichern.

iFrame Redirection: Unter einer „iFrame Redirection“ versteht man das durch Einbetten in einer schadhaften Webseite unbemerkte Umleiten der ursprünglich aufgerufenen Webseite auf eine andere. Dies wird durch Skripte der eingebetteten Webseite bewerkstelligt und kann zur ungewollten Weitergabe sensibler Daten führen. Das Blockieren von Javascript durch Browser-Addons kann diese Art des Angriffs verhindern.

IP-Adresse (Internet Protocol-Adresse): Eine IP-Adresse dient zur eindeutigen Adressierung von Computern und anderen Geräten in einem IP-Netzwerk. Technisch gesehen ist die Nummer eine 32-oder 128-stellige Binärzahl. Das bekannteste

Einsatzgebiet für IP-Adressen ist das Internet. Allen am Internet teilnehmenden Computersystemen werden IP-Adressen zugeteilt. Die IP-Adresse entspricht funktional der Rufnummer in einem Telefonnetz.

I2P-Netzwerk: I2P ist eine Anonymisierungssoftware, die eine zweite Netzwerkebene aufbaut und diese logisch vom Rest des Internets trennt. Die Kommunikation wird auf vier Ebenen verschlüsselt sowie die Identität der Nutzer verschleiert.

Malware: Kurz für Malicious Software (engl. „malicious“: bösartig); Computerprogramme, die vom Benutzer unerwünschte bzw. schädliche Funktionen ausführen.

NTP Reflection: Betreffen Netzwerke in denen IP-Spoofing möglich ist und eine Verbindung zu einem NTP (Network Time Protocol)-Server hat, der in der Regel zur Synchronisation von Uhrzeiten zwischen mehreren Computern eingesetzt wird. Dabei wird vor allem der Befehl „MONLIST“ verwendet, um den zu attackierenden PC zum Absturz zu bringen. Das löst eine Reflexion aus und der Befehl gibt bis zu 600 der zuletzt synchronisierten Computer und deren IP-Adressen zurück. Dadurch kann die Antwort auf die vom Angreifer durchgeführte Anfrage bis zu 200-mal größer sein als die Anfrage, wodurch sich dieses Werkzeug für Denial of Service-Attacken eignet, indem der Angreifer die Source-IP-Adresse des anzugreifenden Computers „spoofed“ und alle Antworten an diesen gerichtet werden. Durch das Deaktivieren des Befehls „MONLIST“ kann dieser Angriff verhindert werden.

Peer to Peer (P2P): In einem Peer-to-Peer-Netz sind alle Computer gleichberechtigt und können sowohl Dienste in Anspruch nehmen als auch Dienste zur Verfügung stellen. Die Computer können als Arbeitsstationen genutzt werden, aber auch Aufgaben im Netz übernehmen.

Phishing: 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: bezeichnet das in der Regel illegale Manipulieren von Telefonsystemen. Dabei ging es normalerweise um die kostenlose Benutzung analoger Telefonleitungen, das Nutzen spezieller kostenfreier Rufnummern für Telefontechniker, über die Verbindungen zu beliebigen Gegenstellen hergestellt werden konnten. „Phreaking“ ist ein Kofferwort aus „phone“ und „freak“.

Polizeitrojaner: siehe Ransomware.

Ransomware: Schadsoftware, bei der sich das Opfer durch Überweisung eines Geldbetrags praktisch freikaufen kann („ransom": Lösegeld). Der Freikauf ist in diesem Zusammenhang mit dem Entfernen einer Sperre oder einer Entschlüsselung von Dateien eines von Ransomware betroffenen Computers zu sehen.

Server: Software im Rahmen des Client-Server-Konzepts oder eine Hardware (Computer), auf der diese Software (Programm) im Rahmen dieses Konzepts abläuft.

Social Engineering: Die Kunst, eine Person zu einer Handlung zu veranlassen oder von etwas zu überzeugen, was objektiv nicht im Interesse dieser Person ist. Oft auch als „The Art of Human Hacking" bezeichnet.

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 Verbreiter als Spammer.

SQL-Injection: siehe Code-Injection

Systemimage: Der Begriff „Image" bezeichnet ein virtuelles Abbild eines elektronischen Speichermediums (z. B. einer Festplatte oder eines USB-Sticks), unter einem Systemimage versteht man im Speziellen das exakte Abbild eines Betriebssystems.

Tor(-Netzwerk): Tor ist ein populärer Anonymisierungsdienst. Er leitet eingehende Daten verschlüsselt über mehrere Server, was die Analyse des Datenverkehrs erschwert bzw. unmöglich macht sowie die Identität des Nutzers verschleiert.

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

Wipe-Programm: Eine Software, die Daten sicher löschen kann. Dabei werden die Daten nicht nur gelöscht sondern auch mit zufällig generierten Daten überschrieben um ein Wiederherstellen zu verhindern.
Würmer: siehe Computerwurm.

Zugangsdaten: 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.

NOTIZEN

WEITERE PUBLIKATIONEN 2015

KRIMINALITÄTSENTWICKLUNG 2014
GELDWÄSCHE 2014
KRIMINALPRÄVENTION 2014
VERFASSUNGSSCHUTZ 2014
SUCHTMITTELKRIMINALITÄT 2014
MENSCHENHANDEL 2014
SCHLEPPEREI 2014
SICHERHEITSBERICHT 2014

KONTAKT

BUNDESKRIMINALAMT
MELDESTELLE „AGAINST CYBERCRIME"
JOSEF HOLAUBEK-PLATZ 1, 1090 WIEN
TEL: +43 (0)1 24836-985025
EMAIL: 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
EMAIL:BMI-II-BK-1-5-PRESSE@BMI.GV.AT

KONZEPT UND DESIGN: ARMIN HALM, ©BUNDESKRIMINALAMT
DRUCK: DIGITALDRUCKEREI DES BUNDESMINISTERIUMS FÜR INNERES; 1010 WIEN
ERSCHEINUNGSDATUM: SEPTEMBER 2015

.BK

BUNDESKRIMINALAMT