Vortrag zum Thema

IT Risiko: Vertrauensschaden

Unter besonderer Berücksichtigung der Fragestellung: "Wo liegen aufgrund der Deckungsbedingungen der Vertrauensschadenversicherung besondere Risiken im IT-Bereich?"
gehalten am 17.01.2002 in München.

Angaben zu Referenten

Dipl.-Ing. Stefan Meisel,
seit über 15 Jahren als Software-Systementwickler tätig, davon die meiste Zeit als Freiberufler im Rahmen einer Ingenieurssozietät mit verschiedenen gleichberechtigten Partnern. Derzeit tätig als Inhaber der Firma SAMSoft ®, Augsburg (http://www.samsoft.de). Spezialgebiet: Große Datenbankanwendungen in vernetzten Client-Server Umgebungen.

Neben dem Sicherheitsinteresse in eigener Sache (man stelle sich die Katastrophe vor, wenn von einem unserer Systeme eine schädliche Software auf ein Kundensystem gelangte) und der Kundenberatung zum Thema Datensicherheit u. a.

Mitglied in der Virus Help Munich (VHM)
Das ist ein Zusammenschluss der führenden deutschen Entwickler und Systemberater im Bereich Software-Sicherheit zum Zweck des gegenseitigen Informationsaustausches. Für nicht-kommerzielle Anwender wird bei Befall mit schädlicher Software Hilfe, Beratung und Unterstützung angeboten. Als Anlaufstelle wird eine Website betrieben http://www.virushelpmunich.de und öffentliche Tagungen abgehalten. Mitglieder sind u.a. Vertreter der Firmen

Howard Fuhs Security, Wiesbaden
Trend Micro Deutschland (Interscan, ScanMail)
H+B EDV Datentechnik (Antivir)
Network Associates Dr. Solomon (Virusscan, TVD)
Symantec, Norton Anti Virus (NAV Solutions)
GEGA Software und Medienservice, Magdeburg (www.av-test.org)
ROSE Software (Hackstop, IRC-Scan)
OpenAntiVirus (openantivirus.org)
AMaViS Development Team (amavis.org)

Computerkriminalität heute

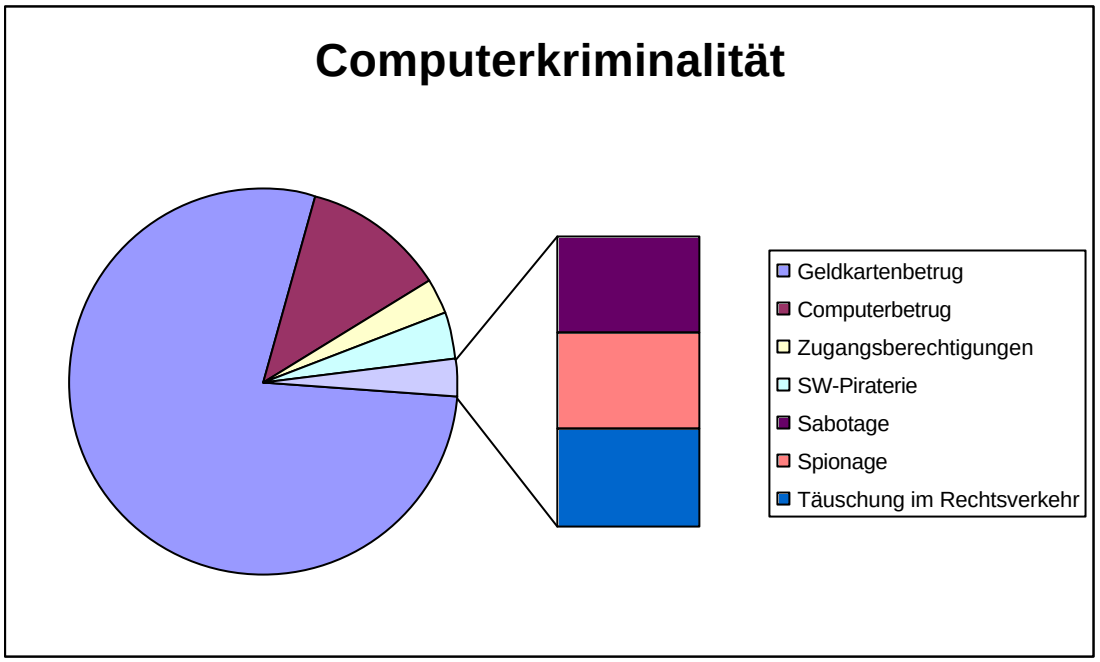
Die Begriffe IT-Risiken, EDV-Sicherheit und Computerkriminalität rufen sofort Vorstellungen wach an die sagenhaften Hacker und Cracker, die nächtelang mit Sonnenbrille auf der Nase durch die Netze geistern, stets auf der Suche nach einem offenen Server oder einer verwaisten Datenleitung, um einzudringen und Unheil zu stiften. Die Realität der Kriminalstatistik sieht etwas anders aus.

Tatsächlich entfällt der meiste heute bekannt gewordene oder gemeldete Teil der Computerkriminalität, nämlich 78 % auf Betrug mittels rechtswidrig erlangter Karten für Geldausgabe- bzw. Kassenautomaten. In 12 % der Fälle wurde Computerbetrug nach §263a registriert also insbesondere

- Abrechnungsmanipulation im Bereich der Gehalts- und Rechnungszahlung,
- Bilanzmanipulationen und
- Kontostandsmanipulationen bei Banken.

Weitere ca. 3 %, mit steigender Tendenz, stellt der strafbare Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (Telefon, Internet) dar. Es verbleiben 7 % gemischte Fälle, die sich aus Fälschung beweiserheblicher Daten oder Täuschung im Rechtsverkehr bei Datenverarbeitung,

Datenveränderung oder Computersabotage, Ausspähen von Daten, und Computer-Software-Piraterie zusammensetzen.



Die gesamte Fallzahl von 56684 im Jahr 2000 und die genannten prozentualen Verteilungen könnten den Anschein erwecken, dass das Thema Computerkriminalität eher eine Randerscheinung des Kreditkartenbetrugs ist. Nicht zu sehen sind aber natürlich diejenigen Fälle, die in keiner Statistik auftauchen, entweder weil sie nicht gemeldet wurden oder nicht als Straftaten erkannt oder ermittelt wurden. Die Ermittlungsbehörden sprechen von der "*Dunkelfeldproblematik*". Über einen großen Anteil nicht verfolgter Straftaten klagt beispielsweise die Branche der Hersteller von Standardsoftwareprodukten, nämlich über die unerlaubte Vervielfältigung, das sogenannte Raubkopieren. Obwohl es sicherlich massenhaft geschieht, gibt es kaum einen Fall, der wirklich bis in die letzte Konsequenz verfolgt wird. In der Statistik schlägt sich dieses Delikt mit 4% nieder.

Besonders schwerwiegend, und in der Statistik ebenfalls stark unterrepräsentiert, ist das Ausspähen von Daten, landläufig als Computerspionage bezeichnet. Ziel des Interesses sind vornehmlich Computerprogramme, Forschungs- und Rüstungsdaten, Daten des kaufmännischen Rechnungswesens sowie Kundenadressen bei öffentlichen Einrichtungen und in der Privatwirtschaft. Der Schaden ist meistens nur schwer zu beziffern und der Geschädigte hat oft kein Interesse an einem Bekanntwerden des Vorfalls. Das Täterprofil der Computerspionage setzt sich aus jugendlichen Hackern, aber auch aus konkurrierenden Wirtschaftsunternehmen und Nachrichtendiensten zusammen. Durch die Digitalisierung des Telefonverkehrs überschneidet sich die Computerspionage mit dem Abhören von Telefongesprächen, so dass Mobiltelefone, Richtfunksender und Satellitenverbindungen bei unverschlüsselt erfolgender Kommunikation leichte Angriffsziele bieten.

Hier möchte ich ein Fallbeispiel vorlesen, das mir freundlicherweise als Vorabzug zu seinem neuen Buch von dem bekannten Datensicherheitsexperten Howard Fuhs, Wiesbaden zur Verfügung gestellt wurde.

Fallbeispiel Erlkönige

[Es folgt das Beispiel einer Medizintechnik-Firma, sich ganz auf die Entwicklung von neuartigen Geräten spezialisiert hat. Plötzlich kam die Konkurrenz mit den gleichen Produkten früher auf den Markt. Dieser Fall von Industriespionage zeigt ein Problem mit dem Outsourcing auf.]

Schadenstechnische Bewertung

Wie so oft in diesen Fällen war es der Unternehmensleitung nicht möglich, die Schadenshöhe auch nur annähernd zu beziffern. Eine erste Schätzung der Unternehmensführung geht von ca. 12 - 20 Mio. DM Umsatzverlust pro Jahr aus. Die Verluste durch die hohen Entwicklungskosten konnten ebenfalls nicht näher benannt werden. Bedingt durch den Umsatzrückgang mussten Kündigungen ausgesprochen werden, womit dieser Vorfall auch eine direkte Schadensauswirkung auf die betroffenen Mitarbeiter hat.

Sicherheitstechnische Bewertung

Der Fall zeigt auf, dass selbst bei Unternehmen in denen ein vorbildliches Datensicherheits-management herrscht, Angriffspunkte vorhanden sind, die dann erfolgreich missbraucht werden können. Gemäß dem alten Sprichwort "Die stärkste Kette ist nur so stark wie ihr schwächstes Glied" haben die Angreifer beim schwächsten Glied in der Datensicherheitskette, dem Prototypenbauer, angesetzt. Obwohl sehr viel für die Datensicherheit unternommen wurde, zeigt dieser Vorfall verschiedene Probleme auf.

1. Datensicherheit ist kein einmal erreichter Zustand, sondern ein dynamischer Prozess der regelmäßiger Kontrolle unterliegen muss. Deshalb ist es notwendig, sowohl die IT-Infrastruktur als auch die getroffenen Datensicherheitsmaßnahmen regelmäßig durch externe und unabhängige Dienstleister einem Sicherheitsaudit zu unterziehen. Die dabei anfallenden Berichte müssen sorgfältig studiert und die darin vorgeschlagenen Verbesserungsmaßnahmen konsequent umgesetzt werden. Durch ein unabhängiges Sicherheitsaudit wäre es eher aufgefallen, dass durch die Vergabe aller Prototypenaufträge an einen Anbieter ein Problem erwachsen könnte, unabhängig davon wie hoch oder niedrig dessen Datensicherheitsstandards sind.

2. Der externe Einkauf von Dienstleistungen muss breit gestreut und damit auf verschiedene Anbieter aufgeteilt werden. Dadurch wird erreicht, dass man nicht zu sehr von einem Anbieter abhängig wird und andererseits der Anbieter nicht umfassende Kenntnisse über interne Vorgänge im Unternehmen erhält oder dessen technisches Know-How komplett erhält.

3. Da auf die Datensicherheitsmaßnahmen bei externen Beschaffungen kein unmittelbarer Einfluss genommen werden kann, muss im Rahmen der Vertragsgestaltung indirekt durch entsprechende Haftungsklauseln Einfluss genommen werden. Sollte ein externer Zulieferer / Dienstleister, der Daten zur Verfügung gestellt bekommt, nicht auf dieses Haftungsklauseln eingehen bzw. nicht bereit sein diese zu akzeptieren, ist es besser von einem Vertrag mit diesem Unternehmen abzusehen.

4. Ein Unternehmen, welches nach ISO 9000 ff zertifiziert ist, muss nicht notwendigerweise über hohe Datensicherheitsstandards verfügen. Dass im Rahmen der ISO-9000 die Datensicherheit keine Berücksichtigung findet, offenbart eine der Schwächen der ISO-Standards.

Soweit dieses Fallbeispiel.
Es war hier einige Male von Schutzmaßnahmen gegen schädliche Softwarebestandteile die Rede, deshalb will ich hier an dieser Stelle einen kleinen Abschnitt mit Begriffsklärungen einschieben.

Definition: Arten schädlicher Software

Grundsätzlich ist ein IT-System nicht nur durch Angriffe von Hackern und Crackern von außen durch die Netze gefährdet, sondern kann auch durch bösartige Software, auch Malware genannt, attackiert werden, die – einmal ausgesetzt - ganz ohne menschliches Eingreifen aktiv werden kann. Je nach Wirkprinzip und Konstruktionsweise wird nach folgenden Grundtypen von Schadensprogrammen klassifiziert:

Virus

Der Computervirus ist der bekannteste und am meisten gefürchtete Softwareschädling. Wir sagen nach Konvention ganz bewusst *der Virus*, wenn es sich um einen Computervirus handelt und *das Virus*, wenn es sich um einen biologischen Virus handelt. Ein Computervirus ist ein Stückchen Softwarecode, das sich an andere Programme anlagert und zusammen mit diesen gestartet wird. Kennzeichnend für einen Virus ist, das er sich vermehrt. Das Virusprogramm ist nicht selbstständig lauffähig und benötigt immer ein anderes Objekt als Transportmittel. Das Transportmittel wird vom Viruscode ausgewählt und infiziert. Dies kann eine ausführbare Datei oder ein Bootsektor sein. Die Tatsache, dass auch Office-Dokumente ausführbare Dateien sind, hat den Makroprogramm-Viren eine große Verbreitung beschert. Ein Virus muss nicht notwendigerweise eine Schadensroutine besitzen. Ein bekannter, neuerer Vertreter der Dateiviren ist der CIH-Virus.

Wurm

Ein Wurm ist ein Schädlingsprogramm, das kein Wirtsobjekt benötigt, um sich zu vermehren. Dieser Typ gehört zu den ältesten Vertretern der Sabotageprogramme. Schon 1988 gelangte der sogenannte "Internet"-Worm zu trauriger Berühmtheit, als er am 2. November im MIT Artificial Intelligence Lab von Robert Morris losgelassen wurde. Innerhalb von 20 Minuten war das Internet dicht – 2200 DECVax und Sun-Maschinen, die mit der BSD-Variante von Unix arbeiteten waren wegen Überlastung ausgefallen. Heute ist es die große Verbreitung des Windows E-Mail-Clientprogramms Outlook, die immer wieder zu großen Ausbrüchen von E-Mail-Würmern führt. Namen wie Melissa, I Love You, Code Red und Nimda bezeichnen Vertreter dieser Gattung.

Trojaner

Als die Griechen unter der Führung des listenreichen Odysseus nach langer Belagerungszeit vor den Stadttoren von Troja ein hölzernes Pferd zurückließen, taten sie dies natürlich in der Hoffnung, die Bürger würden so arglos sein, die Statue mit dem gefährlichen Inhalt in ihre uneinnehmbare Festung hineinzuziehen. Genau so ist die Funktion einer trojanischen Software. Sie gibt vor, etwas Nützliches zu tun, enthält jedoch auch einen schädlichen Inhalt. Als Kurzbezeichnung hat sich "Trojaner" eingebürgert, obwohl die Trojaner in Homers Sage die Opfer waren und nicht die Täter. Trojaner haben, im Gegensatz zu Virus und Wurm, nicht die Fähigkeit, sich zu vermehren. Trojaner können, als Nutzprogramm getarnt, Daten ausspähen und diese an einen externen Angreifer übermitteln. Ein Sonderfall eines Trojaners ist ein Dropper. Dies ist ein Programm, das einen Virus oder Wurm freisetzt. Ein trojanisches Programm, das auf eine Kontaktaufnahme von außen wartet, um externe Steuer- und Spionagebefehle auszuführen, nennt man ein Backdoor. Die prominenten Vertreter der letzten Jahre sind *Netbus* und *Back Orifice*. Wer ein aktives Netbus Backdoor auf seinem Arbeitsplatzrechner hat, kann über das Internet von jedem Platz auf der Welt bei allen seinen Aktivitäten, z.B. Internet-Banking, beobachtet werden.

Bombe

Eine Bombe ist ein Stück Malware, in das keine große Mühe investiert wurde, den schädlichen Inhalt zu verbergen. Sobald das Programm gestartet ist, richtet es Schaden an, und zwar meist keinen geringen. Das einfachste Beispiel ist eine Batch-Datei, die alle Dateien auf der Festplatte löscht. Damit die Bombe überhaupt zur Ausführung kommt, wird sie zur automatischen Ausführung z.B. in das Startverzeichnis eines Rechners kopiert oder einem unbedarften Anwender unter dem Namen "Liesmich" oder "Klickmich" untergeschoben.

Scherzprogramm

Ein Scherzprogramm simuliert auf dem Zielrechner die Funktion eines Virus oder einer anderen Malware. Das Scherzprogramm an sich ist technisch harmlos. Nicht harmlos ist hingegen der verunsicherte Anwender, der womöglich in Panik gerät, einen Administrator bindet oder versucht selbst sein System zu "reparieren".

Hoax

Seit Jahren kursieren E-Mail-Warnungen vor angeblichen Viren, die sich im Internet verbreiten sollen. Symptomatisch für diese "Warnungen", die von gutgläubigen Anwendern leidenschaftlich verbreitet werden, ist die Aufforderung, diese wichtige Botschaft an alle Einträge im Adressbuch und alle Freunde und Verwandten zu schicken. Diese Aufforderung ist ein untrügliches Erkennungszeichen für Hoax-Mails. In diese Kategorie gehören auch Petitionen, Kettenbriefe und Tränendrüsenbriefe. Es wird zum Beispiel behauptet, ein südamerikanisches Kind brauche dringend einen Knochenmarkspender, und dies soll man allen mitteilen, die man kennt. Diese Warnungen oder Aufrufe werden Hoaxes genannt (engl. hoax, altengl. hocus: Scherz, Falschmeldung). Sie enthalten so gut wie niemals einen ernstzunehmenden Hintergrund. Vielmehr stellen diese "Warnungen" die eigentliche Gefahr dar, denn sie richten erheblichen Schaden an, in dem sie Menschen verunsichern und Arbeitszeit binden. Außerdem belasten sie durch ihre nicht geringe Zahl das Internet und seine Mailserver durch nutzlosen Datenverkehr.

Gesetzeslage

Kurze Zusammenstellung der möglicherweise in Betracht zu ziehenden rechtlichen Aspekte der Computerkriminalität.

StGB

§ 1 [Keine Strafe ohne Gesetz]

Eine Tat kann nur bestraft werden, wenn die Strafbarkeit gesetzlich bestimmt war, bevor die Tat begangen wurde.

§ 2 [Zeitliche Geltung]

(3) Wird das Gesetz, das bei Beendigung der Tat gilt, vor der Entscheidung geändert, so ist das mildeste Gesetz anzuwenden.

§ 11 [Personen- und Sachbegriffe]

(3) Den Schriften stehen Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen in denjenigen Vorschriften gleich, die auf diesen Absatz verweisen.

§ 13 [Begehen durch Unterlassen]

(1) Wer es unterläßt, einen Erfolg abzuwenden, der zum Tatbestand eines Strafgesetzes gehört, ist nach diesem Gesetz nur dann strafbar, wenn er rechtlich dafür einzustehen hat, daß der Erfolg nicht eintritt, und wenn das Unterlassen der Verwirklichung des gesetzlichen Tatbestandes durch ein Tun entspricht.
(2) Die Strafe kann nach § 49 Abs. 1 gemildert werden.

§ 15 [Vorsätzliches und fahrlässiges Handeln]

Strafbar ist nur vorsätzliches Handeln, wenn nicht das Gesetz fahrlässiges Handeln ausdrücklich mit Strafe bedroht.

§ 74 [Voraussetzungen der Einziehung]

(1) Ist eine vorsätzliche Straftat begangen worden, so können Gegenstände, die durch sie hervorgebracht oder zu ihrer Begehung oder Vorbereitung gebraucht worden oder bestimmt gewesen sind, eingezogen werden.

§ 74 e [Wirkung der Einziehung]

(1) Wird ein Gegenstand eingezogen, so geht das Eigentum an der Sache oder das eingezogene Recht mit der Rechtskraft der Entscheidung auf den Staat über.

§ 86 [Verbreiten von Propagandamitteln verfassungswidriger Organisationen]

(1) Wer Propagandamittel
im Inland verbreitet oder zur Verbreitung im Inland oder Ausland herstellt, vorrätig hält, einführt oder ausführt oder in Datenspeichern öffentlich zugänglich macht, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Propagandamittel im Sinne des Absatzes 1 sind nur solche Schriften (§ 11 Abs. 3), deren Inhalt gegen die freiheitliche demokratische Grundordnung oder den Gedanken der Völkerverständigung gerichtet ist.

§ 184 [Verbreitung pornographischer Schriften]

(1) Wer pornographische Schriften (§ 11 Abs. 3)
1. einer Person unter achtzehn Jahren anbietet, überläßt oder zugänglich macht,
2. an einem Ort, der Personen unter achtzehn Jahren zugänglich ist oder von ihnen eingesehen werden kann, ausstellt, anschlägt, vorführt oder sonst zugänglich macht,
wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
(2) Ebenso wird bestraft, wer eine pornographische Darbietung durch Rundfunk verbreitet.
(3) Wer pornographische Schriften (§ 11 Abs. 3), die Gewalttätigkeiten, den sexuellen Mißbrauch von Kindern oder sexuelle Handlungen von Menschen mit Tieren zum Gegenstand haben,
1. verbreitet,
2. öffentlich ausstellt, anschlägt, vorführt oder sonst zugänglich macht oder
3. herstellt, bezieht, liefert, vorrätig hält, anbietet, ankündigt, anpreist, einzuführen oder auszuführen unternimmt, um sie oder aus ihnen gewonnene Stücke im Sinne der Nummern 1 oder 2 zu verwenden oder einem anderen eine solche Verwendung zu ermöglichen,
wird, wenn die pornographischen Schriften den sexuellen Mißbrauch von Kindern zum Gegenstand haben, mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren, sonst mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

§ 202 a [Ausspähen von Daten]

(1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 263 a [Computerbetrug]

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
(2) § 263 Abs. 2 bis 5 gilt entsprechend.

§ 265 a [Erschleichen von Leistungen]

(1) Wer die Leistung eines Automaten oder eines öffentlichen Zwecken dienenden Fernmeldenetzes, die Beförderung durch ein Verkehrsmittel oder den Zutritt zu einer Veranstaltung oder einer Einrichtung in der Absicht erschleicht, das Entgelt nicht zu entrichten, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.
(2) Der Versuch ist strafbar.

§ 303 a [Datenveränderung]

(1) Wer rechtswidrig Daten (§ 202 a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.

§ 303 b [Computersabotage]

(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, daß er
1. eine Tat nach § 303 a Abs. 1 begeht oder

2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,
wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.

StPO

§ 94 [Gegenstand der Beschlagnahme]

(1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen.
(2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der Beschlagnahme.

§ 95 [Herausgabepflicht]

(1) Wer einen Gegenstand der vorbezeichneten Art in seinem Gewahrsam hat, ist verpflichtet, ihn auf Erfordern vorzulegen und auszuliefern.
(2) Im Falle der Weigerung können gegen ihn die in § 70 bestimmten Ordnungs- und Zwangsmittel festgesetzt werden. Das gilt nicht bei Personen, die zur Verweigerung des Zeugnisses berechtigt sind.

§ 102 [Durchsuchung beim Verdächtigten]

Bei dem, welcher als Täter oder Teilnehmer einer Straftat oder der Begünstigung, Strafvereitelung oder Hehlerei verdächtig ist, kann eine Durchsuchung der Wohnung und anderer Räume sowie seiner Person und der ihm gehörenden Sachen sowohl zum Zweck seiner Ergreifung als auch dann vorgenommen werden, wenn zu vermuten ist, daß die Durchsuchung zur Auffindung von Beweismitteln führen werde.

§ 103 [Durchsuchung bei sonstigen Personen]

(1) Bei anderen Personen sind Durchsuchungen nur zur Ergreifung des Beschuldigten oder zur Verfolgung von Spuren einer Straftat oder zur Beschlagnahme bestimmter Gegenstände und nur dann zulässig, wenn Tatsachen vorliegen, aus denen zu schließen ist, daß die gesuchte Person, Spur oder Sache sich in den zu durchsuchenden Räumen befindet.

§ 136 [Erste Vernehmung]

(1) Bei Beginn der ersten Vernehmung ist dem Beschuldigten zu eröffnen, welche Tat ihm zur Last gelegt wird und welche Strafvorschriften in Betracht kommen. Er ist darauf hinzuweisen, daß es ihm nach dem Gesetz freistehe, sich zu der Beschuldigung zu äußern oder nicht zur Sache auszusagen und jederzeit, auch schon vor seiner Vernehmung, einen von ihm zu wählenden Verteidiger zu befragen. Er ist ferner darüber zu belehren, daß er zu seiner Entlastung einzelne Beweiserhebungen beantragen kann. In geeigneten Fällen soll der Beschuldigte auch darauf hingewiesen werden, daß er sich schriftlich äußern kann.
(2) Die Vernehmung soll dem Beschuldigten Gelegenheit geben, die gegen ihn vorliegenden Verdachtsgründe zu beseitigen und die zu seinen Gunsten sprechenden Tatsachen geltend zu machen.
(3) Bei der ersten Vernehmung des Beschuldigten ist zugleich auf die Ermittlung seiner persönlichen Verhältnisse Bedacht zu nehmen.

UrhG

§ 2 [Geschützte Werke]

(1) Zu den geschützten Werken der Literatur, Wissenschaft und Kunst gehören insbesondere:
1. Sprachwerke, wie Schriftwerke, Reden und Computerprogramme;
(2) Werke im Sinne dieses Gesetzes sind nur persönliche geistige Schöpfungen.

§ 69 a [Gegenstand des Schutzes]

(1) Computerprogramme im Sinne dieses Gesetzes sind Programme in jeder Gestalt, einschließlich des Entwurfsmaterials.
(2) Der gewährte Schutz gilt für alle Ausdrucksformen eines Computerprogramms. Ideen und Grundsätze, die einem Element eines Computerprogramms zugrunde liegen, einschließlich der den Schnittstellen zugrundeliegenden Ideen und Grundsätze, sind nicht geschützt.

(3) Computerprogramme werden geschützt, wenn sie individuelle Werke in dem Sinne darstellen, daß sie das Ergebnis der eigenen geistigen Schöpfung ihres Urhebers sind. Zur Bestimmung ihrer Schutzfähigkeit sind keine anderen Kriterien, insbesondere nicht qualitative oder ästhetische, anzuwenden.
(4) Auf Computerprogramme finden die für Sprachwerke geltenden Bestimmungen Anwendung, soweit in diesem Abschnitt nichts anderes bestimmt ist.

§ 69 b [Urheber in Arbeits- und Dienstverhältnissen]

(1) Wird ein Computerprogramm von einem Arbeitnehmer in Wahrnehmung seiner Aufgaben oder nach den Anweisungen seines Arbeitgebers geschaffen, so ist ausschließlich der Arbeitgeber zur Ausübung aller vermögensrechtlichen Befugnisse an dem Computerprogramm berechtigt, sofern nichts anderes vereinbart ist.
(2) Absatz 1 ist auf Dienstverhältnisse entsprechend anzuwenden.

§ 69 c [Zustimmungsbedürftige Handlungen]

Der Rechtsinhaber hat das ausschließliche Recht, folgende Handlungen vorzunehmen oder zu gestatten:
1. die dauerhafte oder vorübergehende Vervielfältigung, ganz oder teilweise, eines Computerprogramms mit jedem Mittel und in jeder Form. Soweit das Laden, Anzeigen, Ablaufen, Übertragen oder Speichern des Computerprogramms eine Vervielfältigung erfordert, bedürfen diese Handlungen der Zustimmung des Rechtsinhabers;
2. die Übersetzung, die Bearbeitung, das Arrangement und andere Umarbeitungen eines Computerprogramms sowie die Vervielfältigung der erzielten Ergebnisse. Die Rechte derjenigen, die das Programm bearbeiten, bleiben unberührt;
3. jede Form der Verbreitung des Originals eines Computerprogramms oder von Vervielfältigungsstücken, einschließlich der Vermietung. Wird ein Vervielfältigungsstück eines Computerprogramms mit Zustimmung des Rechtsinhabers im Gebiet der Europäischen Gemeinschaften oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum im Wege der Veräußerung in Verkehr gebracht, so erschöpft sich das Verbreitungsrecht in bezug auf dieses Vervielfältigungsstück mit Ausnahme des Vermietrechts.

§ 69 d [Ausnahmen von den zustimmungsbedürftigen Handlungen]

(1) Soweit keine besonderen vertraglichen Bestimmungen vorliegen, bedürfen die in § 69 c Nr. 1 und 2 genannten Handlungen nicht der Zustimmung des Rechtsinhabers, wenn sie für eine bestimmungsgemäße Benutzung des Computerprogramms einschließlich der Fehlerberichtigung durch jeden zur Verwendung eines Vervielfältigungsstücks des Programms Berechtigten notwendig sind.
(2) Die Erstellung einer Sicherungskopie durch eine Person, die zur Benutzung des Programms berechtigt ist, darf nicht vertraglich untersagt werden, wenn sie für die Sicherung künftiger Benutzung erforderlich ist.
(3) Der zur Verwendung eines Vervielfältigungsstücks eines Programms Berechtigte kann ohne Zustimmung des Rechtsinhabers das Funktionieren dieses Programms beobachten, untersuchen oder testen, um die einem Programmelement zugrundeliegenden Ideen und Grundsätze zu ermitteln, wenn dies durch Handlungen zum Laden, Anzeigen, Ablaufen, Übertragen oder Speichern des Programms geschieht, zu denen er berechtigt ist.

§ 69 e [Dekompilierung]

(1) Die Zustimmung des Rechtsinhabers ist nicht erforderlich, wenn die Vervielfältigung des Codes oder die Übersetzung der Codeform im Sinne des § 69 c Nr. 1 und 2 unerläßlich ist, um die erforderlichen Informationen zur Herstellung der Interoperabilität eines unabhängig geschaffenen Computerprogramms mit anderen Programmen zu erhalten, sofern folgende Bedingungen erfüllt sind:
1. Die Handlungen werden von dem Lizenznehmer oder von einer anderen zur Verwendung eines Vervielfältigungsstücks des Programms berechtigten Person oder in deren Namen von einer hierzu ermächtigten Person vorgenommen;
2. die für die Herstellung der Interoperabilität notwendigen Informationen sind für die in Nummer 1 genannten Personen noch nicht ohne weiteres zugänglich gemacht;
3. die Handlungen beschränken sich auf die Teile des ursprünglichen Programms, die zur Herstellung der Interoperabilität notwendig sind.
(2) Bei Handlungen nach Absatz 1 gewonnene Informationen dürfen nicht

1. zu anderen Zwecken als zur Herstellung der Interoperabilität des unabhängig geschaffenen Programms verwendet werden,
2. an Dritte weitergegeben werden, es sei denn, daß dies für die Interoperabilität des unabhängig geschaffenen Programms notwendig ist,
3. für die Entwicklung, Herstellung oder Vermarktung eines Programms mit im wesentlichen ähnlicher Ausdrucksform oder für irgendwelche anderen das Urheberrecht verletzenden Handlungen verwendet werden.
(3) Die Absätze 1 und 2 sind so auszulegen, daß ihre Anwendung weder die normale Auswertung des Werkes beeinträchtigt noch die berechtigten Interessen des Rechtsinhabers unzumutbar verletzt.

§ 69 f [Rechtsverletzungen]

(1) Der Rechtsinhaber kann von dem Eigentümer oder Besitzer verlangen, daß alle rechtswidrig hergestellten, verbreiteten oder zur rechtswidrigen Verbreitung bestimmten Vervielfältigungsstücke vernichtet werden. (...)
(2) Absatz 1 ist entsprechend auf Mittel anzuwenden, die allein dazu bestimmt sind, die unerlaubte Beseitigung oder Umgehung technischer Programmschutzmechanismen zu erleichtern.

§ 69 g [Anwendung sonstiger Rechtsvorschriften; Vertragsrecht]

(1) Die Bestimmungen dieses Abschnitts lassen die Anwendung sonstiger Rechtsvorschriften auf Computerprogramme, insbesondere über den Schutz von Erfindungen, Topographien von Halbleitererzeugnissen, Marken und den Schutz gegen unlauteren Wettbewerb einschließlich des Schutzes von Geschäfts- und Betriebsgeheimnissen, sowie schuldrechtliche Vereinbarungen unberührt.
(2) Vertragliche Bestimmungen, die in Widerspruch zu § 69 d Abs. 2 und 3 und § 69 e stehen, sind nichtig.

§ 106 [Unerlaubte Verwertung urheberrechtlich geschützter Werke]

(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.

UWG

§ 17 [Verrat von Geschäfts- oder Betriebsgeheimnissen]

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer als Angestellter, Arbeiter oder Lehrling eines Geschäftsbetriebs ein Geschäfts- oder Betriebsgeheimnis, das ihm vermöge des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen, mitteilt.
(2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen,
1. sich ein Geschäfts- oder Betriebsgeheimnis durch
a) Anwendung technischer Mittel,
b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder
c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist,
unbefugt verschafft oder sichert oder
2. ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten Mitteilungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt.
(3) Der Versuch ist strafbar.

Das Teledienstegesetz

§ 1 [Zweck des Gesetzes]

Zweck des Gesetzes ist es, einheitliche wirtschaftliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste zu schaffen.

§ 2 [Geltungsbereich]

(1) Die nachfolgenden Vorschriften gelten für alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt (Teledienste).
(2) Teledienste im Sinne von Absatz 1 sind insbesondere
1. Angebote im Bereich der Individualkommunikation (zum Beispiel Telebanking, Datenaustausch),
2. Angebote zur Information oder Kommunikation, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht (Datendienste, zum Beispiel Verkehrs-, Wetter-, Umwelt- und Börsendaten, Verbreitung von Informationen über Waren und Dienstleistungsangebote),
3. Angebote zur Nutzung des Internets oder weiterer Netze,
4. Angebote zur Nutzung von Telespielen,
5. Angebote von Waren und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit.
(3) Absatz 1 gilt unabhängig davon, ob die Nutzung der Teledienste ganz oder teilweise unentgeltlich oder gegen Entgelt möglich ist.
(4) Dieses Gesetz gilt nicht für
1. Telekommunikationsdienstleistungen und das geschäftsmäßige Erbringen von Telekommunikationsdiensten nach § 3 des Telekommunikationsgesetzes vom 25. Juli 1996 (BGBl. I S. 1120),
2. Rundfunk im Sinne des § 2 des Rundfunkstaatsvertrages,
3. inhaltliche Angebote bei Verteilerdiensten und Abrufdiensten, soweit die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht, nach § 2 des Mediendienste-Staatsvertrages in der Fassung vom 20. Januar bis 7. Januar 1997.
(5) Presserechtliche Vorschriften bleiben unberührt.

§ 3 [Begriffsbestimmungen]

Im Sinne dieses Gesetzes sind
1. "Diensteanbieter" natürliche oder juristische Personen oder Personenvereinigungen, die eigene oder fremde Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln,
2. "Nutzer" natürliche oder juristische Personen oder Personenvereinigungen, die Teledienste nachfragen.

§ 4 [Zugangsfreiheit]

Teledienste sind im Rahmen der Gesetze zulassungs- und anmeldefrei.

§ 5 [Verantwortlichkeit]
(1) Diensteanbieter sind für eigene Inhalte, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.
(2) Diensteanbieter sind für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann verantwortlich, wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern.
(3) Diensteanbieter sind für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, nicht verantwortlich. Eine automatische und kurzzeitige Vorhaltung fremder Inhalte aufgrund Nutzerabfrage gilt als Zugangsvermittlung.
(4) Verpflichtungen zur Sperrung der Nutzung rechtswidriger Inhalte nach den allgemeinen Gesetzen bleiben unberührt, wenn der Diensteanbieter unter Wahrung des Fernmeldegeheimnisses gemäß § 85 des Telekommunikationsgesetzes von diesen Inhalten Kenntnis erlangt und eine Sperrung technisch möglich und zumutbar ist.

§ 6 [Anbieterkennzeichnung]

Diensteanbieter haben für ihre geschäftsmäßigen Angebote anzugeben
1. Namen und Anschrift sowie
2. bei Personenvereinigungen und -gruppen auch Namen und Anschrift des Vertretungsberechtigten.

Einteilung der Risiken

Es zeigt sich, viele IT-Schäden sind

- nicht unmittelbar,
- meist schwer zu beziffern, weil immateriell
- oder insgesamt nur schwer nachweisbar.

Die Kriterien *vorsätzlich*, *unerlaubt* und *Bereicherungsabsicht* liegen trotz erheblicher Schäden oft nicht vor oder sind nicht direkt nachweisbar.

1. Unberechtigte Verwendung

Beispiele:
Nutzung von betriebseigenen Ressourcen für private Zwecke (Ausdruck eines Mailings für den Kegelclub). -> Einzelner Schadensnachweis
Nutzung kostenpflichtiger Internetangebote auf Firmenkosten (Sex-Angebote während der Arbeitszeit).
Buchung von Privatreisen auf Firmenkonditionen oder -kosten.

2. Ausspähen von Daten und Zugangscodes

Beispiele:
Kopieren von speziellen Fertigungs- oder Verwaltungsverfahren.
Verrat von Angebotsbedingungen an einen anderen Anbieter.
Beschaffen von börsenrelevanten Informationen (Insiderwissen).
Plünderung des Firmenkontos (Passwort gestohlen).
Erpressung auf Basis erworbener Kenntnisse.

3. Stehlen von Daten

Beispiele:
Entwenden von Programmen für den eigenen Bedarf (lizenzrechtliche Konsequenzen)
Mitnehmen der Kundendatenbank für die eigene Selbstständigkeit.
Missbrauch, Kopie des Geschäftsbriefkopfs oder Firmenlogos zum Vorspiegeln falscher Voraussetzungen (ev. Rufschädigung).

4. Verändern von Daten

Beispiele:
Bilanzfälschung zur Täuschung des Rechnungsprüfers oder Aufsichtsrats.
Zugriff auf eigene Abrechnungs- oder Zeiterfassungsdaten
(Akkord, Bonussystem, Stundenlöhne).
Fälschen der Lagerpapiere, um Diebstahl zu vertuschen.
Löschen oder Verschwindenlassen von selbst verschuldeten Reklamationsvorgängen.
Schädigen von anderen Mitarbeitern durch Einbau von Fehlern
(Konkurrenzverhalten, Mobbing).
Einbringen von Malware (Viren, Trojaner, Bomben, Würmer) als Schädigung zugunsten eines Mitbewerbers am Markt.
Mitarbeiter bringt Malware beim Kunden ein. (Haftpflicht?)

5. Hardware Diebstahl

Beispiel
Anfang 1994 stellten Mitarbeiter einer deutschen Großbank über Wochen hinweg immer wieder morgens fest, dass aus ihren Workstations Speicherbausteine oder ganze Platinen entnommen worden waren. Ein Fremdmitarbeiter hatte Komplizen mit Schlüsseln versorgt und die Diebstähle in Auftrag gegeben.
In einem großen Werk für PC-Fertigung in Augsburg organisierten einige Mitarbeiter einen schwungvollen Handel mit Festplatten, die direkt aus dem Lager entwendet waren.
In einer Unternehmensberatungsfirma wurde der Notebook des Systemadministrators aus den gesicherten Firmenräumen gestohlen. Auf dem Notebook befand sich die komplette Datenbank des

Unternehmens in komprimierter Form, da der Administrator einige Performancetests durchführen wollte.

6. Hardware-Sabotage

Beispiele:
Eine Rechenanlage wird bewusst beschädigt. Motive: Rache, Geltungsbedürfnis, etc.
Brandstiftung. (verheerende Schäden, auch durch Löschwasser und Rauch)
Sprengstoffanschlag.

Fallbeispiele

Auch die folgende Geschichte stammt aus dem noch unveröffentlichten Buch von Howard Fuhs.

Der Trojanische Server

[Es folgt die Geschichte von dem weltweit operierenden deutschen Großunternehmen. Am Muttersitz des Unternehmens befinden sich ca. 15000 PCs in einem Netz zusammen mit Servern und UNIX-Workstations bis hin zu Main Frames. Es wurde eine Geisterabteilung mit einem Server entdeckt, der über RAS (Remote Access) von fremder Hand gesteuert war.]

Sicherheitstechnische Bewertung

Mit am schlimmsten an diesem geschilderten Fall wiegt die Tatsache, dass wichtige Ermittlungsmöglichkeiten nicht ausgeschöpft wurden, wie z.B. Fangschaltung und Beobachtung des Eindringlings im Computernetzwerk. Dadurch ist über den Eindringling und seine Interessen nichts weiter bekannt. Der entstandene Schaden für das Unternehmen ist nicht quantifizierbar, da es nicht zu ermitteln war auf welche Daten der Eindringling in einem Zeitraum von zwei Jahren Zugriff hatte und wo diese Daten später eventuell gelandet sind (Mitbewerber).

Da der Eindringling auf vielen Systemen über den gesamten Zeitraum hinweg Administratorrechte hatte, war es nicht möglich herauszufinden ob er sich selbst eventuell noch weiter Anwenderaccounts eingerichtet hat. Berücksichtigt man die Größe der EDV und die Anzahl der legitimen Anwender die im Netzwerk arbeiten war es nicht möglich jeden Account auf seine Plausibilität hin zu überprüfen. Es wurde ein Script implementiert welches einfach alle Accounts, die 4 Wochen lang nicht genutzt wurden widerruft. Darüber hinaus führte man eine neue Anwenderauthentifizierung ein womit binnen 6 Monaten alle Anwender neue Accounts bekamen. Die übriggebliebenen Accounts wurden gelöscht.

Um das Problem mit den Vertrauensketten in den Griff zu bekommen, entschied man sich für eine teilweise Neuorganisation des Netzwerkes und der Überprüfung aller Zugriffsrechte der Server untereinander. Bei einem ersten Audit stellte sich heraus, das fast jeder Server in eine Vertrauenskette eingebunden war, die in dieser Form nicht hätte bestehen dürfen.

Für diesen Worst Case der Wirtschaftspionage existierten keinerlei dokumentierte Prozeduren nach denen verfahren werden konnte. Dies führte zu unnötiger Suche nach zuständigen Ansprechpartnern die von dieser Situation ebenfalls überfordert waren. Das Resultat waren der Verlust von wertvoller Zeit, sowie das nicht zur Verfügung stehen von Ressourcen die zur Aufklärung der Vorgänge erheblich beigetragen hätten.

Soweit dieses Fallbeispiel.

Anhang: Quelle Kriminalstatistik

Die am 22.05.01 vorgestellte polizeiliche Kriminalstatistik für das Jahr 2000 weist eine erhebliche Steigerung im Bereich der IT-Wirtschaftskriminalität auf. Betrug bei Kreditkartenumsätzen und beim EC-Lastschriftverkehr stieg um 54 %, Betrug an Geldausgabe- und Kassenautomaten um 21 %.

Deshalb sollen sich die Strafverfolgungsbehörden verstärkt auf die Risikopotenziale der neuen Techniken einstellen, so das Bundesinnenministerium.

2000 wurden 56.684 Fälle (1999: 45.359 Fälle) von Computerkriminalität erfasst. Damit gab es einen starken Anstieg um 25,0 % (1999: -1,5 %). Über vier Fünftel der Fälle, nämlich 44.284 (1999: 36.613), entfielen auf Betrug mittels rechtswidrig erlangter Karten für Geldausgabe- bzw. Kassenautomaten. Auf den eigentlichen Computerbetrug (§ 263a StGB) entfielen 6.600 Fälle (1999: 4.474 Fälle), 268 Fälle (1999: 124 Fälle) auf Fälschung beweiserheblicher Daten oder Täuschung im Rechtsverkehr bei Datenverarbeitung, 513 Fälle (1999: 302 Fälle) auf Datenveränderung oder Computersabotage, 538 Fälle (1999: 210 Fälle) auf Ausspähen von Daten, 2.298 Fälle (1999: 2.224 Fälle) auf Computer-Software-Piraterie und 2.198 Fälle (1999: 1.412 Fälle) auf Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten.

Bürger und Banken sollten wachsamer sein, um den modernen Zahlungsverkehr nicht zum Risiko werden zu lassen, mahnt das Ministerium. Deshalb sei man mit der Wirtschaft und dem Kreditgewerbe im Gespräch, um den Einsatz von Chiptechnologie anstelle des kriminalitätsanfälligen Magnetsstreifens voranzutreiben.

Beim Betrug mittels rechtswidrig erlangter Zahlungskarten (Kreditkartenumsätze und EC-Karten im Lastschriftverfahren) gab es einen auffälligen Anstieg um 54,0 % (1999: + 40,4 %) auf 55.747 Fälle. Eine beachtliche Zunahme gab es mit 44.284 Fällen und damit einem Anstieg um 21,0 % auch beim Betrug mittels rechtswidrig erlangter Karten an Geldausgabe- bzw. Kassenautomaten (Kunden-, Service- und EC-Karten mit PIN). Das BMWi erwartet bei der fortschreitenden Technisierung (z.B. elektronische Geldbörse) und Expansion des Einsatzes neuer Technologien durch Straftäter, dass dieses Deliktsfeld in den nächsten Jahren weiter an Bedeutung gewinnen wird.

Die polizeiliche Kriminalstatistik (PKS) erfasst die der Polizei bekannt gewordenen Straftaten einschließlich der mit Strafe bedrohten Versuche. Im Jahr 2000 ist die Gesamtzahl der insgesamt polizeilich erfassten Straftaten im Vergleich zum Vorjahr um 0,6 % auf 6.264.723 Straftaten zurückgegangen und hat damit den niedrigsten Stand seit 1993 erreicht (1999: 6.302.316, 1998: 6.456.996, 1997: 6.586.165, 1996: 6.647.598, 1995: 6.668.717