.SIAK REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SICHERHEITSAKADEMIE

.SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Krausz, Michael (2009):

Cybercrime. Erläuterungen für die Praxis

SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (1), 83-90.

doi: 10.7396/2009_1_G

Erläuterungen für die Praxis

Cybercrime

MICHAEL KRAUSZ,
Certified Information Security Management Manager und Auditor sowie ausgebildeter Berufsdetektiv.

Der Artikel behandelt die grundlegende Natur von Cybercrime, systematisch aufbereitet und verständlich erklärt für polizeiliche Praktiker und Personen aus dem Justiz- und Sicherheitssektor, die eventuell noch nicht mit Cybercrime in Berührung gekommen sind oder planen in das Thema einzusteigen. Der Artikel erläutert die grundlegend verschiedene Natur von Cybercrime im Vergleich zu herkömmlichen Verbrechen und Vergehen in anschaulicher Weise, die eingesetzte Technik und den hauptsächlichen Täterkreis und gibt Hinweise für die tägliche Arbeit als Ermittler in Fällen von Cybercrime. Der vorliegende Beitrag skizziert taktische Vorgangsweisen bei der Aufklärung von Verbrechen, in denen Computer von den Tätern als zentrale Mittel der Tat eingesetzt wurden.

VORGESCHICHTE UND AKTUELLE SITUATION IN NATIONALER UND INTERNATIONALER BETRACHTUNG

Während Verbrechen und Vergehen, in denen der Computer eine zentrale Rolle als Tatwerkzeug spielt, bis ca. Mitte der 90er Jahre ein beschränktes Nischenthema waren, so ist seit Ende der 90er Jahre eine Explosion der relevanten Delikte im internationalen, aber auch nationalen Rahmen festzustellen. Dazu zählen betrügerische Finanztransaktionen mit gestohlenen Kreditkarteninformationen, das Erschleichen von persönlichen Informationen durch listenreiche E-Mails, Identitätsdiebstahl im weiteren Sinn, um öffentliche oder private Leistungen jeder Art zu erlangen, sowie das organisierte Suchen nach Schwachstellen in Betriebssystemen und Programmen und die systematische Ausnutzung dieser Schwachstellen, um Tatvorbereitungs- oder Tatbegehungshandlungen im Stillen oder durch offene Erpressung zu setzen. Seit Ende der 90er Jahre wurde Cybercrime organisierter, kreativer in Planung und Ausführung, schädlicher und treffsicherer. Weiters rückte auch die militärische Anwendung der Beeinflussung von Computersystemen von außen in den Blickpunkt von Regierungen, sodass nunmehr auch der Begriff „Cyberwar", also der Einsatz von Computern als Mittel der Kriegsführung, entstanden ist. Im Detail betrachtet, unterscheiden sich Cybercrime und Cyberwar nur auf juristischer Ebene, nicht auf technischer. Die eingesetzten Mittel und Methoden sind weitgehend identisch. Cybercrime stellt heutzutage eine ernst zu nehmende Bedrohung für alle Unternehmen und Institutionen dar, deren Funktion auf dem Einsatz von Computern beruht. Dem Autor sind Fälle aus Österreich bekannt, in denen Millionenbeträge durch verschiedenartige Manipulationen, sei es Diebstahl oder Manipulation von Daten, verlorengingen. Besonders betroffen sind vor allem der Finanzsektor, aber auch viele technikнahe Dienstleistungen wie Internet Service Provider, Online-Medien etc.

Für Österreich lässt sich anmerken, dass im Jahr 1987 die ersten auf Cybercrime bezogenen Delikte in das Strafrecht aufgenommen wurden und sich aus diesen ein deutliches Aufholen auf die restliche westliche Welt ergeben hat. Die in Österreich eingeführten Delikte sind durchwegs mit geringer Strafe bedroht, sodass sie im internationalen Vergleich (besonders mit Deutschland und dem anglo-amerikanischen Raum) als eher harmlos gesehen werden können. Auch können in den USA übliche begleitende Maßnahmen wie bei-

spielsweise Computerverbot noch nicht gesetzt werden. Manche Tatbestände wurden nach dem Wissensstand des Autors bisher auch nur sehr selten vor Gericht verhandelt und haben dann auch nicht unbedingt zu Verurteilungen geführt, sodass die strafrechtliche Situation aus Sicht des Sicherheitspraktikers weder eine besonders generalpräventive Wirkung entfaltet noch im Einzelfall zu deutlich gesetzten Signalen führt. Dies wiederum wirkt kontraproduktiv auf betroffene Unternehmen und Behörden, denen dadurch psychologisch ein offensives Vorgehen im Licht der Öffentlichkeit erschwert wird.

CYBERCRIME – DEFINITION

Cybercrime umfasst jene Delikte, in denen ein Computer zum unmittelbaren Tatwerkzeug wird, indem seine besonderen Eigenschaften ausgenutzt werden, um einen materiellen Vorteil zu erlangen oder jemandem einen Nachteil zuzufügen. Der Computer kann dabei, je nach Delikt, auch Tatobjekt sein, wobei er, wiederum durch Verwendung besonderer Programme oder das Ausnutzen seiner spezifischen Eigenschaften, beispielsweise lahmgelegt oder in seine Benutzer-Datenbank eingedrungen wird. Cybercrime liegt also jedesmal vor, wenn der Computer selbst Objekt der Tat oder unmittelbares Tatwerkzeug ist.

Anschaulich beschreiben lässt sich dies wie folgt:

- Wird jemand mit einem Laptop erschlagen, so handelt es sich zweifelsfrei um ein Gewaltdelikt, jedoch wurde der Computer nur durch seine rein physikalischen Eigenschaften zum Tatwerkzeug. Es liegt kein Cybercrime vor. Der Laptop wird für die weitere Untersuchung interessant durch das Vorhandensein von Blutspuren, DNA, Fingerabdrücken oder anderem organischen Material. Die auf dem Laptop enthaltenen Daten sind in diesem Szenario jedoch irrelevant und liefern bestenfalls einen Hinweis auf das Motiv, sofern der Laptop von Täter oder Opfer stammt.
- Erstellt ein Immobiliengutachter ein Wertgutachten über ein Penthouse in Word und gibt dabei einen viel zu niedrigen Wert im Verhältnis zum Verkehrswert an, so hat er zwar den Computer dazu verwendet, die deliktische Handlung zu setzen, es handelt sich jedoch nicht um Cybercrime. Der Computer ist als Medium ersetzbar; ohne Computer würde der Täter eine Schreibmaschine verwenden und könnte damit dasselbe Tatbild verwirklichen.
- Verwendet ein Hacker besonders für diesen Zweck erstellte Programme, um Zugriff auf einen anderen Computer zu erlangen und gelingt ihm dieser Zugriff, so liegt ein Delikt aus dem Cybercrime vor.
- Sucht ein Hacker aus einer kriminellen Organisation im Quellcode eines Programmes nach einer Sicherheitslücke und schreibt er daraufhin ein Programm, das diese Lücke bewusst ausnutzt, so liegt ebenfalls ein Cybercrime-Delikt vor. Begleitend tritt dann oft auch Erpressung mit dieser Sicherheitslücke auf.
- Ein Programmierer, der damit beauftragt wurde, Softwareadaptionen für eine Bank durchzuführen und dabei das Programm so manipuliert, dass jede hundertste Überweisung auf seinem Konto landet, setzt ebenfalls ein Cybercrime-Delikt.
- Wird eine Netzwerkkarte so manipuliert, dass sie unkontrolliert Datenpakete an einen bestimmten Rechner schickt, um ihn lahmzulegen, so liegt ebenfalls ein Cybercrime-Delikt vor.

Zusammenfassend umfasst ein Cybercrime-Delikt eines der folgenden Merkmale:

- Der Computer ist direktes Objekt der

Tat, dadurch, dass Informationen an Dritte gelangen, die im Regelbetrieb nicht an Dritte gelangen würden; dadurch, dass seine Funktionsfähigkeit beeinträchtigt wurde oder dadurch, dass Programm-Eingaben oder Programm-Ausgaben manipuliert wurden bzw. ein Programmablauf so manipuliert wird, dass ein für den Angreifer günstiges, aber ursprünglich nicht intendiertes Ergebnis daraus resultiert. Dieses Ergebnis kann völlig unterschiedliche Formen annehmen, von geknackten Benutzerkonten zu umgelenkten Geldströmen.

- Der Computer wird zum direkten Tatwerkzeug dadurch, dass der Täter Programme einsetzt oder selbst schreibt, die nur dem Zweck dienen, ein bestimmtes Tatbild wie z.B. Identitätsdiebstahl, Manipulation von Bankkonten oder Webseiten, Offenlegung von Benutzerkonten etc. zu verwirklichen.
- Der Computer kann als Medium der Tat nicht aus dem Tatbild weggedacht werden, ohne das Tatbild substantiell zu verändern.
- Das Tatwerkzeug im engeren Sinn ist stets ein besonders für den Tatzweck entwickeltes Programm. Das Programm kann dabei vom Täter selbst entwickelt, zugekauft oder zugekauft und adaptiert worden sein. Es kann sich um Programme handeln, die Computer auf ihre Zugänglichkeit von außen testen, sog. „Port-Scanner“, oder Programme, die entdeckte Schwachstellen ausnützen, sog. „Exploits“.

BESONDERHEITEN

Cybercrime unterscheidet sich deutlich von herkömmlichen Delikten durch die folgenden Elemente:

- Der Täter kann sich in beliebiger geographischer Entfernung vom Opfer befinden. Ein Zugang zu einem Computernetzwerk reicht typischerweise zur Tatbegehung völlig aus. Durch den Entfernungsfaktor wird besonders die Strafverfolgung erheblich erschwert, sodass die Aufklärungsquote von Cybercrime entsprechend niedrig ist. In den USA wird beispielsweise Kreditkartenbetrug mittels Cybercrime überhaupt nicht verfolgt, solange bei einem einzelnen Geschädigten nicht zumindest ein Schaden von USD 150.000,- eingetreten ist, da für Kreditkartenbetrug der US Secret Service als Bundesbehörde verantwortlich ist und dieses Vorgehen eine interne Richtlinie darstellt. Auf Grund dieser geographischen Entfernung kann sich der Täter auch in Ländern und Jurisdiktionen verstecken, deren Strafrecht beispielsweise „weicher“ ist als das Strafrecht des Ziellandes. Das Verhalten des Täters kann damit außerhalb der Signatarstaaten der Cybercrime Convention (EU, USA, Kanada, Japan, Südafrika) straflos bleiben. Innerhalb der EU kann nach dem Grundsatz des Tatorts oder Schadensorts vorgegangen werden, sodass die Strafverfolgung dort einsetzen kann, wo die Tat gesetzt wurde oder dort, wo der daraus resultierende Schaden eingetreten ist. Beliebt als Begehungsorte von Cybercrime sind z.B. Brasilien, China und Russland, da in diesen Ländern diesbezüglich eine wenig rigorose Rechtslage vorliegt. Polen und Tschechien haben die Cybercrime Convention unterzeichnet, aber so wie Österreich, noch nicht ratifiziert.
- Der Täter kann innerhalb von wenigen Sekunden erfolgreich sein. Eine Erkennung ist daher nur mittels besonderer Überwachungssysteme möglich, für die das Opfer entsprechende Hardware und Software beschaffen muss. Falls diese fehlen, kann die Erkennungszeit Wochen oder Monate betragen.

- Der Täter kann mit verheerender technischer Wucht zuschlagen, sodass beispielsweise in einem Fall aus der jüngeren Vergangenheit, die Infrastruktur eines ganzen Landes (Estland) schwer beeinträchtigt wurde.
- Die Tat ist nicht selbstständig auffällig. Ein von einem Täter im Zuge eines Eindringens in ein System ausgelöster Systemabsturz ist grundsätzlich nicht von einem „normalen" Absturz zu unterscheiden. Verwendet der Täter einen Server, in den er eingedrungen ist, etwa nur als Zwischenspeicher für gestohlene Dateien (was beispielsweise Kevin Mitnick, der berühmteste Hacker der Neuzeit, laufend getan hat), so können Monate vergehen, bis diese Dateien entdeckt werden. Im Extremfall ist denkbar, dass das Opfer für den Täter gehalten wird, da die Vorgänge, die zum Eindringen führten, eventuell sehr gut verschleiert wurden.
- Durchdachtes Cybercrime setzt Ausbildung und Training voraus, sodass der Täterkreis von vornherein deutlich eingeschränkt werden kann. Die Ausbildung muss jedoch nicht formalisiert erfolgt sein, ein Täter kann sich sein Wissen auch autodidaktisch angeeignet haben.
- Technische Raffinesse: Cybercrime-Delikte und Gegenmaßnahmen haben sich technisch stets weiterentwickelt, sodass „primitive" Formen sehr wohl auch aussterben. Beispielsweise haben Angreifer, die versuchen, Bankzugangsdaten wie PIN und TAN zu erlangen, mit der Einführung der MOBILE-TAN, d.h. der Übertragung der TAN auf ein Mobiltelefon des Kontoinhabers, technisch keine Chance mehr. Durch dieses technische Katz-und-Maus-Spiel wird natürlich das entsprechend notwendige Wissenslevel auf beiden Seiten des Gesetzes stetig höhergeschraubt. Allerdings erfolgt daraus in der Praxis kein ständiger Trainingsdruck, da die Mehrzahl der Delikte typischerweise mit im Verhältnis zur technischen Spitze einfachen Mitteln erfolgt. Die raffinierten Delikte sind dafür umso schadensträchtiger.
- Ultimative Waffe: Im Sinne der Cybercrime-Delikte haben Hacker schon vor einiger Zeit die ultimative Waffe gefunden: Programme werden von organisierten Banden gezielt auf Schwachstellen untersucht (dazu wird beispielsweise der gestohlene Quellcode von Windows verwendet oder einfach ein System im laufenden Betrieb untersucht, sog. „Reverse-Engineering"). Gefundene Schwachstellen werden dann anderen Banden zur Benutzung verkauft oder Firmen mit der Drohung der Ausnutzung der Schwachstelle erpresst. Dieses Vorgehen stellt deswegen eine ultimative Waffe dar, da kein Unternehmen in der Lage ist, genauso proaktiv zum Schutz seiner Systeme vorzugehen.

Während es also den perfekten Mord in der Praxis nicht gibt, ist das perfekte, nicht erkennbare oder zumindest nicht aufklärbare Cybercrime-Delikt sehr wohl denkbar.

FALLBEISPIELE

Im Folgenden seien einige Beispiele erläutert.

1.) Ein Unternehmen nimmt einen Server außer Betrieb und macht diesen von außen größtenteils, aber nicht vollständig unzugänglich. Gleichzeitig wird die Wartung reduziert, sodass der Server nach wenigen Monaten über bekannte, aber nicht behobene Schwachstellen verfügt. So weit, so fahrlässig. Nun dringt ein Hacker in den Server ein und gelangt in Besitz von Millionen von Kundendaten des Unternehmens samt Adressinformationen und Kontoinformationen inklusive Passwörter. Solche Datensätze werden je nach Umfang mit bis zu drei

Euro pro Stück gehandelt. Ähnlich verhält es sich mit Kreditkartendaten.
Das Unternehmen sitzt in Deutschland, der Hacker in Kanada und nimmt für seine Tat einen Umweg über Brasilien und Polen. Der Fall wird dem Unternehmen dadurch bekannt, dass diese Daten in kleinen Teilen verkauft werden und schließlich ein Jugendlicher in einem öffentlichen Internetforum die Daten zum Verkauf anbietet, weil er schnell zu Geld kommen möchte. Der Jugendliche ist Österreicher, vor Gericht kommt er jedoch nicht wegen eines Cybercrime-Delikts, sondern wegen Betruges, da er im Internetforum angibt, über mehr Daten zu verfügen als er dann tatsächlich einem Scheinkäufer (dem Ermittler) liefert.
Dieser Fall illustriert die vielen praktischen Probleme, begonnen mit der Aushebung des eigentlichen Täters und dem Wust von Begleittätern und Begleitdelikten, durch die sich Ermittler kämpfen müssen.

2.) Analog zu Beispiel 1 verhielt es sich in dem Fall, in dem einem Unternehmen Kundendaten eines Konkurrenten angeboten wurden. Wiederum wurden vollständige Datensätze angeboten. Der Ursprung der Daten konnte trotz sofortiger Zusammenarbeit der beiden betroffenen Unternehmen nicht restlos geklärt werden. Auch in diesem Fall tat sich ein Jugendlicher mit besonderer krimineller Energie hervor.

3.) Im Falle von Industriespionage ist Cybercrime oft als Vorbereitungshandlung zum eigentlichen Delikt, der Verwertung des Betriebsgeheimnisses zu sehen. Auf Grund des deutlich höheren Aufwands zur Ausführung einer Cybercrime-Attacke im Verhältnis zu Bestechung, wird es jedoch seltener angewendet. Firmennetze werden allerdings ständig auf Schwachstellen von außen durch äußere Angreifer geprüft. Ein Zufallstreffer kann nur bei guter Verwaltung der IT-Systeme ausgeschlossen werden. Allein das Netzwerk des Autors, das kaum eine beachtliche Größe erreicht hat, verzeichnet pro Woche zwischen 5.000 und 40.000 Einzelattacken auf die vom Unternehmen des Autors betriebenen IT-Dienste.

TÄTERKREISE

Für Cybercrime-Delikte kommen vor allem die folgenden Täterkreise in Frage[1]:

- Die erfassten Täter sind zu 100 % männlich.
- Jugendliche Täter mit teils erheblicher krimineller Energie und dem Wunsch nach „schnellem Geld“. Ein IT-Hintergrund ist typischerweise durch den Besuch von Fachschulen gegeben. In diesem Fall liegt die typische Altersgruppe zwischen 14 und 19 Jahren. Das Know-how ist im Grunde nur mittelmäßig, aber ausreichend, um gemeinsam mit anderen Tatbilder zu setzen bzw. mit vorhandener Technik selbstständig Tatbilder zu setzen.
- Studenten der Informatik, die allein oder im Auftrag, teils aus dem Umfeld der Industriespionage oder der Organisierten Kriminalität (ohne dass ihnen dies bewusst sein muss), tätig werden. Bereits im Jahre 1996 wurde beispielsweise dem Autor und einem Studienkollegen die damals für Studenten äußerst hohe Summe von 50.000 Schilling angeboten, falls es gelänge, in ein bestimmtes Industrieunternehmen einzudringen, was selbstverständlich abgelehnt wurde. Ein deutscher Hacker war hingegen weniger empfindlich und hat über einen Mittelsmann Betriebsgeheimnisse deutscher Industrieunternehmen sowie schließlich auch Staatsgeheimnisse gegen Geld und Kokain an den KGB verkauft. Dies war der erste

Fall, der die Öffentlichkeit aufrüttelte. Teilweise stellt Hacken allerdings auch ein Spiel dar, dessen Anziehungskraft jedoch mit der Eingliederung in die Erwerbsgesellschaft nachlässt. Der typische Täter ist zwischen 22 und 26 Jahre alt und verfügt über kein auffälliges soziales Verhalten. Er ist nicht an eine bestimmte Subkultur gebunden.

- Erwachsene Innentäter in Unternehmen und Behörden, die allein oder in Verbindung mit einem IT-Spezialisten, Delikte setzen, um dem Unternehmen bewusst Schaden zuzufügen oder sich „nur" zu bereichern. Im Cybercrime wurden bisher kaum Täter beobachtet, die älter als 40 Jahre gewesen wären, vermutlich auf Grund der altersspezifischen Schichtung des notwendigen Know-hows. In technisch einfacher gestrickten Fällen, in denen Ärger dem Arbeitgeber gegenüber eine Rolle gespielt hat, sind hingegen kaum Altersgrenzen beobachtet worden. Typisches Motivmerkmal sind Rachegelüste dem Arbeitgeber gegenüber oder eine materielle Zwangslage.
- Täter, die als Zuträger der Organisierten Kriminalität tätig sind und dabei dem Profil eines berufstätigen IT-Mitarbeiters entsprechen. Zwischen 25 und 45 Jahre alt, handelt es sich um Personen ohne besondere Skrupel, die im Neben- oder Haupterwerb (besonders in Osteuropa) von anonymen Auftraggebern beauftragt werden und Aufträge teilweise in Gruppen von bis zu vier Personen abwickeln. Typischerweise sind diese Täter gut ausgebildet und verfügen über sehr tiefes technisches Fachwissen.

TECHNISCHE ASPEKTE

Im folgenden Abschnitt sollen einige technische Fakten die Komplexität des Themas umreißen.

- In einem Fall von Bilanzfälschung mussten 8 Terabyte an Daten von IT-Forensikern ausgewertet werden. Dies entspricht dem Inhalt von 12.905 CD-ROMs zu 650 MB. Würde man den dazu notwendigen Speicherplatz neu anschaffen, so kann dies, je nach Ausprägung, bis zu 560.000,- Euro kosten.
- Zur Aufklärung eines Falls wurde der gesamte Netzwerkverkehr eines Unternehmens mit 100 Mitarbeitern über ein Oster-Wochenende aufgezeichnet. Es wurden vier Dateien zu je 1 GB (das ca. 1,6-fache einer CD) im Zuge der Aufzeichnungen angelegt. Um diese Dateien in ein auswertbares Format zu konvertieren, mussten sie in einem speziellen Programm geöffnet werden. Das Öffnen alleine dauerte 45 Minuten pro Datei auf einem PC der oberen Leistungsklasse.
- In einem Unternehmen, dessen Umsatzgenerierung wesentlich auf Web-Diensten aufbaut, kann die Datenmenge, die von den Überwachungssystemen erzeugt wird, leicht 500 GB (entspricht 788 CDs) pro Jahr erreichen.
- Für Behörden ist wichtig festzuhalten, dass der Kampf gegen Cybercrime vor allem ein technischer ist. Ressourcenüberlegenheit ist entscheidend, um den Tätern stets einen Schritt voraus zu sein, sei es beim Knacken von Passwörtern verschlüsselter Dateien, bei der Speicherung von sichergestellten Daten oder der CPU-Leistung zur Auswertung solcher Daten.[2]
- Das Knacken eines mittelmäßigen 8-stelligen Passworts kann mit heutiger Rechenleistung zwischen drei Stunden und 21 Tagen dauern. Der Einsatz eines guten 8-stelligen Passworts verlängert diese Frist bereits auf einige 100 Jahre.
- Das Entdecken einer Sicherheitslücke unter Verwendung des Quellcodes eines Programms kann bis zu einer Woche

dauern; die Erstellung eines Programms zur Ausnutzung dieser Lücke bis zu zwei Wochen. Der tatsächliche Einsatz gegen Server eines Unternehmens oder einer Behörde dauert üblicherweise nicht länger als vier Wochen, falls die Software an speziellen Bedingungen angepasst werden muss.

CYBERCRIME-DELIKTE IM ÖSTERREICHISCHEN STRAFRECHT – KURZ GEFASST

In Österreich existieren seit 1987 die folgenden Delikte im Strafgesetzbuch, die unter die im Artikel verwendete Definition von Cybercrime fallen (es wird nur auf solche eingegangen):

- § 118a – Widerrechtlicher Zugriff auf ein Computersystem,
- § 119a – Missbräuchliches Abfangen von Daten,
- § 126a – Datenbeschädigung,
- § 126b – Störung der Funktionsfähigkeit eines Computersystems,
- § 126c – Missbrauch von Computerprogrammen und Zugangsdaten,
- § 148a – Betrügerischer Datenverarbeitungsmissbrauch.

Alle diese Tatbestände entsprechen exakt der verwendeten Definition von Cybercrime und sind durch ihre Bezeichnung in ihrem Kern selbsterklärend. Geht es im § 118a um Zugriff auf ein Computersystem, zu dem man nicht berechtigt ist, beispielsweise mittels gestohlener Passwörter oder mittels einer strukturierten Vorgangsweise, um das System zu „knacken“, so geht es in § 126a um den Computer als Opfer, indem Daten manipuliert, verändert oder gelöscht, aber auch unterdrückt werden oder der Computer in seiner Funktionsfähigkeit beeinträchtigt wird (§ 126b). In der Praxis zielt die Strafverfolgung hierbei auf eine schwerwiegende (gemessen an den Folgen) oder andauernde (länger dauernde) Störung ab, insbesondere geht es um eine völlige Lahmlegung des Systems über einen ausgedehnten Zeitraum. § 126c wiederum stellt besonders jene Tätigkeiten unter Strafe, die als Vorbereitungshandlungen für eines der oben genannten Delikte ausgeführt werden, wie eben die Erstellung besonderer Programme zum Umgehen oder Knacken der Sicherheit von Systemen. §126c ist sehr umfassend formuliert (er beinhaltet Herstellung, Einfuhr, Vertrieb, Veräußerung, das bloße Zurverfügungstellen an Dritte, jede Art der Aneignung und des Besitzes) und kann daher schlagkräftig gegen organisierte Computerkriminalität eingesetzt werden.

§148a dient der Verfolgung jener Straftaten, die dadurch verwirklicht werden, dass auf Programme Einfluss genommen wird, sodass das Ergebnis einer Datenverarbeitung dem Täter einen Vermögensvorteil oder einem anderen einen Vermögensnachteil bringt. Jener Programmierer, der in den siebziger Jahren im Zuge der Programmierung einer Bank-Applikation Rundungsfehler auf sein Konto leitete, fällt zweifelsohne in diese Kategorie. Entscheidend zur Beurteilung ist der Eingriff in den Programmablauf, der dazu führt das Schadensbild zu verwirklichen.

§ 119a behandelt das Mitlauschen und Abfangen von Daten mittels Computern und schützt daher unter anderem auch E-Mail-Verkehr.

RELEVANTE ASPEKTE DER PRAXIS

Für die tägliche Praxis ist folgende Reihenfolge bei der Bearbeitung eines Cybercrime-Falles festzuhalten, die sich als besonders erfolgreich herausgestellt hat:

1. Herausarbeitung der wesentlichen Fakten des Falles mit dem Unternehmen anhand eines standardisierten Fragenkataloges. Dies dient der Vergleichbarkeit ähnlicher Fälle sowie der Erkennung von Verhaltensmustern.

2. Klärung der Zuständigkeit bei allen weiteren Schritten (Tat- bzw. Schadensort bzw. -land) sowie die Schadenshöhe. Gesundes Misstrauen gegenüber von Unternehmen genannten Schadenszahlen, sofern diese nicht nachvollziehbar dargestellt sind, ist durchaus angebracht.
3. Weiters sollte versucht werden, den Täter, soweit möglich, in die beschriebenen Tätergruppen einzuordnen, sodass die beste Vorgangsweise ihm gegenüber deutlich wird.
4. Bei Hausdurchsuchungen: Sicherstellung möglichst aller Datenträger. Dazu gehören neben PCs, Laptops und externen Festplatten auch Telefone mit MicroSD-Karten, digitale Kameras, Uhren mit RAM und USB-Anschluss sowie eventuell Schmuck mit einer Speicherkarte als Anhänger (in Japan sehr beliebt). Auch schwer beschädigte Datenträger können in Speziallabors wieder lesbar gemacht werden. Theoretisch können USB-Sticks leicht in WC-Anlagen verschwinden.
5. Einforderung aller verwendeten Accountdaten von Verdächtigen. Ein Verdächtiger kann beispielsweise über Speicherplatz im Ausland verfügen.
6. Sich in die Lage des Täters zu versetzen ist wesentlich, um die gesicherten Beweise priorisieren zu können, da Auswertungen oft Ressourcen anderer Dienststellen in Anspruch nehmen und typischerweise nach Größe des Falles gewichtet wird.

AUSBLICK

In naher Zukunft ist davon auszugehen, dass auf Grund der zunehmenden technischen Aufrüstung der österreichischen Dienststellen die Lücke zwischen Tätern und Verfolgern geringer wird, wobei die angewandte technische Raffinesse bei großen Fällen steigen wird. Im Mittelfeld der Delikte ist mit einer Abnahme der reinen Cybercrime-Delikte zu rechnen, dafür mit einer Zunahme bei Delikten von Innentätern in Verbindung mit Außentätern, auf Grund der weitaus geringeren Komplexität in der Durchführung. Für sensible Bereiche wie industrielle und universitäre Forschung, Militär, Behörden sowie kritische Infrastrukturen wird Cybercrime zunehmen, da die zu Grunde liegenden technischen Methoden „Grundnahrungsmittel" der Industriespionage wie der Spionage überhaupt geworden sind. Für Österreich ist zu wünschen, dass der einschlägige Know-how-Aufbau bei Polizei und Gutachtern sowie der Grundlagen auch bei Richtern und Anklagebehörden fortschreitet, sodass Cybercrime in Zukunft weiterhin wirksam bekämpft werden kann.

[1] *Anm.: Die nachfolgenden Ausführungen sind Ergebnisse einer Auswertung von Deliktsfällen der Jahre 1998–2008 aus dem Aktenbestand des Autors.*

[2] *Anm.: Die Geschwindigkeit, mit der ein PC Daten verarbeiten kann, wird auch „CPU-Leistung" genannt.*

Weiterführende Literatur:

Balkin, J. M./Eddan, K./Grimmelmann, J. (Eds.) (2007). Cybercrime: Digital Cops in a Networked Environment, New York.

McQuade, S. C. (2005). Understanding and Managing Cybercrime, Boston.

Mitnick, K. D./Simon, W. L./Wozniak, S. (2003). The Art of Deception: Controlling the Human Element of Security, Wiley.

Mitnick, K. D./Simon, W. L. (2005). The Art of Instrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers, Wiley.

Moore, R. (2005). Cybercrime: Investigating High-Technology Computer Crime, Ohio.

Schneier, B. (2004). Secrets and Lies: Digital Security in a Networked World, Wiley.

Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age, Cambridge.