Jörg Ziercke, 1947 geboren in Lübeck. Nach Eintritt in den Dienst der Landespolizei Schleswig-Holstein und Ausbildung zum Kriminalbeamten, Verwendung im operativen Bereich bei Schutz- und Kriminalpolizei sowie beim LKA Kiel. 1977-79 Aufstieg in den höheren Dienst der Kriminalpolizei; Studium an der Polizei-Führungsakademie Münster.1979-85 Leiter der Kriminalpolizei Neumünster und Vertretungsaufgaben des Leiters der Kriminalpolizeidirektion Kiel. 1990-92 Leiter der Landespolizeischule Schleswig-Holstein sowie Unterstützung beim Aufbau der Landespolizeischule Mecklenburg-Vorpommern. 1992-04 Abteilung Polizei im Innenministerium Schleswig-Holstein, ab 1995 Leiter der Abteilung. 2004 Berufung zum Präsidenten des Bundeskriminalamtes.

Jörg Ziercke
Präsident des Bundeskriminalamtes

„Wirtschaftskriminalität und Cybercrime in Deutschland“

Wirtschaftskriminalität

In den vergangenen zehn Jahren wurden in Deutschland jährlich zwischen 80.000 und 100.000 Fälle von Wirtschaftskriminalität registriert. Im vergangenen Jahr bewegte sich diese Zahl mit knapp 80.000 Fällen am unteren Ende dieser statistischen Bandbreite; gegenüber 2010 ein Rückgang von ca. 23%.

Auch der im Jahr 2011 durch Wirtschaftskriminalität verursachte Schaden ist gegenüber dem Vorjahr um etwa 10% auf rund 4,1 Mrd. € gesunken. Dennoch verursachte die Wirtschaftskriminalität auch 2011 über die Hälfte aller registrierten Schäden, die sich bei insgesamt rund 6 Mio. Straftaten auf knapp 8 Mrd. € beliefen.

Dagegen ist der Anteil der Wirtschaftskriminalität an den insgesamt polizeilich registrierten Straftaten eher gering – er liegt im Schnitt zwischen 1 und 2 %. Wer die Gefahren von Wirtschaftskriminalität verstehen will, darf nicht bei den Fallzahlen stehen bleiben, sondern muss die Folgen beachten. Bereits das unmittelbare Schadenspotenzial ist angesichts der genannten Schadenssumme enorm. Zudem ist das mittelbare Schadenspotenzial der Wirtschaftskriminalität sehr groß: Wettbewerbsverzerrungen, gesundheitliche Gefährdungen und Schädigungen Einzelner, Reputationsverluste von Unternehmen oder auch ganzer Wirtschaftszweige bis hin zu Vertrauensverlusten in die Funktionsfähigkeit der bestehenden Wirtschaftsordnung – um nur einige der möglichen Folgen zu nennen. Zu einzelnen Deliktsbereichen, um die Vielfalt von Wirtschaftskriminalität zu verdeutlichen:

- Unter den Bereich der „Anlage- und Finanzierungsdelikte“ werden alle Deliktsformen im Zusammenhang mit der Vermittlung, Erlangung und Gewährung von Krediten, sämtliche Erscheinungsformen der Scheck- oder Wechselreiterei, der Fälschung von Geldmarktinstrumenten und Straftaten in Verbindung mit dem Bankgewerbe sowie nach dem Wertpapierhandelsgesetz gefasst. Im Jahr 2011 wurden in der Polizeilichen Kriminalstatistik (PKS) hierzu fast 8.000 Fälle registriert, ein Rückgang von 36%. Auch der registrierte Schaden in diesem Bereich sank um 40% auf 555 Mio. €.
- Im Bereich der „Betrugs-/Untreuehandlungen i.Z.m Beteiligungen und Kapitalanlagen“ – hierzu zählen z. B. Anlagebetrug, Beteiligungsbetrug, Betrug bei Börsenspekulationen, Prospektbetrug, Untreue bei Kapitalanlagegeschäften, aber auch Fälle des Wertpapierbetruges sowie Verstöße gegen das Kreditwesen- und Wertpapierhandelsgesetz – wurden 2011 rund 7.000 Fälle erfasst, ein Rückgang von knapp 38%. Der Schaden sank hier um ca. 3% von 610 auf 594 Mio. €.
- Im Jahr 2010 wurden fast 11.000 „Arbeitsdelikte“ registriert, fast ebenso viele wie im Vorjahr. Auch der Schaden liegt nahezu unverändert bei ca. 50 Mio. €. Als Arbeitsdelikte werden alle Deliktsformen bezeichnet, die im Zusammenhang mit der Verletzung arbeitsrechtlicher Vorschriften stehen. Neben dem Vorenthalten und Veruntreuen von Arbeitsentgelt – diese Fälle stellen die weit überwiegende Mehrheit dar – sind dies die illegale Vermittlung, Anwerbung und

Beschäftigung nichtdeutscher Arbeitnehmer im Sinne des Sozialgesetzbuches (SGB), das Verleihen und Entleihen von nichtdeutschen Arbeitnehmern ohne eine erforderliche Arbeitserlaubnis sowie Verstöße gegen Anzeigepflichten nach dem SGB, der Handwerksordnung und der Gewerbeordnung. Die Delikte der illegalen Beschäftigung, der illegalen Arbeitnehmerüberlassung sowie der illegalen Ausländerbeschäftigung werden allerdings vorrangig durch die Dienststellen der Finanzkontrolle Schwarzarbeit (FKS) des Zolls verfolgt und finden sich daher nur zu einem geringen Anteil in polizeilichen Statistiken wieder.

- Zu den „Wettbewerbsdelikten" zählen Verstöße gegen das Gesetz gegen den unlauteren Wettbewerb (UWG), Urheberrechtsbestimmungen, gegen das Wettbewerbsrecht nach dem Strafgesetzbuch (StGB) sowie Fälle von Subventionsbetrug. Für das Jahr 2011 wurden rund 2.600 Wettbewerbsdelikte – ein Rückgang von 22% – registriert. Der Schaden ist hingegen von 18 Mio. € im Vorjahr auf 38 Mio. € gestiegen. Die Fälle der Produkt- und Markenpiraterie bilden hier trotz eines Rückganges auch im Jahr 2011 den Schwerpunkt. In diesem Deliktsbereich sind neben der Polizei die Zollbehörden im Rahmen der Überwachung des grenzüberschreitenden Warenverkehrs zuständig. Da der Großteil der gefälschten Waren im Ausland hergestellt und nach Deutschland importiert wird, fällt auch hier eine Vielzahl der Fälle in die Zuständigkeit des Zolls.
- Zum Phänomenbereich der „Insolvenzdelikte" zählen der Bankrott und besonders der schwere Fall des Bankrotts, die Verletzung der Buchführungspflicht, die Gläubiger- und Schuldnerbegünstigung, die Insolvenzverschleppung sowie die Fälle des Leistungs- und Warenkreditbetrugs im Zusammenhang mit Insolvenzen. Mit rund 12.000 registrierten Fällen gab es hier einen leichten Anstieg, obwohl die Zahl der Unternehmensinsolvenzen nach Angaben des Statistischen Bundesamts 2011 leicht sank. Der durch Insolvenzdelikte verursachte Schaden wurde mit ca. 1,5 Mrd. € und damit rund 11% niedriger als im Vorjahr beziffert. Da Insolvenzstraftaten oftmals mit weiteren Begleitdelikten verbunden sind, dürfte der tatsächlich verursachte Schaden weit höher liegen.
- „Gesundheitsdelikte" im Sinne der Wirtschaftskriminalität umfassen den Abrechnungsbetrug im Gesundheitswesen zur betrügerischen Erlangung von Geldleistungen von Selbstzahlern, Krankenkassen, Krankenversicherungen und Beihilfestellen durch Angehörige medizinischer oder pharmazeutischer Berufe sowie durch Krankenhäuser und Sanatorien. Mit knapp 3.000 registrierten Fällen wurde hier ein Rückgang um 24% verzeichnet, der Schaden sank um 11% auf 31 Mio. €.

Die voranschreitende Technisierung und das Outsourcing von Wirtschaftsprozessen durch Onlineüberweisungen und eCommerce führen, verbunden mit der rasant gestiegenen Anzahl an Internetnutzern, zu immer neuen kriminellen Geschäftsmodellen. So werden z. B. seit einigen Jahren vermehrt Pennystocks über das Internet zum Kauf angepriesen. Vorgespiegelt wird ein gewaltiges Kurspotential von bis zu mehreren Tausend Prozent innerhalb kürzester Zeit. Ziel der Täter ist, den Preis der Aktie in die Höhe zu treiben und selbst gewinnbringend zu verkaufen, bevor der Kurs wieder in sich zusammenbricht.

Komplexe Finanzprodukte und Unternehmensstrukturen sowie die Schnelllebigkeit von Transaktionen stellen uns vor erhebliche Beweiserhebungsprobleme. Für Kapitalmarktdelikte, aber auch für andere Deliktsbereiche der Wirtschaftskriminalität gilt zudem: Kaum ein Verfahren ist heute noch ohne internationale Bezüge. Dabei zeigt sich eine Welt

zweier Geschwindigkeiten: einerseits die Finanzmärkte, die in Sekundenschnelle global agieren, andererseits die internationale polizeiliche und justizielle Zusammenarbeit, die an nationale Vorschriften gebunden und durch fehlende Rechtsharmonisierung eingeschränkt und somit langwierig ist.

Korruption

Ein Begleiter der Wirtschaftskriminalität ist die Korruption, die ebenfalls unser Wirtschaftssystem gefährdet. In diesem Bereich sind oftmals feste, international weitverzweigte Täterstrukturen festzustellen – richtiggehende „Korruptionsgeflechte". Auch hier ist von einem großen Dunkelfeld auszugehen. Im Jahr 2011 wurden mehr als 1.500 Korruptionsverfahren in Deutschland gemeldet, gegenüber 2010 ein Rückgang von ca. 16%. Derartige Schwankungen sind in diesem Kriminalitätsfeld nicht ungewöhnlich; hier spielen Großverfahren mit einer Vielzahl von Einzeltaten eine Rolle. Dies zeigt sich auch an den für 2011 gemeldeten knapp 47.000 einzelnen Korruptionsstraftaten, nahezu eine Verdreifachung des Vorjahreswertes; ursächlich hierfür waren mehrere Großverfahren.

Die „Erlangung von Aufträgen" ist seit Jahren mit Abstand das bevorzugte Ziel korruptiven Handelns. Im Mittelpunkt von Korruptionsfällen stehen meist Bargeld und Sachzuwendungen. Statistisch gesehen lag der Schwerpunkt der polizeilich bekannt gewordenen Fälle der Korruption im Jahr 2011 mit einem Anteil von 56% im Bereich der Wirtschaft. Der in den zurückliegenden Jahren festgestellte Trend, dass sich die polizeilich festgestellten Korruptionsfälle aus dem Bereich öffentliche Verwaltung in die Wirtschaft verlagern, hat sich damit bestätigt; 2010 war die Wirtschaft erstmals der am stärksten betroffene Bereich.

Ein verstärkt in den öffentlichen Fokus gerücktes Phänomen ist die „Korruption im Sport". Für die Manipulation von sportlichen Wettkämpfen – bspw. durch Bestechung von Schiedsrichtern oder Sportlern – existiert in Deutschland bislang kein spezieller Straftatbestand, sodass diese Fälle nicht als Korruption, sondern in der Regel als Verdacht des gewerbs- und bandenmäßigen Betruges[1] behandelt werden, wenn auf manipulierte Spiele gewettet wird.

So wird von der Staatsanwaltschaft (StA) Bochum ein Verfahren wegen des Verdachts des gewerbs- und bandenmäßigen Betruges insbesondere durch Spielmanipulation und Wettbetrug im Fußball geführt, das zahlreiche internationale Bezüge aufweist. Die Täter sollen seit 2009 Sportler, Trainer, Schiedsrichter und Offizielle aus verschiedenen hohen europäischen Fußballligen bestochen haben, um Spielergebnisse zu beeinflussen. Auf diese Spiele setzten die Täter hohe Bargeldbeträge bei europäischen und asiatischen Wettanbietern und erlangten so Gewinne in Höhe von mehreren Millionen Euro. Möglichkeiten zur Intensivierung der Korruptionsbekämpfung in Deutschland bestehen aus Sicht des Bundeskriminalamtes (BKA) in der Einrichtung eines bundesweiten Korruptionsregisters, um solche Unternehmen von öffentlichen Aufträgen auszuschließen, die wegen korruptiver Handlungen auffällig geworden sind, und in einer flächendeckenden Einrichtung von Hinweisgebersystemen, verbunden mit Regelungen zu einem umfassenden Schutz für Whistleblower.

Zur Bekämpfung der Manipulation von Sportereignissen wird von verschiedenen Stellen die Einführung eines Straftatbestandes der Bestechlichkeit und Bestechung im Sport für sinnvoll erachtet. Dadurch

1 § 263 StGB bzw. der Beihilfe hierzu.Weitere Straftatbestände, die im Einzelfall verwirklicht sein können, sind § 284 StGB (unerlaubte Veranstaltung eines Glücksspiels), § 285 StGB (Beteiligung am unerlaubten Glücksspiel) oder § 261 StGB (Geldwäsche).

sollen die Strafverfolgungsbehörden bereits gegen Manipulationen an sich vorgehen können, nicht erst gegen vollendete Betrugsdelikte. Entscheidend ist, dass Korruptionsfälle konsequent zur Anzeige gebracht werden. Dies setzt auch eine enge Kooperation zwischen Strafverfolgungsbehörden und Unternehmen voraus, sowohl auf nationaler als auch auf internationaler Ebene. Multinationale Konzerne haben heute ein eigenes Interesse daran, gegen Korruption vorzugehen. Empfindliche Geldstrafen sind wesentlich höher als die zu erwartenden Gewinne; Bestechungsgelder sind nicht mehr refinanzierbar.

Geldwäsche

Ein weiterer Begleiter der Wirtschaftskriminalität ist die Geldwäsche. Eine seriöse Schätzung der Summe gewaschener Gelder ist nicht möglich[2] Grundsätzlich gilt: Alle kriminell erwirtschafteten Gelder sind potenziell Gegenstand von Geldwäsche. 2011 wurden fast 13.000 Verdachtsanzeigen nach dem Geldwäschegesetz (GWG) an die im BKA angesiedelte Financial Intelligence Unit (FIU) Deutschland gemeldet, ein Anstieg um fast 17% gegenüber 2010 und ein Höchststand seit Inkrafttreten des Geldwäschegesetzes (GWG) im Jahr 1993. Seit der Gründung der FIU vor zwölf Jahren wurden etwa 85.000 Verdachtsanzeigen erfasst und ausgewertet. Bei über einem Drittel der Verdachtsanzeigen hat sich der Verdacht einer Straftat erhärtet, vor allem Betrugsdelikte standen dabei im Mittelpunkt. 90% aller Verdachtsanzeigen wurden von den Meldeverpflichteten aus dem Bereich der Kreditinstitute erstattet. Die Anzahl der Verdachtsanzeigen von anderen nach dem GWG Verpflichteten – von „Personen, die gewerblich mit Gütern handeln“ und von der Gruppe der „rechtsberatenden Berufe“ – bewegte sich auch im Jahr 2011 auf sehr niedrigem Niveau. Auch bei diesen müssen wir die notwendige Sensibilisierung erreichen. Mit Nachdruck muss die Aufsicht über die Verpflichteten aus dem gewerblichen Nicht-Finanzsektor weiter verstärkt werden.

Organisierte Kriminalität (OK) und Wirtschaftskriminalität sind eng mit Geldwäsche verwoben: Illegal erlangte Vermögenswerte sollen durch die Einschleusung in den legalen Wirtschaftskreislauf den Straftätern als scheinbar legale Vermögenswerte zur Verfügung stehen und so dem Zugriff der Strafverfolgungsbehörden entzogen werden. Zu den wesentlichen Elementen einer erfolgreichen Kriminalitätsbekämpfung gehört es daher, Straftätern das illegal erwirtschaftete Vermögen wieder zu entziehen. So wurden im Jahr 2010 in über 90% der rund 600 geführten OK-Verfahren auch Finanzermittlungen durchgeführt. Bei 242 Verfahren fanden sich Hinweise auf Geldwäsche. Gleichwohl gelang es lediglich in 154 dieser Verfahren, kriminell erlangtes Vermögen abzuschöpfen. Obwohl im Jahr 2010 ca. 170 Mio. € vorläufig als Vermögenswerte gesichert wurden, ist diese Zahl im internationalen Vergleich überaus gering; in Italien konnten z. B. im Jahr 2010 über 1,2 Mrd. Euro an Vermögenswerten abgeschöpft werden.

Die Abschöpfung kriminell erlangter Vermögenswerte muss erleichtert werden. So muss § 73d StGB (erweiterter Verfall) auf tatunbeteiligte Dritte erweitert werden, da Tatverdächtige immer häufiger ihr Vermögen auf Dritte übertragen. Außerdem sollte es nicht möglich sein, inkriminiertes Vermögen über ein Insolvenzverfahren zu legalisieren und den Opfern der Straftaten hierdurch die Realisierung ihrer Ansprüche zu erschweren.

2 Der Internationale Währungsfonds (IWF) schätzte im Jahr 2000 das Ausmaß der Gelder, welche aus kriminellen Handlungen stammen und gewaschen werden sollen, auf 2-5% des Bruttoinlandsproduktes sämtlicher Staaten der Welt – damals zwischen 600 und 1.500 Milliarden US-Dollar (Siska, 2009, S. 32).

Die FIU arbeitet bei der Geldwäschebekämpfung eng mit der Gemeinsamen Finanzermittlungsgruppe von Zollkriminalamt (ZKA) und BKA, den Zollbehörden und den Geldwäschedienststellen der Länderpolizeien sowie mit der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zusammen. Aber auch Geldwäsche macht natürlich nicht an Staatsgrenzen halt. Daher wächst auch die Kooperation mit ausländischen Stellen kontinuierlich. Die FIU Deutschland hat seit ihrer Errichtung in ca. 6.200 Fällen mit anderen FIU weltweit operative Informationen ausgetauscht. Auf EU-Ebene wird aktuell über die Einführung eines Instrumentes[3] diskutiert, das den Vermögenseinzug auf Basis eines verwaltungsgerichtlichen Verfahrens unter Nutzung des Mittels der Beweislastumkehr ermöglichen soll.

Cybercrime

Es gibt heute kaum noch einen Kriminalitätsbereich, in dem sich die Täter nicht ausgefeilter Technik bedienen und das Internet als Tatmittel nutzen. Dies trifft auf den Bereich der Wirtschaftskriminalität in besonderer Weise zu. 2011 registrierten wir bundesweit rund 11.600 Fälle von Wirtschaftskriminalität – ein Anteil von 15% –, bei denen das Internet als Tatmittel genutzt wurde; 2010 war es bei rund 31.000 Fällen sogar jeder dritte Fall. Für das Jahr 2011 wurden in der PKS insgesamt über 220.000 Fälle mit dem Tatmittel Internet registriert. Dies lässt zwar keine konkreten Aussagen bezogen auf den Bereich Cybercrime zu, zeigt letztlich aber, welche Bedeutung das Internet in den letzten Jahren für die Begehung von Straftaten gewonnen hat.

Straftaten, bei denen Elemente der EDV wesentlich für die Tatausführung sind, werden als „Cybercrime im engeren Sinne“ bezeichnet. Konkret geht es um Computerbetrug (z. B. Phishing im Bereich Onlinebanking), Betrug mit Zugangsberechtigung zu Kommunikationsdiensten, Datenfälschung, Täuschung im Rechtsverkehr bei der Datenverarbeitung, Datenveränderung bzw. Computersabotage und das Ausspähen bzw. Abfangen von Daten. Im Jahr 2011 wurden hierzu knapp 60.000 Fälle registriert, ähnlich viele wie im Jahr zuvor. Der Computerbetrug[4] stellt mit rund 45% aller Fälle die mit Abstand größte Gruppe dar. Der registrierte Schaden aller Cybercrime-Delikte im Jahr 2011 belief sich auf über 71 Mio. € und stieg damit im Vergleich zum Vorjahr um ca. 14%.

Die besondere Dynamik der Cybercrime sowie arbeitsteiliges und staatenübergreifendes Vorgehen zeigen sich besonders beim sog. Phishing im Zusammenhang mit Onlinebanking. Im Jahr 2008 brachte die flächendeckende Einführung des iTAN-Verfahrens hier zunächst einen Rückgang der Fallzahlen mit sich. Bereits 2010 stiegen diese jedoch wieder erheblich um über 80% auf mehr als 5.300 Phishing-Fälle an, dieser Trend hielt 2011 mit einem nochmaligen Anstieg von ca. 20% auf über 6.400 Fälle an. Bei einem durchschnittlichen Schaden von 4.000 € pro Fall lag der Gesamtschaden 2011 bei ca. 25,7 Mio. Euro – 18% mehr als im Jahr 2010. Schätzungen zufolge werden dem BKA nur etwa 20-30% der Phishing-Fälle bekannt, sodass Fallzahlen und Schäden tatsächlich wesentlich höher liegen dürften.

Mittlerweile werden 2/3 der Schadcodes mittels sog. Drive-by-Infections – beim Aufrufen einer für den Besucher und späteren Geschädigten unverdächtigen, aber dennoch infizierenden Internetseite – verteilt. Auf diese Weise können die Täter z. B. Trojaner verteilen, die in der Lage sind, sich in die Abwicklung von Online-Banktransaktionen „zwischen-

3 „Civil Confiscation“ bzw. „Non-Conviction Based Confiscation“

4 Z. B. Phishing im Bereich Onlinebanking, Onlinebetrügereien in eCommerce-Portalen und Carding, der Einsatz illegal abgegriffener Kreditkartendaten zum Warenerwerb

zuschalten“ und Überweisungsdaten zu verändern. Schon seit Ende 2008 wird das deutsche iTAN-Verfahren von solchen Trojanern durch sog. Man-in-the-Middle-Attacken erfolgreich angegriffen.

Mittlerweile geraten auch mobile Endsysteme ins Zielspektrum der Täter: Hierbei wird versucht, parallel zum Computer auch Mobiltelefone zu infizieren, um mögliche SMS-basierte Authentifizierungsverfahren auszuhebeln. Bei einem aktuellen Modus Operandi z. B. spähen die Täter mittels „klassischem Phishing“ die Zugangsdaten von Bankkunden für das Onlinebanking aus. Anschließend richten sie ohne Wissen des Bankkunden das mTAN-Verfahren ein; für den Empfang der mTAN wird dabei eine Mobilnummer der Täter hinterlegt. Der von der Bank per Post zugestellte Aktivierungscode wird von den Tätern abgefangen – bspw. durch Entwenden aus dem Briefkasten des Opfers.

Die digitale Identität in ihren unterschiedlichsten Ausprägungen steht nach wie vor besonders im Interesse von Straftätern. Sie sind an allen Arten von Zugangsdaten interessiert, mit denen sie letztlich zulasten Dritter Verfügungen im Internet vornehmen können, z. B. Bankaccounts, Accounts für soziale Netzwerke oder Kreditkartendaten. Verwertet werden Kreditkartendaten z. B. über das sog. Carding. Dabei erfolgt oftmals eine Art „Arbeitsteilung“ auf Täterseite: Der „Datendieb und -händler“ greift die Kreditkartendaten, z. B. mittels Einsatz von Schadsoftware, beim Opfer ab. Diese werden an den sog. Carder verkauft, der sie zum Onlinekauf von Waren nutzt, die anschließend z. B. über eBay oder von den Tätern selbst betriebene Webshops weiterverkauft werden. Zum Carding liegen uns keine validen Fall- und Schadenzahlen vor. Nach unserer Schätzung waren im Jahr 2009 120.000 Kreditkartenbesitzer in Deutschland betroffen, im Folgejahr bereits 200.000. 2010 lag der Schaden aus betrügerischen Kreditkartenumsätzen nach unserer Einschätzung allein für die deutsche Finanzwirtschaft im mittleren dreistelligen Millionen-Euro-Bereich, ca. 70% dieser Schäden resultierten aus dem Internet-Geschäft.

Ein weiteres Beispiel für den Variantenreichtum der Täter ist der Einsatz sog. Scareware – Software, die Angst erzeugen soll. Der Nutzer wird auf eine Webseite geleitet, die ihm vorgaukelt, dass auf seinem Computer ein Systemscan zu Viren, Trojanern etc. vorgenommen und eine große Anzahl Schadsoftware auf seinem System gefunden wurde. Ihm wird dann ein Tool zur Entfernung der Schadsoftware angeboten. Bei der Ausführung des Tools auf dem Rechner installiert sich eine angebliche Antiviren-Lösung. Diese müsse nach der Installation noch bezahlt und registriert werden. Der von Angst um die Sicherheit seiner Daten beeinflusste Kunde gibt seine Kreditkarteninformationen zur Bezahlung preis. Im Zuge dieses Vorgangs werden weitere Informationen zur Anschrift bzw. zur E-Mail-Adresse des Kunden gefordert. Das installierte Tool, mit dessen Hilfe der Kunde vermeintliche Gefahren für seinen Rechner abwenden wollte, sorgt letztlich dafür, dass sich eine Schadsoftware auf seinem System installiert.

Die Bilanz eines solchen Angriffs ist für den Computernutzer verheerend: Er hat ein nicht funktionierendes Programm erworben und wurde Opfer eines Betrugs, der Täter verfügt über seine Kreditkartendaten inklusive seiner Anschrift und E-Mail-Adresse, die missbraucht werden können, und sein Computer wurde mit Schadsoftware infiziert, mit der seine digitale Identität weiter ausgespäht werden kann. Darüber hinaus kann sein PC ohne sein Wissen an ein Botnetz angeschlossen und für Straftaten missbraucht werden.

Eine ähnliche Systematik steckt hinter der sog. Ransomware[5]. Diese infiziert z.B. beim Surfen im Internet den Computer des Opfers. Diesem

5 to ransom: auslösen, freikaufen

wird anschließend suggeriert, sein Computer sei für strafbare Handlungen verwendet und deshalb gesperrt worden. Zur Entsperrung soll der Benutzer des Computers eine „Strafe“ in Höhe von 100 € mittels eines digitalen Bezahldienstes entrichten. Sollte er nicht zahlen, würde die Festplatte gelöscht. Es werden vergleichsweise geringe Summen gefordert, um einen möglichst großen Anteil der Opfer zu einer Zahlung zu bewegen. Um den Eindruck einer polizeilichen Handlung zu erwecken, nutzen die Täter die Logos von Polizeibehörden sowie von verschiedenen bekannten Antiviren-Herstellern.

Solche „digitalen Erpressungen“ sind in verschiedenen Varianten ein zunehmendes Phänomen, dem sowohl Privatpersonen wie auch Unternehmen zum Opfer fallen können. So werden z. B. kompromittierte Daten, die dem ursprünglichen Berechtigten „gestohlen“ wurden, zum Rückkauf angeboten, oder der Angreifer droht damit, den erfolgreichen Angriff auf die Daten bzw. IT-Infrastruktur eines Unternehmens publik zu machen, und das betroffe-ne Unternehmen wird zur Zahlung eines „Schweigegeldes“ aufgefordert. Die Erpressung von Schutzgeld erfolgt z. B. durch die Androhung von DDoS-Angriffen auf die IT-Infrastruktur eines Unternehmens.

Wie professionell und einträglich das Geschäft mit gestohlenen Daten ist, wird daran deutlich, dass sich im Internet inzwischen ein eigener Markt hierfür herausgebildet hat. In dieser Underground Economy werden alle für die Tatbegehung erforderlichen Einzelkomponenten angeboten, z. B. Schadsoftware, Services für anonyme oder verschlüsselte Kommunikationswege oder zur Erstellung von Falschpersonalien sowie Kreditkartendaten. Auch Teile oder komplette Ausprägungen digitaler Identitäten werden angeboten, die Palette reicht dabei von Zugangsdaten zu Accounts bei ebay, Amazon, T-Online bis hin zu Onlinebanking-Konten; die Aufzählung ist beliebig erweiterbar.

Täter nutzen zudem verstärkt soziale Netzwerke wie Facebook oder StudiVZ vor allem für die Verbreitung von Schadsoftware und andere variantenreiche Betrugsmaschen. Accounts in sozialen Netzwerken werden übernommen, anschließend werden Nachrichten mit betrügerischen Absichten bzw. Schadsoftware an die gesamte Freundesliste des übernommenen Accounts verschickt. Kaum jemand vermutet hinter einer E-Mail oder Chat-Nachricht, die augenscheinlich von einem Freund oder einem Familienmitglied stammt, einen hinterhältigen Betrug. Microsoft kommt in einer Studie zu dem Ergebnis, dass über 50% der Zugriffe auf Phishing-Seiten aus sozialen Netzwerken heraus erfolgen. Mitglieder dieser Plattformen wähnen sich fälschlicherweise in einem geschützten Raum. Auch sog. Botnetze stellen eine lukrative Handelsware innerhalb der Underground Economy dar; darunter versteht man Netze ferngesteuerter Computer, die ohne Wissen ihrer Besitzer über einen Schadcode infiziert wurden. Diese PCs leiten nicht nur die persönlichen Daten des Besitzers an die Täter weiter, sondern dienen Straftätern auch als Werkzeug für weitere Straftaten[6].

Auch Smartphones gewinnen in diesem Zusammenhang an Bedeutung. Ende 2010 wurde in China erstmals eine neue Schadsoftware festgestellt, die auf Smartphones abzielt. Die Infizierung der Geräte erfolgt über manipulierte Apps[7]. Infizierte Geräte sind Teile eines Botnetzes; der Vorteil für die Täter liegt darin, dass Mobiltelefone in der Regel ständig angeschaltet sind, während PCs nach der Nutzung heruntergefahren werden und für das Botnetz nicht mehr zur Verfügung stehen.

6 Z. B. zum Verteilen von Schadsoftware, zum anonymen Versand von Spam-Mails, zum Angreifen von Webseiten und als sog. Proxies auch zur Verschleierung der Identität der Täter

7 App (engl. = application) Apps (in Zusammenhang mit Smartphones) sind Anwendungen, die über die Nutzung der Datenverbindung verschiedene Funktionen und Services erfüllen.

Für Staat und Wirtschaft besonders gefährlich können sog. DDoS[8]-Attacken sein. Dies sind gezielte Angriffe auf die Server z. B. eines Unternehmens oder von Regierungseinrichtungen, auch auf sog. Kritische Infrastrukturen. Dabei werden die Server mit einer Flut von Anfragen bombardiert, bis das System nicht mehr in der Lage ist, diese Flut zu bewältigen, und im schlimmsten Fall zusammenbricht. Für diese Angriffe setzen die Täter in der Regel von ihnen kontrollierte Botnetze ein.

Im Sommer 2011 wurden vermehrt bekannte deutsche Webshops Opfer von DDoS-Attacken. Die Webserver der betroffenen Shops werden so lange angegriffen, bis die Shops nicht mehr erreichbar sind. Da viele Shops ihre Ware nur im Internet anbieten und keinen bzw. nur in geringem Umfang „Ladenverkauf" betreiben, ist dies überaus geschäftsschädigend. Es handelt sich nicht um Einzelfälle. So stellte das Bundesamt für Sicherheit in der Informationstechnik (BSI) z. B. Ende August letzten Jahres DDoS-Attacken gegen ca. 30 Internetpräsenzen deutscher Unternehmen der Nahrungsmittel- und Immobilienbranche fest. Anschließend fokussierten sich die Angriffe auf ca. 60 überwiegend deutsche Unternehmen der Reise- und Hotelbranche. Anfang September 2011 konnten ca. 400 weitere Domains als Angriffsziele festgestellt werden, darunter auch die des Bundesgerichtshofes und der Bundesbank. Es handelt sich um Domains verschiedener Branchen, ein Schwerpunkt ist nicht mehr auszumachen. Neben den DDoS-Attacken erfolgt wie bereits beschrieben eine mit dem Angriff einhergehende Erpressung.

Zahlungskarten-Kriminalität

Technik und Elektronik bieten auch in anderen Bereichen Tatgelegenheiten für Straftäter. In Deutschland sind ca. 57.000 Geldautomaten und über 600.000 POS[9]-Terminals im Einsatz. Schätzungsweise 125 Millionen Zahlungskarten deutscher Emittenten sind an die Kunden ausgegeben, ca. 75% davon sind Debitkarten. Inhaber von Zahlungskarten deutscher Emittenten verfügen zudem im internationalen Vergleich über eine hohe Bonität – insgesamt also ein sehr lukrativer Markt für Kriminelle. Im Jahr 2011 wurden in Deutschland fast 1.300 Fälle des sog. Skimming, also Angriffe auf Geldautomaten, registriert; ein Rückgang von 59% gegenüber dem Vorjahr. Nach unseren Schätzungen lag der aus Skimming resultierende Schaden 2011 bei rund 35 Mio. € und damit 25 Mio. € niedriger als noch im Vorjahr.

Nach wie vor installieren die fast ausnahmslos aus Südosteuropa stammenden Täter Vorbaugeräte zum Auslesen der Kartendaten sowie versteckte Mini-Kameras oberhalb der Tastatur oder im Deckenbereich, z. B. in Rauchmelderattrappen, zur Aufzeichnung der PIN-Eingaben. Alternativ werden Tastaturattrappen angebracht, die die PIN speichern. Für die erfreuliche Entwicklung bei den Fall- und Schadenszahlen ist nach unserer Auffassung maßgeblich die zum 01.01.2011 erfolgte Umstellung auf Chiptechnologie verantwortlich. Bedingt durch diese technische Umstellung im europäischen Zahlungsraum können die Täter, die die abgegriffenen Daten auf die Magnetstreifen gefälschter Karten („white plastics") aufbringen, diese nicht mehr in Europa einsetzen. Dies zwingt sie dazu, den Einsatz ihrer Fälschungen ins außereuropäische Ausland in sog. „Nicht-Chip-Länder" zu verlagern. So wurden 2011 gefälschte Debitkarten vorrangig in den USA, Russland, Mexiko, Argentinien und Kolumbien sowie in zahlreichen weiteren Ländern in Südamerika, Asien und Afrika eingesetzt.

8 Distributed Denial of Service = Angriff zur Verweigerung des Dienstes (eines Servers) durch ein Rechnernetzwerk. Ein Rechnernetzwerk teilt sich die Arbeit („distributed"), um einen leistungsfähigen Server durch eine Unmenge von Anfragen in die Knie zu zwingen.

9 „Point of Sale", elektronische Geräte zur bargeldlosen Zahlung mittels Debitkarte und PIN

Bedauerlicherweise hat eine derart positive Entwicklung wie beim Skimming an Geldautomaten meist auch eine Kehrseite. Mittlerweile weichen die Täter auf andere Tatobjekte aus, um dort Kartendaten und PIN abzugreifen. Im Jahr 2011 wurden erstmals nach 2008 wieder erfolgreich POS-Terminals manipuliert. Im vergangenen Jahr wurden zudem mehrere Tanksäulen von unbemannten SB-Tankstellen manipuliert und die Magnetstreifendaten sowie PIN der dort eingesetzten Zahlungskarten abgegriffen. Auch Fahrkartenautomaten der Deutschen Bahn sind betroffen.

Gemeinsames Ziel von Sicherheitsbehörden und Wirtschaft muss es sein, diesem Ausweichverhalten der Straftäter eine wirkungsvolle gemeinsame Strategie entgegenzustellen. Zudem müssen Kreditinstitute auch für die Verwendung im außereuropäischen Ausland Lösungen anbieten, die die Magnetstreifen auf den Zahlungskarten verzichtbar machen. Zumindest sollten in „Nicht-Chip-Ländern" getätigte Magnetstreifenumsätze besonderen Prozessen unterworfen werden, z. B. durch Limitierung magnetstreifenbasierter Umsätze im Ausland oder standardmäßige Benachrichtigungen (bspw. per SMS) an den Kunden über Auslandstransaktionen.

Kritische Infrastrukturen

Infrastruktursysteme vernetzen Europa und die Welt und bilden neuralgische Knotenpunkte. Sie garantieren zum einen Mobilität, medizinische Versorgung, Energie- und Informationsflüsse, stellen aber auch kritische Schwachstellen dar. Angriffe auf kritische Infrastrukturen können fatale Auswirkungen auf die gesamte Wirtschaft und Gesellschaft haben. Angriffe unter Ausnutzung moderner Kommunikations- und Informationstechnik rücken dabei zunehmend in den Fokus der Sicherheitsbehörden. Alle zwei Sekunden gibt es in Deutschland einen Angriff im Internet, die Grenzen zwischen Kriminalität, Spionage und Terror sind hier unscharf. Auch der gezielte Einsatz von Trojanern, um Prozess- und Produktionsdaten auszuspähen oder zu manipulieren, kann weitreichende Folgen haben. Im Juli 2010 wurde eine Schadsoftware entdeckt, die eine entsprechende Sicherheitslücke ausnutzt und über mobile Datenträger wie USB-Sticks unbemerkt Betriebssysteme in Industrieanlagen infizieren kann.

Ein Ziel dieses Trojaners mit der Bezeichnung STUXNET ist das Ausspähen von Prozess- und Produktionsdaten mittels maßgeschneiderter Datenbankabfragen. Darüber hinaus sollen so Manipulationen und Angriffe auf Prozessleittechniken von kritischen Infrastrukturen möglich sein. So kann dieser Trojaner z. B. falsche Messdaten in die Steuerungssysteme von Energieversorgungsanlagen einspielen, ohne dass eine Fehlermeldung auf einen kritischen Prozess hinweist. Die Programmierung eines derartigen Trojaners ist mit enormem Aufwand und Kosten verbunden. Nach bisherigen Vermutungen sollen über 30.000 Rechner und mindestens 15 Industrieanlagen weltweit infiziert worden sein. Die Schwerpunkte lagen dabei im Iran und in Südasien. Mitte Oktober 2011 berichtete ein IT-Sicherheitsunternehmen, dass ein neuer Trojaner („Duqu") entdeckt worden sei, der Teile des Software-Codes von STUXNET enthalte und deshalb als gefährlich gelte. Dieser Trojaner sei auf Computern von europäischen Unternehmen entdeckt worden, die an der Entwicklung von Industrieanlagen-Software beteiligt sind. Erst im September 2011 wurde bekannt[10], dass es unbekannten Hackern über Monate gelungen war, geheime Daten von Rüstungsfirmen aus Japan, Indien, Israel und den USA auszuspähen. Die Täter verschickten

10 Spiegel-Online vom 20. September 2011

E-Mails mit infizierten PDF-Dateien an Mitarbeiter dieser Unternehmen. Durch das Öffnen dieser Dateien gelangte Schadsoftware in die Computernetzwerke der Firmen, die es den Tätern letztlich gestattete, die gekaperten Rechner zu kontrollieren. Sie sollen auch Zugriff auf geheime Daten gehabt haben.

Spionage

Im Zuge der Globalisierung des Wirtschaftslebens und des damit einhergehenden wachsenden Konkurrenzdrucks nimmt die Gefahr der Ausspähung von Geschäfts- und Betriebsgeheimnissen zu. Dabei wird unterschieden zwischen Wirtschaftsspionage und Konkurrenzausspähung. Wirtschaftsspionage ist ein sog. Staatsschutzdelikt, entscheidendes Kriterium ist dabei eine nachrichtendienstliche Steuerung. Ist kein nachrichtendienstlicher Bezug gegeben oder erkennbar, liegt zumeist ein Fall von Konkurrenzausspähung vor – die illegale Ausforschung durch ein konkurrierendes Unternehmen bzw. eine Einzelperson.

Bei der Konkurrenzausspähung geht es überwiegend um die Weitergabe von Kundendaten[11], aber auch um geheime Produktionsunterlagen, Computerprogramme und andere sensible Firmeninformationen. Im Zentrum der Aufmerksamkeit stehen nahezu alle Unternehmensbereiche, wobei Forschungs- und Entwicklungsabteilungen und damit innovationsabhängige Unternehmen bspw. aus der Pharma- und der Automobilindustrie oder Softwarefirmen besonders gefährdet sind.

Die Ausforschung von Wirtschaftsunternehmen ist aber auch fester Bestandteil der Arbeit zahlreicher Nachrichtendienste von Staaten z. B. in Osteuropa und Asien. Fremde Dienste konzentrieren sich vor allem auf das Ausspähen von Spitzentechnologie und Grundlagenforschung. Angriffsziel sind Konstruktions- und Produktionsabläufe. Zunehmend wächst dabei das Interesse an mittelständischen Firmen, da diese seit einiger Zeit verstärkt in die Forschung und Entwicklung zukunftsweisender Produkte investieren.

Von immer größerer Bedeutung sind auch dabei Angriffe über das Internet. Wirtschaftsspionage und Konkurrenzausspähung kann man heute bequem vom Schreibtisch aus betreiben. Die Täter nutzen neue Technologien und ändern immer wieder ihre Angriffsvarianten auf IT-Systeme. Über das World-Wide-Web werden Trojaner verschickt, die die Computer-Netzwerke der attackierten Firmen infizieren und anschließend deren geistiges Eigentum für die Späher sichtbar und abrufbar machen. Auch die Gefahr durch Lauschangriffe „vor Ort“ schreitet durch die Miniaturisierung und stärkere Leistungsfähigkeit handelsüblicher Elektronik immer weiter fort. Mini-Kameras und Mikrofone, die z. T. in Alltagsgegenständen wie Kugelschreibern, Brillengestellen und Schlüsselanhängern verborgen werden können, eröffnen heute Möglichkeiten, die früher wenn überhaupt nur speziell entwickelter, professioneller nachrichtendienstlicher Technik vorbehalten waren.

Kooperation mit der Wirtschaft

Die veränderten Erscheinungsformen der Kriminalität zeigen deutlich: An einer ganzheitlichen Bekämpfungsstrategie führt kein Weg vorbei. Neben einem konsequenten behördenübergreifenden operativen Handeln ist dabei entscheidend, auch die Wirtschaftsunternehmen in ein Netzwerk der Informationen einzubeziehen. Das Bundeskriminalamt hat in den vergangenen Jahren die Zusammenarbeit mit der Wirtschaft ausgebaut. U. a. wurde die Initiative zu einem intensiven direkten Dialog mit der Wirtschaft, hier insbesondere mit weltweit tätigen deutschen

11 Z. B. von Banken, Personaldienstleistern oder aus dem Bereich des Internethandels

Global Playern, ergriffen; mittlerweile haben sich 54 Unternehmen für diese Form der Zusammenarbeit entschieden. Unternehmen verfügen oftmals über wichtige Informationen, die Erkenntnisse des BKA ergänzen und in Früherkennungsstrategien einfließen können. Im Gegenzug können Unternehmen für Gefährdungslagen sensibilisiert werden und entsprechende Schutzvorkehrungen ergreifen. Wie erwähnt ist das Anzeigeverhalten seitens der Wirtschaft bei Cybercrime-Sachverhalten defizitär.

U. a. um dieses unbefriedigende Anzeigeverhalten zu verbessern, haben die Polizeibehörden der Länder und das BKA „Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime“ erarbeitet. Diese Leitlinien sollen betroffenen Unternehmen konkrete Hinweise zum Verhalten bei Cyber-Angriffen geben und zudem Unsicherheiten im Zusammenhang mit der Anzeige solch strafrechtlich relevanter Vorfälle nehmen. So werden u. a. Gesetzesgrundlagen vorgestellt, Verhaltensempfehlungen für Firmenleitung und Systemadministratoren gegeben, Möglichkeiten und Grundsätze der polizeilichen Ermittlungsarbeit dargestellt und zentrale Ansprechstellen bei der Polizei in Bund und Ländern benannt. Diese Handlungsempfehlungen stehen in gedruckter Form sowie als Online-Version unter www.bka.de zur Verfügung. ■