Arbeitspapier / Abteilung Wirtschaft

Georg Disterer

Gezielte Angriffe auf betriebliche Informationssysteme:

Typologien von Motiven und Tätern

Arbeitspapier 07-2009
ISSN Nr. 1436-1035 (print) ISSN Nr. 1436-1507 (Internet)

Gezielte Angriffe auf betriebliche IT-Systeme: Typologien von Motiven und Tätern

Georg Disterer

1	Einleitung	1
1.1	Entdeckung und Ermittlung bei Angriffen	3
1.2	Verfolgung und juristische Bewertung	4
1.3	Schutzziele und Sicherungsmaßnahmen	5
2	Angriffsmotive	8
2.1	Habgier	9
2.2	Ausweglosigkeit	11
2.3	Neugier	11
2.4	Ehrgeiz und Geltungsdrang	12
2.5	Spionage	12
2.6	Sabotage	14
2.7	Rache und Vergeltung	15
2.8	Neid	16
2.9	Vandalismus	16
2.10	Ergänzungen	17
3	Täter und Tätergruppen	19
4	Verbreitete Angriffsarten	21
5	Ausblick	25
Literatur		26

1 Einleitung

Schon lange müssen Betreiber von IT-Systemen damit rechnen, dass die Systeme angegriffen und in der Folge unbefugt und missbräuchlich genutzt werden. Frühe Fälle sind etwa für das Jahr 1961 verzeichnet, als am MIT das Abrechnungsverfahren des Großrechners durch spezielle Programme unterlaufen wurde und die Programmierer so Rechnerkapazitäten nutzen konnten, ohne die Kosten dafür tragen zu müssen[1]. Derartige Hacker (i.S.v. „Einbrecher“), die damals auch Kontrollen der Telefonsysteme ausschalteten und dadurch unentgeltlich telefonierten, lösten in der Öffentlichkeit durchaus positive Assoziationen aus, da sie als übermächtig wahrgenommene Konzerne und Mo-

1 Vgl. Cross (2008) S. 44.

nopole mit technischem Geschick ausmanövrierten. In Spielfilmen der 70er und 80er Jahre wurden Hacker stilisiert und als Vertreter des Widerstands gegen das Establishment dargestellt.

Allerdings sind auch schon seit den 60er Jahren Vermögensschäden durch Manipulationen an IT-Systemen bekannt, mit denen Gehalts- oder Rechnungszahlungen umgeleitet oder Kontostände verändert wurden[2]. Die ersten Schadprogramme, die sich über Übertragungsnetze fortpflanzen und IT-Systeme außer Funktion setzten - so genannte „Würmer“ – werden für das Jahr 1988 notiert[3].

Missbrauch von IT-Systemen ist somit als Begleiterscheinung anzusehen, die nur schwer vermeidbar ist, solange Angreifer zwischen dem erzielbaren Eigennutz und dem notwendigen Aufwand sowie dem Risiko der Entdeckung bzw. Bestrafung abwägen und zum Ergebnis kommen, dass ihr Handeln lohnenswert erscheint. Unter dem Begriff >> Angriff << (engl.: attacks) fallen alle vorsätzlichen Handlungen mit dem dezidierten Ziel, die IT-Systeme eines Unternehmens zu zerstören, zu schädigen oder zu missbrauchen. Die Konzentration auf Angriffe als **vorsätzliche und gezielte Handlungen** schließt zwei Kategorien bedrohlicher Einflussnahmen auf IT-Systeme aus der Diskussion aus: Irrtümliche Handlungen (etwa Handhabungs- oder Bedienungsfehler, aus Unkenntnis oder Unfähigkeit oder aufgrund von Fehleinschätzung) oder versehentliche Handlungen (etwa Handhabungs- oder Bedienungsfehler aus Unachtsamkeit oder Nachlässigkeit). Zudem sind weitere Bedrohungen (engl.: threads) und resultierende Schäden aus der Diskussion ausgeschlossen: Missbräuchliche Nutzung von IT-Systemen können für Unternehmen erhebliche Risiken bergen, wenn Störungen der betrieblichen Abläufe und der Ausfall von IT-Systemen resultieren. Beispielsweise gehen aktuell bei Unternehmen so viele unerwünschte Emails (SPAM) ein, dass deren Identifikation und Bearbeitung bestenfalls Kosten verursachen, schlimmstenfalls zum Ausfall der Email-Server führen[4]. Da der überwiegende Anteil dieser Mails der Produktwerbung dient, werden SPAM-Mails hier nicht unter der Rubrik „Angriff“ diskutiert, da bei ihnen das Ziel der dedizierten Zerstörung (bzw. der Schädigung oder des Missbrauchs) der IT-Systeme (hier: Email-Server) der betroffenen Unternehmen nicht im Vordergrund steht.

2 Vgl. Dannecker (1996) S. 1288.
3 Vgl. Mohay/Anderson/Collie/Vel/McKemmish (2003) S. xiii, Cross (2008) S. 51.
4 Angaben zum Anteil unerwünschter Mails schwanken: Lediglich 13 bis 15 % aller eingehender Mails werden als „erwünscht“ angesehen, vgl. MAAWG (2008) S. 2, für die deutsche Bundesverwaltung wird ein Anteil von 1,5% erwünschter Mails angenommen, vgl. Bundesamt für Sicherheit in der Informationstechnik (2009) S. 24.

Weitere essentielle Bedrohungen der IT-Systeme, die nicht unter den Begriff Angriff fallen, sind höhere Gewalt (z.B. Naturereignisse und -katastrophen wie Hochwasser, Blitz, Erdbeben), kriegerische Handlungen, technische Mängel und technisches Versagen (wg. Materialermüdung, Materialfehler, Qualitätsmängel oder Verschleiß und Alterung von Komponenten), Funktionsmängel (z.B. durch Entwicklungs- oder Produktionsfehler), organisatorische Mängel (mangelnde Zuständigkeiten und Kompetenzen, inkonsistente Vertreterregelungen, unzureichende Kontrollen, fehlende Ressourcen für Schutzmaßnahmen) oder Handhabungs- oder Bedienungsfehler. Zu diesen Bedrohungen gibt es klassische Gegenmittel wie redundante Auslegung technischer Systeme (z.B. Prozessoren und Speicherplatten), zusätzliche dezidierte Geräte (z.B. Notstromaggregate), Weiterbildung/Schulung/Training oder organisatorische oder technische Kontrollen.

1.1 Entdeckung und Ermittlung bei Angriffen

Technische Grundlagen für Angriffe und Ursachen für Probleme bei der Ermittlung von Angreifern liefern Schwächen im Entwurf und der Implementierung von betrieblichen Informationssystemen und sowie der Standards und Protokolle (z.B. TCP/IP für das Internet), auf denen sie basieren. So ist im Internet durch Fälschung oder Verschleierung von Adressangaben eine anonyme Kommunikation möglich. Die Inhalte der Kommunikation können verschlüsselt werden, so dass Angegriffene oder Überwachungs- oder Verfolgungsbehörden keine Möglichkeiten haben, auf Gefahren aufmerksam zu werden und auf die Verursacher zu schließen. Die große Anzahl von Rechnern, die an das Internet angeschlossen sind, schafft viele Möglichkeiten des Zugangs und des Angriffes anderer Rechner, die in weiter Ferne lokalisiert sein können („remote Zugriff“). Auch die relativ geringe Sensibilität vieler Benutzer des Webs - abzulesen am bedenkenlosen Nutzen etwa beim Herunterladen von Software o.ä. oder dem unbedachten Umgang mit Passworten – erzeugt Sicherheitslücken und erleichtert Angreifern ihr Werk.

Die Aufdeckung und Ermittlung bei Angriffen ist zudem durch die dafür notwendigen technischen Kenntnisse und Ausrüstungen erschwert, die den Verfolgungsbehörden oft nicht im ausreichenden Maß zur Verfügung stehen. Wenn Angreifer über Ländergrenzen hinweg tätig sind, wird zudem eine internationale Zusammenarbeit notwendig, die auch durch unterschiedliche nationale Gesetzgebungen erschwert wird.

Auch stehen von der Gesellschaft geforderte Freiheitsrechte und Interessen der Verfolgungsbehörden oft im Widerspruch zueinander, wie an der Diskussion um die Vorratsdatenspeicherung beispielhaft abzulesen ist. Das Grundrecht der Benutzer auf informa-

tionelle Selbstbestimmung kann im Internet wirksam nur durch die Anonymität der Nutzung gewährleistet werden, demgegenüber stehen die Interessen der Strafverfolgungsbehörden nach angemessenen und wirksamen Ermittlungs- und Verfolgungsmöglichkeiten. Das entsprechende Gesetz trat in Deutschland zum 1.1.2008 in Kraft und schreibt Anbietern von Telediensten die Speicherung von Verbindungsdaten für eine gewisse Zeit vor, damit Ermittlungs- und Verfolgungsbehörden ggf. davon Gebrauch machen können. Demgegenüber wird argumentiert, die Vorratsdatenspeicherung verstoße gegen das Recht der informationellen Selbstbestimmung der Benutzer sowie gegen das Brief-, Post- und Fernmeldegeheimnis.

1.2 Verfolgung und juristische Bewertung

Eine Verfolgung von Angreifern durch staatliche Stellen wie Staatsanwaltschaft und Polizei kommt nur in Frage, wenn die Angriffe durch einschlägige Gesetze erfasst sind. Dabei wird der Begriff Computerkriminalität (engl.: computer crime) inhaltlich verschieden gefasst. Unter „Computerkriminalität im engeren Sinne“ werden Angriffe gefasst, bei denen IT-Systeme in den Tatbestandsmerkmalen enthalten sind, z.B. der Betrug mit rechtswidrig erlangten Debitkarten (und PIN) oder mit rechtswidrig erlangten Zugangsberechtigungen zu IT-Systemen, Fälschung beweiserheblicher Daten, Computersabotage, Ausspähen und Abfangen von Daten und Softwarepiraterie.[5]

Unter „Computerkriminalität im weiteren Sinne“ wird gefasst, wenn IT-Systeme als Tatmittel zur Planung, Vorbereitung oder Ausführung von Taten eingesetzt werden, die von traditionellen Rechtsnormen erfasst sind, z.B. die Verbreitung inkriminierter Inhalte, Kettenbriefe, das Angebot von Hehlerware und unerlaubten Glücksspiels, die Aufforderung zu Straftaten, die Abwicklung von Rauschgiftgeschäften, der Handel mit Menschen oder Waffen, Betrugsdelikte in Zusammenhang mit Online-Shops (etwa: Anbieter erhält Zahlung per Vorkasse und liefert nicht oder nicht adäquat; oder: Nachfrager erschleicht sich Lieferung unter falscher Identität) oder Verletzungen des Urheberrechts.[6]

Zur Legitimierung der Strafbewährung mancher Angriffsformen auf IT-Systeme musste der Gesetzgeber dezidiert tätig werden, da Strafbarkeitslücken bestanden. So setzt § 263 StGB für den Betrugstatbestand vor, dass ein eigennütziger Vermögensvorteil bzw. die Schädigung des Vermögens eines anderen durch die Erregung eines Irrtums erzielt wird. Jedoch wird z.B. bei einem Angriff auf ein IT-System zur Manipulation von Kon-

5 Vgl. LKA Wiesbaden (2008) S. 9-10, Cross (2008) S. 11, [Vgl. Dannecker (1996) S. 1285 f].

tendaten keine Person getäuscht[7], so dass kein Irrtum vorliegt; die Alltagsweisheit „Irren ist menschlich“ kann hier also in der Funktion einer Begriffsbestimmung verstanden werden. Entsprechend wurde 1986 im Zuge des zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität (WiKG) der neue § 263a zum Computerbetrug ins Strafgesetzbuch eingefügt, der im Gesetzestext ausdrücklich als Betrug ansieht, wenn zur Erlangung eines rechtswidrigen Vermögensvorteils 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.

Entsprechend sind die klassischen Straftatbestände ergänzt worden, um neue Formen der Kriminalität in Zusammenhang mit Computern dezidiert zu erfassen, wie z.B. in Zusammenhang mit Angriffen auf IT-Systemen

- § 263a StGB Computerbetrug
- § 202a StGB Ausspähen von Daten
- § 202b StGB Abfangen von Daten
- § 303a StGB Datenveränderung
- § 303b StGB Computersabotage.

Daneben ist bei einer juristischen Bewertung eine Reihe weiterer Gesetze und Vorschriften zu beachten, z.B. Gesetze zum Datenschutz wie das Bundesdatenschutzgesetz (BDSG) sowie bereichsspezifische Regelungen wie für die Telekommunikation das Telekommunikationsgesetz (TKG), das Informations- und Kommunikationsdienstegesetz (IuKDG), dabei insbesondere das Teledienstedatenschutzgesetz (TDDSG).

1.3 Schutzziele und Sicherungsmaßnahmen

Die betriebliche Informationsverarbeitung unterliegt wirtschaftlichen, legalen, ethischen u.a. Ansprüchen und Auflagen. Um die Erfüllung zu gewährleisten ist es notwendig, entsprechende Qualitätseigenschaften von IT-Systemen zu bestimmen und diese Qualitäten vor bedrohlichen Umständen zu schützen. Die Ansprüche und Auflagen sind im Grundsatz weitestgehend unabhängig vom Einsatz von IT-Systemen, sondern eher generell und (auch) tradiert. Die besonderen Potentiale von IT-Systemen erfordern jedoch

---

6 Vgl. LKA Wiesbaden (2008) S. 9-10, Cross (2008) S. 11, [Vgl. Dannecker (1996) S. 1285 f]
7 Vgl. Dannecker (1996) S. 1288.

eine dezidierte Formulierung, spezielle Methoden der Risikobestimmung und -abschätzung und besondere Schutzmaßnahmen.

Primär sind folgende zentrale Qualitätseigenschaften betrieblicher IT-Systemen[8] durch Angriffe gefährdet – und damit bei der Ermittlung des Schutzbedarfs eines Unternehmen und bei der geeigneter Entwicklung Schutzmaßnahmen zuvorderst zu beachten:

Verfügbarkeit des Systems: Das System gewährleistet die unbeeinträchtigte Nutzung im Rahmen der Berechtigung der Benutzer, d.h. Störungen, Wartezeiten o.ä. Erschwernisse sollten nicht vorkommen.

Integrität des Systems: Das System gewährleistet, dass Daten nicht unberechtigt und unbemerkt manipuliert werden können; die Gewährleistung umfasst die Autorisierung und Authentizität der Benutzer sowie die Zurechenbarkeit von Zugriffen.

Vertraulichkeit des Systems: Das System gewährleistet, dass keine unberechtigte Informationsgewinnung möglich ist. Im Bereich des Ecommerce umfasst dies z.B. die Wahrung der Anonymität der Benutzer, sodass etwa keine Bewegungs-, Kommunikations- oder Zugriffsprofile unberechtigt und unbemerkt erstellt werden können.

Nachgeordnete Qualitätseigenschaften – vor allem im Zusammenhang mit der Forderung nach Integrität des Systems – sind die Authentizität und die Verbindlichkeit der IT-Systeme.

Authentizität des Systems: Das System gewährleistet für Daten, für die Autorisierungen (Berechtigungen) notwendig sind, das Benutzer vor Zugriffen eindeutig identifiziert werden und die Identifikation verifiziert wird. Zur Verifikation müssen Kennzeichen herangezogen werden, deren Echtheit überprüfbar oder deren Glaubwürdigkeit hinreichend ist (z.B. Passwort, biometrische Merkmale …).

Verbindlichkeit (Zurechenbarkeit) des Systems: Das System gewährleistet für Daten und Funktionen, für die das notwendig ist[9], das alle Zugriffe nachträglich eindeutig dem jeweiligen Benutzer zuordenbar sind. Damit kann der Benutzer den Zugriff nachträglich nicht abstreiten[10].

---

8 So bei: Bursch (2005) S. 19, Mohay/Anderson/Collie/Vel/McKemmish (2003) S. 35, Eschweiler/Psille (2006) S. 29-31, Eckert (2001) S. 9.

9 Für viele gängige Daten und Funktionen ist die Verbindlichkeit der Systeme nicht notwendig, z.B. für öffentliche Auskunftssysteme wie Telefonbuch, Fahrplan etc. Für manche Daten und Funktionen kann die Verbindlichkeit eines Systems auch zwingend eingeschränkt werden müssen, etwa wenn zur Wahrung des Datenschutzes Zugriffe nicht protokolliert werden dürfen.

10 Authentizität ist Voraussetzung für Verbindlichkeit.

Die Schutzziele sind durch unterschiedliche Angriffe auf verschiedene Weise gefährdet:

- Wenn Endgeräte eines IT-Systems gestohlen oder zerstört sind, dann ist die Verfügbarkeit gefährdet, da ein regulärer Benutzer dadurch gehindert werden kann, auf das System zuzugreifen.

  Die Verfügbarkeit wird ebenso gefährdet, wenn Verarbeitungs- oder Übertragungskapazitäten eines Systems durch gezielte Angriffe so stark belastet werden, dass für reguläre Benutzer ausreichende Kapazitäten nicht zur Verfügung stehen.

- Wenn der Zugriffsschutz eines IT-Systems umgangen oder überwunden werden kann, dann ist die Integrität gefährdet, da dann Änderungen an den Daten vorgenommen werden können – etwa zur Umleitung von Geld- oder Güterströmen.

  Die Integrität wird ebenso gefährdet, wenn Informationen beim Austausch zwischen IT-Systemen unbemerkt manipuliert werden können, z.B. indem Angaben zu Bankkonten o.ä. geändert werden.

- Wenn ein Dritter unbefugt die elektronische Abwicklung von Geschäften - z.B. den Kauf von Aktien – „belauschen“ kann, dann ist die die Vertraulichkeit gefährdet.

  Die Vertraulichkeit wird ebenso gefährdet, wenn die Eingabe von Authentisierungsdaten durch berechtigte Benutzer (z.B. Benutzername, Passwort) von anderen beobachtet oder aufgezeichnet werden kann, da mit den gewonnenen Informationen Missbrauch betrieben werden kann.

- Wenn der Sender einer Nachricht eine falsche Identität vorgeben kann, dann ist die Authentizität des IT-Systems gefährdet, etwa wenn in Emails ein falscher Absender vorgetäuscht wird.

  Die Authentizität ist ebenso gefährdet, wenn Benutzer ein System mit den Authentisierungsdaten anderer Personen (z.B. Benutzername, Passwort) nutzen können.

- Wenn Benutzer, die mit einem IT-System Änderungen an Informationen vornehmen, diese Änderungen später abstreiten können, dann ist die Verbindlichkeit des Systems gefährdet.

  Die Verbindlichkeit ist ebenso gefährdet, wenn Änderungen an Informationen so vorgenommen werden können, dass sie nachträglich nicht den Verursachern zugeordnet werden können.

Die Sicherungsmaßnahmen müssen verschiedene Ansätze aufgreifen: vorsorglich (präventiv) und reaktiv, technisch und organisatorisch, kontrollierend und agierend. Für den Entwurf und die Umsetzung entsprechender Maßnahmen liegen einige umfangreiche Anleitungen und Referenzmodelle vor, z.B.:

- Grundschutzhandbuch … vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellt und weiterentwickelt
- ITSEC Information Technology Security Evaluation Criteria … von einigen europäischen Ländern aufgestellt
- ISO/IEC TR 13335-1: Guidelines for the management of IT Security … als internationale Norm
- ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements … als internationaler Standard für ein IT-Sicherheitsmanagementsystem
- ISO/IEC 27002 (bis Mitte 2007: ISO/IEC 17799) … als internationaler Standard mit Vorschlägen für Sicherheitskontrollen

Die Notwendigkeit für Unternehmen, ausreichende Sicherheitsmaßnahmen zu etablieren, wird nicht nur durch das Eigeninteresse der Beteiligten wie Eigentümer, Kunden, Lieferanten u.ä. bestimmt, sondern auch durch verschiedene gesetzliche Pflichten. So sind etwa Zugriffs- und Zugangskontrollen für IT-Systeme mit rechnungslegungsrelevanten Daten durch die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) vorgeschrieben, die vom Finanzministerium zur Erläuterung von Handelsgesetzbuch und Abgabenordung aufgestellt sind und der Sicherstellung der Ordnungsmäßigkeit, Vollständigkeit und Richtigkeit der Rechnungslegung dienen. Daten von Kunden und Lieferanten unterliegen den Datenschutzbestimmungen. Viele Branchen sind darüber hinaus von spezifischen Gesetzen betroffen, so etwa Banken, für die laut § 25a Abs. 1 KWG (Kreditwesengesetz; in der Fassung vom 1.11.2007) ausdrücklich gilt: „Ein Institut muss … über angemessene Sicherheitsvorkehrungen für den Einsatz der elektronischen Datenverarbeitung verfügen …“.

2 Angriffsmotive

Generell gleichen die Motive von Angreifern auf Systeme der betrieblichen Informationsverarbeitung jenen von klassischen Tätern. Im Folgenden sind mögliche Motive sowie Merkmalsbeschreibungen und Beispiele aufgeführt[11].

11 Vgl. auch Eschweiler/Psille (2006) S. 49-55, Geschonneck (2004) S. 14-20.

2.1 Habgier

Hierzu gehören der Diebstahl sowohl materieller (beispielsweise Geräte) als auch immaterieller Güter (beispielsweise Daten), die gewinnbringend genutzt werden, Ressourcen wie Verarbeitung-, Übertragungs- und Speicherungskapazitäten sowie Software, die unbefugt und eigennützig genutzt werden. Das grundsätzliche Vorgehen ähnelt dem bei einem klassischem Diebstahl oder Betrug und ist geprägt vom Streben des Angreifers nach persönlichem materiellem Vorteil. Das Erkennen eines solchen Angriffs ist schwierig, da bei immateriellen Gütern wie Daten und Software die Aneignung durch Kopieren möglich ist, ohne das Original zu verändern. Beispiele:

- Folgendes Geschehen hat im Jahr 2008 große Aufmerksamkeit erregt[12]: Der externe IT-Mitarbeiter einer Bank in Liechtenstein kopiert im Jahr 2002 unrechtmäßig Kundendaten und schleust sie auf Datenträger aus dem Unternehmen. Nach dem Ende seiner Tätigkeit erpresst er seinen ehemaligen Auftraggeber mit der Drohung, die Daten weiterzugeben. Die Erpressung scheitert, der Ex-Mitarbeiter wird verhaftet und verurteilt, muss die Strafe jedoch nicht verbüßen. Er wendet sich daraufhin an den deutschen Nachrichtendienst und bietet der Daten an, da sie Indizien für Strafverfolgungsmaßnahmen wegen Steuerhinterziehung gegen einige der Bankkunden liefern. Er erhält ca. 4 Mio. Euro und eine neue Identität. Der US-Senat führt eine Untersuchung durch, um zu klären, ob und in welchem Maß US-Bürgern, deren Daten sich auch auf den Datenträgern befinden, von der Bank Beihilfe zur Steuerhinterziehung geleistet wurde. Die Bank muss Schadensersatzklagen fürchten, da sie betroffene Kunden nicht von dem Diebstahl ihrer Daten unterrichtet hat. Das zuständige Gericht muss ggf. die Bank verurteilen, die sich im Besitz der Regierungsfamilie des Landes befindet. Die Bank erleidet Vertrauensschaden bei ihren Kunden und Imageschaden in der Öffentlichkeit.
- Ein IT-Dienstleistungsunternehmen in USA wickelt Transaktionen ab von 220 Institutionen, die Kreditkarten ausgeben, und deren rund 100 Millionen Kreditkarteninhabern. Bei einem Angriff werden Transaktionsdaten »mitgelesen« und ermöglichen den Angreifern u.a., Einkäufe zulasten der fremden Kreditkarten in Kaufhäusern durchzuführen[13].

12 Vgl. Ramelsberger (2008), Richter (2008), Ritzer (2008a), Ritzer (2008b), Nitschmann/Leyendecker (2008).
13 Vgl. Gold (2009), Krebs (2009a).

- Ein Mann erlangt über ein externes Terminal unberechtigten Zugang zum System für Kontoführungen und Zahlungsabwicklungen der Citibank und löst 40 Überweisungen von Kundenkonten auf sein eigenes Konto aus[14].
- Mehrere Männer in Thailand und Indien greifen die IT-Systeme von Online-Brokern in USA an und verschaffen sich Zugang zu Kundenkonten, in deren Namen sie dann Transaktionen durchführen. Ablauf: Die Angreifer kaufen auf eigenen Namen und eigene Rechnung Wertpapiere und treiben dann deren Wert mit Käufen im Namen der »gekaperten« Kunden hoch, um anschließend die eigenen Wertpapiere mit Gewinn zu verkaufen[15].
- Eine Mitarbeiterin der NASA korrespondiert von ihrem Arbeitsplatz privat über eine Dating-Seite im Web mit einem Mann aus Nigeria. Eine Mail von ihm enthält im Anhang ein Schadprogramm (»Spyware«), das ihm Zugang zu persönlichen Daten zu Bankkonten und zu Sozialversicherungen und Führerscheinen verschafft[16].
- Ein IT-Mitarbeiter verschafft sich über das IT-System persönliche Daten eines Mitglieds der Unternehmensleitung mit denen er Zahlungen zu seinen Gunsten fingiert, indem er auf fremden Namen bei Banken im WWW Kredite beantragt[17].
- Eine Mitarbeiterin eines Unternehmens, das Lohn- und Gehaltsabrechnungen für andere Unternehmen erstellt, späht die Zugangsdaten von Kollegen aus und verschafft sich damit unberechtigt Zugang zu den IT-Systemen. Ihr Ehemann arbeitet bei einem der Unternehmen, für die Lohnzahlungen errechnet und angewiesen werden. Durch Manipulation der Daten ihres Ehemannes erhält dieser Überzahlungen[18].
- Zwei Mitarbeiter des internen Rechnungswesens nutzen den Zugang zu den IT-Systemen des Unternehmens, um unberechtigt Anteilsscheine des Unternehmens zugunsten ihrer Depots zu buchen[19].
- Ein 18-jähriger Mann greift das IT-System einer (populären) Online-Community an und verschickt an die Kunden unberechtigt 1.5 Millionen Instant Messages, die Werbung für Finanzdienstleistungen und Pornografie enthalten. Danach meldet er

14 Vgl. Casey (2004) S. 79.
15 Vgl. US Department of Justice (2007a).
16 Vgl. US Department of Justice (2008a).
17 Vgl. US Attorney of Justice (2008b).
18 Vgl. US Department of Justice (2008b).
19 Vgl. Department of Justice (2001).

sich als Urheber bei dem Unternehmen und bietet an, das IT-System gegen solche Angriffe zu schützen. Zudem verlangt er, zukünftig exklusiv Werbemails über das System versenden zu dürfen. Da das Unternehmen nicht reagiert, droht er mit der Veröffentlichung seiner Angriffsmethode[20].

- Bei einem Angriff auf ein System des Bundesstaates Virginia (USA), mit dem von Apothekern und Krankenhäusern Medikamentenmissbrauch verfolgt bzw. verhindert wird, kommen viele Patienten- und Verschreibungsdaten in die Hände von Erpressern, die Forderungen in Millionenhöhe stellen. Zur Erhöhung des Drucks wird das System der Behörde so gestört, dass der laufende Betrieb erst nach erheblichen Anstrengungen wiederhergestellt werden kann[21].

2.2 Ausweglosigkeit

Angriffe werden zur Linderung akuter finanzieller Not, die als essentiell empfundene wird, durchgeführt. Die Not ist oft ausgelöst durch Suchtverhalten wie Spielsucht, Kaufsucht, Drogensucht u.ä. der Angreifer oder nahe stehenden Personen. Beispiel:

- Ein Mitarbeiter manipuliert mit dem IT-System einer der Bank und mithilfe eines Kollegen den Stand seines eigenen Bankkontos mit dem Ziel, das Überziehen seiner Kreditlinien durch Verluste beim Glücksspiel zu vertuschen[22].

2.3 Neugier

Hierbei wollen Angreifer ihre Kenntnisse und Fähigkeiten oder technische Möglichkeiten ausprobieren und Befriedigung von Neugier, Spieltrieb, Wissensdurst o.ä. befriedigen. Meist liegt ein nur geringes Unrechtsbewusstsein vor, da der Angriff als Spiel, Test oder Experiment angesehen wird. Der für einen Angriff betriebene Aufwand kann sehr hoch sein. Meist findet keine absichtliche Schädigung des Angriffsziels statt. Beispiele:

- Ein Student in den USA will seine erlernten Fähigkeiten im Umgang mit Computern ausprobieren und sendet ein Programm (Wurm) über das Internet, das in andere Rechnersysteme eindringt – ohne dort gezielten Schaden anzurichten. Allerdings repliziert und verbreitet sich das Programm so schnell, dass eine große Anzahl von Rechnern wegen Überlastung zusammenbricht[23].

---

20 Vgl. US Department of Justice (2005).
21 Vgl. Krebs (2009b).
22 Vgl. US Department of Justice (2008c).
23 Vgl. Casey (2004) S. 62f.

- Ein arbeitsloser IT-Experte aus London greift vom heimischen Computer zahlreiche IT-Systeme des US-Verteidigungsministeriums, der US Army, US Navy, US Air Force sowie der NASA an und manipuliert Daten und Programme. Er verteidigt sich später damit, dass er Hinweise gesucht habe, dass die US-Administration Beweise für die Existenz exterritorialen Lebens verheimliche[24].

2.4 Ehrgeiz und Geltungsdrang

Angreifer streben nach Aufmerksamkeit, Prestige und sozialer Anerkennung. Erfolgreiche Angriffe werden in der sozialen Umgebung des Angreifers als Zeichen von Mut und Kompetenz gewertet und mit entsprechender Anerkennung belohnt. Meist herrscht ein geringes Unrechtsbewusstsein vor, vielmehr wird der Angriff als Wettkampf oder Herausforderung angesehen. Der betriebene Aufwand für einen Angriff kann - je nach Ehrgeiz und Hartnäckigkeit des Angreifers - sehr hoch sein.

- Ein Hacker aus Saudi Arabien manipuliert die Webseite von Microsoft so, dass dort ein Foto von – in Hackerkreisen unpopulären - Bill Gates in misslicher Lage auftaucht: Gates wird gerade von einer Sahnetorte o.ä. mitten im Gesicht getroffen. Über dem Foto prangt der stolze Hinweis des Hackers „owned by Cyber-Terrorist“. In Hackerkreisen gilt der Angriff auf Gates bzw. Microsoft moralisch als gerechtfertigt und die Überwindung der Sicherheitsmaßnahmen von Microsoft als Bravourstück. Im Ergebnis wird die Webseite verunstaltet („website defacing“), der Werfer der Torte durch die Veröffentlichung des Fotos glorifiziert und der Hacker erntet Anerkennung in seiner Szene[25]

- Ein Schüler ist fasziniert von der Möglichkeit, mit Virenprogrammen Webseiten von Unternehmen angreifen zu können. Er wetteifert mit anderen Programmierern derartiger Programme, will „besser sein“ und erringt durch seine Erfolge (u.a. Sasser) Anerkennung in der Schulklasse und Clique, wo er sonst wenig integriert ist[26].

2.5 Spionage

Hierzu gehören das gezielte Ausspähen, Sammeln und Auswerten vertraulicher Informationen, u.a. in Form der Einsichtnahme in Datenbanken oder des Abhörens bzw. Mitlesens von Kommunikation und Datenübertragung. Die Angriffe werden oft im Auftrag

24 Vgl. Sturcke (2008), US District Court Virginia (2002).
25 Vgl. Almeida (2007).
26 Vgl. Stillich (2004).

Dritter durchgeführt. Dabei setzen die Angreifer konspirative Mittel ein, um unerkannt zu bleiben. Die Angriffe werden oft über langen Zeitraum durchgeführt. Dabei werden oft Insiderwissen, lückenhafte Kontrollen oder mangelnde Aufmerksamkeit ausgenutzt. Beispiele:

- Chinesische Hacker, die staatlichen Stellen zugeordnet werden, versuchen in IT-Systeme deutscher Behörden (u.a. Kanzleramt, Wirtschafts-, Forschungs- und Außenministerium) und belgischer Behörden einzudringen, um Wirtschaftsspionage zu betreiben[27]. Das Bundesamt für Verfassungsschutz verzeichnet verstärkte Angriffe aus China während und nach aktuellen Ereignissen wie dem Besuch des Dalai Lama in Deutschland oder den Olympischen Spielen in China[28].
- Eine aktuelle Studie aus Nordarmerika berichtet über mindestens 1.295 Rechnern in 103 Ländern der Welt, deren Besitzer alle in Zusammenhang mit dem Land Tibet und dem Dalai Lama stehen, davon ca. 30 Prozent wichtige diplomatische, politische, ökonomische oder militärische Institutionen. Angreifer haben diese Rechner zu einem Rechnernetz verknüpft, um auf den Rechnern gespeicherte Informationen auszuspähen und Kommunikation und Datenübertragungen zwischen den Rechnern abzuhören[29].
- Das Bundeswirtschaftsministerium warnt ausdrücklich vor Industriespionage durch Angriffe auf IT-Systeme und schätzt, dass jedes fünfte Unternehmen schon einmal Ziel von Angriffen war und dass bundesweit Schäden in Milliardenhöhe drohen[30].
- Das Übertragungsnetzwerk zwischen den Unternehmen, die für das US-Verteidigungsministerium das Kampfflugzeug F-35 Lightning II entwickeln, ist angegriffen worden. Dabei sind in erheblichem Umfang Daten gestohlen worden. Die Untersuchungen weisen darauf hin, dass die Angriffe aus China stammen – ohne dass eine Beziehung zu staatlichen Stellen nachgewiesen ist[31].
- Einem Mitarbeiter eines Unternehmens, das feuerfeste Oberflächenmaterialen entwickelt und vertreibt, wird vorgeworfen, er habe sich über das IT-System unbe-

27 Vgl. NN (2007), NN (2008).
28 Vgl. NN (2009).
29 Vgl. Sevdev/Munk (2009).
30 Vgl. Bundeswirtschaftsministerium (2009).
31 Vgl. Gorman/Cole/Dreazen (2009).

rechtigt Zugang zu vertraulichen Produktionsunterlagen verschafft und dann ein eigenes Unternehmen zum Vertrieb derartiger Materialien gegründet[32].

- Durch das Abhören (Sniffing) von Datenübertragungen werden Zugangscodes (Benutzername, Passwort) des IT-Systems der Universität Mannheim ausgespäht, um damit Zugang zu Informationen eines Forschungsprojekts zu erlangen[33].
- Ein IT-Mitarbeiter von Morgan Stanley verschafft sich Zugang zu Kundenlisten und Preis- und Kalkulationsunterlagen, um damit ein Konkurrenzunternehmen zu gründen[34].
- Durch eine fingierte Hochzeit und gefälschte Dokumente erlangt eine Libanesin die US-Staatsbürgerschaft und letztlich eine Anstellung beim FBI. Dort nutzt sie die IT-Systeme unberechtigt, um Anfragen zu Verwandten und Bekannten durchzuführen und Informationen über Untersuchungen zu internationalen Terroristengruppen zu erlangen[35].

2.6 Sabotage

Ziel ist die schwerwiegende Schädigung des Angriffsopfers durch die Beschädigung (schlimmstenfalls Zerstörung) bedeutsamer materieller oder immaterieller Güter. Diese Angriffe richten sich z.B. gegen wirtschaftliche Konkurrenten oder politische Gegner und werden oft für wirtschaftlich, politisch oder terroristisch motivierte Auftraggeber ausgeführt. Das Erkennen oder Bemerken der Angriffe ist relativ einfach, kommt jedoch meist zu spät. Beispiele:

- Ein externer IT-Mitarbeiter einer Polizeibehörde erhält unberechtigten Zugriff auf das behördliche IT-System und ändert damit Akten zur Strafverfolgung von ihm sowie von Freunden, indem er offene Fälle als »erledigt« kennzeichnet[36].
- Ein Hacker greift die IT-Systeme von Universitäten und Forschungseinrichtungen an und nimmt schwerwiegende Manipulationen vor, die die Systeme zeitweise ausfallen lassen oder fehlerhaft arbeiten lassen[37].

32 Vgl. US Attorney (2008a).
33 Vgl. Lux/Peske (2002) S. 200-201.
34 Vgl. US Attorney (2007a).
35 Vgl. US Department of Justice (2003).
36 Vgl. Casey (2004) S. 10.
37 Vgl. Casey (2004) S. 76.

- Ein Unternehmen beauftragt einen Angreifer, die Webseiten eines Konkurrenzunternehmens auszuschalten[38].
- Im Jahr 1983 wird von der terroristischen Vereinigung „Rote Zellen“ ein Sprengstoffanschlag mit Millionenschaden auf das Rechenzentrum von MAN verübt, um gegen deren Beteiligung an der Herstellung von Cruise Missiles und Pershings zu demonstrieren[39].
- Im Jahr 1970 verursachte ein terroristischer Anschlag auf das Rechenzentrum der Universität von Wisconsin einen hohen Schaden[40].

2.7 Rache und Vergeltung

Hier erfolgen Angriffe oft als Reaktion auf Handlungen des Angriffsziels, die als Unrecht empfunden werden, und zielen auf die Schädigung eines bestimmten Unternehmens oder bestimmter Personen durch Beschädigung oder Zerstörung bedeutsamer materieller oder immaterieller Güter. Der Antrieb ist überwiegend emotional (Hass, Wut, Frustration u.ä.) und auf sichtbaren Schaden ausgelegt, um das empfundene Unrecht auszugleichen. Selten werden Angriffe dieser Art im Auftrag Dritter durchgeführt. Die Angriffe werden meist mit relativ kurzer Vorbereitungszeit vorgenommen für Angriffe, es handelt sich eher um spontanes Vorgehen. Das Erkennen oder Bemerken der Angriffe ist relativ einfach, kommt jedoch meist zu spät. Beispiele:

- Ein IT-Mitarbeiter wird wegen Diebstahls entlassen. Allerdings hinterlässt er in den IT-Systemen des Unternehmens Programme, die an einem von ihm festgelegten Datum umfangreiche Datenbestände löschen[41].
- Ein ehemaliger Mitarbeiter verschafft sich unberechtigt Zugang zu den IT-Systemen seines vormaligen Arbeitgebers und manipuliert Daten eines wichtigen Kunden, so dass das Unternehmen und der Kunde schweren finanziellen Schaden erleiden[42].
- Ein entlassener IT-Mitarbeiter bringt 11.000 Virenprogramme in das IT-System des ehemaligen Arbeitsgebers ein[43].

38 Vgl. US Department of Justice (2006a).
39 Vgl. NN (1983).
40 Vgl. Schutz (1992) S. 31.
41 Vgl. Casey (2004) S. 543.
42 Vgl. US Attorney (2008b).
43 Vgl. Gassner (2004).

- Ein entlassener Mitarbeiter verschafft sich nach seiner Kündigung Zugang zu dem Mailserver seines ehemaligen Arbeitsgebers und sorgt dafür, dass alle Mails bei den Providern als SPAM geblockt werden[44].
- Ein IT-Mitarbeiter einer Bank platziert auf von ihm betreuten IT-Systemen Schadprogramme, die auf sein Kommando zeitgesteuert aktiv werden können (»Zeitbomben«). Wegen Disziplinarvergehen wird dem Mitarbeiter fristlos gekündigt. Einige Tage danach zerstören die Schadprogramme Daten und beeinträchtigen damit 50.000 Kundenkonten[45].
- Einem IT-Mitarbeiter wird vom Arbeitgeber zum Ende Monats gekündigt. Während der Kündigungsfrist nutzt der Mitarbeiter seine Zugangsrechte zu den IT-Systemen und löscht wichtige Software, zugleich verschleiert er seine Aktivitäten durch Manipulation der IT-Systeme. Der angerichtete Schaden für das Unternehmen ist beträchtlich[46].

2.8 Neid

Der Tatantrieb ist hier überwiegend emotional und zielt auf den Ausgleich einer als ungerecht oder unverdient angesehener Ungleichverteilung materieller oder immaterieller Güte. Angriffe werden oft von Innentätern durchgeführt, deren Neid von Beobachtungen am Arbeitsplatz ausgelöst wird. Beispiel:

- Ein Mann neidet einem Mitarbeiter der US Navy seinen Arbeitsplatz als Systemadministrator. Er greift daher das IT-System der Navy an, um Schaden anzurichten und damit den Systemadministrator zu diskreditieren[47].

2.9 Vandalismus

Auch hier erfolgt der Angriff meist aufgrund eines überwiegend emotionalen Antriebs und ist auf sichtbaren Schaden ausgelegt durch Beschädigung oder Zerstörung bedeutsamer materieller oder immaterieller Güter. Dies geschieht selten im Auftrag Dritter. Beispiele:

- Ein ehemaliger externer IT-Mitarbeiter von DaimlerChrysler nutzt seine internen Kenntnisse und greift über ein Terminal im Empfangsbereich eines Werkes von

44 Vgl. Department of Justice (2008d).
45 Vgl. US Department of Justice (2006b).
46 Vgl. US Department of Justice (2004).
47 Vgl. US Attorney (2007b).

DaimlerCrysler das IT-System an. Das von ihm initiierte Löschen wichtiger Daten erzwingt, dass ein Werksbereich für einige Stunden geschlossen werden muss[48].

- Ein IT-Mitarbeiter eines Medizinunternehmens fürchtet nach einer Fusion um seinen Arbeitsplatz und platziert vorsorglich Schadprogramme, die auf sein Kommando aktiv werden können (»Zeitbomben«). Obwohl seine Beschäftigung später nicht mehr in Gefahr ist, versucht er, die Schadprogramme automatisch an seinem nächsten Geburtstag auszulösen[49].

2.10 Ergänzungen

Mit der aufgeführten Klassifikation treten Motive hervor, die häufig und ausgeprägt zu beobachten sind, auch wenn Abgrenzungen nicht immer eindeutig möglich sind und in der Realität Kombinationen oder Vortäuschungen von Motiven vorkommen mögen. So wird etwa bei einer Erpressung aus Habgier oft eine Sabotage angedroht. Auch werden die Motive bei Tätergruppen zwischen den Gruppenmitgliedern durchaus variieren, so z.B. bei Angriffen, die der Wirtschaftsspionage dienen: Meist sucht ein Auftraggeber, der vertrauliche Informationen erlangen will, jemanden, der diese Aufgabe gegen Bezahlung aus Habgier, aus Rache oder aus anderen Gründen durchführt.

Ergänzend zu beachten sind folgende Besonderheiten:

- Die Auswahl der Beispiele soll einige besonders prägnante Fälle sowie das breite Spektrum der Handlungsweisen - auch innerhalb der aufgeführten Klassen - zeigen. Dabei sind einige Beschreibungen von Beispielen aus Veröffentlichungen von Staatsanwaltschaften u.ä. Anklage- bzw. Verfolgungsbehörden entnommen und daher als begründete Verdächtigungen einzustufen.
- Manche erfolgreiche Angriffe so genannter Hacker unterstützen eine gewisse Skepsis gegenüber dem Einsatz umfassender IT-Systeme und erfahren daher moralische Unterstützung in der Öffentlichkeit. Die Konnotation zum Begriff »Hacker« ist dabei auch positiv und trägt Respekt und Anerkennung für deren Kompetenz und Geschick – anders etwa als bei analogen Begriffen der klassischen Kriminalität. Zudem sind die Angriffsopfer oft große, unpersönlich und mächtig erscheinende, globale - also ohne lokale Wurzeln agierende - Unternehmen, die wenig Sym-

48 Vgl. US Department of Justice (2007b).
49 Vgl. US Department of Justice (2007c).

pathie oder Mitleid, sondern oft klammheimliche Freude über ihre Missgeschicke auslösen.

- Unter technisch affinen, meist jüngeren Menschen werden Angriffe auf IT-Systeme als Herausforderungen angesehen, die wie im Sport als Wettkampf angenommen werden. Die dazu erscheinenden Veröffentlichungen in der Presse schüren diesen Eindruck[50] und sorgen für eine gewisse Attraktivität dafür, sich mit Angriffsmethoden und -werkzeugen zu beschäftigen.
- Im Bereich der Angriffe durch Außentäter über elektronische Kommunikationswege scheint heute die größte Gefahr nicht mehr von Einzelnen auszugehen, die Angriffe aus Gründen der persönlichen Bereicherung, der angestrebten sozialen Anerkennung, aus Publizitätssucht oder aufgrund politischer Anschauungen verüben. Vielmehr wird zunehmend eine mafiös strukturierte, organisierte Kriminalität beobachtet, die allein der persönlichen Bereicherung dient[51].
- Bei Angriffen aller Motivlagen nimmt der Einsatz konspirativer Mittel zur Verschleierung und Ablenkung eventueller Verfolger zu. Dabei werden vor allem die Identität von Angreifern (durch Manipulation von Absenderangaben), der Ursprung von Angriffen (durch sog. »Zombie«-Rechner) und die Motive von Angriffen verschleiert. Im Internet werden diese Verschleierungen begünstigt durch Schwächen bzw. Mängel der eingesetzten Protokollfamilie TCP/IP.
- Durch die erhöhte Aufmerksamkeit der Medien für aktuelle Angriffe auf IT-Systeme werden die Verwundbarkeit der Unternehmen sowie Details zu Angriffsmitteln und -wegen stärker öffentlich. Dies lockt potentielle Täter an, die mit der reinen Androhung von Angriffen Zahlungen erpressen wollen; Erpressung gilt mittlerweile als ernstes Problem[52].
- Zusätzlich zu den aufgeführten Motivationen existieren solche wie Publizitätssucht und geistige Verwirrung, die kaum zu erkennen sind.
- Eine wesentliche Gefahr geht von Angreifern aus, die nicht ein genau konturiertes Motiv erkennen lassen, sondern lediglich durch eine günstige Gelegenheit verleitet werden. So können Mängel bei Abwehr- und Kontrollmaßnahmen dazu führen, dass Angreifer die Gelegenheit (z.B. ein unbenutztes Terminal, ein herumliegen-

50 Vgl. Kremp (2009).
51 Vgl. Kempf (2009) S. 1, LKA Wiesbaden (2008) S. 8.

des Laptop, ein Notizzettel mit Zugangsdaten zu einem IT-System …) nutzen, ohne zuvor ein solches Vorhaben geplant oder gezielt vorbereitet zu haben. Der Anteil solcher opportunistischer Angriffe wird für erheblich gehalten, so weist eine Studie einen Anteil von 39 Prozent an allen Angriffen aus[53].

3 Täter und Tätergruppen

Mögliche Angreifer zu kennen und analysieren zu können ist wichtig, um im Risikomanagement Eintrittswahrscheinlichkeiten und Umfänge potentieller Schäden abzuschätzen und dann zielgerichtet Schutzmaßnahmen zu entwickeln und umzusetzen[54]. Zudem können tatsächliche Angriffe besser erkannt und untersucht werden. Damit werden Maßnahmen der Prävention und Reaktion gegen Angriffe verbessert.

Als Täter für Angriffe auf die Informationsverarbeitung eines Unternehmens kommen grundsätzlich Innentäter in Frage, also Mitarbeiter, die sich Zugriff auf Systeme der Informationsverarbeitung verschaffen können, oder Außentäter, also Externe, die sich einen derartigen Zugriff verschaffen können. Exakte Hinweise auf die Größenverhältnisse der Täterkreise variieren[55]; es ist davon auszugehen, dass mehr als die Hälfte aller Angriffe von Innentätern ausgeübt werden, allerdings auch ein hoher Anteil durch gemeinschaftliches Handeln von Innen- und Außentätern durchgeführt wird. Da Innentäter für Angriffe Insiderwissen (zu internen Abläufen, Gewohnheiten, Schwachstellen, sozialen Beziehungen …) einsetzen können, muss bei ihnen mit größerem Angriffserfolg und höheren Schäden gerechnet werden[56]. Zudem stehen Innentätern im Grundsatz zugleich alle Möglichkeiten von Außentätern zur Verfügung. Allerdings ist durch weltumspannende Kommunikationsnetze wie das Internet die Anzahl potentieller Außentäter, die sich über diese Netze ortsunabhängig Zugriff auf Systeme der Informationsverarbeitung verschaffen können, sehr groß und heterogen. Eine Einschätzung zu Motiven, Kenntnissen, Ressourcen ist daher nahezu unmöglich, es muss mit „allem“ gerechnet werden.

Bei Innentätern sind folgende Gruppen zu berücksichtigen:

---

52 Vgl. Kempf (2009) S. 3.
53 Vgl. Baker/Hylender/Valentine (2008) S. 18.
54 Vgl. Eschweiler/Psille (2006) S. 50.
55 Vgl. etwa PWC (2007) S. 39, D'Arcy/Hovav (2007) S. 113, Richardson (2008) S. 14.
56 Vgl. D'Arcy/Hovav (2007) S. 113.

- Reguläre Benutzer eines IT-Systems, die zu einem Zugriff berechtigt sind, können diesen Zugriff missbrauchen z.B. wenn sie ein Gerät am Arbeitsplatz beschädigen oder wenn Mitarbeiter der Buchhaltung gezielt falsche €-Beträge oder Kontonummern eingeben.
- Reguläre Benutzer eines IT-Systems, die zu einem (speziellen) Zugriff nicht berechtigt sind und sich diesen Zugriff gezielt verschaffen (z.B. durch Beschaffung des Schlüssels zu einem Geräteraum oder durch Eingabe von Benutzernamen und Passwort einer anderen Person) und dann missbrauchen.
- IT-System- und Servicetechniker und IT-Administratoren eines Unternehmens besitzen oft weit reichende Zugangs- und Zugriffsberechtigungen für viele IT-Systeme und können damit Angriffe ausführen. Ähnliches gilt für externe IT-System- und Servicetechniker, die im Auftrag eines Unternehmens Zugang und Zugriff zu IT-Systemen haben. Daneben haben oftmals Reinigungs- und Sicherheitspersonal und Lieferanten Zugang und Zugriff zu IT-Systemen

Sicherlich muss bei Außentäter von gewissen IT-Kenntnissen und -Fähigkeiten ausgegangen werden, die notwendig sind, um Angriffe durchzuführen. Jedoch nutzen Außentäter zunehmend die Unterstützung im WWW zugänglicher Programme und Baukästen, die beim Entwurf und der Durchführung von Angriffen unterstützen. Ein Angreifer muss so nicht mehr über fundierte technische Fähigkeiten verfügen, sondern kann sich vorgefertigter Werkzeuge bedienen, die im z.B. WWW in entsprechenden Foren relativ offen angeboten werden[57]. Nach Schätzungen sind weltweit 500 bis 1.000 Hacker mit hohem technischem Wissen aktiv, die Angriffe selbstständig technisch entwerfen und durchführen, dagegen sind ca. 100.000 so genannte „script kids“ aktiv, deren Angriffe auf vorgefertigten Werkzeugen aufsetzen[58]. Die für einen Angriff notwendigen Kenntnisse sind daher geringer als früher.

Der Kreis der Außentäter ist wegen der weltumspannenden, offenen Kommunikationsnetze (z.B. Internet) nur beschränkt einzugrenzen oder zu kategorisieren. Aus Nutzungsstatistiken für das Jahr 2007 in Deutschland lassen sich kaum Eingrenzungen für soziodemografische Merkmale ableiten:

57 Vgl. Disterer/Alles/Hervatin (2005) S. 106.
58 Vgl. Geschonneck (2004) S. 14-15.

- 97 % aller Unternehmen (ab 10 Mitarbeiter) setzen IT-Systeme ein[59], 84 % aller Unternehmen (ab 10 Mitarbeiter) verfügen über eine Breitbandanschluss an das Internet[60],
- 82% aller Haushalte verfügen über einen PC[61], 56 % aller Haushalte verfügen über einen Breitbandanschluss an das Internet[62],
- 75 % der Bevölkerung (im Alter über 16 und unter 74) hat in den letzten 3 Monaten das Internet genutzt[63]; in der Altersklasse 14 bis 29 Jahre sind über 90 % und in der Altersklasse ab 65 Jahre etwa 30 % als Internetnutzer zu bezeichnen[64], 72 % aller Männer und 58 % aller Frauen sind Internetbenutzer[65].

Daher muss mit folgendem - breiten - Spektrum an möglichen Tätern gerechnet werden[66]:

- Mitarbeiter
- Gruppen der organisierten Kriminalität
- Terroristischen Vereinigungen
- Regierungen und regierungsnahe Organisationen
- Wettbewerber
- Kunden, Lieferanten, Vertrags und Kooperationspartner
- Klassische Hacker
- Im Auftrag Dritter aktive Hacker

4 Verbreitete Angriffsarten

Im Folgenden sind einige weit verbreitete[67] Arten von Angriffen beschrieben; zudem geben die in Abschnitt 2 gegebenen Beispiele Hinweise auf weitere Angriffsarten.

Diebstahl mobiler Endgeräte: Die zunehmende Nutzung von Computern auch im privaten Bereich sowie die Miniaturisierung und Verbreitung mobiler Endgeräte führt dazu,

59 Vgl. TNS (2009) S. 160.
60 Vgl. TNS (2009) S. 211.
61 Vgl. TNS (2009) S. 164.
62 Vgl. TNS (2009) S. 89.
63 Vgl. TNS (2009) S. 177.
64 Vgl. TNS (2009) S. 173.
65 Vgl. TNS (2009) S. 188.
66 Vgl. Skoudis/Liston (2006) S. 8-11.
67 Vgl. Richardson (2008) S. 15, Bundesamt für Sicherheit in der Informationstechnik (2009) S. 19-31, PWC (2007) S. 14.

dass betrieblich benutzte Endgeräte zu einem attraktiven und relativ leicht zugänglichen Diebesgut geworden ist; die resultierenden Probleme sind für die Unternehmen erheblich[68]. Notebooks, Laptops, PDAs, Mobiltelefone mit IT-Funktionalitäten werden vielfach außerhalb der physischen Schutzmauern der Unternehmen eingesetzt und sind so für Angreifer an vielen öffentlichen Orten relativ leicht greifbar, besonders an Orten, an denen die Aufmerksamkeit der Besitzer niedrig ist oder leicht abgelenkt werden (Flughafen, Bahnhof, Restaurant …). Bestenfalls tritt für das Unternehmen nur ein Vermögensschaden durch Verlust eines Gerätes ein, schlimmstenfalls werden die Schutzziele der Integrität und Vertraulichkeit verletzt und erheblicher Schaden ausgelöst, wenn ein Gerät genutzt wird, um in die IT-Infrastruktur (Hardware, Netze, Anwendungen) vorzudringen und missbräuchlich zu benutzen.

Ausschleusen wichtiger Informationen: Die Miniaturisierung der Speichermedien ist in den vergangenen Jahren sehr weit fortgeschritten, etwa abzulesen an den handelsüblichen Medien im Entwicklungsverlauf: 5,25 Zoll Diskette mit 360 KB, 3,5 Zoll Diskette mit 1,4 MB, CD mit 800 MB, DVD mit 4,3 GB, USB-Stick mit 64 GB. Damit steigt die Gefahr, dass wichtige Informationen – meist von Innentätern – aus dem Unternehmen ausgeschleust werden. Zudem können Täter Email oder andere Kommunikationswege nutzen, um Informationen (z.B. zu Kunden, Neuentwicklungen oder anstehenden Vorhaben) unbemerkt auszuschleusen und missbräuchlich zu verwenden. Das Schutzziel der Vertraulichkeit der IT-Systeme ist dadurch gefährdet.

Gefährdungen durch externes Personal: Bei Wartungs- und Reparaturarbeiten der IT-Infrastruktur müssen Unternehmen häufig auf externe Expertise und Arbeitskräfte zurückgreifen. Dem externen Personal muss dafür Zutritts- bzw. Zugangsrechte zur IT-Infrastruktur gewährt werden. Vor einem Wartungs- oder Reparatureinsatz kann aber nur schwer der notwendige Umfang von Zutritts- bzw. Zugangsrechten abgesehen werden, so dass Rechte eher großzügig eingeräumt werden oder – aus Nachlässigkeit – nach einem Einsatz eingeräumt bleiben. Zudem sind Wartungs- oder Reparaturarbeiten schwierig zu überwachen und zu kontrollieren. In akuten (Not-)Fällen, in den Arbeiten sehr eilig durchgeführt werden müssen, kommt hinzu, dass der Druck der Situation und Hektik die Aufmerksamkeit für Sicherheitsaspekte absinken lassen wird. Damit bekommt externes Personal mit der Einräumung von Zutritts- und Zugangsrechten die Möglichkeit, unter Umgehung von Sicherheitsmaßnahmen Angriffe durchzuführen. Die

68 Vgl. Richardson (2008) S. 15.

Integrität und Vertraulichkeit der IT-Systeme sind unmittelbar bedroht, denkbar ist auch, dass gezielte Eingriffe der Täter die Verfügbarkeit der Systeme gefährden.

Ausspähen oder Ermitteln von Zugangsdaten: Der Zugang zu betrieblichen Informationssystemen ist in der Regel durch Authentisierungsverfahren geschützt, die Benutzer zur Eingabe von Erkennungsdaten (Benutzername, Passwort …) anhalten, bevor der Zugang gewährt wird. Die Zugangsdaten können auf unterschiedliche Wege zu Angreifern gelangen: Benutzer agieren nicht ausschließlich intern und innerhalb des Unternehmen, sondern im Rahmen ihrer Beschäftigung (z.B. mit Kunden und Lieferanten) oder privat (z.B. mit Verwandten und Freunden) über die Grenzen des Unternehmens hinaus. Auch die Organisation selber, z.B. ein Unternehmen, besitzt etablierte Schnittstellen (z.B. zu staatlichen Stellen, Kunden und Lieferanten), die Angriffspunkte bieten, um die primären Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit zu kompromittieren. Durch Methoden des Social Engineerings oder der Täuschung können Benutzer eines IT-Systems dazu gebracht werden, ihre Zugangsdaten Dritten zu nennen. Unter dem Begriff „Social Engineering“[69] werden Methoden zusammengefasst, mit denen ein unberechtigter Zugang zu Informationssystemen erlangt wird, indem z.B. die Mitarbeiter eines Unternehmens gezielt ausgehorcht werden. Dabei werden menschliche Eigenschaften wie Vertrauen, Hilfsbereitschaft, Respekt vor Autorität, Unachtsamkeit oder Trägheit ausgenutzt, um unzulässiges Handeln auszulösen.

So gibt ein Angreifer zum Beispiel im Telefonat mit einem Systemadministrator vor, eine Führungskraft des Unternehmens zu sein, der dringend Zugang zum Informationssystem benötigt, jedoch sein Passwort vergessen hat. Der Wunsch an den Systemadministrator nach Herausgabe des Passwortes wird durch den Angreifer verstärkt durch einen Appell an die Hilfsbereitschaft des Mitarbeiters und seine Bereitschaft der Unterstützung der Führungskräfte in dringenden Fällen bzw. dem Lob entsprechender Eigenschaften wie „flexibel“, „unkonventionell“, „den kurzen Dienstweg nehmend“. Hilfsweise kann der Druck auf den Systemadministrator verstärkt werden durch Ausspielen der Autorität der vermeintlichen Führungskraft und durch Anspielen auf dessen disziplinarische Möglichkeiten. In vielen Fällen wird der Systemadministrator letztlich nachgeben, das Passwort herausgeben und damit - mit guten Gewissen - unzulässig handeln. Über dieses Beispiel hinaus bietet die umfängliche betriebliche Nutzung von Kommunikationsdiensten wie Telefon und Email viele Möglichkeiten, unter der Vorspiegelung falscher Identitäten

69 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2007) S. 735-737.

an Zugangsdaten zu gelangen. Per Email geschieht dies derzeit häufig im Zuge von „Phishing“-Angriffen (zusammengesetzt aus „Passwort“ und „Fishing“), bei denen Angreifer durch hinterlistig formulierte Anfragen den Benutzern Passworte, Kreditkartendaten o.ä. entlocken.

Zudem werden Zugangsdaten häufig aus Nachlässigkeit und Bequemlichkeit als Gedächtnisstütze auf Merkzetteln o.ä. notiert und können von Dritten eingesehen werden. Durch Manipulation von öffentlich zugänglichen Geldautomaten können Zugangsdaten der Kunden (Kundennummer, PIN) von Dritten mitgelesen werden. Eine Ermittlung der Zugangsdaten ist möglich, wenn die Zugangsdaten zu leicht zu erkennen oder zu erraten sind. So bestehen die Benutzernamen häufig aus Vor- und Nachnamen der Benutzer und sind damit leicht zu eruieren. Aus Unwissenheit oder Bequemlichkeit werden von den Benutzern häufig simple Passwörter gewählt (z.B. Namen von Monaten, Lebenspartnern, Kindern, Haustieren), die von Angreifern mit Hilfe von geeigneten Wortlisten und einem Computer in relativ kurzer Zeit durchzuprobieren sind. Die Integrität und Vertraulichkeit der IT-Systeme ist damit bedroht.

Missbrauch von Systemfunktionalitäten: Die für den normalen Betrieb vorgesehenen IT-Systemfunktionalitäten können bei einem Angriff – durch Unterlaufen der Sicherheitsmechanismen oder Nutzung von Sicherheitslücken – missbräuchlich genutzt werden, indem Informationen (z.B. Kontodaten bei Zahlungsflüssen) von den Angreifern zu ihren Gunsten manipuliert werden. Die Integrität der IT-Systeme ist damit gefährdet und es droht ein erheblicher Vermögensschaden.

Kompromittierung von Rechnern mit Schadsoftware: Die Verbindungen eines Unternehmens zum Internet werden von Angreifern vielfältig genutzt, um maliziöse Software („malware“) in die IT-Systeme einzubringen und damit Schaden auszulösen. Die Schadsoftware kann dabei auf verschiedenen Wegen eingeschleust werden: Sehr häufig sind Viren und Würmer in den Anhängen von EMails verborgen[70]. Auch Software, die von nicht vertrauenswürdigen Webseiten stammt, kann derartige Schadsoftware enthalten. Bei in den letzten Jahren zunehmenden Angriffen wird die Schadsoftware beim Surfen im Web vom Benutzer unbemerkt auf einen Rechner geschleust („drive-by-download“), wenn Angreifer die Seiten vertrauenswürdiger Unternehmen entsprechend manipuliert haben. Auch werden Benutzer von den Angreifern durch Links in Emails aufgefordert, manipulierte Web-Seiten zu besuchen und dort das Herunterladen von

70 Vgl. Richardson (2008) S. 15.

Schadsoftware auszulösen. Oder den Benutzern kompromittierter Webseiten wird beim Starten eines Videos eine fingierte Fehlermeldung eingeblendet, nach der zum Abspielen des Videos das Herunterladen spezieller Software (in den Meldungen als „Software-Treiber oder „Updates“ o.ä. verharmlost) notwendig sei. Angriffe dieser Art werden begünstigt durch die komplexe Funktionalität, die Web-Browser mittlerweile bieten und die relativ geringe Aufmerksamkeit, die der Sicherheit von Web-Browsern und Web-Servern von allen Beteiligten (z.B. Benutzer, IT-Verantwortliche, Hersteller und Anbieter) entgegen gebracht wird[71]. Die Auswirkungen der Schadsoftware sind unterschiedlich und reichen von der Ausführungen unsinniger Befehle, die den Benutzer ärgern oder stören, bis zum Blockieren des Rechners („Absturz“), dem Aufzeichnen des Benutzerverhaltens (z.B. welche Seiten im Web angesteuert werden) oder von Zugangsdaten („key-logging“) oder dem Ändern oder Löschen von Informationen. In der Regel erfordert die Wiederherstellung des normalen Betriebszustands des Rechners erheblichen Aufwand.

Überlastung der IT-Systeme: Angreifer können es darauf absehen, die IT-Systeme eines Unternehmens zu überlasten. Dies kann etwa durch das Senden von Tausenden von Emails an Mailadressen im Unternehmen oder von Tausenden Anfragen an IT-Systeme (z.B. nach dem Lieferstatus eines Produktes) innerhalb weniger Sekunden geschehen („flooding“). Dafür werden auch fremde Rechner eingesetzt, die mit Schadsoftware kompromittiert und zu Netzen („Bot-Nets“) zusammengeschlossen werden, ohne dass deren Benutzer das erkennen. So werden zum Angriff die Verarbeitungs- und Übertragungskapazitäten sehr vieler fremder Rechner („Zombie-Rechner“) missbraucht. Die Anzahl der genutzten Rechner erreicht Millionenwerte und die Kommerzialisierung der Szene ist mittlerweile so weit fortgeschritten, dass Angreifern Bot-Netze dieser Art zur Miete angeboten werden[72]. Ziel der Angriffe ist der Versand von SPAM-Mails oder die Verfügbarkeit eines im Visier stehenden IT-Systems so wesentlich zu verschlechtern, dass legitimen Benutzer der Systeme keine oder nur unzureichende Systemleistungen zur Verfügung gestellt werden („denial-of-service“)[73].

5 Ausblick

Mit der Möglichkeit von Angriffen auf die betrieblichen IT-Systeme sowie deren Missbrauch muss heute gerechnet werden, diese Gefahren sind als Begleiterscheinung der

71 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2009) S. 20-21, Provos/Rajab/Mavrommatis (2009).
72 Vgl. Barnitzke (2009).
73 Vgl. Disterer/Alles/Hervatin (2007), Richardson (2008) S. 15.

zunehmenden IT-Durchdringung der Geschäftsprozesse der Unternehmen anzusehen. Entsprechend konsequent sind Risikomanagement auszurichten und Sicherheitsvorkehrungen zu treffen.

Generell gleichen die Motive und persönlichen Merkmale von Angreifern auf Systeme der betrieblichen Informationsverarbeitung jenen von klassischen Tätern. Eine Auswahl prägnanter Beispiele zeigt das breite Spektrum der Handlungsweisen der Täter. Heute ist davon auszugehen, dass die größte Gefahren für betriebliche IT-Systeme nicht mehr von Einzelnen auszugehen, sondern mit mafiös strukturierter, organisierter Kriminalität gerechnet werden muss, die allein der persönlichen Bereicherung dient. Technische Mängel und Schwächen der zugrunde liegenden Protokolle erleichtern den Einsatz konspirativer Mittel zur Verschleierung und zur Ablenkung eventueller Verfolger. Daher ist die Entdeckung, Ermittlung und Verfolgung von Tätern schwierig.

Literatur

Almeida, M. (2009). Microsoft.com defaced, Bitshield vom 5.3.2007; www.bitshield.com/Link200705MS_Defaced.html [2009-03-19].

Baker, W. H., Hylender, C. D., Valentine, J. A. (2008). Data Breach Investigations Report; www.verizonbusiness.com [2008-07-03].

Barnitzke, A. (2009). Bot-Netze: Russen-Bande rekrutiert riesige Zombie-Armee, Computer Zeitung vom 22.4.2009; www.computerzeitung.de/articles/bot-netz_russen-bande_rekrutiert_riesige_zombie-armee:/2009018/31924141_ha_CZ.html?thes=8001,9781,10228,10232& tp=/ausrichtungen/sicherheit [2009-04-26].

Bayer, M. (2005). Wirft Audi seine Blackberrys raus?, Computerwoche vom 8.6.2005; www.computerwoche.de/knowledge_center/mobile_wireless/557254/index.html [2009-02-11].

Bremmer, M. (2008). Indien droht RIM mit Blackberry-Verbot, Computerwoche vom 4.6.2008; www.computerwoche.de/knowledge_center/mobile_wireless/557254/index.html [2009-02-11].

Bundesamt für Sicherheit in der Informationstechnik (2007). IT-Grundschutzkataloge. Bonn: BSI.

Bundesamt für Sicherheit in der Informationstechnik (2009). Die Lage der IT-Sicherheit in Deutschland. Bonn: BSI.

Bundesamt für Verfassungsschutz (2009). Verfassungsschutzbericht 2008. Köln: BfV.

Bundeswirtschaftsministerium (2009). Bundeswirtschaftsministerium unterstützt Unternehmen beim Schutz gegen Computerkriminalität, 20.1.2009; www.bmwi.de/BMWi/Navigation/Presse/pressemitteilungen, did=286748.html [2009-03-19].

Bursch, D. (2005). IT-Security im Unternehmen - Grundlagen, Strategien, Check-Up, Berlin: VDM.

Casey, E. (2004). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 2. Auflage. London: Elsevier.

Corporate Trust (Hrsg.) (2007). Studie Industriespionage; http://www.corporate-trust.de/pdf/STUDIE_191107.pdf [2009-02-09].

Cross, M. (2008). Scene of the Cybercrime, 2. Aufl., Burlington: Elsevier.

Dannecker, G. (1996). Neuer Entwicklungen im Bereich der Computerkriminalität: Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung, in: Betriebsberater, 1996, Nr. 25, S. 1.

D'Arcy, J., Hovav, A. (2007). Deterring Internal Information Systems Misuse, in: Communications of the ACM, Bd. 50, 2007, Nr. 10, S. 113-117.

Disterer, G., Alles, A., Hervatin, A. (2005). Denial-of-Service-Angriffe auf Webserver, in: Handbuch der modernen Datenverarbeitung HMD, 2005, Nr. 245, S. 102-112.

Drews, V.-M. (2009). Kellerei zeigt Datendieb an, in: Hannoversche Allgemeine Zeitung, 18.2.2009, S. 17.

Eckert, C. (2001). IT-Sicherheit: Konzepte - Verfahren - Produkte, München: Oldenbourg.

Eschweiler, J., Psille, D.E.A. (2006). Security@Work - Pragmatische Konzeption und Implementierung von IT-Sicherheit mit Lösungsbeispieln auf Open-Source-Basis, Berlin et al.: Springer.

Gassner, S. (2009). Computerkriminalität bedroht den deutschen Mittelstand, www.silicon.de/sicherheit/management/0,39039020, 39171050,00/computerkriminalitaet+bedroht+den+deutschen+mittelstand.htm [2009-03-19].

Geschonneck, A. (2004). Computer-Forensik - Systemeinbrüche erkennen, ermitteln, aufklären, Heidelberg: DPunkt.

Gold, S. (2009). First arrests in Heartland Payment Systems data breach, Infosecurity. vom 16.2.2009; www.infosecurity-magazine.com/news/090216_HeartlandArrests.html [2009-03-19].

Gorman, S., Cole, A., Dreazen, Y. (2009). Computer Spies Breach Fighter-Jet Project, Wall Street Journal vom 21.4.2009; online.wsj.com/article/SB124027491029837401.html [2009-04-21].

Kempf, D. (2009). ITK-Branche im Würgegriff der Hacker-Industrie?, Vortrag im Rahmen des BITKOM-Forums Sicherheit »Industrialisierung der Computerkriminalität«, 2009; www.bitkom.de/de/termine/102_55152.aspx [2009-02-09].

Krcmar, H. (2005). Informationsmanagement (4. Auflage). Berlin: Springer.

Krebs, B. (2009a). Payment Processor Breach May Be Largest Ever, Washington Post vom 20.1.2009; voices.washingtonpost.com/ securityfix/2009/01/payment_processor_breach_may_b.html?hpid= topnews [2009-02-26].

Krebs, B. (2009b) Hackers Break Into Virginia Health Professions Database, Washington Post vom 4.5.2009; voices.washingtonpost.com/securetyfix/2009/05/hackers_break_into_virginia_he.html [2009-05-05].

Kremp, M. (2009). Last Browser Standing, SpiegelOnline vom 24.3.2009; www.spiegel.de/netzwelt/tech/0,1518,614979,00.html [2009-04-02].

LKA Landeskriminalamt Nordrhein-Westfalen (2008). Computerkriminalität - Lagebild 2008, Düsseldorf.

Lux, C., Peske, T. (2002). Competitive Advantage und Wirtschaftsspionage - Analyse, Praxis, Strategie. Wiesbaden: Gabler.

Mohay, G., Anderson, A., Collie, B., Vel, O.d., McKemmish, R. (2003). Computer and Intrusion Forensics. Norwood: Artech.

Nitschmann, J., Leyendecker, H. (2008). Steuerskandal: Vier DVDs aus Liechtenstein, Sueddeutsche vom 14.3.2008; www.sueddeutsche.de/finanzen/287/301284/text [2009-02-16].

NN (1983). Anschlag auf südhessisches Rechenzentrum zeigt Schwächen bei der Security-Planung auf: MAN-Bombe läßt DV-Sicherheitsleute aufhorchen, Computerwoche vom 30.09.1983; www.computerwoche.de/1180467 [2009-06-26].

NN (2008). Spionage-Angriffe auf belgische Computer, Heise vom 3.5.2008; www.heise.de/newsticker/Spionage-Angriffe-auf-belgische-Computer--/meldung/107340 [2009-03-19].

NN (2009). Chinesen verstärken Cyber-Attacken auf deutsche Regierung, Spiegel Online vom 4.4.2009; www.spiegel.de/netzwelt/web/0,1518,druck-617374,00.html [2009-04-04].

NN (2007). Chinesische Trojaner auf PCs im Kanzleramt, Spiegel Online vom 25.8.2007; www.spiegel.de/netzwelt/tech/0,1518,501954,00.html [2009-03-19].

Pößneck, L. (2005). Handy-Viren: Die Geschichte des PCs wiederholt sich, 2005; www.silicon.de/mobile/wireless/0,39039018,39176869,00/handy_viren+die+geschichte+des+pcs+wiederholt+sich.htm [2009-03-22].

Postinett, A. (2008). Mobile Unsicherheit - Sicherheitslücke bei Blackberry, Handelsblatt vom 16.7.2008; www.handelsblatt.com/technologie/mobile-welt/sicherheitsluecke-bei-blackberry;2012272 [2009-02-16].

Provos, N., Rajab, M.A., Mavrommatis, P. (2009). Cybercrime 2.0: When the Cloud turns dark. Communications of the ACM, Bd. 53, Nr. 4, S. 43-47.

PWC PriceWaterhouseCoopers (2007). Wirtschaftskriminalität 2007 - Sicherheitslage der deutschen Wirtschaft, 2007; www.eulerhermes.de/de/dokumente/veruntreuung-wirtschaftskriminalitaet-2007.pdf/veruntreuung-wirtschaftskriminalitaet-2007.pdf [2009-02-09].

Ramelsberger, A. (2008). Steueraffäre: Der zweite Mann, Süddeutsche Zeitung vom 25.2.2008; www.sueddeutsche.de/politik/416/434164/text [2009-02-16].

Richardson, R. (2008). CSI Computer Crime and Security Survey; Computer Security Institute and Federal Bureau of Investigation; www.gocsi.com/forms/csi_survey.jhtml [2009-03-20]

Richter, N. (2008). Geschäfte in der Telefonzelle, Süddeutsche Zeitung vom 18.7.2008; www.sueddeutsche.de/finanzen/266/448759/text [2009-02-16].

Ritzer, U. (2008). Steuersünder wollen Bank verklagen, Süddeutsche Zeitung vom 20.7.2008; www.sueddeutsche.de/finanzen/908/302904/text [2009-02-16].

Ritzer, U. (2008). Tippgeber in Todesangst, Süddeutsche Zeitung vom 12.3.2008; www.sueddeutsche.de/finanzen/288/301285/text [2009-02-16].

RSA (2007). The Confessions Survey: Office Workers Reveal Everyday Behavior that Places Sensitive Information at Risk; www.rsa.com/company/news/releases/pdfs/RSA-insider-confessions.pdf [2008-06-12].

Schultz, H.C. (1992). Computerkriminalität, München: Beck.

Schulzki-Haddouti, C., Mobilmachung der Killerprogramme, SpiegelOnline vom 24.2.2007; www.spiegel.de/netzwelt/mobil/0,1518,468239,00.html [2009-03-22].

SevDev Group, Munk Centre for International Studies (2009). Information Warfare Monitor: Tracking GhostNet - Investigating a Cyber Espionage Network; www.infowar-monitor.net/ghostnet [2009-03-31].

Skoudis, E., Liston, T. (2006). Counter Hack Reloaded: A Step-by-Step Guide to Computer Attaks and Effective Defenses, 2. Aufl., Upper Saddle River et al.: Prentice Hall.

Stillich, S. (2009). Der Wurm von der Wümme, Stern vom 11.11.2004; www.stern.de/computertechnik/internet/:Sasser-Programmierer-Der-Wurm-W%FCmme/ 25454.html?id=525454&eid=501069&pr=1 [2009-03-27].

Sturcke, J. (2008). Hacker Gary McKinnon loses appeal against extradition to US, 28.8.2008; www.guardian.co.uk/technology/2008/aug/28/hacking.security [2009-04-03].

TNS Infratest (Hrsg.) (2009). Monitoring Informationswirtschaft - 12. Faktenbericht, Sekundärstudie im Auftrag des Bundesministeriums für Wirtschaft und Arbeit; aus Internet: www.bmwi.de [2009-06-25].

US Attorney (2007a). Man pleads guilty to stealing Morgan Stanley trade secrets relating to hedge funds, 1.2.2007; www.usdoj.gov/criminal/cybercrime/chilowitzPlea.pdf [2009-03-27].

US Attorney (2007b). Former Navy contractor sentenced for damaging Navy computer system, 5.4.2007; www.usdoj.gov/criminal/cybercrime/sylvestreSent.pdf [2009-03-27].

US Attorney (2008a). News release, 7.10.2008; www.usdoj.gov/criminal/cybercrime/dierking-Charge.pdf [2009-03-19].

US Attorney (2008b). Computer tech pleads guilty to identify theft of Calpine corporation executive, 2.9.2008; www.usdoj.gov/criminal/cybercrime/smithPlea.pdf [2009-03-16].

US Department of Justice (2001). Former Cisco Systems, Inc. Accountants Sentenced for Unauthorized Access to Computer Systems to, 26.11.2001; www.usdoj.gov/criminal/cybercrime/Osowski_TangSent.htm [2009-03-31].

US Department of Justice (2003). Local FBI Employee Indicted for Public Corruption, 5.11.2003; www.usdoj.gov/criminal/cybercrime/fudgeIndict.htm [2009-03-31].

US Department of Justice (2004). Former employee of a massachusetts high-technology firm charged with computer hacking, 23.8.2004; www.usdoj.gov/criminal/cybercrime/angleCharged.htm [2009-03-31].

US Department of Justice (2005). New York Teen Pleads Guilty to Making Extortion Threats Against Internet Company, 22.3.2005; www.usdoj.gov/criminal/cybercrime/grecoPlea.htm [2009-03-31].

US Department of Justice (2006a). Michigan Man Gets 30 Months for Conspiracy to Order Destructive Computer Attacks on Business Competitors, 25.8.2006; www.usdoj.gov/criminal/cybercrime/araboSent.htm [2009-03-27].

US Department of Justice (2006b). Former technology manager sentenced to a year in prison for computer hacking offense, 23.6.2006; www.usdoj.gov/criminal/cybercrime/sheaSent.htm [2009-03-27].

US Department of Justice (2007a). Hackers from India Indicted for Online Brokerage Intrusion Scheme that Victimized Customers and Brokerage Firms, 12.3.2007; www.usdoj.gov/criminal/cybercrime/marimuthuIndict.htm [2009-03-27].

US Department of Justice (2007b). Former computer contractor pleads guilty to hacking Daimler Chrysler parts distribution wireless network, 1.6.2007; www.usdoj.gov/criminal/cybercrime/johnsPlea.pdf [2009-03-27].

US Department of Justice (2007c). Former systems administrator admits planting “logic bomb” in company computers, 19.9.2007; www.usdoj.gov/criminal/cybercrime/linPlea2.pdf [2009-03-27].

US Department of Justice (2008a). Nigerian man pleads guilty and is sentenced to 18 months by Nigerian Court for computer intrusion in the United States, 22.4.2008; www.usdoj.gov/criminal/cybercrime/adejumoSent.pdf [2009-03-28].

US Department of Justice (2008b). San Jose Woman charged with fraud in connection with a protected computer, 30.10.2008; www.usdoj.gov/criminal/cybercrime/leotiotaIndict.pdf [2009-03-16].

US Department of Justice (2008c). Former assistant bank branch manager pleads guilty to fraud and related activity in connection with computers, 4.1.2008; www.usdoj.gov/criminal/cybercrime/covelliPlea.pdf [2009-03-16].

US Department of Justice (2008d). Former IT manager sentenced to prison for hacking into previous employer's computer system and causing damage, 3.11.2008; www.usdoj.gov/criminal/cybercrime/barnesSent.pdf [2009-03-19].

US District Court Virgina (2002). United States of America vs. Gary McKinnon, 2002; news.findlaw.com/hdocs/docs/cyberlaw/ usmck1102vaind.pdf [2009-04-04].

Zetter, K. (2009). Card Processor Admits to Large Data Breach, Wired vom 20.1.2009; blog.wired.com/27bstroke6/2009/01/card-processor.html [2009-02-26].