fg sec

fachgruppe security
der schweizer
informatiker-gesellschaft

Forensic Computing

Roger Auinger
Peter R. Bitterli
Daniel Brunner
Daniel Eugster
Dr. Paul Schöbi
Stephan Schwab
Dirk Spacek
Anne-Marie Suter
Prof. Dr. Rolf H. Weber

Impressum:

Beiträge: Mitglieder der Arbeitsgruppe "Forensics"

Abbildungen: Mitglieder der Interessengruppe "Forensics"

Redaktion und Gestaltung: Roger Auinger und Michel Frisk, adverum ag, Zollikon ZH

Druck: Fotorotar AG, Egg ZH

Vorwort

Die Informationstechnologien haben heute Einfluss auf praktisch alle Bereiche unserer Gesellschaft. Die von ihnen verwalteten Daten und ihre Verbindung durch Netzwerke ergeben ein immenses Potential für deliktische Handlungen. So geben in Umfragen fast 85 Prozent der befragten Unternehmen an, Computerverstösse festgestellt zu haben. Es ist anzunehmen, dass rund zwei Drittel aller Unternehmen finanzielle Einbussen durch Computerverstösse erleiden, ob sie nun diese bemerken oder nicht. Basierend auf diesen Erkenntnissen lässt sich ableiten, dass vielerorts das nötige Bewusstsein oder die entsprechenden Kontrollen fehlen bzw. nicht greifen. Auch in der Schweiz könnte das Bewusstsein noch verbessert und durch konkrete Vorkehrungen zur Verhinderung von Wirtschaftsdelikten erweitert werden. Volkswirtschaftlich abstrahiert ist jedes Unternehmen auch implizit ein Opfer, obwohl es nicht direkt von einem wirtschaftsdeliktischen Vorfall betroffen sein muss. Schliesslich verringern diese aus deliktischen Handlungen entstehenden Verluste das Bruttoinlandprodukt. Dieser Denkansatz kann auf eine tiefere Ebene übertragen werden: So ist bewiesen, dass das Auftreten von Wirtschaftsdelikten auch die Zufriedenheit von Mitarbeitern beeinträchtigt, welche nicht direkt an Delikten beteiligt waren.

Um die erwähnten Risiken zu minimieren und im Endeffekt die Rentabilität eines Unternehmens zu steigern, sind zwei Punkte zu beachten. Zum einen ist es essentiell, angemessene Vorkehrungen zur Verhinderung von Delikten zu treffen. Zum anderen ist es für betroffene Unternehmen von grosser Bedeutung, bei Verdachtsmomenten entsprechend professionell vorzugehen, um wenigstens den Schaden minimieren oder um entwendete Mittel rückschaffen zu können. Des Weiteren hat sich in der Praxis gezeigt, dass oftmals die Aufdeckung eines kleinen Falles die Verhinderung eines grösseren Deliktes bewirkte. Somit hat die Durchführung von Massnahmen zur Aufdeckung eines Falles auch eine präventive Wirkung.

Insbesondere KMUs haben in den wenigsten Fällen eine interne "Eingreiftruppe", welche bei Wirtschaftsdelikten, bei denen der Computer das Tatwerkzeug darstellt, die notwendigen Untersuchungen führen können. Sowohl für KMUs als auch für grosse Unternehmen ist dieser auf schweizerische Verhältnisse angepasste Leitfaden ein guter Einstiegspunkt, welcher die wichtigsten Schritte bei computerforensischen Untersuchungen aufzeigt, die rechtlichen Möglichkeiten erklärt oder vor Stolpersteinen warnt.

Mit den Themen und Fragestellungen rund um den Bereich "Computer Forensic" beschäftigte sich eine interdisziplinäre Arbeitsgruppe "Forensics" der Fachgruppe Security der Schweizerischen Informatikergesellschaft (SI) während zwei Jahren. Die Mitglieder dieser Arbeitsgruppe in alphabetischer Reihenfolge:

Leiter der Arbeitsgruppe:

Roger Auinger ist geschäftsführender Partner der adverum ag. Er befasst sich mit der Untersuchung von wirtschaftskriminellen Vorkommnissen, bei welchen im Allgemeinen ein Geld- oder Wertefluss betroffen ist. Seine Ermittlungen im Bereich "Computer Forensic" beinhalten Untersuchungen im Zusammenhang mit dem zweckentfremdeten Gebrauch von IT-Ressourcen (Missbrauch), Datendiebstahl und Hackerattacken.

Die adverum ag erbringt Dienstleistungen in den Bereichen: Forensic Services und Informationssicherheit. adverum unterstützt Kunden mit der notwendigen Innovation und im verantwortungsvollen Handeln bei Fragestellungen und Problemen in den Bereichen Wirtschafts- und Computerkriminalität.

Roger.Auinger@adverum.ch
http://www.adverum.ch

Mitglieder der Arbeitsgruppe:

Peter R. Bitterli ist Leiter und Inhaber der Firma Bitterli Consulting AG und ist seit 1984 im Gebiet der Revision, Kontrolle und Sicherheit der Informationstechnologie tätig.

Die Bitterli Consulting AG ist in drei miteinander verwandten Gebieten tätig: 1) Analyse/Review von Systemen, 2) Beratung bezüglich der IT-Revision und 3) Beratung bezüglich der Systemsicherheit (Informationssicherheit). Sie unterstützt Kunden bei der Durchführung von Risikoanalysen, Benchmarking z.B. für IT-Sicherheit nach BS7799-1:1999 resp. ISO 17799 oder IT-Governance nach COBIT sowie bei Prüfungen in komplexen IT-Umgebungen.

PRB@bitterli-consulting.ch
http://www.bitterli-consulting.ch

Daniel Brunner ist der Leiter IT Investigation und Review bei UBS im Unternehmensbereich Wealth Management und Business Banking. In dieser IT Risk Control Funktion leitet er eine Gruppe, welche für die Entwicklung von IT Ermittlungs- und Überprüfungsmethoden sowie deren Umsetzung verantwortlich ist.

Die UBS ist ein weltweit führendes Finanzdienstleistungsunternehmen im Wealth-Management-Geschäft. Die UBS ist einer der grössten Vermögensverwalter. Im Investment Banking und Wertschriftengeschäft ist die UBS einer der wichtigsten globalen Anbieter und in der Schweiz die Nummer eins im Individual- und Firmenkundengeschäft.

Dani.Brunner@ubs.com
http://www.ubs.com

Daniel Eugster arbeitet im Risk Management der Migrosbank. Er ist dort verantwortlich für die Bereiche operationelle Risiken und IT-Sicherheit. In seiner vorherigen Funktion bei einer grossen Wirtschaftsprüfungs- und Beratungsunternehmung unterstützte er u.a. Firmen im Rahmen von Fraud Investigation auf der technischen Ebene.

Die Migrosbank ist mit einer Bilanzsumme von knapp 25 Mia Franken und etwas über 1'100 Vollzeitstellen die sechstgrösste Schweizer Bank.

Daniel.Eugster@migrosbank.ch
http://www.migrosbank.ch

Dr. Paul Schöbi ist Geschäftsführer der cnlab ag und ist seit 25 Jahren im Bereich der Datensicherheit mit Schwerpunkt Netzwerksicherheit tätig.

Die cnlab ag offeriert professionelle Lösungen im Internet/Intranet und Netzwerksicherheits-Bereich. Ihre Dienstleistung basiert auf einer wissenschaftlichen Expertise aus Forschung, Entwicklung, Beratung und Sicherheitsprüfungen im Internetumfeld. Auf dieser Basis ist die cnlab ag in der Lage, eine professionelle Sicherheitsberatungsdienstleistung zu erbringen, welche moderne e-business Applikationen vom Benutzerarbeitsplatz über die Serverapplikation bis hin zu den "backend" Legacy-Systemen beinhaltet.

Paul.Schoebi@cnlab.ch
http://www.cnlab.ch

Stephan Schwab ist Leiter des Kommissariates Ermittlungen IT bei der Bundeskriminalpolizei in der Abteilung Wirtschaftskriminalität. Das Kommissariat Ermittlungen IT beschäftigt sich mit der elektronischen Beweismittelsicherung sowie der Aufarbeitung und der Auswertung von Beweisen in Strafverfahren.

Die Bundeskriminalpolizei führt Vorermittlungen und gerichtspolizeiliche Verfahren in jenen Bereichen durch, die in der Kompetenz des Bundes liegen. Damit erfüllt sie die Funktion der Gerichtspolizei der Bundesanwaltschaft der Schweiz. Weiter koordiniert sie interkantonale und internationale Ermittlungsverfahren. Sie stellt den kriminalpolizeilichen Austausch mit INTERPOL sicher.

Stephan.Schwab@fedpol.ch
http://www.fedpol.ch

Dirk Spacek ist lic. iur und derzeit wissenschaftlicher Assistent am Lehrstuhl von Prof. Rolf H. Weber, Universität Zürich. Er doktoriert im Themenbereich des Immaterialgüter- und Medienrechts.

lst.Weber@rwi.unizh.ch
http://www.rwi.unizh.ch/

Anne-Marie Suter, dipl. Mathematikerin ETH mit Exec. MBA HSG-Abschluss, ist in der Informatik Sicherheit der Zürcher Kantonalbank tätig. Ihre Haupttätigkeitsgebiete liegen in der Erarbeitung von Sicherheitsvorgaben, Beratung in Projekten, Beurteilung von Risikoanalysen und Sicherheitskonzepten sowie der Überwachung der Einhaltung von Sicherheitsstandards.

Die Zürcher Kantonalbank (ZKB) ist die marktführende Zürcher Universalbank mit nationaler Ausrichtung und einem internationalen Beziehungsnetz. Die ZKB gehört mit einem Kundenvermögen (inklusive Treuhandanlagen und Festgelder, ohne Kontoguthaben) im Wert von 75,4 Mrd. Franken zu den grössten Vermögensverwaltern der Schweiz.

Anne-Marie.Suter@zkb.ch
http://www.zkb.ch

Prof. Dr. Rolf H. Weber, Studium der Rechtswissenschaften an der Universität Zürich; Gerichtssekretär am Bezirksgericht Uster, Anwaltspatent (1978); wissenschaftlicher Assistent am juristischen Seminar der Universität Zürich (Dr. iur. 1979); Visiting Scholar an der Harvard Law School (1980/81); ab 1982 Partner der Anwaltskanzlei Wiederkehr Forster in Zürich; seit 1986 – nach Habilitierung im Bereich Wirtschaftsrecht – Privatdozent; seit 1992 Titularprofessor; seit 1995 Ordinarius für Privat- und Wirtschaftsrecht an der Universität Zürich; Leiter des Zentrums für Informations- und Kommunikationsrecht; Direktor am Europa Institut Zürich; Forschungsschwerpunkte im Internet-, Informatik-, Medien-, Wettbewerbs-, Banken-, Vertrags-, Gesellschafts- und Europarecht.

lst.Weber@rwi.unizh.ch
http://www.rwi.unizh.ch/weberr/home.htm

Besten Dank für die Unterstützung:

Thomas Köppel, vormals im Bundesamt für Polizei beim Dienst für Analyse und Prävention, Bern.

Inhaltsübersicht

Diese Publikation ist in die folgenden Themenbereiche gegliedert. Die aufgeführten Personen haben schwerpunktsmässig in den entsprechenden Kapiteln mitgearbeitet:

Inhaltsverzeichnis

1 Einleitung

1.1 Der grössere Kontext - Bedrohungen der Cyber-Gesellschaft

Informationen aller Art sind in vielen Bereichen zum entscheidenden Produktionsfaktor und damit zur Basis von Sicherheit und wirtschaftlicher Prosperität geworden. Entsprechend folgenschwere Auswirkungen können der Verlust oder die Korrumpierung von Information haben. Ausser in Fachkreisen ist die Bedrohung unserer modernen Gesellschaft durch Risiken der Informationstechnologien trotz der grossen Virenangriffen der letzten Monate und anderer Informatikpannen noch immer zu wenig bekannt.

Praktisch alle Gebiete in Wirtschaft und öffentlicher Verwaltung sind auch von diesen negativen Auswirkungen betroffen. Die modernen Informationstechnologien beeinflussen namentlich auch die Kriminalitätsbekämpfung und die innere Sicherheit. Gerade das weltumspannende Internet mit seiner an sich positiven – sicherheitstechnisch allerdings problematischen – grossen technischen Offenheit wird immer mehr auch für illegale Aktivitäten benützt.

1.2 Breites Spektrum von Angriffsmöglichkeiten

Möglichkeiten zum Missbrauch der Informationstechnologien, ihrer Netzwerke und damit vor allem auch der damit verwalteten Daten sind z.B.:

- "Hacker", die Daten verändern und zentrale Firmeninformationen entwenden,
- Viren, die wichtige Daten löschen,
- eingeschleuste "Sniffer"-Programme, die Passwörter stehlen (kopieren),
- ausländische Nachrichtendienste oder private Firmen, die systematisch Kommunikationen überwachen und aufzeichnen,
- Terroristen, die ihr Zerstörungswerk nicht mehr mit Bomben, sondern durch die Störung oder Lahmlegung kritischer Systeme wie z.B. Betriebsleitzentralen der Luftfahrt oder auch Steuerungssysteme öffentlicher Infrastrukturen vollbringen.

Ein wichtiges Problem bei der Erkennung und noch besser bei der Verhinderung solcher Taten ist, dass die Strafverfolgung und auch die Nachrichtendienste in den meisten Fällen immer noch national (um nicht zu sagen kantonal) agieren, während die Informationstechnologien nationale Grenzen im "Cyberspace" praktisch zum Verschwinden gebracht haben. Der Angriffspunkt für eine kriminelle oder im schlimmeren Fall terroristische Tat zum Beispiel im Kanton Zürich kann problemlos in Australien oder in Südafrika liegen.

Während illegale Aktionen gegen oder auch unter Benützung von Informationsinfrastrukturen im kleineren Rahmen als "Cyberkriminalität" eine neue Ausprägung bereits etablierter Kriminalität darstellen und damit in die eingespielte Zuständigkeit von kantonaler, respektive zum Teil nationaler Polizei und Gerichten fallen, können solche Aktivitäten im grösseren Rahmen als "Cyberterrorismus" oder sogar "Cyber Warfare" auch sicherheitspolitisch relevant werden und damit die nationale und internationale Stufe direkt involvieren. Ein weitreichendes elektronisches Lahmlegen von kritischen Infrastrukturen wie die Stromversorgung, die Telekommunikation oder das Eisenbahnnetz bedroht auch unmittelbar die nationale und internationale Sicherheit.

Während Forensic Investigation zur Untersuchung von Cyberkriminalität angewandt wird, könnte sie natürlich auch in den anderen genannten Fällen relevant werden, z.B. zur Sicherung von Beweismitteln im Fall von elektronischer Spionage.

1.3 Computerkriminalität, Informatikkriminalität, Cyberkriminalität

Informatik- und Computerkriminalität sind zwei Begriffe für dasselbe Thema: die Deliksarten, bei denen ein Computer als Tatmittel und/oder Tatobjekt verwendet wird (zur rechtlichen Ausgestaltung in der Schweiz siehe Kapitel 2.3). Heute hat sich zusätzlich der Begriff Cyberkriminalität eingebürgert, um dem spezifischen Aspekt der Vernetzung der Computer Rechnung zu tragen. Die Vernetzung führt vor allem zu Problemen, weil der Tatort überall auf der Welt sein kann und der Täter nicht am Tatort anwesend sein muss. Dies führt zu grossen Problemen der rechtlichen Abgrenzung, der internationalen Rechtshilfe und zu Schwierigkeiten, solche Fälle zeitgerecht aufzuklären.

Cyberkriminalität umfasst spezifisch neue Deliktsformen: unbefugte Datenbeschaffung, unbefugtes Eindringen in ein Datenverarbeitungssystem, Datenbeschädigung und betrügerischen Missbrauch einer Datenverarbeitungsanlage. Unter "unechter Cyberkriminalität" versteht man bekannte Kriminalitätsformen, die mit den modernen Mitteln der Technologie begangen werden, so zum Beispiel die Verbreitung von rassendiskriminierendem oder extremistischem Gedankengut, der Aufruf zu Gewalttaten, das in Umlaufbringen von kinderpornografischem Material, die Abwicklung von Betrugsgeschäften oder die Geldwäscherei auf elektronischem Weg.

In der Kategorie Cyberkriminalität sind häufig Einzeltäter aktiv. Allerdings sind auch Aktivitäten organisierter krimineller Gruppen beispielsweise im Bereich des Betrugs oder der Geldwäscherei sehr verbreitet. Bereicherungsabsichten und Sabotage sind häufige Motive für die kriminellen Taten.

Beim Cyberterrorismus sind in erster Linie ideologisch-politisch motivierte Gruppierungen aktiv. Bei extremistisch beziehungsweise terroristisch motivierten Angriffen steht vielfach politische Erpressung im Vordergrund. Häufig sind Systeme von Regierungen oder anders gesinnten Gruppierungen Ziel der Attacken. Zwar sind in dieser Kategorie erst Einzelfälle bekannt, die Wahrscheinlichkeit ist aber gross, dass die Zahl der Vorfälle künftig zunimmt.

1.4 Hohes Risiko und noch mangelnde Strafverfolgung

Das Schadenspotenzial im Bereich der Cyberkriminalität ist als hoch einzustufen. Viele Angriffe auf Informationsinfrastrukturen bleiben verborgen, weil sie nicht erkannt oder den zuständigen Stellen nicht gemeldet werden.

Wie akut sich das Risiko von Cyberkriminalität darstellt, wird mit der Umfrage bezüglich Computerkriminalität, die jährlich durch das amerikanische Computer Security Institute (CSI) in Zusammenarbeit mit dem Federal Bureau of Investigation (FBI) durchgeführt wird[1], zum Ausdruck gebracht:

- 85 Prozent der antwortenden Firmen und Organisationen stellten Computerverstösse fest.
- 65 Prozent erlitten finanzielle Einbussen durch Computerverstösse. 35 Prozent (186 antwortende Firmen) quantifizierten die Kosten auf insgesamt über $ 377'000'000.
- 91 Prozent stellten Missbräuche des Internetzugangs durch ihre Mitarbeiter fest, zum Beispiel durch Herunterladen von pornografischen Bildern oder durch Softwarepiraterie.
- 94 Prozent entdeckten Computerviren.

In der Schweiz existiert bislang keine umfassende Statistik über die bei den Strafverfolgungsbehörden eingegangenen Anzeigen. Die Polizeiliche Kriminalstatistik (PKS) erfasst als Teilstatistik lediglich ausgewählte Delikte. Die Informatikkriminalität gehört nicht dazu. Für einen *gesamtschweizerischen Überblick* über die Fälle im Bereich Cyberkriminalität kann daher einzig die vom Bundesamt für Statistik (BFS) geführte schweizerische Urteilsstatistik (SUS) herangezogen werden.

---

[1] Vgl. „2001 Computer Crime and Security Survey“, CSI / FBI (http://www.gocsi.com/prelea_000321.htm). Die statistischen Auswertungen basieren auf 538 Antworten von Firmen der Privatwirtschaft, von öffentlichen Anstalten und Organisationen sowie von Universitäten in den Vereinigten Staaten von Amerika.

Zu Artikel 150bis StGB liegen in der SUS noch keine Urteile vor. Für die anderen Artikel werden die folgenden Zahlen ausgewiesen:

	Art. 143	Art. 143bis	Art. 1444bis	Art. 147	Art. 150	Art. 150bis
1994	0	1	2	0	0	0
1995	1	0	14	52	59	0
1996	2	1	18	225	84	0
1997	2	0	131	370	116	0
1998	2	1	21	378	131	0

Tabelle 1: Urteilsstatistik des Bundes

Die Aufstellung zeigt, dass für die relevanten Artikel des StGB zwar bisher erst relativ wenige Urteile gesprochen wurden, die Zahlen aber insbesondere bei den Artikeln 147 StGB und Artikel 150 StGB steigende Tendenz aufweisen.

Die Kriminalstatistik des Kantons Zürich (KRISTA), die im Gegensatz zur PKS die erfassten Informatikdelikte enthält, weist für die letzten Jahre folgende Zahlen aus:

	Computerdelikte (Art. 143, 143bis, 144bis, 147)	Davon Art. 147
1995	2565	2553
1996	1034	1024
1997	1549	1510
1998	1886	1872
1999	1706	1693
2000	2441	2395
2001	3435	3410
2002	6364	6315

Tabelle 2: Kriminalstatistik des Kantons Zürich (KRISTA)

Erfahrungsgemäss wird im Kanton Zürich etwa ein Viertel aller in der Schweiz erfassten Straftaten begangen. Es ist zudem davon auszugehen, dass es sich bei den meisten Straftaten nach Artikel 147 StGB um nicht mit dem Internet in Beziehung stehende Delikte handelt (Geldautomatenbetrug etc.).

1.5 Schlussfolgerung

Die grosse Anzahl von technischen Möglichkeiten, ein Delikt zu begehen, stellt die Ermittler, die sowohl unternehmensinterne als auch externe Personen oder Organisationen sein können, vor neue Herausforderungen. Diese neuen Anforderungen erstrecken sich über die folgenden Themengebiete wie Jurisprudenz, Verfahrenstechnik und Technologie.

Um in einer entsprechenden Situation, z.B. bei einem Verdacht auf eine Delinquenz, in den Ansätzen richtig reagieren zu können, bedarf es im Normalfall eine proaktive Vertrautheit mit der Thematik computerforensischer Untersuchungen. Bei jeder Vor- und Hauptuntersuchung gibt es rechtliche Grenzen, welche von der untersuchenden Organisation nicht überschritten werden dürfen, da die eigenen Interessen einem höheren und somit stärkeren Recht unterliegen. Bei der effektiven Durchführung einer forensischen Analyse gibt es zahlreiche Punkte, die gebührend berücksichtigt werden müssen, um den Ermittlungserfolg nicht zu gefährden. Hierbei sind es oftmals technische Herausforderungen, welche es zu meistern gibt und die zumeist ihren wesentlichen Teil zu einer erfolgreichen Ermittlung beitragen.

Ein vorgestellter Vorgehensansatz soll jedem Unternehmen ermöglichen, zu einem beliebigen Zeitpunkt eine Gefährdungsanalyse des eigenen Unternehmens auf Anfälligkeit oder bereits auf Vorhandensein von Computerdelinquenz durchzuführen.

Eine Untersuchung ist erst dann als abgeschlossen zu betrachten, wenn die entsprechenden Lehren aus diesem Fall gezogen und korrigierende Massnahmen eingeleitet wurden, welche eine präventive Funktion innerhalb des internen Kontrollsystems übernehmen.

2 Rechtliche Rahmenbedingungen für Forensic Computing

2.1 Einleitung

Im gegenwärtigen "Informationszeitalter" erleben neue Kommunikations- und Geschäftsmöglichkeiten und damit aber auch verschiedene neue Risiken einen starken Bedeutungszuwachs: Angesichts der technologischen Entwicklungen (schnellere Mikroprozessoren, Digitalisierung, verbesserte Übertragungstechniken) verlieren Transportwege ihre Zuordnung zu bestimmten Formen der Kommunikation und werden multifunktionell. Mittels digitaler Technologien können Daten, Töne oder Bilder über zahlreiche, unterschiedlich ausgestaltete Netze angeboten und bezogen werden, und zwischen Netzen, Endgeräten und Diensten sind sog. Konvergenzen entstanden[2].

Deshalb erstaunt es nicht, dass immer mehr Unternehmen Online-Präsenz anstreben und sich um Marktanteile im elektronischen Geschäftsverkehr bemühen; diese Tatsache eröffnet jedoch nicht nur wirtschaftlichen, sondern ebenso kriminellen Bestrebungen neue Horizonte. Der verstärkte Einbezug des Internets in den geschäftlichen Alltag, das verbesserte Verständnis von EDV-Konzepten in der Bevölkerung, die oftmals veralteten und ineffizienten Sicherheitsvorkehrungen betroffener Wirtschaftseinheiten sowie die internationale Ausprägung des Geschäftslebens sind Gründe dafür, weshalb auch ein rascher Anstieg illegaler Aktivitäten im Internet feststellbar ist[3].

Aus informationstechnologischer Sicht lassen sich Best Practices umschreiben, deren Zweck die Vereinheitlichung der Infrastruktur und die Vereinfachung der Prozessabläufe darstellt. Überblicksmässig sind folgende Aspekte als Basis für die angemessene Ausführung von Forensic Computing Services von Bedeutung[4]:

2 WEBER, E-Commerce, 4 ff.

3 WEBER/UNTERNÄHRER, Wirtschaftsterrorismus, 366.

4 WEBER, E-Governance, 352 f (inkl. Illustration).

Vereinheitlichung der Infrastruktur	Vereinfachung der Prozessabläufe
▪ Aggregation vorhandener Informationen ▪ Einheitlicher Zugang zu Datensammlungen ▪ Einmalige Datenbeschaffung für alle relevanten Zwecke ▪ Integration der Interface-Stellen mit Drittpersonen ▪ Monitoring und Erfolgsmessung	▪ Umschreibung von integrierten Informationsverarbeitungsprozessen ▪ Klare Zugangsregelung für Datensammlungen ▪ Vereinheitlichte Regeln mit Bezug auf Datenbedürfnisse

In grösseren Unternehmen ist es in der Zwischenzeit üblich geworden, mittels adäquater Software ein Management-Informations-System (MIS) als Führungsinstrument für eine zielgerichtete und kontrollierte Umsetzung von Strategien und Massnahmen einzurichten. Zu den Anforderungen an die MIS-Software gehören[5]:

Technische Anforderungen	Funktionale Anforderungen
▪ Benutzerfreundliche Oberfläche ▪ Client-Server-Architektur ▪ Netzwerk- und Multiuser-Fähigkeit ▪ Standardschnittstellen ▪ Offene, nicht-proprietäre Datenbanken ▪ Portabilität	▪ Sicherstellen der Datensicherheit ▪ Automatische Datenerfassung ▪ Unterstützung von Datensammlungen, Konsolidierung ▪ Flexible/gestaltbare Bauelemente ▪ Abstimmung und Plausibilitätsprüfung ▪ Reporting und Datenanalyse

Opfer von Cyberstraftaten sind keineswegs nur Private. Im "Global Village" lassen sich Datentransportwege auch für Anschläge auf Unternehmen, Unternehmensverbände oder sogar Regierungen effizient einsetzen. Der in diesem Zusammenhang auftauchende Begriff des "Cyberterrorismus" kennzeichnet Verhaltensweisen, welche auf planmässige und vorbereitete Anschläge gegen die politische Ordnung und Infrastruktur eines Staates abzielen[6]. In Paris existiert bereits die EGE (École de Guerre Économique), eine "Schule für den Wirtschaftskrieg". Ziel der konspirativen Lehrwerkstatt ist die

5 WEBER, E-Governance, 352 f (inkl. Illustration).

6 WEBER/UNTERNÄHRER, Wirtschaftsterrorismus, 368; SCHWARZENEGGER, E-Commerce, 333 ff.

Ausbildung in Angriffs- und Verteidigungsmethoden, mit denen sich Unternehmen und Regierungen im Wettlauf der Globalisierung auseinandersetzen müssen. Die Schule wird bisweilen sogar von der französischen Regierung herangezogen, wenn es um mutmassliche Störaktionen gegen die heimische Industrie geht[7].

Projekte der Informations- und Kommunikationstechnik sind erfahrungsgemäss volatil. Finanzinstitute – als Vorreiter der EDV-Einführung – haben nicht selten die bittere Erfahrung machen müssen, dass sich die Wunschvorstellungen mit den neuen Techniken nicht verwirklicht haben. Zur Formulierung einer gesunden Unternehmenspolitik gehört somit auch ein E-Governance-Leitbild, welches die organisationsmässige Informationsverteilung innerhalb eines Unternehmens regelt[8]. Unerlässlich ist die Gewährleistung von Informationssicherheit und Datenschutz; Vertraulichkeit, Integrität wie auch Verfügbarkeit von Informationen stellen weitere unabdingbare Voraussetzungen eines funktionierenden "Information and Communication Technology" (ICT)-Konzeptes dar.

Die in der Wirtschaft neu aufgekommene Gattung von kriminalitätsbekämpfenden Dienstleistungen, die sich als "Forensic Computing Services" bezeichnen lassen, bezweckt gemäss dem Drei-Säulen-Prinzip "Prävention, Aufklärung und Unterstützung"[9]. Prävention soll dazu dienen, das Risiko in Bezug auf Vergehen zu beurteilen und sog. "Red Flags" (d.h. Warnsignale) zu entwickeln, um die Eintrittswahrscheinlichkeit von Schäden zu minimieren[10]. Bei der Verbrechensaufklärung stehen die Eruierung virtueller Spuren und die Beweismittelsicherung im Vordergrund. Weil Internet- und Computerkriminalität einen neuen und relativ erfahrungsarmen Gefahrenbereich darstellen, sind Strafverfolgungsbehörden oft überfordert, was deren Unterstützung durch sicherheitsbewusste Organisationen nahe legt; die Forensic Computing Services können dabei insbesondere als technische Spezialisten mitwirken[11].

Ziel des folgenden Beitrages soll sein, einen allgemeinen Überblick über die Rechtsgrundlagen zu liefern, welche den Rahmen für eine effiziente E-Governance, Information-Security und Tätigkeit der Forensic Computing Services bilden.

---

7 MICHAEL MÖNNINGER, Der Krieg der Köpfe, in: DIE ZEIT, 20.02.2003, Nr. 9, 53.

8 WEBER, E-Governance, 349.

9 SCHATZMANN, 186.

10 ANNE VAN HEERDEN/NAVITA SRIKANT, KPMG-Clarity 2003, 31.

11 SCHATZMANN, 187.

2.2 Strafrecht

2.2.1 Ausgangslage: Handlung erfüllt einen Straftatbestand

Das Strafrecht ist ein Teil des öffentlichen Rechts. Es umfasst die Gesamtheit der Rechtsnormen, welche an bestimmte Arten menschlichen Verhaltens gewisse Strafen oder Massnahmen knüpfen. Eine Handlung zieht strafrechtliche Sanktionen nach sich, sofern sie einen *gesetzlichen Tatbestand* erfüllt sowie *rechtswidrig* und *schuldhaft* ausgeübt wird:

Tatbestandsmässigkeit: Ein Tatbestand umfasst die Gesamtheit sämtlicher Voraussetzungen, an welche eine Norm Sanktionen knüpft. Grundsätzlich sind Straftaten nur in vorsätzlicher Weise, somit mit Wissen und Willen, begehbar. Die fahrlässige Verletzung einer Norm ist nur strafbar, sofern das Gesetz dies ausdrücklich vorsieht. Nachfolgend wird – bei Fehlen von Hinweisen auf fahrlässig begehbare Delikte – grundsätzlich von vorsätzlich begangenen Delikten ausgegangen. Der Täter muss sich somit der unter Strafe gestellten Tathandlungen bewusst sein und die von ihm unternommene Handlung wollen.

Rechtswidrigkeit: Rechtswidrig ist ein strafrechtlich tatbestandsmässiges Verhalten, wenn keine vorrangige Gegennorm (Rechtfertigungsgrund) das Verhalten als erlaubt erscheinen lässt. Mögliche Rechtfertigungsgründe sind z.B. die Notwehr, der Notstand oder die Einwilligung des Verletzten.

Schuld: Ein strafrechtlich tatbestandsmässiges Verhalten ist schuldhaft, wenn der Täter die Fähigkeit hat, das Unrecht seiner Tat einzusehen und sich dieser Einsicht gemäss rechtskonform zu verhalten. Diese Fähigkeit fehlt ihm z.B. im Falle der Zurechnungsunfähigkeit[12].

12 REHBERG/DONATSCH, Strafrecht I, 71 ff.

2.2.2 Begriff der "Computerkriminalität"

Darüber, was unter Computerkriminalität zu verstehen ist, besteht weltweit Uneinigkeit. Grundsätzlich lassen sich jedoch drei Konstellationen von Fällen herauskristallisieren, in denen der Computer eine Rolle spielen kann:

- *Computer als Ziel*: In diese Kategorie fallen Delikte, welche Datenverarbeitungssysteme oder Teile davon mittels Datenübertragungseinrichtungen von aussen angreifen und solche Systeme verändern.

- *Computer als Tatwerkzeug*: Der Computer wird in diesem Fall als unterstützendes Tatwerkzeug herbeigezogen. Mögliche Delikte sind Urkunden- bzw. Banknotenfälschung, aber auch die Verbreitung und Speicherung von pornographischem Material, Erpressung, Betrug etc.

- *Computer als zufälliges Hilfsmittel*: Von dieser Konstellation ist dann auszugehen, wenn der Computer für die Tatbegehung zwar nicht notwendig wäre, aber doch eingesetzt wird (z.B. als blosses Schreibinstrument für Drohbriefe)[13].

13 SCHATZMANN, 186.

In der strafrechtlichen Rahmenordnung ergeben sich daher sowohl spezifische wie auch unspezifische Computerdelikte. Die folgende Darstellung soll hierfür eine tabellarische Übersicht bieten[14]:

Spezifische Computerdelikte	Nicht spezifische Computerdelikte
▪ Unbefugte Datenbeschaffung (Art. 143 StGB) ▪ Unbefugtes Eindringen (Hacken) in ein Datensystem (Art. 143bis StGB) ▪ Datenbeschädigung (Art. 144bis StGB) ▪ Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB) ▪ Erschleichen einer Leistung (Art. 150 StGB) ▪ Urkundenfälschung (Art. 251 i.V.m. Art. 110 StGB) ▪ Denial of Service-Attacken	▪ Verletzung von Immaterialgüterrechten ▪ Unlauterer Wettbewerb ▪ Verletzung von Schweigepflichten (Art. 162, 320, 321 StGB) ▪ Pornographie (Art. 197 StGB) ▪ Unerlaubte Glücksspiele ▪ Überwachung ▪ Rassendiskriminierung (Art. 261bis StGB)

2.2.3 Spezifische Computerdelikte

2.2.3.1 Unbefugte Datenbeschaffung (Art. 143 StGB)

Art. 143 StGB stellt denjenigen Täter unter Strafe, der durch einen unbefugten Zugriff besonders geschützte Daten beschafft, die einem Anderen zustehen. Eine solche Beschaffung liegt vor, sobald der Täter die unmittelbare Verfügungsgewalt über diese Daten erlangt, z.B. durch Kopieren auf Diskette oder Anzapfen eines Datenübermittlungsvorganges. An der Voraussetzung des unbefugten Zugriffs kann es jedoch mangeln, wenn der Täter die Daten benützen darf oder wenn er im Rahmen eines Arbeitsverhältnisses dazu verpflichtet ist[15]. Weil dieser Tatbestand grosse Ähnlichkeiten zum Diebstahl (Art. 139 StGB) aufweist, wird in der Lehre teilweise auch von "Datendiebstahl" oder von "Datenspionage" gesprochen[16].

---

14 Zusätzlich fallen noch die Tatbestände des Betruges (Art. 147 StGB) und des wirtschaftlichen Nachrichtendienstes (Art. 273 StGB) in Betracht, auf deren detaillierte Erörterung vorliegend aber verzichtet wird. Beide Straftatbestände sind den nicht spezifischen Computerdelikten zuzurechnen, weil deren Begehung keinen Beizug eines Computers erfordert.

15 REHBERG/ECKERT/FLACHSMANN, Tafeln, 70.

16 SCHMID, Computerkriminalität, 105.

2.2.3.2 Unbefugtes Eindringen (Hacken) in ein Datensystem (Art. 143bis StGB)

Art. 143bis StGB verbietet das unbefugte Eindringen in ein fremdes, besonders geschütztes Datenverarbeitungssystem auf dem Wege von Datenübertragungseinrichtungen (z.B. Telefonleitungen oder drahtlose Kanäle). Dieses Delikt unterscheidet sich vom Datendiebstahl (Art. 143 StGB) dadurch, dass keine Aneignung von Daten erforderlich ist. Der Täter (Hacker) dringt also wegen der technischen Herausforderungen in ein fremdes System ein, ohne jedoch Daten beschädigen zu wollen[17]. Eine Software (oder eine Technik), die Verwendung findet, um Sicherheitsvorkehrungen, welche dem Schutz geheimer Informationen dienen, zu umgehen oder auszuschalten, wird Crack genannt[18]. Der Tatbestand ist mit dem "Eindringen", d.h. mit dem Überwinden der ersten Zugangsschranken zur Datenverarbeitung, vollendet. Findet das Eindringen nicht über drahtgebundene Wege statt, z.B. wenn der Täter unbefugt in einen Computerraum eindringt und sich alsdann an ungesicherten Datensystemen über die Tastatur zu schaffen macht, findet Art. 143bis StGB keine Anwendung. Ein solches Verhalten liesse sich jedoch möglicherweise als Hausfriedensbruch (Art. 186 StGB) qualifizieren. SCHWARZENEGGER hebt hervor, dass ungesicherte Datensysteme durch die Annahme des Hausfriedensbruches (Art. 186 StGB) nicht genügend in kompensierender Weise geschützt werden (man denke z.B. an Labtop-Computer im Zug oder Restaurant). Immerhin lässt sich diskutieren, ob auch völlig ungesicherte Computersysteme geschützt werden sollen[19].

Im Zusammenhang mit Art. 33 StGB (Notwehr) wird in Kreisen der "Forensic Services" bisweilen die Thematik des "Hacking Back" angesprochen: Unternehmen haben ein Interesse daran, Eindringlinge nicht nur abzuhalten, sondern, falls ein Eindringen bereits mehrmals stattgefunden hat, auch ausfindig zu machen. Vertreter der Forensic Services zielen darauf ab, durch ein "Rückwärtshacken" die Identität des Täters ausfindig zu machen. Materiell stellt sich indessen die Frage, ob ein solches Vorgehen durch das Notwehrrecht (Art. 33 StGB) rechtfertigbar ist und wie private Schutz- und Kontermassnahmen von Unternehmen gestaltbar sind:

- Grundsätzlich liegt eine Notwehrsituation nur so lange vor, als ein Angriff andauert. Ist der Angriff oder die Verletzung von Rechtsgütern bereits abgeschlossen, stehen dem Angegriffenen keine Befugnisse aus Art. 33 StGB mehr zu[20]. Selbst wenn die Tathandlung mit dem Eindringen in ein Computersystem als vollendet er-

17 WIDMER/BÄHLER, 300.

18 WEBER/UNTERNÄHRER, Wirtschaftsterrorismus, 376.

19 SCHWARZENEGGER, FS Trechsel, 316, FN 51.

20 REHBERG/DONATSCH, 183.

achtet wird[21], hält die Wirkung indessen an, solange der Hacker im Computersystem verweilt[22]. Denn hier ist weiterhin mit der Möglichkeit zu rechnen, dass der Täter Zugangsschranken durchbrechen oder eventuell andere Delikte wie eine Datenbeschädigung (Art. 144bis StGB) oder einen Datendiebstahl (143 StGB) begehen könnte. Eine Hacking Back-Aktion erweist sich daher als notwehrrechtlich legitim, bis der Hacker das System verlassen hat. Die Ermittlung und die Durchsetzung des materiellen Strafrechts durch das Verhängen von Sanktionen ist hingegen allein Aufgabe des Staates (Grundsatz des staatlichen Straf- und Justizmonopols). Private Strafen und Selbstjustiz sind somit grundsätzlich ausgeschlossen[23].

- Eine gute Möglichkeit, mehr über einen Hacker in Erfahrung zu bringen, geben die sog. "Honeypots". Solche Einrichtungen dienen dazu, Systeme zu imitieren, in die ein Hacker gerne einbrechen möchte, tatsächlich wird der Hacker dadurch vom wahren Netzwerk ferngehalten. Den "Honeypots" werden oft für Hacker einladende Namen, wie financials.firmenname.ch gegeben; der "Honeypot" erweist sich somit als eine Art Falle. Für Unternehmen bringt ein "Honeypot" folgende Vorteile:
  - Der Administrator kann den Hacker beobachten und die Verletzlichkeit seines eigenen Systems beurteilen.
  - Der Hacker kann gestoppt und eventuell sogar ermittelt werden.
  - Durch die langfristige Studie des Verhaltens von Hackern können Designer sicherere Systeme schaffen[24].

Als ergänzend anwendbare Strafnorm im Zusammenhang mit Hackern fällt der neu eingeführte Art. 150bis StGB in Betracht, welcher den Hersteller, den Importeur und Exporteur sowie den Installateur von Geräten, deren Bestandteile oder Datenverarbeitungsprogramme zur unbefugten Entschlüsselung codierter Rundfunkprogramme oder Fernmeldedienste bestimmt und geeignet sind, unter Strafe stellt. Die Bestimmung, eingeführt durch das Fernmeldegesetz vom 30. April 1997, ergänzt insoweit Art. 150 StGB (Erschleichen einer Leistung), als sie eine Reihe von Vorbereitungshandlungen im Zusammenhang mit der Beschaffung von Mitteln zu solchem illegalen Tun unter Strafe stellt[25].

---

21 TRECHSEL, 143bis N 6.

22 REHBERG/DONATSCH, 183; BGE 102 IV 4.

23 SCHMID, Strafprozessrecht, 21.

24 www.auditmypc.com/freescan/readingroom/honeypot.asp.

25 REHBERG, Schweizerisches Strafgesetzbuch, Art. 150bis N 109.

2.2.3.3 Datenbeschädigung (Art. 144bis StGB)

Art. 144bis StGB verbietet, durch Handlungen in ungefugter Weise Daten eines Anderen zu löschen, zu verändern oder unbrauchbar zu machen (z.B. durch Einfügen neuer Passwörter oder Codes). Der Tatbestand von Art. 144bis StGB wird deshalb auch als "Computersabotage" bezeichnet. Anwendungsfälle sind teilweise harmlos und amüsant (wie z.B. das Eindringen in den Computer der CIA, um den Ausdruck Central Intelligence Agency zu "Central Stupidity Agency" abzuändern), teilweise hingegen auch sehr gefährlich. Darunter fallen vor allem die Verbreitung von Viren, welche Datenverarbeitungssysteme zum vollständigen Erliegen bringen können[26]. Viren sind definitionsgemäss Programme, die sich selbst kopieren. Als unangenehme Nebenerscheinung haben manche Viren eine destruktive Wirkung auf die Software und teilweise auch auf die Hardware eines Computers[27]. Art. 144bis Abs. 2 StGB stellt daher ebenso die Hersteller von Virenprogrammen unter Strafe, welche wissen oder annehmen müssen, dass diese Programme zum Zweck von unbefugter Datenbeschädigung eingesetzt werden[28].

2.2.3.4 Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB)

Art. 147 StGB verbietet, durch unrichtige, unvollständige oder unbefugte Verwendung von Daten oder vergleichbare Vorgehensweisen auf einen Datenverarbeitungsvorgang einzuwirken und dadurch eine Vermögensverschiebung zu bewirken, sodass bei einem Anderen ein Vermögensschaden entsteht. Ein Einwirken auf den Datenverarbeitungsvorgang liegt vor, wenn dadurch ein unzutreffendes (unrichtiges) Verarbeitungsergebnis ausgelöst wird. Beispielsweise ist an einen Hacker zu denken, der ein Computerprogramm in der Weise manipuliert, dass Zahlungen zu Lasten anderer Konten auf sein Konto überwiesen werden.

---

26 WIDMER/BÄHLER, 301.

27 WEBER/UNTERNÄHRER, Wirtschaftsterrorismus, 369.

28 TRECHSEL, Art. 144bis N 1 ff.

Die gesonderte Normierung einer "unbefugten" Verwendung will den Fall erfassen, in welchem Daten zwar richtig, aber von einer unberechtigten Person verwendet werden. Dem Gesetzgeber ist es dabei insbesondere um eine Erfassung derjenigen Fälle gegangen, in denen ein Dritter eine auf einen anderen Namen lautende Kreditkarte bei der Bedienung eines Automaten einsetzt[29]. Art. 147 StGB stellt auch Tathandlungen unter Strafe, die eine "vergleichbare Einwirkung" wie die unrichtige, unvollständige oder unbefugte Verwendung von Daten darstellen. Hierunter sind v.a. Einwirkungen auf Hardware oder elektronische Impulse, die von aussen erfolgen, zu verstehen, bei welchen nicht unmittelbar in die Daten selbst eingegriffen wird[30].

2.2.3.5 Erschleichen einer Leistung (Art. 150 StGB)

Das Erschleichen einer Leistung stellt eine Handlung dar, die darauf abzielt, eine Leistung, die einem grösseren Publikum gegen Entgelt angeboten wird, durch unlauteres Verhalten unentgeltlich zu erlangen[31].

Im Zusammenhang mit der Computerkriminalität ist diese Bestimmung deswegen von Bedeutung, weil der sog. "Zeitdiebstahl" am Computer, d.h. die unentgeltliche Inanspruchnahme von Dienstleistungen einer Datenverarbeitungsanlage, die nur gegen Entgelt angeboten wird, unter diesen Tatbestand fällt[32]. Denkbare Beispiele wären das direkte Hantieren an einer Datenverarbeitungsanlage bzw. deren Eingabegeräten wie Terminals, Einlesegeräten oder Disketten- bzw. Magnetbandstationen. Eine weitere Möglichkeit läge darin, über Datenverarbeitungskanäle Zugang zur anvisierten Datenverarbeitungsanlage zu erhalten und diese alsdann im Online-Verfahren für eigene Zwecke arbeiten zu lassen[33].

---

29 TRECHSEL, Art. 147 N 6.

30 TRECHSEL, Art. 147 N 7; SCHMID, Computerkriminalität, § 7 N 77.

31 STRATENWERTH, § 16 N 50 ff.

32 Art. 150 Abs. 4 StGB.

33 SCHMID, Computerkriminalität, § 9 N 27.

2.2.3.6 Urkundenfälschung (Art. 251 i.V.m. Art. 110 StGB)

Gemäss Art. 110 Ziff. 5 StGB sind Urkunden Schriften oder Zeichen, die bestimmt und geeignet sind, eine Tatsache von rechtlicher Bedeutung zu beweisen. Die Aufzeichnung auf Bild- und Datenträgern steht der Schriftform gleich, sofern sie demselben Zweck dient. Als Datenträger kommen z.B. die Hard Disk, Disketten, Magnetbänder (z.B. bei gewöhnlichen Tonbandkassetten) oder Magnetstreifen auf irgendwelchen Codekarten in Frage. Bildträger hingegen sind vorab Filme oder andere Medien, auf denen Schriften oder Zeichen in stark verkleinerter Form, aber als Bild gespeichert werden. Um von einer Urkunde im strafrechtlichen Sinne sprechen zu können, sind – besonders bezogen auf Daten – folgende Voraussetzungen erforderlich:

- Menschliche Gedankenäusserung

  Der Urkundenbegriff erfordert die dauerhafte Verkörperung einer menschlichen Gedankenäusserung. Rein mechanische Aufzeichnungen sind keine Urkunden, sondern lediglich Augenscheinobjekte[34]. Auch Stammdaten (wie z.B. der Personal- oder Kundenbestand eines Unternehmens) und Eingabedaten (z.B. Ausrichtung einer Gehaltszulage an die in den Stammdaten figurierenden Arbeitnehmer) sind menschliche Gedankenäusserungen. Ebenso stellen automatisiert erarbeitete Ergebnisse (z.B. ein völlig automatisiert erstelltes Kontoblatt) menschliche Gedankenäusserungen dar, weil sie direkt oder indirekt durch menschliche Handlungen veranlasst sind.

- Erkennbarkeit des Ausstellers

  Anonyme Schriften, hinter denen keine erkennbare Person steht, geniessen nicht das erhöhte Vertrauen einer Urkunde. Die Erkennbarkeit des Ausstellers bei Dateneingaben ist grundsätzlich mit zwei Mitteln erreichbar:

  1. Elektronische bzw. digitale Signaturen können die Garantiefunktion des Ausstellers sachgerecht erbringen.

  2. Der Garantierende ergibt sich oft aus den mit der Datenverarbeitungsanlage verbundenen Umständen. Im Aussenverhältnis übernimmt in aller Regel der Betreiber der Datenverarbeitung des Unternehmens die Garantiefunktion, während der Verantwortliche im Innenverhältnis in der Regel ohne weiteres erkenn- oder mindestens ermittelbar ist. Es genügt also, wenn im Aussenverhältnis ersichtlich ist, aus welchem Unternehmen bzw. welcher Datenverarbeitungsanlage der fragliche Output stammt.

---

34 TRECHSEL, Art. 251 N 2; zum Begriff des Augenscheins vgl. hinten Ziff. 2.6.1.

- Perpetuierungsfunktion

  Eine traditionelle Schrifturkunde wird auf einer festen Unterlage verkörpert; sie ist für den künftigen Gebrauch somit dauernd haltbar. Versucht man Aufzeichnungen auf Bild- und Datenträgern festzuhalten, ergeben sich naturgemäss Schwierigkeiten, dieselbe "dauernde Erhaltbarkeit" zu bewerkstelligen, weil sich gewisse Datenregistrierungen leicht verändern lassen. Daher müssen die Daten durch spezielle Massnahmen gegen unbefugte Eingriffe besonders gesichert sein.

- Beweiseignung und Beweisbestimmung

  Nur jene Datenregistrierungen besitzen Urkundenqualität, welche bestimmt und geeignet sind, gerade die darin aufgezeichnete(n) Tatsache(n) zu beweisen. Beweiseignung ist grundsätzlich gegeben, wenn gesetzliche Bestimmungen oder die allgemeine Verkehrsübung einem Beweismittel die Geeignetheit ausdrücklich beimessen. In Frage dürften vorab die kaufmännische Buchführung sowie die datenverarbeitungsgemässe Abwicklung von Transaktionen im Bereich von Banken und ähnlichen Institutionen kommen. Darunter fallen z.B. auch die in Art. 15 des Börsengesetzes vorgeschriebenen Journale über getätigte Effektengeschäfte. Ferner sind elektronisch gespeicherte, öffentliche Register (Grundbuch, Zivilstands- und Handelsregister) als geeignete Beweismittel denkbar. Beweiseignung liegt weiter vor, wenn der Aussteller einer Codekarte oder anderer Ausweisschriften mit Datenträgern dem Inhaber mit dem Code die Berechtigung erteilt, die Karte absprachegemäss einzusetzen[35].

  Art. 251 StGB (Urkundenfälschung) stellt – im Zusammenhang mit dem vorhin erwähnten Urkundenbegriff – Fälschungshandlungen solcher Urkunden unter Strafe. Zu unterscheiden ist danach, ob der tatsächliche Aussteller der Urkunde dem angegebenen Aussteller entspricht, die Urkunde mithin "echt" ist oder eine "unechte" Urkunde vorliegt. Eine echte Urkunde kann nur insoweit Fälschungshandlungen unterliegen, als ihr Inhalt unwahr ist. Man spricht in solchen Fällen von einer Falschbeurkundung. Eine unechte Urkunde, d.h. eine solche, deren ersichtlicher Aussteller nicht ihr tatsächlicher Aussteller ist, kann hingegen durch verschiedene Massnahmen wie z.B. der gesamten Anfertigung eines falschen Inhaltes mit Fälschung von Unterschriften oder dem nachträglichen Einschieben von Worten (bzw. Daten) bei einer bereits von einem Dritten angefertigten Urkunde und weiteren Variationen gefälscht werden. Hier spricht man von einer Urkundenfälschung im engeren Sinne[36].

---

35 SCHMID, Computerkriminalität, § 3 N 34 ff.

36 REHBERG/ECKERT/FLACHSMANN, 189.

2.2.3.7 Denial of Service-Attacken

Denial of Service-Attacken (DoS-Attacken) stellen einfache, jedoch sehr effektive Angriffsmöglichkeiten auf den mit dem Internet verbundenen Computer dar. Der DoS-Täter setzt ein Programm in Gang, das einen Internet-Dienst durch überhöhten Datenverkehr zum Erliegen bringt (Überschwemmungstaktik) oder die betroffene Datenverarbeitungsanlage aufgrund eines Softwarefehlers in eine Endlos-Schlaufe leitet und abstürzen lässt (Torpedotaktik). Bei den genannten Vorgängen wird weder die Software noch die Hardware beschädigt, sondern vielmehr "nur" vorübergehend ausser Gefecht gesetzt. Werden für die DoS-Attacke mehrere Computer ("Agents") eingesetzt, spricht man von einer "Distributed Denial of Service"-Attacke. Für den Täter ist dieses Vorgehen günstig, weil er einerseits den behindernden Datenverkehr vervielfachen kann und andererseits Abstand von den die Attacke ausführenden Rechnern zu gewinnen und das Risiko der Rückverfolgung zu verkleinern vermag[37].

Die rechtliche Würdigung von DoS-Attacken legt eine Anwendung Art. 143bis StGB (Unbefugtes Eindringen in eine Datenverarbeitungsanlage) und Art. 144bis StGB (Datenbeschädigung) nahe. Art. 143bis StGB kann indessen kaum zur Anwendung gelangen, weil ein Eindringen in eine Datenverarbeitungsanlage, d.h. ein Durchbrechen von Zugangssperren, nicht stattfindet. Am ehesten lässt sich eine DoS-Attacke als Datenbeschädigung (Art. 144bis StGB) unter der Tathandlungsvariante des "Unbrauchbarmachens" gespeicherter oder übermittelter Daten betrachten[38].

2.2.4 Nicht spezifische Computerdelikte

Eine Reihe von weiteren strafrechtlichen Tatbeständen und in anderen Rechtsgebieten verankerten Bestimmungen kann im Zusammenhang mit Computern und Computernetzwerken von Unternehmen relevant sein, auch wenn sie die Betätigung eines Computers nicht voraussetzen und ebenso ohne einen solchen in strafbarer Weise begangen werden können.

---

37 WEBER/UNTERNÄHRER, Wirtschaftsterrorismus, 376. SCHWARZENEGGER, E-Commerce, 365 ff, hält bei DoSA die Strafnormen der Nötigung (Art. 181 StGB) und allenfalls der Störung von Betrieben, die der Allgemeinheit dienen (Art. 239 StGB), für anwendbar.

38 WEBER/UNTERNÄHRER, Wirtschaftsterrorismus, 378.

2.2.4.1 Verletzung von Immaterialgüterrechten

Immaterialgüterrechte kennzeichnen eine bestimmte Gattung von Eigentumsrechten, und zwar die Rechte des geistigen Eigentums. Immaterialgüterrechte stellen nach aktueller Lehre dem Eigentum nachgebildete, ausschliessliche und absolute Rechte dar. Sie bestehen positiv aus Handlungsbefugnissen und negativ aus Abwehrrechten, die sich gegen jedermann richten[39]. Darunter fallen im einzelnen Patentrechte, Markenrechte, Designrechte, Urheberrechte und weitere Rechte von geringerer Relevanz. Eine Verletzung solcher Rechte, z.B. durch das Abändern, das Vervielfältigen oder den gewerbsmässigen Gebrauch durch unberechtigte Dritte, kann strafrechtliche Sanktionen (Gefängnis, Busse) nach sich ziehen[40].

Um eine Verletzung von Immaterialgüterrechten durch Dritte durch Internetauftritte zu verhindern, drängt es sich auf, vor der Aufschaltung einer Website entsprechende Abklärungen zu treffen, sich die für die Website erforderlichen Rechte möglichst zu sichern und gegebenenfalls auch Schutzrechte anzumelden[41]. Erschwerend kommt die Tatsache hinzu, dass der Bestand von Urheberrechten registermässig nicht überprüft werden kann, weil es im schweizerischen Urheberrechtsgesetz kein materielles Prüfungsverfahren gibt, das die urheberrechtliche Schützbarkeit festlegt. Der Bestand eines Urheberrechts hängt somit nicht von der Erfüllung bestimmter Formalitäten wie z.B. einem Copyright-Zeichen (©) ab[42].

2.2.4.2 Unlauterer Wettbewerb

Das Bundesgesetz über den unlauteren Wettbewerb (UWG) bezweckt den Schutz der Wettbewerbsteilnehmer vor unlauterem oder verfälschendem Wettbewerb. Als "unlauter" wird in der Regel ein Geschäftsverhalten bezeichnet, das in gegen Treu und Glauben verstossender Weise das Verhältnis zwischen Mitbewerbern oder zwischen Anbietern und Abnehmern beeinflusst, so auch Befugnisse der Wirtschaftsteilnehmer in unfairer Weise missbraucht[43]. Das UWG umschreibt ein Reihe von Fällen, die als unlauter betrachtet werden können, z.B. unlautere Werbe- und Verkaufsmethoden, die Verleitung zur Vertragsverletzung oder -auflösung, die Verwertung fremder Leistungen, die Verletzung von Fabrikations- und Geschäftsgeheimnissen, die Nichteinhaltung von Arbeitsbedingungen oder die Verwendung missbräuchlicher Geschäftsbedingungen (Art. 3 - 8 UWG). Eine Verletzung von Lauterkeitsnormen ist gemäss Art. 23 UWG in

---

39 RIEMER, § 13 N 298; REHBINDER, Urheberrecht, N 1 f.

40 Art. 81 ff PatG; Art. 61 MSchG, Art. 41 ff DesG, Art. 67 ff URG.

41 KIKINIS, 223.

42 BARRELET/EGLOFF, Art. 29 N 3.

43 VON BÜREN/MARBACH, 191 f, 200 f.

Bezug auf die Grundtatbestände strafrechtlich relevant, nicht aber die Generalklausel von Art. 2 UWG. Der vorsätzlich unlauter handelnde Wettbewerbsteilnehmer kann auf Antrag mit Gefängnis oder Busse bestraft werden.

Zur Behebung unlauterer Angriffstaktiken bedarf es allerdings nicht der sofortigen Einschaltung von Juristen. Aus dem Blickwinkel der Öffentlichkeit verlängert ein Prozess die Krise, denn ein rechtliches Vorgehen löst in vielen Fällen eine Abwehrhaltung aus. Die Presse empfindet zudem oft für kleinere Prozessparteien mehr Sympathie als für Grossunternehmen. Es ist sinnvoll zuerst herauszufinden, wer der Gegner ist und was er wirklich will. Erst dann soll versucht werden, durch Verhandlungen den Streit beizulegen. Falls dies nicht gelingt, empfiehlt es sich schliesslich, die notwendigen rechtlichen Schritte einzuleiten[44].

2.2.4.3 Verletzung von Schweigepflichten (Geheimnisschutznormen)

Schweigepflichten sind Normen, welche die in einem öffentlichen Interesse liegende vertrauliche Behandlung gewisser Informationen gewährleisten. Die Verletzung solcher Geheimnispflichten durch Preisgabe von vertraulichen Informationen an einen unwissenden Dritten wird in Art. 320 StGB (Verletzung des Amtsgeheimnis) und Art. 321 StGB (Verletzung des Berufsgeheimnisses) unter Strafe gestellt. Art. 321 StGB (Verletzung des Berufsgeheimnisses) zählt mehrere Berufsgattungen auf, die sich durch die Schweigepflicht auszeichnen. Darunter fallen namentlich Geistliche, Rechtsanwälte, Verteidiger, Notare, zur Verschwiegenheit verpflichtete Revisoren, Ärzte, Zahnärzte, Apotheker, Hebammen sowie Hilfspersonen, denen infolge ihrer Anstellung ein Berufsgeheimnis offenbart worden ist. Dem Amtsgeheimnis (Art. 320 StGB) unterstehen Beamte und Behördenmitglieder.

Die Verletzung des Amts- oder Berufsgeheimnisses ist auch nach Beendigung des amtlichen Verhältnisses bzw. Arbeitsverhältnisses strafbar[45].

---

44 JANAL, Internet-Sicherheit für Unternehmen, 193 f.

45 Art. 320 Ziff 1. Abs. 2, Art. 321 Ziff. 1 Abs. 3 StGB.

Art. 162 StGB schützt das Fabrikations- oder Geschäftsgeheimnis. Darunter fallen z.B. Bezugsquellen von Waren, Werbekonzepte oder die Organisation eines Betriebes, Herstellungsverfahren und Konstruktionspläne, die nicht offenkundig oder allgemein zugänglich sind. Vorausgesetzt wird, dass der Täter dieses Geheimnis infolge einer gesetzlichen oder vertraglichen Pflicht hätte bewahren sollen. Bei Arbeitsverträgen statuiert z.B. Art. 321a Abs. 4 OR sowie bei Aufträgen Art. 398 (Sorgfaltspflicht bei der Erfüllung von Aufträgen) eine Geheimhaltungspflicht. Im Falle anderer Vertragsverhältnisse muss eine solche Geheimhaltungspflicht ausdrücklich oder zumindest sinngemäss vereinbart werden. Offenbart der Täter ein Fabrikationsgeheimnis an einen beliebigen Dritten, macht er sich im Sinne von Art. 162 StGB strafbar[46].

2.2.4.4 Pornographie (Art. 197 StGB)

Der Begriff Pornographie bezeichnet Darstellungen oder Darbietungen grob sexuellen Inhalts[47]. Wer pornographische Schriften, Ton- oder Bildaufnahmen, Abbildungen, andere Gegenstände solcher Art oder pornographische Vorführungen einer Person unter 16 Jahren anbietet bzw. öffentlich ausstellt, macht sich gemäss Art. 197 Ziff. 1 StGB strafbar. Eine öffentliche Präsentation für erwachsene Personen ist hingegen straflos, wenn die Besucher im Voraus auf den pornographischen Charakter hingewiesen werden[48]. Ein effizienter Jugendschutz wie auch der rechtlich erforderliche Hinweis pornographischer Inhalte an die Öffentlichkeit, kann durch plakative Warnungen bewerkstelligt werden, bei denen nach dem Durchlesen der Information die Wahl zwischen einer "ENTER"- und einer "EXIT"-Taste zur Verfügung steht[49]. Ob eine Enter/Exit-Zugangskontrolle genügt oder eine weitergehende Alterskontrolle erfolgen muss, ist derzeit in der Schweiz noch nicht gerichtlich entschieden.

---

46 REHBERG/ECKERT/FLACHSMANN, Tafeln, 117. Die Verletzung von Schweigepflichten kann gemäss Art. 320, 321 oder 162 StGB nur in vorsätzlicher Weise begangen werden. Der Täter muss somit vom Geheimnischarakter wissen und die Offenbarung der Informationen an Aussenstehende wollen. Die fahrlässige Verletzung von Schweigepflichten ist strafrechtlich zwar nicht relevant, kann jedoch auf vertragsrechtlicher Ebene durchaus eine Sorgfaltspflichtverletzung darstellen und Schadenersatzforderungen aus unsorgfältiger Vertragserfüllung mit sich ziehen. Das einen Auftrag (Art. 394 ff OR) kennzeichnende Vertrauensverhältnis z.B. erfordert meist Diskretions- und Geheimhaltungspflichten, die im Gegensatz zum Strafrecht bereits mit leichter Fahrlässigkeit verletzt werden können (vgl. OR-WEBER, Art. 398 N 11).

47 TRECHSEL, Art. 197 N 4.

48 Art. 197 Ziff. 2 Abs. 2 StGB.

49 WIDMER/BÄHLER, 295. Zur Pflicht des Arbeitgebers, den unerwünschten Empfang pornographischer E-Mails bei Arbeitnehmern zu verhindern, vgl. hinten Ziff. 2.3.1.4.

Ein übermässiger und daher auffälliger Konsum von pornographischen Inhalten über das Internet durch einen Mitarbeiter muss nicht per se ein Problem darstellen. Doch kann ein solches Verhalten im Sinne der "Gefährdungsanalyse"[50] möglicherweise als "red flag"-Gefährdungsindikator auffallen und ein genaueres Augenmerk auf den Mitarbeiter erfordern. Der Konsum sollte zudem nur in dem Mass erfolgen, solange die ordnungsgemässe Arbeitsverrichtung ungehindert ihren Fortgang nehmen kann; ansonsten sind von Seiten des Arbeitgebers Sanktionen durchaus als legitim zu erachten[51].

2.2.4.5 Unerlaubte Glücksspiele

Glücksspiele dienen der Befriedigung von Spiellust und Spekulation. Die übermässige Teilnahme eines Mitarbeiters an solchen Spielen kann – wie bereits beim Konsum von pornographischen Inhalten erwähnt – einen "red-flag"-Gefährdungsindikator darstellen, welcher eine erhöhte Beobachtung des Arbeitnehmers zu rechtfertigen vermag. Gleichfalls sollte die Teilnahme an solchen Spielen nur in dem Mass erfolgen, solange die ordnungsgemässe Arbeitsverrichtung ungehindert ihren Fortgang nehmen kann; ansonsten erscheinen Sanktionen von Seiten des Arbeitgebers als legitim. Die derzeit in den USA geführte Diskussion, ob der Arbeitgeber die Pflicht hat, den Arbeitnehmer vom übermässigem Spielkonsum in schützender Weise abzuhalten, beurteilt sich nach den persönlichkeitsrechtlichen Regeln[52].

Glücksspiele sind verschiedenartig gestaltbar und unterliegen unterschiedlichen Rechtsgrundlagen. Die gesetzliche Ordnung gewährleistet sowohl präventive als auch nachträgliche Rahmenbedingungen zum Schutze des Bürgers vor einer Spiel- und Verschwendungssucht.

a) Präventiver Schutz

Verschiedene Gesetze versuchen den Bürger in präventiver Weise vor einer Verleitung zu exzessiver Spiel- und Verschwendungssucht zu schützen. Die präventiven Schutznormen verbieten bzw. regulieren das Zustandekommen von öffentlichen Spielinstituten. Dadurch soll die potentielle Gefahr für das Abhalten von Spielen bereits in einem Anfangsstadium eingeschränkt werden.

Unternehmen, die Spiele betreiben bei denen gegen Leistung eines Geldeinsatzes ein Gewinn in Aussicht gestellt wird, welcher vorwiegend vom Zufall abhängt (Glücksspiele), unterliegen dem Bundesgesetz über Spielbanken (SBG). Als Glücksspiel gilt das Betreiben von Spielautomaten und ähnlichen Apparaten (Art. 3 Abs. 1 SBG). Online-Spielbanken bestehen schon seit längerer Zeit und unterliegen denselben rechtlichen Bestimmungen wie gewöhnliche Spielbanken. Das Errichten und Betreiben von Spielbanken erfordert eine Standort- und Betriebskonzession durch den Bundesrat (Art. 10

---

50 Vgl. hinten Ziff. 3.1.2.

51 Zur aufgeworfenen Frage, ob der Arbeitgeber die Pflicht trägt, den Arbeitnehmer vor Pornographie (z.B. pornographischen Mails) zu schützen, sei auf die Darstellung des Persönlichkeitsschutzes im Arbeitsverhältnis verwiesen (vgl. hinten Ziff. 2.3.1.4).

52 Vgl. hinten Ziff. 2.3.1.4.

und Art. 16 SBG). Weil ein rechtlicher Anspruch auf eine Konzession gegenüber dem Staat grundsätzlich nicht besteht, ist der Entscheid des Bundesrates auch nicht anfechtbar (Art. 16 SBG).

Lotterien (Veranstaltungen, bei denen gegen Leistung eines Einsatzes ein vermögensrechtlicher Vorteil als Gewinn in Aussicht gestellt wird, über dessen Erwerb planmässig durch Zufall entschieden wird[53]), sind nach dem Lotteriegesetz (LG) grundsätzlich verboten. Ausnahmen gelten für Tombolas (Lotterien, die an öffentlichen Anlässen durchgeführt werden) und Lotterien zu gemeinnützigen Zwecken (Art. 2 Abs. 1 LG, Art. 5 ff LG). Ob solche Ausnahmen im Internet Anwendung finden können, ist bei der Abhaltung von Tombolas eher zu verneinen, weil trotz gleichzeitigen schriftlichen Kommunikationsmöglichkeiten im Internet (Chats) ein direkter Zusammenhang zwischen der Abgabe von Losen und dem veranstalteten Chat nicht besteht. Die Abhaltung von Lotterien zu gemeinnützigen oder wohltätigen Zwecken erscheint hingegen auch über das Internet denkbar.

b) Nachträglicher Schutz

Falls eine Person an einem Spiel oder einer Wette dennoch teilgenommen hat, ergänzt die Rechtsordnung die Stellung von Spielteilnehmern durch einen nachträglichen Rechtsschutz. Die aus Wette und Spiel resultierenden Rechtsverhältnisse begründen zwar Forderungen, doch sind diese gemäss Art. 513 OR nicht durchsetzbar, weil der Staat den Rechtsschutz verweigert (Naturalobligation)[54]. Dies hat für den Veranstalter zur Folge, dass er seine Ansprüche aus Glücksspielen zivilrechtlich auf dem Wege einer Klage oder direkten Betreibung nicht zu realisieren vermag.

Innerhalb eines Unternehmens kann es sich als sinnvoll erweisen, die Mitarbeiter über die fehlende Einklagbarkeit von Spielforderungen zu informieren. Bei fehlender Kenntnis dieses Umstandes könnten sich bestimmte Mitarbeiter nämlich durch hohe Spielschulden genötigt sehen, verbotenerweise in die Kasse des Unternehmens zu greifen. Eine Information über die entsprechenden Rechtsgrundlagen stellt somit zugleich eine präventive Massnahme dar[55].

---

53 Art. 1 Abs. 2 LG (Lotteriegesetz).

54 HUGUENIN, 126.

55 Zur Pflicht des Arbeitgebers, den Arbeitnehmer vom übermässigem Spielkonsum abzuhalten, vgl. hinten Ziff. 2.3.1.4.

2.2.4.6 Überwachung

a) Überwachungshandlungen nach Art. 179 StGB

Die Art. 179 StGB folgenden Strafbestimmungen schützen den Geheim- oder Privatbereich. Mit Strafsanktionen versehen sind z.B. die Verletzung des Schriftgeheimnisses, das Abhören und Aufnehmen fremder Gespräche, das Inverkehrbringen und Anpreisen von Abhör-, Ton- und Bildaufnahmegeräten sowie das unbefugte Beschaffen von besonders schützenswerten Personendaten. Gemäss Art. 179^{quinquies} StGB sind die betroffenen Handlungen jedoch nicht strafbar, wenn für Hilfs-, Rettungs- und Sicherheitsdienste Notrufe aufgezeichnet werden. Diese Regelung trägt dem Umstand Rechnung, dass die systematische Aufzeichnung der bei Ambulanzzentralen, Polizei, Feuerwehr usw. eingehenden Notrufe unabdingbar ist, um eine rasche und wirkungsvolle Intervention sicherzustellen.

Ebenso ist die amtliche Überwachung in Ausübung ausdrücklicher, gesetzlicher Befugnisse (z.B. von Polizeibeamten) nicht strafbar, wenn unverzüglich die Genehmigung eines zuständigen Richters eingeholt wird (Art. 179^{octies} StGB). Die Einzelheiten der Überwachung durch staatliche Behörden finden sich im BÜPF. Das Gesetz regelt die Überwachung des Post- und Fernmeldeverkehrs im Rahmen eines Strafverfahrens des Bundes oder eines Kantons.

b) Überwachung im Arbeitsverhältnis

Überwachungsmassnahmen von Seiten des Unternehmens gegenüber seinen Arbeitnehmern sind durch die heutige Elektronik leicht zu handhaben. In Frage kommen die Überwachung des E-Mail-Verkehrs und der Internetnutzung, Nutzung des Intranets, Nutzung des internen und externen Telefonverkehrs oder die Installation von Videokameras im Büro. Überwachungs- und Kontrollsysteme, die nicht der Sicherheit oder der Erfassung der Arbeitsleistung dienen, sondern vornehmlich die Absicht verfolgen, das Verhalten der Arbeitnehmer am Arbeitsplatz zu überwachen, sind gemäss Art. 26 der Verordnung 3 zum Arbeitsgesetz verboten. Zwar dürfen externe Daten wie z.B. das Datum und die Zeit eines abgeschickten E-Mails eines Mitarbeiters eingesehen werden, hingegen dürfen die Inhalte seiner E-Mails nicht gelesen werden.

Daher wird der Arbeitnehmer in der Regel ein eigenes E-Mail-Konto für private Zwecke haben. Anonym durchgeführte Kontrollen sind bei konkreten Verdachtsmomenten hingegen ohne vorherige Ankündigung zulässig[56]. Als anerkannte Gründe für die Überwachung von Mitarbeitern gelten unter anderem:

- Kontrolle der Einhaltung des Verbots privater Telefongespräche, privater E-Mails oder des Surfens im Internet zu privaten Zwecken.

- Kontrollen aus Sicherheitsgründen (z.B. Kontrolle von E-Mails zum Fernhalten von Viren, Spamming-Mails und Pornographie).

Weitergehende Überwachungsmassnahmen des E-Mail- oder Telefonverkehrs sind mit arbeitsvertraglicher Einwilligung der Arbeitnehmer – wie in vielen Grossunternehmen der Fall – zulässig.

Überwachungsmassnahmen von Arbeitnehmern werfen auch datenschutzrechtliche Fragen auf. Der Arbeitgeber darf Daten über seine Mitarbeiter nur bearbeiten, soweit dies zur Durchführung des Arbeitsverhältnisses notwendig ist (Art. 328b OR). Unter "Bearbeiten" versteht das Datenschutzgesetz das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten unabhängig von den angewandten Mitteln und Verfahren (Art. 3 lit. e DSG). Eine Erfassung von Mitarbeiterdaten aus "Neugier" oder "Interesse" ist unzulässig[57].

Ergänzend zu den erwähnten Rechtsnormen hat der Eidgenössische Datenschutzbeauftragte einen Leitfaden über die Internet- und E-Mail-Überwachung am Arbeitsplatz für öffentliche Verwaltungen und für die Privatwirtschaft publiziert. Dieser Leitfaden legt unter anderem die wichtigsten Voraussetzungen wie auch zulässigen Sanktionen gegen missbräuchliche Verhaltensweisen der Arbeitgeber dar[58].

---

56 REHBINDER, Arbeitsrecht, 233; ROSENTHAL, 361; WEBER, E-Commerce, 28 ff; S.a. SCHWARZENEGGER, FS Trechsel, 319, FN 65 (die Cybercrime Convention verlangt von den Signatarstaten den Schutz des Fernmeldegeheimnisses auch im Arbeitsverhältnis).

57 ROSENTHAL, 361.

58 Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz, www.edsb.ch/d/themen/internet/index.htm.

2.2.4.7 Rassendiskriminierung (Art. 261bis StGB)

Art. 261bis StGB verbietet das Ausrufen oder öffentliche Verbreiten rassistischer Inhalte oder Ideologien, die gröbliche Verharmlosung oder Rechtfertigung von Völkermord oder anderen Verbrechen gegen die Menschlichkeit sowie die Verweigerung von für die Allgemeinheit bestimmten Leistungen gegenüber Personen gestützt auf rassistische Motive. Als rassistisch sind grundsätzlich diskriminierende oder verleumderische Auffassungen gegenüber einer bestimmten Rasse, Ethnie oder Religion zu verstehen[59]. Rassistische Inhalte sind im Intranet eines Unternehmens wie auch im Internet oder E-Mail- Verkehr problemlos austauschbar.

Ein öffentlicher Aufruf oder eine öffentliche Verbreitung liegt dann vor, wenn ein grösserer, nicht durch persönliche Beziehungen zusammenhängender Personenkreis, der auch zufällig wahrnehmende Personen umfassen kann, die betreffenden Informationen wahrnimmt[60].

59 Allgemein zum Rassendiskriminierungstatbestand vgl. TRECHSEL, Art. 261bis N 6, 10 ff.

60 Eine rassistische Information über die Qualität eines IT-Mitarbeiters oder über einen (auch erfolglosen) Hacker auf der Homepage des betroffenen Unternehmens wäre deshalb unzulässig.

2.2.5 Ausnahmen von der Strafbarkeit

Die Erfüllung eines strafrechtlichen Tatbestandes stellt grundsätzlich die Verletzung einer Norm dar. Hingegen ist es möglich, dass ein solches Verhalten von der Rechtsordnung nicht bestraft wird, wenn gewisse Rahmenbedingungen vorliegen. In Frage kommen Rechtfertigungsgründe für eine Straftat, welche die Rechtswidrigkeit einer Tat oder das Fehlen der Schuldfähigkeit eines Täters wie z.B. die Zurechnungsunfähigkeit aufheben.

2.2.5.1 Gesetzliche, amtliche oder berufliche Pflichten

Verschiedene Normen auferlegen gewissen Beamten oder Berufsangehörigen Pflichten, die einzelne strafrechtlich an sich relevante Handlungen rechtfertigen können. Zu denken ist beispielsweise an den Waffeneinsatz von Polizeibeamten oder die Einhaltung von Rechtssätzen, welche den zur Wahrung von Berufsgeheimnissen Verpflichteten vorschreiben, gewisse bei ihrer Tätigkeit festgestellte strafbaren Handlungen (z.B. § 15 des zürcherischen Gesundheitsgesetzes) oder Suchtveranlagungen (vgl. Art. 14 Abs. 4 SVG) zu melden.

2.2.5.2 Agent Provocateur

Ein Agent Provocateur ist strafrechtlich betrachtet ein Anstifter (Art. 24 StGB). Grundsätzlich ist ein Anstifter, d.h. jemand, der die Begehung eines Verbrechens bei einer anderen Person auslöst, ebenso strafbar wie der Täter. Im Falle des Agent Provocateur liegt hingegen eine Person vor, deren Verhalten darauf ausgeht, die von ihm zu strafbarem Verhalten bestimmte Person beim Deliktsversuch zu überführen. Weil in dieser Konstellation das Ziel gerade darin besteht, keine Straftat zu verursachen, bleibt eine solche Anstiftung straflos[61].

61 REHBERG/DONATSCH, Strafrecht I, 126.

Anders hingegen ist ein "Agent Provocateur" zu beurteilen, der Angestellter einer Strafverfolgungsbehörde ist (sog. Undercover Agents, V-Leute). Die Grenzen der Zulässigkeit solcher Vorgehensweisen durch Polizeibeamte sind strafrechtlich und strafprozessual umstritten, weil sie dem Grundsatz des "fair trial" widersprechen[62].

2.2.5.3 Notwehr und Notstand

Notwehr (Art. 33 StGB) und Notstand (Art. 34 StGB) stellen allgemeine Normen dar, welche strafrechtlich an sich relevante Handlungen rechtfertigen können, die zur Abwendung von besonderen Gefahren eingesetzt werden. Das Gesetz erklärt Tathandlungen als straflos, welche von durch diese Bedrohungslagen gefährdeten Personen in verhältnismässiger Weise begangen wurden. Das Vorliegen solcher Situationen und die Verhältnismässigkeit der getroffenen Schutzmassnahmen müssen in jedem Fall individuell beurteilt werden[63].

---

62 SCHMID, Strafprozessrecht, 68. Der beim Hackertatbestand erwähnten „Honeypot“ (vgl. vorne Ziff. 2.2.3.2) unterscheidet sich vom Agent Provocateur wie folgt: Für eine Anstiftung i.S.v. Art. 24 StGB ist ein Dreiparteienverhältnis zwischen Anstifter, Angestiftetem (d.h. dem eigentlichen Täter) und Opfer erforderlich. Strafgrund für den Anstifter (den Agent Provocateur) ist die Erweckung eines Tatentschlusses beim Angestifteten, ein Opfer zu schädigen. Die „Honeypot“-Konstellation stellt hingegen ein Zweiparteienverhältnis zwischen dem Unternehmen, welches die „Honeypots“ in der eigenen Computerinfrastruktur einsetzt, und dem Täter dar. Eine Anstiftungskonstellation liegt mithin nicht vor. Zudem muss zwischen einem anstiftenden Verhalten und der gestützt darauf verübten Tat ein logischer Kausalzusammenhang bestehen. Der Hacker dringt jedoch nicht in ein Datensystem ein, weil „Honeypots“ eingerichtet wurden, sondern weil ihn die Versuchung reizt. Der Honeypot selbst stellt lediglich eine Abfangvorrichtung dar, welche die Bestrebungen des Hackers auf eine ungefährliche Ebene umleitet.

63 Vgl. vorne Ziff. 2.2.3.2.

2.3 Persönlichkeits- und Datenschutzrecht

2.3.1 Persönlichkeitsrecht

2.3.1.1 Begriff

Der Begriff des Persönlichkeitsschutzes umfasst sämtliche Rechtsnormen, welche personenbezogene Rechtsgüter wie z.B. die körperliche und die psychische Integrität, die Freiheit, die Ehre (d.h. den Ruf und das Ansehen) und das Privatleben bzw. die Intimsphäre schützen (Art. 28 ff ZGB)[64]. Die angesprochenen Rechtsgüter sind im elektronischen Informationsaustausch – infolge der teilweise technisch mangelhaften Datensicherheit – potentiell gefährdet. Über das Internet werden zum Teil grosse Mengen an privaten oder intimen Gedanken ausgetauscht. Provider sammeln beispielsweise Daten aus E-Mails und verwalten die zugehörigen Accounts. Daher kann ein E-Mail Benutzer direkt gegen einen Provider persönlichkeitsrechtlich vorgehen, wenn er die Inhalte oder Adressaten seiner E-Mails unrechtmässig verwendet[65].

Eine widerrechtliche Persönlichkeitsverletzung liegt grundsätzlich nur vor, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder eine Gesetzesbestimmung gerechtfertigt ist (Art. 28 Abs. 2 ZGB).

2.3.1.2 Spamming

Eine weiteres Internet-Problem, das ein persönlichkeitsrechtliches Vorgehen nahe legt, ist das "Spamming", d.h. das unaufgeforderte Zusenden von Werbung. Das Spamming kann dann erheblich negative Wirkungen haben, wenn ein E-Mail-Nutzer mit Werbung geradezu überhäuft und dadurch belästigt wird. Übermässige und unaufgeforderte E-Mail-Werbung vermag eine Persönlichkeitsverletzung gemäss Art. 28 ZGB zu verursachen, wenn der fehlende Empfangswille des Empfängers unbeachtet bleibt. Der mutmassliche Wille des Adressaten, keine Nachrichten empfangen zu müssen, reicht grundsätzlich bereits aus[66]. Die Spamming-Problematik hat auch in der parlamentarischen Debatte über die im Gange befindliche Totalrevision des Fernmeldegesetzes (FMG) Spuren hinterlassen. Der neu vorgesehene Art. 45a FMG fordert von Fernmeldedienstanbietern Sicherungsmassnahmen, welche die Übermittlung von unaufgeforderten Werbemitteilungen an Kunden verhindern, die dazu nicht ihre ausdrückliche Zustimmung gegeben haben. Hiermit würde eine Abkehr vom ursprünglichen Opt-out-Modell, gemäss welchem die Kunden mittels eines Vermerks im Telefonbuch anzeigen müssen, dass sie keine Werbemitteilungen empfangen möchten, zum Opt-in-Modell, welches

---

64 RIEMER, § 13 N 335 ff.

65 ROSENTHAL, 26.

66 SENN, Werbung mit E-Mails, sic! 2002, 91.

den Versand von Werbemitteilungen grundsätzlich von einer Einwilligung der Kunden abhängig macht, vollzogen. Im derzeitigen Vernehmlassungsverfahren findet die vorgeschlagene Bestimmung keinen positiven Nachhall. Verschiedene Unternehmensverbände bemängeln die undifferenzierte Anwendbarkeit der Bestimmung auf sämtliche Telekommunikationsdienste (Telefon, Fax, SMS und E-Mail) und stellen die Umsetzbarkeit einer solchen Kontrolle durch die Fernmeldedienstanbieter in Frage. Eine Neu-Akquisition von Kunden mit den Mitteln der Telekommunikation würde mit einer Opt-in-Regelung zudem erschwert. Ob diese Einwände im Parlament wegen einer möglichen Benachteiligung gegenüber anderen Kommunikationsdiensten (wie etwa der Post, der bisher keine vergleichbare Pflicht auferlegt worden ist) Gehör finden, lässt sich schwer prognostizieren[67].

2.3.1.3 Namensanmassung

Die Persönlichkeit umfasst auch das Recht auf einen Namen. Wird jemandem die Führung seines Namens bestritten oder erfolgt eine Namensanmassung, liegt eine Persönlichkeitsverletzung vor (Art. 29 ZGB). Wer heute Standard-E-Mail-Programme benützt, kann nicht sicher sein, wer der Absender ist, denn es ist relativ leicht, die Anschlusskennung und das Passwort zu fälschen. Ein Konkurrent kann eine falsche Adresse bewusst verwenden und z.B. rassistische oder sexistische Bemerkungen verschicken, mit der möglichen Folge, dass die Empfänger wegen Abneigung einen Boykott gegen das vermeintlich betroffene Unternehmen organisieren[68].

---

67 Vgl. Stellungnahmen zur geplanten Revision des Fernmeldegesetzes und seiner Ausführungsbestimmungen von CALLNET (Branchenverband der Schweizer Call Center Betreiber) und ECONOMIESUISSE. Beide Verbände verweisen zudem auf die vom Schweizerischen Direktmarketingverband (SDV) ins Leben gerufene „Robinsonliste". Privatpersonen, welche keine adressierte Werbung mehr in ihrem Briefkasten erhalten wollen, können sich in diese Datenbank eintragen lassen. Sämtliche SDV-Mitglieder haben sich einem Ehrenkodex verpflichtet, Personen der Robinsonliste nicht mit adressierter Werbung zu beliefern.

68 JANAL, Internet-Sicherheit für Unternehmen, 24.

Soweit nicht bei Unternehmen, die im Handelsregister eingetragenen sind, der firmenrechtliche Schutz greift, kommt ein persönlichkeitsrechtliches Vorgehen gestützt auf Art. 29 ZGB wegen Namensanmassung in Betracht[69]. Zur Verbesserung der Informationssicherheit eines Unternehmens sollten neben dem rechtlichen Vorgehen wegen Namensanmassung auch technische Schutzmassnahmen bereitgestellt werden, welche eine Authentifizierung des Geschäftspartners ermöglichen. Eine zuverlässige Authentifizierung kann mittlerweile in Deutschland, nicht aber in der Schweiz durch öffentlich anerkannte Zertifizierungsdienste bewerkstelligt werden[70].

2.3.1.4 Persönlichkeitsrecht im Arbeitsrecht

Das Arbeitsvertragsrecht konkretisiert den Schutz der Persönlichkeit im Rahmen von Arbeitsverhältnissen. Der Arbeitgeber hat die Persönlichkeit des Arbeitnehmers zu achten und zu schützen, auf dessen Gesundheit gebührlich Rücksicht zu nehmen und für die Wahrung der Sittlichkeit zu sorgen (Art. 328b OR).

Eine widerrechtliche Persönlichkeitsverletzung liegt grundsätzlich nur vor, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch eine Gesetzesbestimmung gerechtfertigt ist (Art. 28 Abs. 2 ZGB)[71].

Besondere Rahmenbedingungen sind arbeitsrechtlich bei Überwachungs- und Durchsuchungshandlungen zu beachten[72].

---

69 WEBER, E-Commerce, 153 ff. Auf die Unlauterkeit des Vorganges der Namensanmassung und Versendung von E-Mails mit gefälschten Adressen wird an dieser Stelle nicht eingegangen. Namensanmassungen im technischen Sinne werden oft für strafrechtlich relevante Betrugshandlungen eingesetzt.

70 JANAL, Internet-Sicherheit für Unternehmen, 25; vgl. auch hinten Ziff. 2.3.3.1.

71 Vgl. vorne Ziff. 2.2.4.6 b) und hinten Ziff. 2.3.2.

72 Vgl. für Einzelheiten vorne Ziff. 2.2.4.6 b), hinten Ziff. 2.3.2. und Kapitel 4.

Im Hinblick auf die Durchsuchung von Schubladen oder privaten Taschen der Mitarbeiter sind persönlichkeitsrechtliche Schranken zu beachten, weil bei der Suche private und intime Gegenstände gefunden werden können. Eine vertragliche Einwilligung des Mitarbeiters zu solchen Durchsuchungsmassnahmen, sofern im Rahmen der Ungültigkeit von übermässigen Bindungsverträgen (Art. 27 ZGB) überhaupt zulässig, vermag gegebenenfalls Abhilfe zu leisten[73]. Weiter können Erfordernisse des Arbeitsverhältnisses (Art. 328 Abs. 2 OR) es rechtfertigen, teilweise Schränke oder Schubladen öffnen zu müssen. Eine weiter zu beachtende Rahmenbedingung stellt das strafrechtlich geschützte Schriftgeheimnis (Art. 179 StGB) dar, welches grundsätzlich verbietet – falls eine besondere Berechtigung nicht vorliegt – eine fremde Schrift zu öffnen. Private Briefe dürfen daher vom Arbeitnehmer nicht geöffnet werden[74].

73 Eine vertragliche Einwilligung in die Kontrolle zu jeder Zeit von privaten Taschen hält vor Art. 27 ZGB kaum stand. Anders zu beurteilen ist hingegen eine Einwilligung in die Kontrolle von Schränken und Schubladen, weil es dem Arbeitnehmer zumutbarer erscheint, persönliche (bzw. verdachtserregende) Gegenstände vom Arbeitsplatz fernzuhalten.

74 Eine Ausnahme statuiert BGE 114 IV 17 insofern, als an das Unternehmen adressierte Briefe mit dem Zusatzvermerk „zu Handen von“ als nicht privat zugestellte Briefe gelten und daher vom Vorgesetzten geöffnet werden dürfen. Zur strafrechtlichen und persönlichkeitsrechtlichen Würdigung von weiteren Überwachungsmassnahmen vgl. vorne Ziff. 2.2.4.6.

2.3.1.5 Klagerechte

Dem Kläger stehen verschiedene Möglichkeiten zur Verfügung, gegen Persönlichkeitsverletzungen vorzugehen. Er kann

- eine drohende Verletzung verbieten (Unterlassungsklage, Art. 28a Abs. 1 Ziff. 1 ZGB).
- beantragen, eine bestehende Verletzung zu beseitigen (Beseitigungsgklage, Art. 28a Abs. 1 Ziff. 2 ZGB).
- beantragen, die Widerrechtlichkeit einer Verletzung festzustellen, wenn sich diese weiterhin störend auswirkt (Feststellungsklage, Art. 28a Abs. 1 Ziff. 3 ZGB).
- verlangen, dass eine Berichtigung oder das Urteil Dritten mitgeteilt oder veröffentlicht wird (Urteilsveröffentlichung, Art. 28a Abs. 2 ZGB).
- vorsorgliche Massnahmen verlangen. Darunter wird ein Vorgehen verstanden, durch welches Rechtsverletzungen vorsorglich durch einstweilige Verfügungen verboten oder beseitigt werden, bevor eine richterliche Entscheidung stattgefunden hat. Vorausgesetzt wird in diesem Fall der Nachweis einer zeitlichen Dringlichkeit, die Glaubhaftmachung einer Rechtsverletzung und die Verhältnismässigkeit der vorsorglichen Massnahme gegenüber der drohenden oder bereits eingetretenen Rechtsverletzung (vgl. z.B. § 227 Zürcher ZPO). Falls sich die vorsorglichen Massnahmen jedoch als unbegründet erweisen, schuldet der Gesuchsteller für den beim vorsorglich Eingeklagten verursachten Schaden einen Ersatz.
- sofern durch eine Persönlichkeitsverletzung ein finanziell nachweisbarer Schaden entstanden ist, auf Schadenersatz und Genugtuung klagen sowie die Herausgabe des Gewinns einleiten (Art. 28a Abs. 3 ZGB).
- sofern eine Persönlichkeitsverletzung durch Beiträge in periodisch erscheinenden Medien stattgefunden hat, eine Gegendarstellung beantragen, d.h. ein in knapper Form auf den Gegenstand der beanstandeten Darstellung verfassten Text publizieren lassen (Art. 28g ff ZGB).

2.3.2 Datenschutzrecht

Das Datenschutzgesetz (DSG) konkretisiert den Persönlichkeitsschutz im Bereich des Bearbeitens von personenbezogenen Daten. Es enthält Grundsätze für Datenbearbeitungen sowie Regelungen über Rechtsansprüche und Verfahren. Besonders zu erwähnen ist die Einrichtung einer Aufsichts- und Beratungsstelle für den Datenschutz: der Datenschutzbeauftragte.

Die Möglichkeit, Kommunikationen und Geschäfte über das Internet abwickeln zu können, birgt gleichzeitig datenschutzrechtliches Verletzungspotential. Weil jede elektronische Transaktion eine Datenspur in entsprechenden Log-Büchern von Servern mit Rechneradresse, Datum, Zeit, Aktion und Zugriffsobjekt hinterlässt, können durch den Datenverwalter aussagekräftige Profile über die Vorlieben und Bedürfnisse von Nutzern erstellt werden. Zwar geben die Log-Bücher die Identität von Internetnutzern nicht direkt wieder, doch sind anhand weiterer Informationen verschiedene Querbezüge möglich. Das Data Mining, eine neue analytische Technik gestützt auf Methoden der künstlichen Intelligenz, Daten aufzuspüren und zu kombinieren, stellt z.B. eine solche Verfahrensmethode dar. "Cookies" dienen im Internet der Aufrechterhaltung eines definierten Verbindungszustandes, der es erlaubt, Präferenzen eines Nutzers serverseitig zu speichern und clientseitig durch ein die Nutzerpräferenz ausdrückendes Cookie festzuhalten[75]. Auch wenn es nur zur Speicherung einer Identifikationsnummer, nicht von persönlichen Daten des Nutzers kommt, kann der Anbieter ein Nutzerprofil dank der Identifikationsnummer erstellen.

Datenschutzrechtlich relevant sind im Internet verschiedene Datenarten. Grundsätzlich müssen Stammdaten (z.B. Identifikationszeichen, Login-Zeichen), Verbindungsdaten (z.B. registrierte Besuche oder Datenaustausche im Internet), Inhaltsdaten (z.B. der Inhalt eines verfassten E-Mail Textes), Entgeltdaten (z.B. Abrechnungsdaten, welche im Falle von elektronischen Geschäftsabwicklungen beim Access oder Service Provider gespeichert werden) und Kommunikationsdaten (z.B. News Group Beiträge) unterschieden werden[76].

75 WEBER, E-Commerce, 450.

76 WEBER, E-Commerce, 449 ff.

Das Datenschutzgesetz stellt verschiedene Bearbeitungsgrundsätze auf, welche teilweise in der VDSG (Verordnung zum Datenschutzgesetz) näher konkretisiert werden:

- Daten sind rechtmässig zu beschaffen (Art. 4 Abs. 1 DSG).
- Daten dürfen nur nach den Grundsätzen von Treu und Glauben und in verhältnismässiger Weise bearbeitet werden (Art. 4 Abs. 2 DSG).
- Die Datenbearbeitung hat nach dem ursprünglich angegebenen oder sich aus den Umständen oder Gesetz ergebenden Zweck zu erfolgen (Zweckbindung, Art. 4 Abs. 3 DSG).
- Der Datenbearbeiter hat sich über die Richtigkeit der Daten zu vergewissern (Art. 5 Abs. 1 DSG).
- Daten dürfen nicht ins Ausland bekanntgegeben werden, wenn das ausländische Recht keinen qualitativ vergleichbaren Datenschutz bietet (Art. 6 Abs. 1 DSG).
- Datensammlungen müssen durch angemessene technische und organisatorische Massnahmen gesichert werden (Art. 7 Abs. 1 DSG).

Ähnlich wie bei Art. 28 ZGB geht auch das DSG davon aus, dass eine Datenbearbeitung nur zulässig ist, wenn die Persönlichkeit der betroffenen Person dabei nicht widerrechtlich verletzt wird (Art. 12 Abs. 1 DSG). Eine widerrechtliche Persönlichkeitsverletzung liegt in folgenden Fällen vor (Art. 12 Abs. 2 DSG):

- Bearbeitung von Daten entgegen der Grundsätze von Art. 4, 5 Abs. 1, 6 Abs. 1 und 7 Abs. 1 DSG, nämlich:
    - unrechtmässige Beschaffung, z.B. durch absichtliche Täuschung, Drohung, Gewalt.
    - Bearbeitung wider Treu und Glauben, etwa durch Belauschen von Gesprächen.
    - fehlende Eignung und Erforderlichkeit von Daten (hinsichtlich Inhalt und Umfang der Daten.
    - Art und Weise der Bearbeitung, Dauer der Aufbewahrung usw.).
    - Bearbeitung unter Änderung des anfänglichen Zweckes.
    - Bearbeitung von unrichtigen Daten.
    - Bekanntgabe ins Ausland trotz fehlendem Datenschutz.
    - ungenügende Sicherheit.
- Bearbeitung gegen den ausdrücklichen Willen des Betroffenen;
- Bekanntgabe von besonders schützenswerten Daten oder Persönlichkeitsprofilen an Dritte.

Liegt einer der erwähnten Fälle vor, handelt es sich – sofern kein Rechtfertigungsgrund anrufbar ist – um eine Persönlichkeitsverletzung (Art. 13 DSG). Einen Rechtfertigungsgrund kann z.B. darstellen:

- die Einwilligung der betroffenen Person.
- ein überwiegendes privates Interesse der die Daten bearbeitenden Person oder Institution.
- ein überwiegendes öffentliches Interesse.
- das Gesetz.

Im Falle einer gesetzlichen Pflicht oder einer Einwilligung der betroffenen Person ist die Datenbearbeitung zulässig. In Bezug auf die Einwilligung stellt sich allenfalls die Frage, ob eine solche gültig ist. Die betroffene Person kann nur dann eine gültige Einwilligung erteilen, wenn sie sich über die Konsequenzen der Datenbearbeitung im Klaren ist. Dazu erweist sich vorgängig eine Aufklärung über den Umfang, Zweck und die Art und Weise der Datenbearbeitung als notwendig. Pauschale Einwilligungsklauseln, beispielsweise in allgemeinen Geschäftsbedingungen, stellen oft keine genügende Aufklärungsgrundlage dar.

Strittig sind oft auch Fälle, die Interessenabwägungen erforderlich machen. Das Gesetz zählt mögliche Fälle auf, bei denen ein überwiegendes Interesse der Daten bearbeitenden Person oder Institution in Betracht kommt (Art. 13 Abs. 2 DSG). Die Aufzählung der Rechtfertigungsgründe ist nicht als abschliessend zu verstehen. Folglich sind auch weitere, nicht ausdrücklich erwähnte Fallkonstellationen denkbar, in welchen der Datenbearbeiter ein überwiegendes Interesse an seiner Tätigkeit geltend machen kann. Im Zweifelsfalle obliegt die Entscheidung über diese Kriterien dem Richter.

Wer durch eine Datenbearbeitung in seiner Persönlichkeit verletzt wird, kann sich auf die in Art. 28 - 28l ZGB geregelten Rechtsbehelfe berufen (Art. 15 DSG)[77].

77 Vgl. auch Ziff. 2.3.1.5.

2.4 Vertragsrecht

Das veränderte technologische Umfeld macht es notwendig, Konzepte des klassischen allgemeinen Vertragsrechts zu überdenken. Die Kenntnis der vertragsrechtlichen Grundprinzipien vermindert das Gefahrenpotential der sich negativ entwickelnden Geschäftsszenarien, welche einer effizienten Informationssicherheit langfristig ebenso abträglich sein können wie ungenügende technische Sicherheitsmassnahmen.

2.4.1 Allgemeine Vertragsprinzipien im Internet

a) Identifikationsproblematik

Im Internet erweist sich bei Vertragsschlüssen bereits die Identifikation der Vertragsparteien als grundlegendes Problem. Ein Besteller kann gegenüber dem Anbieter nämlich vorgeben, jemand anderer zu sein. Nach bundesgerichtlicher Rechtsprechung entfällt in solchen Fällen die Anwendbarkeit der vertretungsrechtlichen Gutglaubensvorschriften (Art. 33 ff OR), weil ein gültiges Vertretungsverhältnis zumindest voraussetzt, dass der Vertragsschliessende bekannt gibt, als Vertreter für einen Dritten zu handeln. Fehlt die Vertragsparteienidentifikation, bleibt dem Betroffenen im Einzelfall nur die Möglichkeit, auf die ungerechtfertigte Inanspruchnahme durch den Getäuschten hinzuweisen und die Kontakte abzubrechen. Dadurch kann sowohl auf eigener als auch auf der Seite des getäuschten Vertragspartners ein zusätzlicher Aufwand reduziert werden.

Ein weiteres Erfordernis für einen gültigen Vertragsabschluss stellt die Handlungsfähigkeit beider Parteien dar. Möglichkeiten, die Handlungsfähigkeit des Vertragspartners zu überprüfen, bieten sich aber im Internet derzeit nicht. Weil der gute Glaube in die Handlungsfähigkeit des Vertragspartners nicht geschützt wird, trägt der handlungsfähige Vertragspartner das Risiko, ein Geschäft mit einem Handlungsunfähigen einzugehen. Der Vertrag ist – sofern er mit einem Handlungsunfähigen abgeschlossen wird – ungültig[78].

Um die erwähnten Unsicherheiten zu minimieren, erweist sich das Verwenden von digitalen Signaturen als empfehlenswerte Methode. Das Verfahren für digitale Signaturen basiert auf Paaren von mathematisch sich entsprechenden Schlüsseln (mehrhundertstellige Zahlen, die aufgrund ihrer Grösse nicht erraten werden können). Der geheime Signierschlüssel wird vom Internetteilnehmer verwendet, um sein Dokument zu signieren. Der öffentliche Prüfschlüssel steht hingegen jedermann zu und wird vom Empfänger benötigt, um die empfangene Nachricht zu dechiffrieren. Sofern der private und der öffentliche Schlüssel übereinstimmen, kann auf die Authentizität der die Nachricht absendenden Person geschlossen werden[79].

---

78 JÖRG, 5 ff.

79 SCHLAURI, 62 ff.

Die Authentifizierung einer Person bietet den im Rechtsverkehr Teilnehmenden eine faktische Sicherheit, die Identifikation einer Mitteilung zu überprüfen. Daraus darf jedoch nicht – gemäss dem heutigen Stand des Rechts – auf die Erfüllung gesetzlicher Formvorschriften geschlossen werden. Verträge, deren gültiger Abschluss das Erfüllen von Formerfordernissen voraussetzen wie z.B. der einfachen oder qualifizierten Schriftlichkeit oder der öffentlichen Beurkundung können nach heutigem Stand des Rechts durch digitale Signaturen noch nicht formgerecht abgeschlossen werden. Ein neuer Art. 14 Abs. 2^{bis} OR soll – laut der nationalrätlichen Debatte über die Verabschiedung eines Bundesgesetzes über die elektronische Signatur (ZertES) – in Zukunft die Gleichstellung von digitaler Signatur und handschriftlicher Unterschrift herbeiführen. Erhöhte Formerfordernisse, namentlich die qualifizierte Schriftlichkeit, bei welcher nicht nur eine Handunterschrift, sondern die handschriftliche Verfassung von weiteren Inhalten erforderlich ist (wie z.B. bei Testamenten), oder die öffentliche Beurkundung durch einen Notar sind indessen auch nach Verabschiedung der erwähnten Gesetzesrevision durch digitale Signaturen nicht erfüllbar[80].

b) Austausch von Willenserklärungen

Um einen Vertrag abschliessen zu können, ist der Austausch gegenseitiger Willenserklärungen notwendig. Im elektronischen Geschäftsverkehr ist es unbestritten, dass Willenserklärungen auch am PC erstellt und elektronisch mittels E-Mail, Telex, Telefax, Teletex oder Videotex übermittelt werden können. Weil der Zugang von Willenserklärungen den Zeitpunkt eines Vertragsabschlusses begründet, müsste für den elektronischen Geschäftsverkehr geklärt werden, ab wann eine Willenserklärung als zugegangen gilt. Das Zugangsprinzip besagt, dass eine Erklärung dann ihre Wirkung entfaltet, wenn sie im Herrschaftsbereich des Empfängers eintrifft und unter normalen Umständen mit deren Kenntnisnahme gerechnet werden kann. Im geschäftlichen Verkehr muss der Geschäftspartner, der seine E-Mailadresse öffentlich bekannt gibt, damit rechnen, dass Post ankommt. Insofern trifft ihn während den offiziellen Arbeitsstunden eine "Abrufobliegenheit". Im Privatverkehr wird hingegen nicht mehr erwartet werden können, als dass der Private einmal pro Tag seine elektronische Post überprüft[81].

Der Zeitpunkt des Vertragsabschlusses hängt auch von der direkten Kommunikationsmöglichkeit beider Vertragspartner ab. Das schweizerische Obligationenrecht unterscheidet in Art. 4 ff OR Anträge unter Anwesenden oder Abwesenden. Die Unterscheidung dieser beiden Antragsarten begründet unterschiedliche Zugangszeitpunkte für Willenserklärungen. Während bei Anträgen unter Anwesenden die Willenserklärungen unmittelbar auszutauschen sind, findet bei Verträgen unter Abwesenden (z.B. Verträge

80 SIMON SCHLAURI, Das Signaturgesetz vor dem Nationalrat, Jusletter vom 16. Juni 2003 (www.weblaw.ch).

81 WEBER/JÖHRI, Vertragsschluss im Internet, 45.

per Briefverkehr) eine zeitliche Verzögerung statt. Der Antragsteller bleibt solange gebunden, als er den Eingang der Antwort bei ihrer ordnungsmässigen und rechtzeitigen Absendung erwarten darf (Art. 5 Abs. 1 OR). Im elektronischen Geschäftsverkehr ist grundsätzlich vom Vertragsabschluss unter Abwesenden auszugehen, weil die weit überwiegende Anzahl von Verträgen im Internet nicht interaktiv, sondern per E-Mail oder per Mausklick zustande kommt, was eine gewisse Zeitverzögerung zur Folge hat. Sofern mit elektronischen Kommunikationsmitteln ein interaktiver Austausch von Willenserklärungen bewerkstelligt werden kann (wie z.B. im Falle des Internet Relay Chat (IRC) oder Videoconferencing), ist indessen von einem Vertragsabschluss unter Anwesenden auszugehen. Die Willenserklärungen gelten in diesem Fall vom Zeitpunkt der Äusserung an als ausgetauscht und haben daher einen unmittelbaren Vertragsabschluss zur Folge[82].

c) Angebot und Annahme

Das schweizerische Obligationenrecht unterscheidet zwischen Angeboten und Einladungen zur Offertstellung. Die beiden Ausdrücke unterscheiden die Verbindlichkeit von verschiedenen Antragsformen. Ein Angebot setzt grundsätzlich einen verbindlichen Antrag mit einem erkennbaren Abschlusswillen voraus. Art. 7 Abs. 3 OR lässt die Auslage von Waren mit Angabe des Preises in der Regel als Angebot gelten. Ein Angebot kann sich demnach auch an einen unbestimmten Adressatenkreis richten. Im Internet ist jedoch bei vielen Angeboten über Websites nicht hinreichend feststellbar, ob der Verkäufer in jedem Fall liefern kann, weshalb allgemein von einer Einladung zur Offertstellung auszugehen ist. Lässt sich hingegen aus den Umständen auf einen deutlichen Abschlusswillen schliessen, z.B. durch Zusicherungen, Bekanntgabe des Lagerbestandes oder Erwähnung der Reproduzierbarkeit der Leistung, so darf der Kunde den Inhalt der Website als verbindliches Angebot verstehen[83].

Als unverbindlich qualifiziert werden muss hingegen ein Antrag, wenn ein ablehnender Vorbehalt angefügt wird. Das Versenden von Tarifen, Preislisten und dgl. bedeutet an sich keinen Antrag (Art. 7 Abs. 2 OR). Dieser unverbindlichen Antragsform entspricht die Verbreitung von Produktinformationen auf elektronischem Weg, beispielsweise mittels Videotex oder Teleshopping.

82 JÖRG, 7 ff.

83 Vgl. JÖRG, 10 ff; THOT/GIMMY, 3 ff.

d) Übernahme von Allgemeinen Geschäftsbedingungen im Internet

Allgemeine Geschäftsbedingungen (AGB) sind für eine Vielzahl von Verträgen vorformulierte Vertragsbedingungen, die eine Vertragspartei der anderen bei Abschluss des Vertrages stellt. AGB können vom Vertragspartner selbst oder von einem Interessenverband vorformuliert sein. Entscheidend ist, dass die AGB nicht zwischen den Parteien im Einzelnen ausgehandelt werden, sondern für eine Vielzahl von Verträgen vorformuliert sind[84]. Im elektronischen Geschäftsverkehr ergeben sich in Bezug auf die Übernahme von AGB zudem spezifische Probleme technischer Natur[85]. Die AGB werden erst mit Abschluss des Vertrages zum festen Vertragsbestandteil, auch wenn der Text nicht wirklich gelesen wurde (Globalübernahme). Aus der bundesgerichtlichen Rechtsprechung haben sich in Bezug auf die Globalübernahme von AGB jedoch folgende Regeln herausgebildet:

- Eine Globalübernahme von AGB ist nicht anzunehmen, wenn die zustimmende Partei keine Möglichkeit hatte, den Inhalt der AGB zur Kenntnis zu nehmen[86].
- Nach der Ungewöhnlichkeitsregel werden ungewöhnliche Klauseln, mit welchen eine übernehmende Partei nicht gerechnet hat und zur gegebenen Zeit auch nicht rechnen musste, nicht zum Vertragsinhalt[87].
- Unklarheiten in AGB werden als Auslegungsgrundsatz zu Lasten des Ausstellers ausgelegt[88].

Im Internet lässt sich die Möglichkeit zur Kenntnisnahme von AGB am besten erfüllen, wenn die AGB als separates Bildschirmelement zwingend eingeblendet werden oder der Hinweis auf AGB mit einem Hyperlink verknüpft ist, welcher das Auffinden vereinfacht[89]. Beim Vorliegen einer Hyperlinkverknüpfung sollte die Speicherung allerdings ohne allzu grosse Zeitverzögerungen erfolgen, sonst wird der Vorgang vom Konsument als Hindernis empfunden und es besteht das Risiko, dass der Kunde den Inhalt der AGB ignoriert. Ein weiteres Verständigungserschwernis können zudem die unübersichtliche Gestaltung und die mangelhafte Lesbarkeit auf dem Bildschirm wie auch die im internationalen Geschäftsverkehr unübliche Sprache darstellen.

84 SCHWENZER, 270.

85 WEBER, E-Commerce, 326.

86 BGE 100 II 200.

87 BGE 119 II 443.

88 BGE 124 III 155.

89 WIDMER/BÄHLER, 164; JÖRG, 16.

2.4.2 EDV-Verträge

Der EDV-Vertrag stellt ein Auffangbecken für verschiedene, in jüngster Zeit aufkommende EDV-orientierte Dienstleistungen dar. Der EDV-Vertrag ist kein im Gesetz vorgesehener Vertragstypus, sondern ein nicht nominatbezogenes Vertragskonzept (Innominatkontrakt). Die Handhabung solcher Vertragsverhältnisse ist deshalb relativ schwierig, weil verschiedene Vertragselemente in analoger Weise zur Anwendung herbeigezogen werden müssen. Unter den Oberbegriff EDV-Vertrag fallen:

- Hardware- und Softwareverträge, d.h. Verträge über die Beschaffung oder Entwicklung bzw. Wartung von Hardware.
- Dienstleistungsverträge, z.B. EDV-bezogene Beratung und Schulung.
- Provider-Verträge. Typisch für diese Verträge ist, dass Soft- und Hardware beim Kunden gar nicht oder nur als unbedeutende Zusatzleistungen von Relevanz sind. In aller Regel wird bei diesen Verträgen das Recht eingeräumt, Hard- und Software von einem entfernten Ort aus zu nutzen. Darunter fallen z.B. der Internet-Access-Vertrag und der E-Mail-Vertrag zwischen dem Internetnutzer und dem Access-Provider oder der Website-Hosting-Vertrag, bei welchem sich der Hosting-Provider verpflichtet, dem Kunden Speicherkapazität für eine Website zur Verfügung zu stellen[90].

Software- und Hardwareverträge legen bei mangelhafter Leistung die analoge Anwendung von gewährleistungsrechtlichen Normen nahe. Der Kunde hat bei der Lieferung von Standardsoftware daher regelmässig einen Anspruch auf Wandelung oder Minderung nach Kaufvertragsrecht (Art. 205 OR) oder bei Individualsoftware nach Werkvertragsrecht (Art. 368 OR). Die Providerverträge stellen ebenfalls Innominatkontrakte dar, deren Internetbezogenheit bzw. fehlende Lieferung von körperlichen Gegenständen im Falle einer mangelhaften Erfüllung ein Zurückgreifen auf verschiedene, der konkreten Leistung angemessene Rechtsfiguren erfordert. In Frage kommen bei den einzelnen Providerverträgen Normen des Werk-, Auftrags- oder Mietrechts. Sofern sich keine Gewährleistungsansprüche dieser Vertragstypen als adäquat erweisen, verbleibt die Möglichkeit des Rückgriffs auf Art. 97 OR (allgemeine Bestimmung über die Schlechterfüllung im Vertragsrecht) [91].

90 HUGUENIN, 219 ff.

91 HUGUENIN, 219 ff; WEBER, E-Commerce, 345 ff.

Das mangelhafte Erbringen der EDV-vertragstypischen Leistungen kann für ein Unternehmen – sofern es als Käufer, Auftraggeber, Werkbesteller oder Mieter auftritt – erhebliche Einbussen in Bezug auf Investitionen im Informatikbereich verursachen. Mängel sollten daher nach dem Zeitpunkt der Entdeckung dem Vertragspartner gegenüber möglichst bald geäussert werden, um eine Korrektur zu erwirken. Die frühe Geltendmachung ist nicht zuletzt deswegen zu empfehlen, weil Gewährleistungsklagen innert kurzer Fristen verjähren[92].

2.4.3 Ausservertragliches Haftpflichtrecht

Das schweizerische Obligationenrecht sieht neben der vertraglichen Haftung auch eine ausservertragliche Inpflichtnahme von Personen vor. Die ausservertragliche Haftpflicht soll Schädigungen zwischen Personen, die in keiner vertraglichen Bindung zu einander stehen, durch eine Zahlungspflicht ausgleichen. Grundsätzliche Voraussetzungen für die Annahme einer ausservertraglichen Haftpflicht bilden der Eintritt eines Schadens, der ziffernmässig bestimmbar ist, eine adäquate Kausalität (logischer Zusammenhang) zwischen der vorgenommenen Handlung und dem eingetretenen Schaden, eine Widerrechtlichkeit (d.h. Verletzung von absoluten Rechtsgütern oder einer spezifischen Schutznorm) und ein Verschulden des Schädigers (Vorsatz oder Fahrlässigkeit).

Ein ausservertraglicher Schaden kann im Internet durch verschiedene Handlungen verursacht werden. Als Schädiger kommen sowohl die eigentlichen Inhaltsproduzenten (Personen und Unternehmen, die Inhalte auf einer Website positionieren) als auch Provider, d.h. Inhaltsträger oder Zugangsvermittler, in Betracht[93]. Eine ausservertragliche Haftpflicht vermag beispielsweise aufzuleben, wenn Immaterialgüterrechte oder wettbewerbsrechtliche Normen[94] verletzt werden, weil zwischen dem Verletzter eines Immaterialgüterrechts bzw. einer wettbewerbsrechtlichen Norm und dem entsprechenden Immaterialgüterrechtsinhaber bzw. Wettbewerbsteilnehmer i.d.R. keine vertragliche Beziehung besteht. Eine Haftpflicht kann des Weiteren aus der Verletzung datenschutzrechtlicher Normen durch den Access Provider resultieren.

Soweit Host-Provider betroffen sind, wird diskutiert, ob eine ausservertragliche Haftung für fremde Inhalte zu ihren Lasten angenommen werden könne. Ein Unterlassen des Host-Provider haftungsbegründende Inhalte von seiner Präsentationsplattform fernzuhalten und eine dadurch ermöglichte Verbreitung dieser Inhalte könnten als ausservertraglich schädigendes Verhalten betrachtet werden, sofern dem Provider zumutbar ist,

---

92 Die Frist für die Geltendmachung von Sachmängeln beträgt im Kauf- und im Werkvertragsrecht ein Jahr nach Ablieferung an den Käufer oder Werkbesteller (Art. 210 und 371 OR).

93 WEBER, E-Commerce, 499 ff.

94 Vgl. vorne Ziff. 2.2.4.1 und 2.2.4.2.

die auf das Netz transferierten Inhalte zu kontrollieren[95]. Eine solche Inhaltskontrolle erweist sich aber erfahrungsgemäss als sehr aufwändig. Weil derjenige, der eine Website über einen Provider präsentabel hält, den Inhalt auch jederzeit modulieren kann, ist es dem Provider i.d.R. nicht zumutbar, die Vielzahl von Inhalten auf ihre Legalität zu überprüfen[96]. Diskutiert wird derzeit auch, ob die Setzung von Hyperlinks auf Websites mit rechtsverletzenden Inhalten eine ausservertragliche Schädigung darstellt oder nicht. Die Beurteilung dieser Frage hängt massgeblich davon ab, inwieweit der Linksetzer die Möglichkeit hat, vom Bestehen rechtswidriger Inhalte auf den verlinkten Websites Kenntnis zu nehmen. Sofern bestimmte Situationen ein einhelliges Wissen des Linksetzers nahe legen, kann dieser u.E. ausservertraglich haftbar gemacht werden[97].

2.4.4 Vereinbarung zwischen (geschädigtem) Unternehmen und Täter

Dass Verträge gewisse inhaltliche Mindestanforderungen erfüllen müssen, um Gültigkeit beanspruchen zu können, stellt auch für Unternehmen im Umgang mit Tätern aus dem eigenen Hause eine bedeutende Tatsache dar. Aus Angst vor Imageschäden bevorzugen viele Unternehmen, gestützt auf einen erfolgreichen Beizug von Computer-Forensic-Diensteanbietern, eine vertragliche Vereinbarung mit dem Täter abzuschliessen ("goldener Handschlag"), anstatt eine offizielle Strafuntersuchung in Gange zu setzen. Staatsanwälte stehen der Ermittlungstätigkeit von Computer-Forensic-Diensteanbietern mit gemischten Gefühlen gegenüber, weil diese von Unternehmen in wirtschaftlich kompatibler Weise eingesetzt werden, während Staatsanwälte der Aufgabe nachgehen sollten, Offizialdelikte von Amtes wegen zu ahnden[98].

Grundsätzlich steht einer Vereinbarung zwischen dem geschädigten Unternehmen und dem Täter nichts entgegen. Weil im schweizerischen Strafprozessrecht keine Anzeigepflicht herrscht[99], bleibt es dem Opfer gestattet, seinen Schaden durch eine private Vereinbarung auszugleichen. Diese Vereinbarung muss aber vor dem Gesetz standhalten, um gültig zu sein. Schranken stellen nach wie vor die Unzulässigkeit eines übermässig bindenden (Art. 27 ZGB), sittenwidrigen oder

---

95 ROLF H. WEBER, Zivilrechtliche Haftung im Internet, in: OLIVER ARTER/FLORIAN S. JÖRG (Hrsg.): Internet-Recht und Electronic Commerce Law, 3. Tagungsband, Bern 2003, Ziff. 4.1.2. und 4.3.2.

96 WEBER, E-Commerce, 515 ff.

97 Vgl. dazu analoge Überlegungen bei der Haftung von Informationszugangsvermittlern in: ROLF H. WEBER, Zivilrechtliche Haftung im Internet, erschienen in: ARTER OLIVER/JÖRG FLORIAN S. (Hrsg.): Internet-Recht und Electronic Commerce Law, 3. Tagungsband, Bern 2003, Ziff. 3.2.2. und 4.1.2; WEBER, E-Commerce, 517 ff.

98 SONIA SHINDE, Tatort Chefetage, in: DIE ZEIT, 27.03.2003, Nr. 14, 36.

99 SCHMID, Strafprozessrecht, § 48 N 775; vorbehalten bleibt eine Strafverfolgung bei Offizialdelikten.

widerrechtlichen Vertragsinhaltes (Art. 20 OR) dar. Unter letzterem Kriterium wäre z.B. eine Vereinbarung zu verstehen, deren vom geschädigten Unternehmen gestellte Forderung einen strafrechtlichen Charakter annähme (etwa die Vereinbarung zwischen dem Unternehmen und dem Täter, für die nächsten zwei Jahre kostenlose Überstunden zu leisten, ansonsten das Unternehmen die Akten an die Strafbehörden übergeben würde). Solche Vereinbarungen sind als Nötigung (Art. 181 StGB) oder Erpressung (Art. 156 StGB) zu qualifizieren und erweisen sich wegen Verstosses gegen Art. 20 OR als widerrechtlich. Die Diskussion ist aber insoweit von beschränkter praktischer Bedeutung, als die Ungültigkeit einer solchen Vereinbarung nur vom Gericht festgestellt werden kann. Dies kann nicht im Interesse des Täters liegen, denn er würde das Risiko laufen, dass die ihn belastenden Akten damit unverzüglich durch den Zivilrichter an die Strafbehörden übermittelt würden.

Sofern eine behördliche Strafuntersuchung jedoch bereits im Gange ist, bestehen keine Möglichkeiten, diese zu unterbrechen oder aufzuhalten. Das Opportunitätsprinzip ermöglicht allerdings aus Zweckmässigkeitsgründen, vorab in Beachtung des Verhältnismässigkeitsgrundsatzes ein Absehen von der Durchführung einer Strafuntersuchung (z.B. § 39a Zürcher StPO). Die Anwendung des Opportunitätsprinzips steht jedoch vollumfänglich im Ermessen der Untersuchungsbehörden[100].

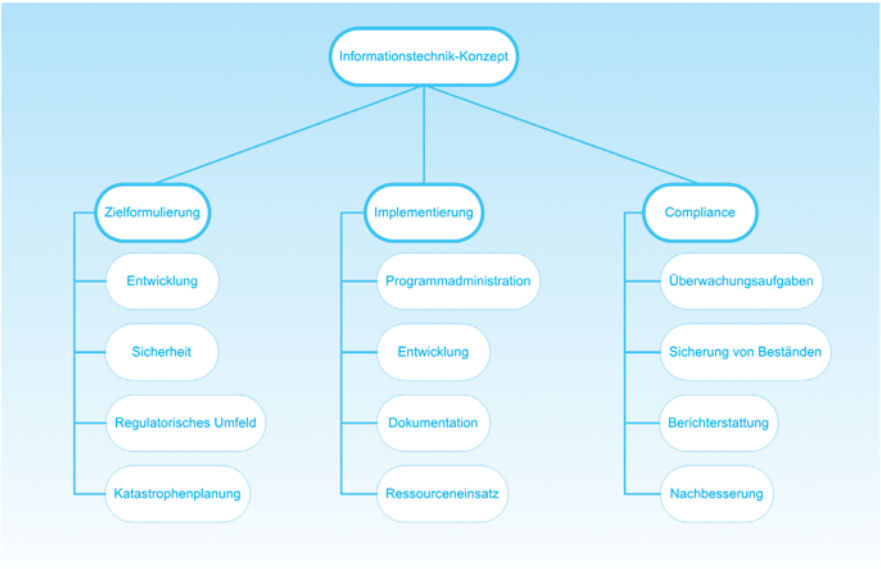
100 SCHMID, Strafprozessrecht, § 8 N 102 f.

2.5 Gesellschafts- und Bankenrecht

2.5.1 Gesellschaftsrechtliche Zuständigkeit für IT-Infrastruktur

Abgesehen von der Frage, welche Gesetzesnormen eine umfassende Informationssicherheit gewährleisten, legen gesellschaftsrechtliche Bestimmungen in Unternehmen eine Kompetenzverteilung fest, aus welcher sich Verantwortlichkeiten für die Informationssicherheit eines Unternehmens ergeben. Die Frage nach dem für Informationssicherheit zuständigen Organ in einem Unternehmen ist sowohl für die interne Unternehmenskommunikation wie auch für die externe Haftungsbegründung von erheblicher Relevanz.

Juristische Personen weisen grundsätzlich drei Arten von Organen auf: ein Willensbildungsorgan (wie z.B. eine Vereinsversammlung oder eine Generalversammlung), ein Geschäftsführungs- und Vertretungsorgan (wie z.B. ein Vorstand oder ein Verwaltungsrat), welches die laufenden Geschäfte besorgt, und ein Kontrollorgan (wie z.B. eine Revisionsstelle), welches das Finanzgebaren des Unternehmens überprüft. Von der Geschäftsleitung wird erwartet, dass ein Konzept des Einsatzes der Informations- und Kommunikationstechnik ausgearbeitet und implementiert wird. Im Rahmen eines solchen Informationstechnik-Konzept stellen grundsätzlich drei Bereiche Voraussetzung für eine sinnvolle unternehmerische Führung dar[101]:



101 WEBER, E-Governance, 354 ff (inkl. Illustration).

Im Rahmen von Kapitalgesellschaften – fortan am Beispiel der Aktiengesellschaft erläutert – muss überprüft werden, welchen Organen die Verantwortung für sichere IT-Strukturen auferlegt werden kann. Art. 716a Ziff. 5 OR behält die Grundsatzfragen der Unternehmensführung (Oberleitung) der Aktiengesellschaft dem Verwaltungsrat zur Entscheidung vor. Prinzipielle Konzeptentscheide bedeuten nicht die Pflicht zur Vornahme einer Detailkontrolle durch den Verwaltungsrat. Zutreffend wird in der Lehre dafür gehalten, dass der Verwaltungsrat ohne besondere Veranlassung nicht einer permanenten Pflicht unterstehe zu einem "legal audit" über das gesetzmässige Verhalten der Geschäftsleitung und der Angestellten[102]. Die Oberaufsicht umfasst jedoch normative und betriebswirtschaftliche Aspekte, d.h. die Tätigkeit des Verwaltungsrats setzt nicht nur die formelle Einhaltung von Gesetzen und Statuten voraus, sondern verlangt auch die Überprüfung von Zweckmässigkeit und Opportunität der Geschäftsführung.

Problemfelder der Informationstechnologie stellen keine unternehmerische Detailfrage, sondern eine grundsätzliche Aufgabe dar, welche in praktisch allen grösseren Unternehmen direkte Auswirkungen auf Systemsteuerungs- und Regelungstechnikeinrichtungen hat. Es erscheint daher als sachgerecht, dem Verwaltungsrat die Pflicht aufzuerlegen, sich zumindest für die IT-Sicherheitsproblematik zu interessieren und sich von der Geschäftsleitung über die getätigten Vorkehrungen informieren zu lassen[103]. Eine Vernachlässigung dieser Pflicht sollte eine ausreichende Basis für die Begründung einer Pflichtverletzung bzw. Widerrechtlichkeit im Falle einer gegen den Verwaltungsrat angehobenen Verantwortlichkeitsklage (Art. 754 OR) darstellen.

Ausserhalb des Gesellschaftsrechts können andere verpflichtende Einzelnormen gefunden werden, welche eine Subsumtion sicherer IT-Strukturen nahelegen. Art. 3 Abs. 2 lit. c des Bundesgesetz über Banken und Sparkassen (BankG) macht beispielsweise die Bewilligung für die Aufnahme der Geschäftstätigkeit einer Bank abhängig vom Nachweis einer "Gewähr für die einwandfreie Geschäftsführung". Hierunter werden intellektuelle Fähigkeiten und Fachkenntnisse des mitarbeitenden Personals verstanden. Bei Führungskräften gehört auch die Fähigkeit der Schaffung einer adäquaten Organisationsstruktur dazu[104]. Weil Finanzinstitute angehalten sind, geeignete Instrumente für das rasch ansteigende Volumen der Online-Bankgeschäfte bereitzustellen[105], und der Informatik in Finanzinstituten seit längerem eine Regelungs- und Steuerungsfunktion

---

102 WEBER, Informatik und Jahr 2000, 23.

103 WEBER, Informatik und Jahr 2000, 22 ff.

104 BEAT KLEINER/URS P. ROTH/DIETER ZOBL, in: KLEINER BEAT/LUTZ BENNO/ROTH P. URS/SCHWOB RENATE/ZOBL DIETER (Hrsg.), Kommentar zum Bundesgesetz über die Banken und Sparkassen, Art. 3 N 108 f, Zürich, Basel, Genf 2002.

105 WEBER, E-Commerce, 598.

zukommt, erweisen sich sichere IT-Strukturen und IT-geschultes Personal auch aus der Sicht des Bankengesetzes als Basisvoraussetzung für einen einwandfreien Geschäftsführungsnachweis. Des Weiteren stellt die Gewährleistung von sicheren IT-Strukturen im Rahmen von "Outsourcing-Transaktionen" ein relevantes Kriterium dar. Eine IT-Outsourcing-Transaktion zeichnet sich durch den Transfer von Vermögenswerten/Angestellten/Verträgen sowie die anschliessende Erbringung von IT-Dienstleistungen und allenfalls weiteren Lenkungsaufgaben durch den Outsourcing-Anbieter aus. Regulatorische Massnahmen zu diesen Transaktionen wurden von der EBK (Eidgenössische Bankenkommission) bereits in einem Rundschreiben zum Outsourcing festgelegt, welches für die ihr unterstehenden Finanzinstitute (Banken, Privatbankiers, Sparkassen) Geltung beansprucht[106]. Eine umfassende Checkliste zum Outsourcingvertrag haben ausserdem die SWICO (Schweizerischer Wirtschaftsverband der Informations-, Kommunikations- und Organisationstechnik) und SwissICT (Schweizerischer Verband der Informations- und Kommunikationstechnologie) erarbeitet[107].

2.5.2 Elektronischer Zahlungsverkehr

Angesichts der steigenden Bedeutung des Internets erweist es sich auch für Finanzdienstleistungsinstitute langfristig als unvermeidlich, traditionelle Dienstleistungen über elektronische Kanäle alternativ anzubieten. Aus diesem Grunde bieten Finanzdienstleistungsunternehmen über das Internet vermehrt Informationsbeschaffungsmöglichkeiten (z.B. Abfragen von Konto und Depotinformationen), elektronische Kontoführungsmethoden (Online-Überweisungen) oder Möglichkeiten zum Wertpapierhandel (Online-Brokerage) an. Die erwähnte Leistungserbringung erfordert jedoch sachgemässe technische Sicherungsvorkehrungen wie z.B. die Abschirmung einzelner Rechnersysteme durch Firewalls sowie die Einrichtung von kryptographischen Verfahren bei Kommunikationen zwischen bestimmten Sendern und Empfängern. Des Weiteren ist auch eine rechtliche und ordnungspolitische Rahmenregulierung erforderlich, welche allen bisher erläuterten konzentrischen Rechtsnormen vollumfänglich Rechnung trägt[108].

---

106 EBK-RS 99/2 vom 26. August 1999, zuletzt geändert am 22. August 2002 (EBK-Mitteilung Nr. 23 vom 5. September 2002) (vgl. www.ebk.ch/d/publik/rundsch/index.htm).

107 ROLF H. WEBER, IT-Outsourcing: Praxis und Rechtsfragen, in: jusletter, 24.03.2003, (www.weblaw.ch).

108 WEBER, E-Commerce, 567.

Von Bedeutung ist bei elektronischen Transaktionen deren "Nachvollziehbarkeit". Transaktionen müssen zu deren Empfänger zurückverfolgbar sein. Diese Notwendigkeit ergibt sich aus der Sicht einer Bank bereits aus der bei Transaktionsgeschäften erforderlichen, auftragsrechtlichen Sorgfaltspflicht (Art. 398 OR)[109], denn der Beweis des ordnungsgemässen Zustandekommens einer Transaktion kann gezwungenermassen nur durch eine Rückverfolgung zu deren Empfänger erbracht werden. Gleichfalls muss eine Bank, um nicht dem Vorwurf der Geldwäscherei (Art. 305bis StGB) ausgesetzt zu sein, empfangene Gelder auf ihren Ursprung hin überprüfen. Die Nachvollziehbarkeit einer Transaktion stellt somit für die Bank als Empfängerin eines Transaktionsinhaltes gleichfalls eine Voraussetzung dar, um die strafrechtlichen Rahmenbedingungen ihres Geschäftszweiges zu erfüllen.

109 ROLF H. WEBER, Elektronische Abwicklung von Effektentransaktionen, in: WIEGAND WOLFGANG, E-Banking, Berner Bankenrechtstag 2002, Band 9, Bern 2003, 56 ff.

2.6 Beweisrecht

Das Beweisverfahren im Rahmen eines gerichtlichen Prozesses dient der Ermittlung der Wahrheit bzw. Korrektheit einer Behauptung. Zu beweisen sind grundsätzlich nur Tatsachen. Rechtsätze muss das Gericht kennen mit Ausnahme des anwendbaren ausländischen Rechts und des Gewohnheitsrechts[110]. Das Prozessrecht ist in der Schweiz kantonal geregelt. Derzeit hat jeder Kanton seine eigene gerichtliche Verfahrensregelung. Zu differenzieren ist zudem zwischen dem Zivilrecht (welches das Personen-, Ehe- und Familienrecht, Vertrags- und Wirtschaftsrecht umfasst), dem Verwaltungsrecht und dem Strafrecht. Das Beweisverfahren im Strafprozess unterscheidet sich erheblich vom zivilrechtlichen Verfahren, weshalb im Folgenden auf einzelne Abweichungen hinzuweisen ist.

2.6.1 Beweismittel

a) Arten von Beweismitteln

Das schweizerische Prozessrecht kennt als Beweismittel die Parteibefragung, das Zeugnis, den Augenschein (Beweiserhebung durch die eigene Sinneswahrnehmung des Gerichts, z.B. Besichtigung eines Unfallortes durch gerichtliche Sachverständige), das Gutachten und die Urkunden. Das computer- und internetbezogene Umfeld lässt die Frage aufwerfen, welche Daten eine dem gewöhnlichen Geschäftsverkehr entsprechende Urkundenqualität aufweisen.

Elektronische Daten (E-Mails, Formulare) werden vor Gericht an sich nicht als Urkunden anerkannt. Der Ausdruck einer E-Mail oder von Daten aus einem ausgefüllten Bildschirmformular wird hingegen vor Gericht zugelassen sein. Eine ausgedruckte Mail gibt allerdings nur den Anschein, dass die betroffene Partei diese E-Mail erhalten hat; die Gegenpartei wird indessen behaupten, dass die geschickte Mail nicht von ihr stamme oder inhaltlich verändert worden sei, was sich in der Regel nur über die Begutachtung des E-Mail Systems bzw. über Log Bücher nachweisen lässt. Deshalb ist zu empfehlen, mittels technischer Lösungen (wie z.B. digitalen Unterschriften oder anderen technischen Vorkehren) das Beweisrisiko zu mindern.

---

110 SPÜHLER/VOGEL, Zivilprozessrecht, § 44 N 7 ff.

Gemäss derzeitiger Rechtslage sind digital signierte Dokumente jedoch nur als Augenscheinsdokumente zugelassen. Mangels Fachkunde und mangels technisch schlechter Ausrüstung der Gerichte dürften regelmässig auch Sachverständigungsgutachten notwendig sein. Die Botschaft zum Entwurf des Bundesgesetzes über Zertifizierung im Bereich der elektronischen Signatur (ZertES) geht davon aus, dass mit der Neueinführung von Art. 14 Abs. 2bis OR eine Gleichsetzung von Handunterschrift und digitaler Signatur im Prozessrecht bewirkt werde, zumindest sofern die Gerichte über die entsprechende Infrastruktur verfügen[111].

b) Erlangung von Beweismitteln

aa) Zivilprozessrecht

Die Beschaffung von Beweismitteln muss mit legalen Mitteln erfolgen. Beweismittel, die durch Verletzung prozessualer Normen, welche bestimmt oder geeignet sind, die Beibringung dieses Beweismittels zu verhindern, gewonnen wurden (z.B. Zeugenaussagen ohne Hinweis auf das Zeugnisverweigerungsrecht), sind im Prozess grundsätzlich unzulässig. Im Falle der Verletzung von materiell-rechtlichen Normen bei der Erlangung von Beweismitteln ist hingegen umstritten, ob solche Beweismittel verwertet werden können. Im Einzelfall muss zwischen der Schwere der Verletzungshandlung und dem Rechtsschutzinteresse der beweisführenden Partei abgewogen werden[112].

bb) Strafprozessrecht

Im Strafprozessrecht gelten ebenfalls Beweisverwertungsverbote. Aussagen aus nicht korrekt durchgeführten Einvernahmen oder Beweismittel, die von Behörden in strafbarer Weise erlangt wurden (z.B. durch Hausfriedensbruch, Nötigung, unerlaubte Verwendung von Aufnahmegeräten) sind im Regelfall unverwertbar, weil die kantonale Strafprozessordnung für diese Fälle eine Ungültigkeit der Beweise ausdrücklich vorschreibt. Wenn Beweise durch die Verletzung anderer Normen erlangt worden sind, die keine ausdrücklichen Beweisverwertungsverbote vorsehen, muss im Einzelfall geprüft werden, ob die verletzte Norm dem Schutz des Beschuldigten dient oder einen anderen Adressatenkreis tangiert. Ob Beweisverbote eine Fernwirkung annehmen können, d.h. ob Beweismittel, welche direkt oder indirekt aufgrund verbotener Beweise erlangt wurden, auch als ungültig zu betrachten sind, ist in der herrschenden Lehre umstritten[113].

111 SCHLAURI, 91; vgl. auch vorne Ziff. 2.4.1, a).

112 SPÜHLER/VOGEL, Zivilprozessrecht, § 48 N 96 ff.

113 SCHMID, Strafprozessrecht, § 38 N 610.

Im Strafverfahren sammeln grundsätzlich die Ermittlungsbehörden (Kriminalpolizei) die Beweismittel, weil sie den Ankläger (Staatsanwalt/Bezirksanwalt) in seinem Vorgehen unterstützen. Allerdings ist es durchaus möglich, dass auch Private gewisse Beweise eigenmächtig sammeln. Privaten stehen aber grundsätzlich nicht die gleichen Befugnisse wie den Strafverfolgungsbehörden zu, sie können z.B. nicht selbständig Hausdurchsuchungen durchführen, Urkunden herausverlangen oder Einvernahmen durchführen. Solche Vorgehensweisen durch Private sind strafbare Handlungen, die Beweise mithin deliktisch erlangt und sollten von den Strafverfolgungsbehörden nicht beachtet werden. Nur ausnahmsweise erweist sich ein privates Handeln wegen der Wahrung höherrangiger eigener Interessen als gerechtfertigt (z.B. wenn ein Bedrohter ein Gespräch in unerlaubter Weise auf einem Tonbandgerät registriert)[114].

Sofern Forensic Services die Strafvollzugsbehörden unterstützen und in ihrem Auftrag gewisse Beweise sichern, sind sie nicht länger als "privat" agierende Subjekte zu betrachten und können in legaler Weise an einer Beweismittelbeschlagnahme mitwirken. Werden die Forensic Services jedoch von privater Seite angefragt, Beweise zu sichern, handeln sie als private Unternehmen; d.h. Beweissicherungen sind nur soweit zulässig, als die einzelnen Sicherungsmassnahmen keine strafbaren Handlungen darstellen. Sofern strafrechtlich geschützte Güter des (mutmasslichen) Täters betroffen sind, müsste bei der jeweiligen Beweissicherung das Einverständnis des Täters oder eine Wahrung höherrangiger Interessen vorliegen, um die erlangten Beweise verwertungsfähig zu halten.

cc) Editionspflicht, Hausdurchsuchung und Beschlagnahme

Sowohl Prozessordnungen wie auch das materielle Recht (z.B. Art. 963 OR: Editionspflicht für Buchführungspflichtige) sehen Editionspflichten vor. Editionspflichten auferlegen dem Prozessgegner und Dritten eine Herausgabepflicht von Sachen, insbesondere Urkunden, in deren Besitz sie sich befinden und die für das Beweisverfahren benötigt werden. Kommen diese Personen im Zivilverfahren der Editionspflicht nicht nach, wird das entsprechende Verhalten bei der freien Beweiswürdigung berücksichtigt oder der behauptete Urkundeninhalt als erwiesen angenommen (Beweislastumkehr bei Vereitelung der Beweisgrundlagen)[115]. Sofern in einem strafrechtlichen Verfahren der Editionspflicht nicht Folge geleistet wird, kann im zweiten Schritt von den Strafverfolgungsbehörden zu einer Hausdurchsuchung und zu einer Beweismittelbeschlagnahme von Gegenständen geschritten werden[116].

---

114 SCHMID, Strafprozessrecht, § 38 N 612.

115 SPÜHLER/VOGEL, Zivilprozessrecht, § 48 N 115 ff.

116 SCHMID, Strafprozessrecht, § 46 N 742 f.

2.6.2 Beweislast

Die Beweislastverteilung regelt, welche Partei den Beweis für eine behauptete Tatsache erbringen muss. Im zivilrechtlichen Verfahren gilt grundsätzlich die Regel von Art. 8 ZGB. Derjenige, der aus dem Vorhandensein einer behaupteten Tatsache Rechte ableiten will, muss deren Vorhandensein beweisen, sofern das Gesetz es nicht anders bestimmt. Dies kann der Fall sein, wenn eine gesetzliche Bestimmung die Beweislast ausdrücklich einer anderen Partei auferlegt (sog. "Beweislastumkehr").

Im Strafprozessrecht gilt hingegen die Offizialmaxime. Weil an der Ahndung von Straftaten ein öffentliches Interesse besteht, muss der Staat von Amtes wegen beim Vorliegen einer Straftat den Täter zur Rechenschaft ziehen. Im Strafprozess stehen somit immer der Staat, vertreten durch einen Staatsanwalt/Bezirksanwalt, dem Beschuldigten gegenüber. Angesichts der in Art. 6 Ziff. 2 EMRK statuierten Unschuldsvermutung gilt im Strafprozess der Grundsatz der Beweisbedürftigkeit, d.h. der verfolgende Staat hat dem Beschuldigten alle objektiven und subjektiven Tatbestandsmerkmale nachzuweisen[117].

117 SCHMID, Strafprozessrecht, § 38 N 599.

3 Gefährdungsanalyse

3.1 Grundlagen der Gefährdungsanalyse

Die für Informationssicherheit, generelle Sicherheit, Risk Management usw. verantwortlichen Stellen möchten gerne "auf Knopfdruck" feststellen, ob ihr Unternehmen bezüglich Risiken im Bereich der IT-Sicherheit im allgemeinen oder Computerkriminalität im besonderen gefährdet ist.

Leider lässt sich diese Frage nicht so einfach beantworten, tragen doch zahlreiche Faktoren zu einer hohen oder allenfalls mangelhaften Sicherheit bei. Zudem sind die Zusammenhänge zwischen diesen Faktoren komplex und nicht immer eindeutig beurteilbar. Dennoch wird in diesem Kapitel zuerst theoretisch und dann anhand einiger Beispiele ein pragmatischer Ansatz zur Risikoanalyse vorgestellt, der eine Antwort auf die Frage der Gesamtgefährdung liefert.

Jede Handlung in einem IT-System hinterlässt Spuren und damit auch Spuren von kriminellen Handlungen. Nebst den *direkten* Spuren z.B. in Form von Protokolleinträgen findet man aber auch eine ganze Reihe von *indirekten* Hinweisen, welche auf eine unerwünschte, möglicherweise deliktische Handlung aufmerksam machen können. Es gilt, diese Hinweise zu einem möglichst frühen Zeitpunkt wahrzunehmen und entsprechend zu reagieren, im Idealfall bevor dieses Ereignis überhaupt stattgefunden hat.

Man kann zwischen verschiedenen Arten von Hinweisen unterscheiden:

- Förderliche Faktoren (enabler)
- Warnsignale (red flags)
- Auslöser (trigger)

Förderliche Faktoren sind solche, die das Auftreten von Fehlern einerseits aber auch von deliktischen Handlungen andererseits begünstigen. Sie werden auch mit indirekten Gefährdungsindikatoren bezeichnet. *Warnsignale* sind in der Regel offensichtliche Anzeichen dafür, dass "etwas" nicht mehr in Ordnung ist. Da sie ein (deliktisches) Ereignis direkt anzeigen, werden sie oft auch "direkte Gefährdungsindikatoren" genannt. Ferner existieren typische Auslöser einer deliktischen Handlung, also bestimmte Ereignisse, welche eine Person dazu bringen können, eine deliktische Handlung zu begehen. Das Vorhandensein möglicher Auslösersituationen gibt also ebenfalls indirekte Hinweise für eine potentielle Gefährdung.

Die Zuordnung der verschiedenen Faktoren zu einer der drei Gruppen indirekte Gefährdungsindikatoren, direkte Gefährdungsindikatoren oder Auslöserindikatoren ist nicht immer eindeutig.

3.1.1 Förderliche Faktoren (*enabler*)

Analysiert man Geschehnisse im Bereich der IT-Sicherheit, lässt sich feststellen, dass eine gewisse Zahl von Faktoren das Auftreten von Fehlern einerseits aber auch von deliktischen Handlungen andererseits begünstigt:

- hohe Komplexität der Geschäftsabläufe
- grosses Transaktionsvolumen
- fehlende Sicherheitskonzepte, Richtlinien und Standards
- unwirksame oder fehlende Sicherheitsmassnahmen
- fehlendes Internes Kontrollsystem (IKS), mangelhaftes Kontrollverfahren
- fehlende Funktionentrennung
- Fehlende Nachvollziehbarkeit (Protokollierung), fehlende Überwachung
- blindes Vertrauen in Technik oder Einzelpersonen (Wer überwacht den Chef?)
- fehlendes Sicherheitsbewusstsein

3.1.1.1 Hohe Komplexität der Geschäftsabläufe

Die meisten der schon seit Jahren etablierten Geschäftsprozesse sind an sich bereits recht komplex. In den letzten Jahren hat hier vor allem im Zusammenhang mit E-Commerce oder E-Business ein Wandel zu einer weiteren Automatisierung und höheren Integration verschiedener, bis anhin unabhängiger Teilprozesse stattgefunden. Dieser Wandel führte zu einer weiteren Zunahme der Komplexität. Das wiederum führt oft dazu, dass kaum jemand mehr den Überblick über die Gesamtzusammenhänge hat und die Prozesse wirklich versteht. Dies erschwert es in der Praxis, die deliktischen Aktionen eines Täters zu verhindern oder wenigstens zu erkennen.

Auch wenn man argumentieren kann, dass diese Komplexität nun einmal zu den heutigen Geschäftsprozessen gehört, bestehen innerhalb eines Unternehmens nach wie vor Prozesse unterschiedlicher Komplexität. Diese Information kann daher für eine Gefährdungsanalyse innerhalb eines Unternehmens zur besseren Differenzierung zwischen verschiedenen Bereichen verwendet werden.

3.1.1.2 Grosses Transaktionsvolumen

In einigen Unternehmen werden pro Tag mehrere Hunderttausende, manchmal sogar weit über 1 Million Transaktionen abgewickelt. Doch auch bei kleineren Unternehmen sind es schnell einmal ein paar Hundert oder Tausend. Die Wahrscheinlichkeit, dass jemand unter so vielen gültigen Transaktionen eine bestimmte – in irgendeiner Form manipulierte – Transaktion findet, ist verschwindend klein.

3.1.1.3 Fehlende Sicherheitskonzepte, Richtlinien und Standards

Fehlende wie ungenügende Sicherheitskonzepte, Richtlinien oder Standards ermöglichen für sich alleine keine deliktischen Handlungen. Jedoch kann man bei einem Unternehmen ohne ein sorgfältiges, für dieses Unternehmen angepasstes Sicherheitskonzept davon ausgehen, dass erstens zahlreiche unerkannte Sicherheitslücken bestehen und zweitens die implementierten Sicherheitsmassnahmen wenig wirksam sind. Ohne klare interne Vorschriften werden Sicherheitsmassnahmen kaum konsequent implementiert (z.B. für das Härten eines Internet-Webservers) und von den Mitarbeitern und anderen Benutzern eingehalten (z.B. Richtlinien für Umgang mit vertraulichen Informationen). Sie werden damit ihre Funktion nicht erfüllen und führen darüber hinaus dazu, dass sich Mitarbeiter und Verantwortliche in falscher Sicherheit wähnen.

3.1.1.4 Unwirksame oder fehlende Sicherheitsmassnahmen

Für viele (Informatik-) Mitarbeiter ist Sicherheit ein Fremdwort. Zwar hat sich die Ausbildung in den letzten Jahren gerade in diesem Bereich wesentlich verbessert, doch fehlt es ausgerechnet in der heutigen Zeit in den meisten Unternehmen am klaren Willen, erstens solche ausgebildeten Spezialisten zu beschäftigen und zweitens das vorhandene Wissen zur Implementation von wirksamen Sicherheitsmassnahmen auch anzuwenden. Dies führt fast zwangsläufig dazu, dass zahlreiche unerkannte (und teilweise auch erkannte) Sicherheitslücken bestehen. In vielen Fällen sind Massnahmen zwar implementiert, aber nicht ausreichend konsequent und oft ohne den notwendigen Sachverstand. Der zunehmende Kostendruck führt ebenfalls dazu, dass Sicherheitsmassnahmen ohne grosse Priorität und oft nur mit bescheidenstem Budget angepackt werden.

3.1.1.5 Fehlendes Internes Kontrollsystem (IKS), mangelhaftes Kontrollverfahren

Der Begriff "Kontrollen" wird definiert durch die Konzepte, Verfahren, Praktiken und Organisationsstrukturen, welche eine angemessene Gewissheit verschaffen, dass die Geschäftsziele erreicht und dass unerwünschte Ereignisse verhindert oder erkannt und korrigiert werden. Kontrollen nehmen damit zur Erreichung der Unternehmensziele, Vermögensschutz, Genauigkeit und Zuverlässigkeit der Buchführung und Einhaltung der Geschäftspolitik eine zentrale Stellung ein.

Anwendungsabhängige Kontrollen sollen die ordnungsmässige und sichere Verarbeitung der Daten gewährleisten und den Nachweis der Richtigkeit der Ergebnisse erbringen. Die Unternehmung stellt mit anwendungsabhängigen Kontrollen sicher, dass alle relevanten Geschäftsfälle in den Applikationen vollständig, richtig, gültig und nachprüfbar erfasst, in das System eingegeben und von diesem verarbeitet, gespeichert und ausgegeben werden.

Neben den anwendungsabhängigen Kontrollen sind auch die anwendungsunabhängigen Kontrollen bekannt, also Kontrollen in übergeordneten Bereichen wie Betrieb von Netzwerk und Rechenzentrum, Entwicklung und Unterhalt von Anwendungen oder die Notfallplanung. Auch die anwendungsunabhängigen Kontrollen spielen bei der Vermeidung von (Computer-) Delikten eine – allenfalls leicht untergeordnete – Rolle.

Sind diese internen Kontrollen zwar vorhanden, aber nicht oder nur ungenügend wirksam, werden Fehler nicht verhindert, zu spät entdeckt oder nicht zeitgerecht resp. nicht richtig korrigiert.

3.1.1.6 Fehlende Funktionentrennung

Kein wesentlicher Geschäftsvorfall und kein kritischer Arbeitsschritt oder Prozess sollte durch eine einzige Person in irgendeiner Form korrumpiert werden können. Arbeitsabläufe sind derart auszugestalten, dass dieselbe Angelegenheit von zwei Seiten her, unabhängig voneinander bearbeitet wird, um die Abstimmung der Ergebnisse zu ermöglichen. Die Funktionen- resp. Gewaltentrennung ist eine typische und sehr zentrale Massnahme zur Verhinderung von unerwünschten (deliktischen) Ereignissen. Wo sie fehlt, ist mit einer massiv höheren Gefährdung zu rechnen.

Es kann nicht allgemein verbindlich festgelegt werden, welche Funktion mit welcher anderen Funktion vereinbar ist oder in welchen Fällen die Funktionentrennung strikte einzuhalten ist. Die genaue Ausgestaltung der Funktionentrennung hängt von der Grösse der Firma und der Organisationseinheit, der Art der Geschäftstätigkeit, der Art der Funktion (Planung, Entscheidung, Ausführung, Kontrolle), der zur Verfügung stehenden bzw. einsetzbaren Hilfsmitteln und allenfalls auch von bestehenden Vorschriften ab.

Leider ist in vielen Unternehmen die Ansicht verbreitet, dass auf höheren Hierarchiestufen eine Funktionentrennung überflüssig sei. Statistiken zeigen, dass zwischen 50 und 80% aller Delikte von oberen Managementstufen ausgeübt werden und erst möglich wurden, weil man auf dieser Stufe die Funktionentrennung als nicht mehr notwendig betrachtet (Fachleute sprechen hier von "Control Override").

3.1.1.7 Fehlende Nachvollziehbarkeit (Dokumentation)

Um kurzfristig Geld zu sparen, werden in vielen Fällen wichtige Dokumentationsaufgaben weggelassen. Die meisten Geschäftsprozesse sollten aber aufgrund geltender Gesetze zu einem späteren Zeitpunkt nachvollziehbar sein. Neben der generellen Dokumentation der Arbeitsschritte und -prozesse bedingt dies die Aufbewahrung von Originalen (Aufträgen, Quittungen, Lieferscheinen und anderen Belegen) sowie die Protokollierung der Geschäftsdaten einerseits und weiterer Informationen andererseits (Audit Trail). Dazu gehört auch die Identität derjenigen Personen, welche an diesem Geschäftsprozess beteiligt waren. In zahlreichen Fällen werden solche Protokolle aus Kostengründen nicht geführt. In anderen Fällen sind die protokollierten Informationen unvollständig oder nicht zuverlässig, weil sie mit einfachen Mitteln verfälscht werden können. Auch dort, wo Protokolle geführt werden, werden diese in der Praxis oft nur geschrieben und nie von einer zweiten, unabhängigen Instanz zu einem späteren Zeitpunkt kontrolliert, so dass Manipulationen unerkannt bleiben (siehe Kapitel 3.1.1.8 Ungenügende Überwachung).

3.1.1.8 Ungenügende Überwachung

Die Überwachung der Abwicklung von Geschäften resp. genereller die Überwachung der Abwicklung von Prozessen oder Verfahren ist Teil eines Kreislaufs, eines mehrphasigen Lebenszyklus: Prozesse und Verfahren müssen geplant, angeordnet, ausgeführt, dokumentiert, auf Zielabweichungen kontrolliert und dann entsprechend korrigiert werden (6 Phasen). Vereinfacht spricht man auch von Anordnen, Überwachen und Korrigieren bezeichnet (3 Phasen). Ohne Überwachung kann nicht verifiziert werden, ob Anordnungen befolgt oder vorgegebene Prozesse eingehalten werden. Überwachung wird damit aber zu einer der wichtigsten Führungsaufgaben. Etwas überspitzt formuliert, muss jede einmal erfolgte Anordnung periodisch oder zu einem vorgegebenen Zeitpunkt auf ihre Einhaltung überprüft werden.

Analog zur Nachvollziehbarkeit wird die Überwachung wegen der damit verbundenen Kosten häufig vernachlässigt. Heutzutage fehlt auch vielfach die Zeit, um sich Überwachungsaufgaben anzunehmen. Dass wegen der mangelnden Überwachung die Risiken zunehmen können, ohne dass dies erkannt wird, ist dem Management zwar bewusst. Da aber zu einem späteren Zeitpunkt der kausale Zusammenhang zwischen der mangelhaften Überwachung und dem entstandenen Schaden fehlt, wird in der Regel nichts unternommen, um die Überwachung zu verstärken.

Einzige Ausnahme sind hier diejenigen Themen, wo Vorschriften von Behörden existieren, welche eine solche Überwachung klar anfordern und den Nachweis der erfolgten Überwachung verlangen (z.B. EBK-Richtlinien, Sarbanes-Oxley etc.).

3.1.1.9 Blindes Vertrauen in Technik oder Einzelpersonen

Typisch menschlich ist die Reaktion auf einen Computerausdruck – man hält die angezeigten Informationen für richtig, auch wenn andere Signale vielleicht auf Fehler hindeuten ("Alles, was aus dem Computer kommt, muss ja richtig sein, oder?"). Ein ähnliches Verhalten zeigt sich sowohl gegenüber langjährigen Mitarbeitern als auch gegenüber Vorgesetzten: man vertraut ihnen blindlings ("Wer überwacht den Chef?"). Dies ist ein eigentlich kultureller Aspekt, der vor allem im asiatischen Raum besonders verbreitet ist. Dieser Punkt geht häufig einher mit dem "fehlenden Sicherheitsbewusstsein" (siehe Kapitel 3.1.1.10 Fehlendes Sicherheitsbewusstsein).

Blindes Vertrauen in die Technik oder in Einzelpersonen ist im Zusammenhang mit unerwünschten Ereignissen – insbesondere mit deliktischen Handlungen – ein Hauptgrund, warum so grosse Schäden auftreten.

3.1.1.10 Fehlendes Sicherheitsbewusstsein

Ein sicherheitsbewusstes Verhalten ist uns Menschen bis zu einem gewissen Grad fremd. Der Grund dafür liegt in der (an sich positiven) Eigenschaft, negative Erlebnisse zu verdrängen und zu vergessen. Wenn man längere Zeit nichts Negatives über etwas gehört hat, geht man davon aus, dass grundsätzlich alles in Ordnung (das heisst sicher) ist. Passiert dann doch etwas, ist die erste Reaktion oft massiv überhöht. Doch bereits innert Tagen oder Wochen ist bereits wieder das ursprüngliche Verhalten "normal".

Ohne das notwendige Sicherheitsbewusstsein bei allen Mitarbeitern und Vorgesetzten werden bestehende Sicherheitsmassnahmen umgangen oder nicht richtig angewandt.

3.1.2 Warnsignale (*red flags*)

Es gibt eine ganze Reihe von Warnsignalen, welche bereits zu einem recht frühen Zeitpunkt auf eine möglicherweise deliktische Tätigkeit aufmerksam machen (können). Einerseits sind dies die Folgen der unerwünschten Handlungen selbst (also z.B. eine Vermögensverschiebung zwischen dem betrogenen Unternehmen resp. dessen Kunden und dem Betrüger). Auf der anderen Seite sind dies Symptome im Zusammenhang mit dem oft erheblichen Aufwand, der notwendig ist, um die Delikte selbst zu begehen resp. deren Spuren zu verwischen.

Warnsignale sind zum Beispiel:

- Storni, Korrekturbuchungen
- Auffälligkeiten im Prozessablauf
- zahlreiche Kundenreklamationen
- Anfragen der Presse/Medien
- viele Überstunden, Wochenendarbeit, keine längeren Ferien
- Schlüsselpersonen, ohne die es nicht geht
- Lebensstil und Einkommen stimmen nicht überein
- ungewöhnliches gesellschaftliches Umfeld, unerwartete Veränderungen im gesellschaftlichen Umfeld
- unkooperatives oder sonstwie auffälliges Verhalten
- atypische Kundenbeziehungen

Besonders "interessant" sind im Zusammenhang mit (möglicher) Geldwäscherei die folgenden Warnsignale:

- besonders grosse, für den Kunden unübliche Transaktionen
- Anlieferung von Banknoten oder anderen Inhaberpapieren von hohem Wert
- aussergewöhnlich grosse Volumen
- Durchlauftransaktionen (Eingänge, welche direkt und fast vollständig wieder abfliessen)
- plötzlich auftretende Aktivitäten bei "schlafenden" Konten
- Transaktionen an Geldinstitute in bestimmten Entwicklungs- und Schwellenländern, Krisen- oder Kriegsgebieten

3.1.2.1 Storni, Korrekturbuchungen

Wenn ein Geschäftsprozess richtig implementiert wurde, lassen sich Korrekturen von Zahlungen usw. ausschliesslich durch Stornierung und anschliessende Neueingabe der Transaktionen vornehmen. Muss also aus irgendeinem Grund eine Korrekturbuchung vorgenommen werden, so ist dafür eine entsprechende Stornobuchung notwendig. Durch Überwachung der Storno-Rate resp. der Korrekturbuchungen lassen sich Fehler oder eben Manipulationen entdecken.

Man muss sich bewusst sein, dass jede Art von Geschäftsprozessen und auch jede Kontrollkultur eine typische aber individuelle Storno-Rate aufweist. Eine Abweichung der aktuellen Storno-Rate nach oben (oder evtl. auch nach unten) kann auf mögliche Manipulationen aufmerksam machen. Bereicherungen dieser Art führen in der Regel dazu, dass ein Konto- oder Depotsaldo nicht mehr stimmt. Bei Kundenreklamationen gibt sich der Täter natürlich extrem freundlich und korrigiert die entsprechenden Kontounterlagen und -salden. Er muss aber dafür das vom betreffenden Konto abgebuchte Geld neu beschaffen, indem er seinen alten Bezug irgendwie korrigiert und dann das Geld von einem anderen Konti neu abbucht. Wie bei einem Schneeballsystem nimmt die Zahl der notwendigen Korrekturbuchungen laufend zu. Damit steigt auch die Storno-Rate pro Geschäftsart, Transaktionstyp, Abteilung oder Mitarbeiter erkennbar an.

Interessant ist, dass auch eine Abweichung der typischen Storno-Rate nach unten ein Indiz ist für mögliche Probleme. Der Grund für diese eher überraschende Tatsache ist eigentlich einleuchtend: es ist unwahrscheinlich, dass ohne ersichtlichen Grund die Zahl der Fehler weniger wird. Daher muss angenommen werden, dass die betroffenen Mitarbeiter irgendeinen Weg gefunden haben, Fehler durch Umgehung der Stornofunktion zu korrigieren. Falls dies möglich wäre, könnten aber auch deliktische Manipulationen vorgenommen werden.

Ein Überwachungssystem müsste also für jeden typischen Geschäftsprozess die Stornorate oder die Zahl der Korrekturtransaktionen durch die Einhaltung einer oberen und unteren Grenze überwachen.

3.1.2.2 Auffälligkeiten im Prozessablauf

Das obige Beispiel lässt sich auf sämtliche Geschäftsprozesse resp. Transaktionen verallgemeinern. Bei Finanzdienstleistern (vorwiegend Banken) oder Kreditkartenunternehmen sind bereits seit Jahren Systeme im Einsatz, welche ungewöhnliche Transaktionen als "verdächtig" kennzeichnen und die zuständigen Personen (z.B. Kundenberater oder Vorgesetzte) alarmieren.

Über diese Art Systeme gibt es bereits in der Fachliteratur genügend Informationen, so dass dieser Themenbereich in der nachfolgenden Diskussion mehrheitlich ausgeschlossen wird.

3.1.2.3 Zahlreiche Kundenreklamationen

Wenn Kunden eines Unternehmens einen Fehler bemerken, wenden sie sich in der Regel an den jeweiligen Kundenbetreuer, der die Sache untersucht und in Ordnung bringt. Ganz allgemein werden in den meisten Fällen Reklamationen vom zuständigen Sachbearbeiter behandelt. Wie bereits erwähnt sind die Kundenbetreuer am ehesten in der Lage, sich an den Kundenvermögen zu vergreifen.

Misst man die Zahl der Kundenreklamationen und wertet sie z.B. nach Geschäftsart, Fachbereich oder zuständigem Mitarbeiter aus, kann man "relativ einfach" systematischen resp. wiederkehrenden Manipulationen auf die Spur kommen. Dies ist der Grund, warum es z.B. in verschiedenen Ländern Pflicht ist, sämtliche Kundenreklamationen von einer unabhängigen Stelle entgegenzunehmen und die Abarbeitung durch die Revision überwachen zu lassen (was aber seinerseits zu einer Verwässerung der Unabhängigkeit der Revision führen kann).

3.1.2.4 Anfragen der Presse/Medien

Studiert man die kritische, eher konsumentenorientierte Presse, so findet man immer wieder Fälle, welche (anscheinend) für die betroffenen Unternehmen überraschend kamen. Anfragen der Presse zu bestimmten Vorkommnissen aber auch Anfragen zum Beispiel an den internen Ansprechpartner für Problemfälle sind in der Regel ein klarer Indikator dafür, dass ein ernsthaftes Problem z.B. in der Kontoführung vorliegt. Analysiert man derartige Fälle systematisch, sollte dem verantwortlichen Vorgesetzten eine Häufung bereits zu einem frühen Zeitpunkt auffallen!

3.1.2.5 Überstunden, Wochenendarbeit, keine längeren Ferien

Häufig fliegen deliktische Manipulationen erst dann auf, wenn der betreffende Mitarbeiter verunfallt und daher so lange nicht mehr zur Arbeit erscheinen kann, dass ein anderer Mitarbeiter einspringen muss.

Im Falle des Kundenbetreuers als Täter kann dieser im Normalfall alle auftretenden Anfragen und Probleme zur Zufriedenheit der Kunden lösen. Das ganze Konstrukt fällt also erst dann auf, wenn der Täter nicht mehr in der Lage ist, seine (deliktische) Arbeit durchzuführen. Dies versucht er natürlich auf jeden Fall zu vermeiden. Solche Personen sind auch durch Krankheiten und Verletzungen kaum von der Arbeit abzuhalten. Sie werden gerade wegen ihrem unermüdlichen Einsatz auch an Abenden, Wochenenden usw. von ihren Kollegen und Vorgesetzten häufig sehr geschätzt.

Einschlägige Sicherheitsstandards empfehlen aus diesem Grund zusammenhängende Ferien von mindestens fünf (in der Schweiz zehn) Tagen.

3.1.2.6 Schlüsselpersonen, ohne die es nicht geht

Schlüsselpersonen, ohne die es nicht geht, sind schon aus der Optik der Stellvertretung (Verfügbarkeit) für das Unternehmen ein Risiko. Schon ein kurzfristiger Ausfall z.B. wegen eines Unfalls könnte dazu führen, dass ein kritischer Geschäftsprozess nicht ausgeführt wird.

Hat man in einem Bereich eine Schlüsselperson, so ist bei den anderen Mitarbeitern in der Regel nur wenig Kenntnis über den entsprechenden Bereich vorhanden. Ist der Täter diese Schlüsselperson, kann er ungestört schalten und walten, ohne dass er die Einmischungen Dritter zu befürchten hat. Auch im Normalfall, wo die Schlüsselperson nicht selber der Täter ist, fördert er durch sein personenzentriertes Verhalten Delikte. Einerseits monopolisiert er Fachwissen, was zu Intransparenz führt, auf der anderen Seite hat er aufgrund seiner Schlüsselposition häufig (zu) viel Arbeit und kann Fehler und andere verdächtige Vorkommnisse gar nicht selber untersuchen.

3.1.2.7 Lebensstil und Einkommen stimmen nicht überein

Ein weiteres Warnsignal ist die offensichtliche Nichtübereinstimmung von Einkommen und Ausgaben. Aufgrund des Persönlichkeitsschutzes ist es nicht möglich, einen Mitarbeiter zu überwachen, um herauszufinden, wie er zu seinem Geld kommt. Anfragen über deklarierte Einkommen und Vermögen werden von Steuerbehörden in der Regel nur zurückhaltend oder gar nicht beantwortet. Einen Strafregisterauszug zu erhalten ohne Einwilligung des Verdächtigten ist kaum möglich, und ein Betreibungsregisterauszug wird in den meisten Fällen auch nicht weiterhelfen.

Bleibt noch die direkte Anfrage beim Verdächtigten. Die möglichen Antworten sind nicht unbedingt aussagekräftig. Was heisst zum Beispiel "Ich gehöre zur (reichen) Familie XY"? Ist das jetzt wirklich der reiche Sohn dieser reichen Familie oder der armgehaltene Sohn der reichen Familie, der einen Schein aufrechterhalten will.

Dieser Abschnitt zeigt auch sehr gut auf, wie unbefriedigend Abklärungen in diesem Teilbereich sein können. Auch bei Vorliegen klarer, nicht widerlegbarer Indizien hat man als Vorgesetzter wie als Prüfer oft keine Möglichkeit, die Situation wirklich zu klären. Unter Umständen macht sich der Prüfer, Mitarbeiter oder Vorgesetzte noch selbst eines Deliktes schuldig, wenn er die entsprechenden Informationen von Dritten einfordert oder selber an Dritte weitergibt.

3.1.2.8 Ungewöhnliches gesellschaftliches Umfeld oder unerwartete Veränderungen

Das gesellschaftliche Umfeld ist in der Regel nur ein schwacher Indikator. Es ist in unserer Kultur und vor allem auch in den Städten normal, dass ein Unternehmen wenig über das gesellschaftliche Umfeld seiner Mitarbeiter weiss. Deswegen ist es oft auch schwierig, Veränderungen in diesem Umfeld zu erkennen. Nichtsdestotrotz könnte das persönliche Umfeld eines Mitarbeiter wertvolle Hinweise (Warnsignale) liefern.

3.1.2.9 Unkooperatives oder sonstwie auffälliges Verhalten

Es ist klar, dass ein Täter nicht interessiert sein kann an weitergehenden Abklärungen in seinem Verantwortungsbereich. Bei Revisionen oder anderen Untersuchungshandlungen sind solche Personen daher eher unkooperativ, wenn nicht sogar widerborstig. Oft werden auch subtile Verzögerungstaktiken angewandt im Wissen, dass Untersuchungen in der Regel zeitlich limitiert sind. Kann der Täter z.B. die Herausgabe eines Protokolls, einer Überwachungsliste oder eines Abstimmkreises lange genug hinauszögern, wird der Prüfer weiterziehen (müssen), ohne alle notwendigen Informationen erhalten zu haben.

Auch dieses Warnsignal ist nicht eindeutig: unkooperatives Verhalten kann auch erklärt werden mit Stress, Zeitdruck, grundsätzlicher Abneigung z.B. gegenüber Revisoren oder externen Personen (erst recht bei externen Revisoren!).

In einigen Fällen kann eher von auffälligem Verhalten gesprochen werden. Ein Beispiel ist der Mitarbeiter, der plötzlich die Bürotüre zumacht, damit er ungestört seinen Tätigkeiten nachgehen kann (z.B. betrügerische Manipulationen, Anschauen oder Download von Pornographie, Internet-Casinos, usw.).

3.1.2.10 Atypische Kundenbeziehungen

In jedem Unternehmen gibt es typische und wahrscheinlich auch atypische Kundenbeziehungen. Für eine Bank sind z.B. Transaktionen zwischen Kunden und Mitarbeitern sicherlich atypische Beziehungen, welche näher untersucht werden müssten. Analog sind direkte Geschäfte zwischen zwei Kunden, welche von demselben Mitarbeiter betreut werden vielleicht theoretisch möglich, in der Praxis zumindest bei einem grösseren Unternehmen eher selten.

3.1.2.11 Warnsignale im Zusammenhang mit möglicher Geldwäscherei

Es gibt zahlreiche Warnsignale, welche auf mögliche Geldwäscherei aufmerksam machen können, sprengt aber den Rahmen der vorliegenden Gefährdungsanalyse.

3.1.3 Auslöser einer deliktischen Handlung (Trigger)

Es erstaunt immer wieder, dass langjährige, zuverlässige Mitarbeiter plötzlich zu Delinquenten werden. In vielen Fällen werden diese Personen erst durch ein bestimmtes Ereignis (Trigger) zu einer deliktischen Handlung angestossen.

Als mögliche Auslöser von deliktischen Handlungen gelten:

- schlechtes Arbeitsklima, ständige Überforderung, Zeitdruck, Leistungsdruck
- unklare Führungsstruktur, inkompetente Führung (Stil, Schwächen)
- hohe Personalfluktuation (auch beim Kader)
- Androhung einer Entlassung, erfolgte Entlassung, Arbeitsplatzabbau
- überschwänglicher Lebensstil und entsprechende Bedürfnisse
- Alkohol, Drogensucht und andere Krankheiten
- Krisen im persönlichen Umfeld (schwere Krankheiten, Scheidung)

3.1.3.1 Schlechtes Arbeitsklima, ständige Überforderung, Zeitdruck, Leistungsdruck

Leider hat sich in den letzten Jahren das Arbeits- resp. Betriebsklima in vielen Unternehmen geradezu dramatisch verschlechtert. Befragt man massgebende interne Stellen (z.B. das mittlere Management, den Personaldienst) zu ihrer Einstufung der Arbeitszufriedenheit, erhält man oft stark beschönigte Antworten. In Wirklichkeit sind viele Mitarbeiter überfordert und stehen unter einem immensen Leistungsdruck. In Kombination mit anderen Faktoren (z.B. inkompetente Führung) wirkt dieser Stress negativ und oft stark belastend.

Aus einer langjährigen Loyalität gegenüber dem Arbeitgeber wird so eine starke Unzufriedenheit, manchmal sogar Hass. Vielleicht kommt ein verärgerter Mitarbeiter zum Schluss, er verdiene etwas Besseres und bedient sich dann gleich selber in der Kasse.

3.1.3.2 Unklare Führungsstruktur, inkompetente Führung (Stil, Schwächen)

Ein einmaliger oder allmählicher Wandel im organisatorischen Umfeld an sich muss nichts Schlechtes darstellen. Wenn jedoch Unternehmen häufig andere Unternehmen aufkaufen oder von diesen aufgekauft werden und damit permanent im Umbruch sind, besteht oft keine klare Führungsstruktur mehr. Aus der Optik des Täters reicht so etwas bereits in seinem unmittelbaren Umfeld, ohne dass eine Vergrösserung der Verletzbarkeit des Unternehmens erfolgt. Ein schwacher Führungsstil kann generell Stress und damit auch starke negative Gefühle auslösen. Zudem nehmen schwache Führungskräfte ihre Überwachungsaufgaben kaum ausreichend wahr. Sie werden damit sowohl zum Auslöser von deliktischen Handlungen wie auch zum Grund, dass diese nicht erkannt werden.

3.1.3.3 Hohe Personalfluktuation (auch beim Kader)

Bedingt durch rasches Wachstum, Reorganisationen aber auch Führungsschwächen besteht in einigen Betrieben eine extrem hohe Personalfluktuation. Dies führt dazu, dass bereits nach kurzer Zeit kaum jemand mehr in der Organisation tätig ist, der die Zusammenhänge der Geschäftsprozesse versteht. Daraus folgt sowohl eine erhöhte Fehleranfälligkeit in Kombination mit einer erschwerten Fehlersuche als auch, dass einzelne langjährige Mitarbeiter sich in solchen Situationen geradezu ein kleines "Königreich" einrichten können, weil sie die Einzigen sind, welche die komplexen Prozesse noch verstehen (siehe Kapitel 3.1.1.9 Blindes Vertrauen in Technik oder Einzelpersonen).

3.1.3.4 Androhung einer Entlassung, erfolgte Entlassung, Arbeitsplatzabbau

Rache ist für viele Personen ein starker Motivator, um Unrecht anzurichten. Androhung, Ankündigung oder auch die Mitteilung einer Entlassung können bei an sich zuverlässigen Mitarbeitern Rachegefühle freisetzen und zudem bestehende Hemmschwellen abbauen. Da eine Entlassung in den Augen des Entlassenen praktisch immer ungerecht ist, beinhaltet jede Entlassung eine potentielle Gefahr, dass sich dieser Mitarbeiter mittels Sabotage oder Veruntreuung verlustlos halten möchte.

3.1.3.5 Überschwänglicher Lebensstil und entsprechende Bedürfnisse

Es wurde bereits erwähnt, dass eine Diskrepanz zwischen Einkommen und Lebensstil ein Warnsignal für deliktische Handlungen sein kann. Ebenso offensichtlich ist die Tatsache, dass das Aufrechterhalten eines bestimmten Lebensstils wegen den dafür benötigten grossen finanziellen Mitteln schnell einmal zum Auslöser werden kann. Zwar bestehen grosse Unterschiede innerhalb der Gesellschaft (so ist z.B. die durchschnittliche Überschuldung durch Kleinkredite eines Amerikaners weitaus grösser als diejenige eines Schweizers), doch lassen sich in Abhängigkeit von Herkunft und Alter gewisse Zusammenhänge erkennen. Wie bereits mehrfach an anderer Stelle erwähnt, ist es aber schwierig, von solchen Signalen auf potentielle deliktische Tätigkeiten zu schliessen. Sicher ist, dass Anschaffungen in irgendeiner Form bezahlt werden müssen, – entweder mit dem eigenen Geld, dem des Arbeitgebers oder von Drittpersonen.

3.1.3.6 Alkohol, Drogensucht und Krisen

Finanzielle Probleme verursacht durch Alkohol- oder Drogensucht sowie durch schwerwiegende Krankheiten können zu Auslösern von kriminellen Handlungen werden. Ebenso kann dies den Finanzbedarf direkt und geradezu dramatisch ansteigen lassen.

Gerade im zentraleuropäischen Umfeld sind Krisen im persönlichen Umfeld häufig Auslöser: schwere Krankheiten in der Familie oder der psychische und finanzielle Druck bei Scheidungen führen häufig zu einer Verschiebung des Wertebildes und manchmal zu deliktischen Handlungen.

3.1.4 Auslöser der Untersuchung

Forensische Untersuchungen werden in der Regel erst durchgeführt, wenn ein konkreter Tatverdacht besteht. Mögliche Auslöser von Untersuchungshandlungen sind z.B. (siehe auch Kapitel 4.2.1 Meldungseingang):

- Vorfälle werden über Help Desk, Sicherheitsdienst etc. gemeldet
- Vorfälle werden von Kunden/Lieferanten/Partnern gemeldet
- vermutete Schwachstellen werden über Help Desk, Sicherheitsdienst etc. gemeldet
- internes Kontrollsystem deutet auf Vorfälle hin
- Reaktionen in der Öffentlichkeit machen auf Vorfälle aufmerksam (Presse/Medien)
- Behörden untersuchen Vorfälle (Polizei, Gerichte)
- Selbstanzeige des Delinquenten
- laufende Untersuchungen geben Hinweise auf weitere Delikte
- periodisch durchgeführte Gefährdungsanalyse zeigt erhöhte Risikosituation an (siehe Kapitel 3.2 Durchführung der Gefährdungsanalyse)

3.2 Durchführung der Gefährdungsanalyse

3.2.1 Einführung

Die Durchführung einer Gefährdungsanalyse in der eigenen Unternehmung besteht im wesentlichen darin, die zahlreichen verschiedenen Gefährdungsindikatoren zu bewerten und zu einer schlüssigen Aussage zusammenzufassen. Dies wird in der beschriebenen Form höchstens im Bereich der Kreditkartenorganisationen und Finanzdienstleister (vor allem Banken) überhaupt durchgeführt. Es ist aber offensichtlich, dass nicht nur solche Unternehmen zum Opfer eines internen oder externen Angriffs werden können, sondern dass dies grundsätzlich jedem Unternehmen unabhängig von seiner Grösse geschehen kann. Es ist daher für jedes Unternehmen grundsätzlich sinnvoll, eine Gefährdungsanalyse durchzuführen.

Im vorhergehenden Kapitel 3.1 Grundlagen der Gefährdungsanalyse wurde aufgeführt, dass es förderliche Faktoren (enabler), Warnsignale (red flags) und mögliche Auslöser (trigger) gibt. Alle Faktoren weisen als *direkte* oder *indirekte* Indikatoren auf eine potentielle Gefährdung hin:

a) Förderliche Faktoren (enabler), welche die Durchführung von deliktischen Handlungen vereinfachen oder dafür sorgen, dass diese nicht erkannt werden:

- Komplexität der Geschäftsabläufe
- Volumen (Anzahl Geschäftsvorfälle, Anzahl Transaktionen, Umsatz in Stück oder Franken)
- Qualität der Sicherheitskonzepte (Vollständigkeit, Übereinstimmung mit Best Practice)
- Vorhandensein von allgemeinen Richtlinien und Standards
- Vorhandensein von Sicherheitsmassnahmen und ihre Wirksamkeit
- Qualität des Internen Kontrollsystems (IKS)
- Grad der Funktionentrennung
- Grad der Nachvollziehbarkeit (Protokollierung) von Geschäften und Handlungen
- Qualität der Überwachung (zeitnah, umfassend)
- Grad des Vertrauens in Technik oder in Einzelpersonen
- Grad des Sicherheitsbewusstseins

b) Warnsignale (red flags), welche direkte Hinweise zu möglicherweise bereits erfolgten deliktischen Handlungen geben:

- Stornorate
- Anzahl/Verteilung von Korrekturbuchungen
- Anzahl und Art der Kundenreklamationen
- Anfragen der Presse/Medien zu bestimmten Vorfällen oder Personen
- Überstunden
- Häufigkeit und Dauer der Wochenendarbeit
- Ferien, die ausschliesslich tageweise genommen werden
- Schlüsselpersonen, die sich unabkömmlich gemacht haben
- Unausgewogenheit von Lebensstil und Einkommen
- unkooperatives Verhalten gegenüber Mitgliedern des IKS oder den Revisoren
- atypische Kundenbeziehungen

c) Auslöser (trigger), welche deliktische Handlungen auslösen können:

- schlechtes Arbeitsklima
- dauernde Über-/Unterforderung
- Zeitdruck
- hoher Leistungsdruck
- länger dauernde unklare Führungsstruktur
- inkompetente Führung (Stil, Schwächen)
- hohe Personalfluktuation (auch beim Kader)
- Androhung einer Entlassung, erfolgte Entlassung, Arbeitsplatzabbau
- überschwänglicher Lebensstil und entsprechende Bedürfnisse
- Alkoholsucht, Drogensucht und andere Krankheiten
- Krisen im persönlichen Umfeld (schwere Krankheiten, Scheidung)

Betrachtet man diese Aufzählung genauer, so ist erkennbar, dass einzelne dieser Faktoren objektivere Aussagen geben als andere: eine Stornorate z.B. in % ist eine Zahl, welche von mehreren sachkundigen Personen in der Regel übereinstimmend gemessen wird. In diesem Zusammenhang spricht man auch von *harten* Faktoren. *Harte* Faktoren sind z.B.

- Branche des Unternehmens
- Grösse des Unternehmens
- Ort der Geschäftstätigkeit
- eingesetzte Technologien, z.B.
    - Internet
    - Fernwartung
    - Remote Access

Faktoren, die man als subjektiv betrachtet bezeichnet, nennt man *weich*. Typische Aussagen sind "es ist ok", "der Prozess ist in Ordnung", "das Interne Kontrollsystem ist stark". Was im einzelnen bedeutet, dass es zu einem zu einem grossen Teil von der jeweilig urteilenden Person abhängt. *Weiche* Fakten sind typischerweise Aussagen von (oder über) Mitarbeitern oder zu ihrem Verhalten:

- Ausbildungsstand (Know-how, Bildung)
- Kultur (innerhalb Unternehmen, Herkunft und Zusammensetzung der Mitarbeiter)
- Motivation (Geld, Einfluss, Mobbing)
- Loyalität gegenüber Arbeitgeber
- Internes Kontrollsystem (IKS)

Es wurde bis anhin unterschieden zwischen der Art von Faktoren (Begünstigung von deliktischen Handlungen, Auslöser von deliktischen Handlungen oder Warnsignale) sowie zwischen *harten* (objektiven) und *weichen* (subjektiven) Kriterien.

a) Faktoren, welche Auskunft über die Einfachheit zur Ausführung von deliktischen Handlungen geben (enabler):	objektiv	subjektiv
Komplexität der Geschäftsabläufe		X
Volumen (Anzahl Geschäftsvorfälle, Transaktionen, Umsatz)	X	
Qualität der Sicherheitskonzepte (Vollständigkeit etc.)		X
Vorhandensein von allgemeinen Richtlinien und Standards		X
Vorhandensein und Wirksamkeit von Sicherheitsmassnahmen		X
Qualität des IKS		X
Grad der Funktionentrennung		X
Grad der Nachvollziehbarkeit von Geschäften und Handlungen		X
Qualität der Überwachung (zeitnah, umfassend)		X
Grad des Vertrauens in Technik		X
Grad des Vertrauens in Einzelpersonen		X
Grad des Sicherheitsbewusstseins		X

b) Faktoren, welche direkte Hinweise zu möglicherweise erfolgten deliktischen Handlungen geben (red flags):	objektiv	subjektiv
Stornorate	X	
Anzahl/Verteilung von Korrekturbuchungen	X	
Anzahl und Art der Kundenreklamationen	X	
Anfragen der Medien zu bestimmten Vorfällen oder Personen		X
Überstunden	X	
Häufigkeit und Dauer der Wochenendarbeit	X	
Ferien, die tageweise genommen werden	X	
Schlüsselpersonen, die sich unabkömmlich gemacht haben		X
Unausgewogenheit von Lebensstil und Einkommen		X
unkooperatives Verhalten		X

c) Faktoren, welche deliktische Handlungen auslösen können (trigger):	objektiv	subjektiv
schlechtes Arbeitsklima		X
dauernde Über-/Unterforderung		X
Zeitdruck		X
hoher Leistungsdruck		X
länger dauernde unklare Führungsstruktur		X
inkompetente Führung (Stil, Schwächen)		X
hohe Personalfluktuation (auch beim Kader)	X	
Androhung einer Entlassung, Entlassung, Arbeitsplatzabbau		X
überschwänglicher Lebensstil und entsprechende Bedürfnisse		X
Alkoholsucht, Drogensucht und andere Krankheiten		X
Krisen im persönlichen Umfeld		X

Tabelle 3: Zuordnung der verschiedenen Faktoren zu den aufgeführten Kategorien

3.2.2 Erfassung von Faktoren einer Gefährdungsanalyse

Bei einer Gefährdungsanalyse spielt der Aufwand zur Erhebung der notwendigen Informationen eine wesentliche Rolle. Typischerweise sind harte Faktoren einfacher zu erheben. In den meisten Fällen handelt es sich hier um Zahlen, welche bereits in irgendeinem System geführt werden oder aus diesen Systemen leicht ermittelt werden können.

Weiche Faktoren hingegen müssen oft in mühsamer Handarbeit ermittelt werden. Nicht nur ist der Aufwand für die Datenerhebung grösser, die Auswertung von verschiedenen qualitativen Einzelbewertungen ist in der Regel auch wesentlich aufwändiger. Bei der Diskussion des Aufwandes muss die sinnvolle Häufigkeit der Erhebung mitberücksichtigt werden. So wird man die Mitarbeiterzufriedenheit kaum öfters als 2-4 mal pro Jahr messen, während man die Stornorate täglich ermittelt.

Was ist der Zweck dieser Diskussion? Es ist offensichtlich, dass kein Unternehmen alle oben aufgeführten Faktoren erheben und regelmässig aktualisieren kann. Es gilt, aus der grossen Zahl von möglichen Faktoren diejenigen auszuwählen, welche bei tragbarem Aufwand den grössten Ertrag liefern.

3.2.3 Vorgehen zum Analysieren der Gefährdungsfaktoren

Das Vorgehen zum Analysieren der aufgeführten Gefährdungsfaktoren besteht im Prinzip aus den folgenden Schritten:

- Erheben/Sammeln
- Auswerten
- Darstellen
- Kommunizieren
- Handeln
- und allenfalls einem "Neu-Kalibrieren" der Kriterien und ihrer Massstäbe

3.2.3.1 Sammeln/Erheben

Um die "richtigen" Kriterien zu finden, müssen diese für die betreffende Organisation aufgrund der folgenden Informationen bewertet werden:

- Was ist die Quelle dieser Informationen?
- Wie zuverlässig sind diese Informationen (Qualität)?
- Wann können oder müssen die Daten erhoben werden und wie häufig (Zeitpunkt)?
- Besteht die Möglichkeit, mit der Zeit statistische Informationen zu gewinnen, so dass Trendanalysen vorgenommen werden können?
- Wie, wer, wann, wo werden die Informationen erhoben?
- Welche Hilfsmittel stehen für die Erhebung der Informationen zur Verfügung?
- Wie gross ist der Aufwand für die Erhebung der Informationen?

Die nachfolgende Tabelle zeigt für einige ausgewählte Beispiele eine mögliche Beurteilung der oben aufgeführten Fragen auf. Die verschiedenen Spaltenköpfe sind grösstenteils selbstsprechend. Das Merkmal "Zeitpunkt" bezeichnet, wie wichtig eine Früherkennung des unerwünschten Ereignisses oder der Risikobewältigung ist.

a. Faktoren, welche Auskunft über die Einfachheit zur Ausführungvon deliktischen Handlungen geben (*enabler*):	Quelle	Qualität	Zeitpunkt	Statistik	Erhebung	Hilfsmittel	Aufwand
Komplexität	Revision	hoch	spät	nein	manuell	-	hoch
Volumen	Anwendung	hoch	aktuell	ja	automatisch	Anwendung	mittel
Qualität der Sicherheitskonzepte	Untersuchung	hoch	spät	nein	manuell	Benchmark	mittel
Richtlinien und Standards	Untersuchung	hoch	spät	nein	manuell	-	mittel
Sicherheitsmassnahmen	Untersuchung	hoch	spät	teilweise	manuell	-	mittel
Qualität des Internen Kontrollsystems (IKS)	Revision	hoch	spät	nein	manuell	-	hoch
Grad der Funktionentrennung	Revision	hoch	spät	nein	manuell	-	mittel
Grad der Nachvollziehbarkeit	Revision	hoch	spät	teilweise	manuell	-	mittel
Qualität der Überwachung	Revision	mittel	spät	nein	manuell	-	hoch
Vertrauen in Technik	Befragung	niedrig	spät	nein	manuell	-	mittel
Vertrauen in Einzelpersonen	Befragung	niedrig	spät	nein	manuell	-	mittel
Grad des Sicherheitsbewusstseins	Untersuchung	niedrig	spät	nein	manuell	-	mittel

b. Faktoren, welche direkte Hinweise zu möglicherweise erfolgten deliktischen Handlungen geben (red flags):	Quelle	Qualität	Zeitpunkt	Statistik	Erhebung	Hilfsmittel	Aufwand
Stornorate	Anwendung	hoch	aktuell	ja	automatisch	Anwendung	mittel
Korrekturbuchungen	Anwendung	hoch	spät	ja	automatisch	Anwendung	mittel
Kundenreklamationen	Untersuchung	mittel	spät	ja	manuell	-	mittel
Medienanfragen	Untersuchung	mittel	spät	ja	manuell	-	mittel
Überstunden	Personalanwendung	mittel	aktuell	ja	automatisch	Anwendung	mittel
Wochenendarbeit	Anwendung	hoch	aktuell	ja	automatisch	Anwendung	mittel
tageweise Ferien	Untersuchung	mittel	spät	ja	manuell	-	mittel
Schlüsselpersonen	Untersuchung	niedrig	spät	nein	manuell	-	hoch
Lebensstil und Einkommen	Untersuchung	niedrig	spät	nein	manuell	-	hoch
unkooperatives Verhalten	Untersuchung	niedrig	spät	nein	manuell	-	hoch

c. Faktoren, die Situationen aufzeigen, welche deliktische Handlungen auslösen können (trigger):	Quelle	Qualität	Zeitpunkt	Statistik	Erhebung	Hilfsmittel	Aufwand
Arbeitsklima	Untersuchung	niedrig	früh	nein	manuell	-	hoch
Über-/Unterforderung	Untersuchung	niedrig	früh	nein	manuell	-	hoch
Zeitdruck	Untersuchung	mittel	früh	nein	manuell	-	mittel
Leistungsdruck	Untersuchung	niedrig	früh	nein	manuell	-	mittel
Führungsstruktur	Untersuchung	niedrig	früh	nein	manuell	-	hoch
Führung (Stil, Schwächen)	Befragung	niedrig	spät	nein	manuell	-	hoch
Personalfluktuation	Personalanwendung	hoch	früh	ja	automatisch	Anwendung	niedrig
Entlassung, Arbeitsplatzabbau	Personalanwendung	mittel	früh	ja	manuell	Anwendung	hoch
Lebensstil	Untersuchung	niedrig	spät	nein	manuell	-	hoch
Alkoholsucht, Drogensucht und andere Krankheiten	Untersuchung	niedrig	spät	nein	manuell	-	hoch
persönliches Umfeld	Untersuchung	niedrig	spät	nein	manuell	-	hoch

Tabelle 4: Mögliche Beurteilung aufgeführter Fragen

3.2.3.2 Auswerten

Die auswertende Stelle muss das notwendige Know-how haben, unabhängig arbeiten können, nicht selbst in die zu untersuchenden Fälle verwickelt zu sein und von den Betroffenen und Beteiligten anerkannt werden. Bei der Auswahl der Person oder der Stelle müssen also folgende Fragen beantwortet werden:

- Ist eine Auswertung losgelöst von dem produktiven Betrieb (Produktion) möglich?
- Ist diese Stelle unabhängig?
- Ist diese Stelle kompetent?
- Hat diese Stelle alle notwendigen Kompetenzen, um die Informationen auszuwerten und allenfalls Alarm auszulösen?
- Wo (physisch (Ort, Raum), logisch (HW, SW-Umgebung)) findet die Auswertung statt?
- Wie häufig kann/muss die Auswertung durchgeführt werden (Periodizität: stündlich, täglich, 1x pro Jahr)?
- Sind die statistischen Grenzen, Limiten und Möglichkeiten bekannt (z.B. Benfordsches Gesetz)?
- Wie können verschiedene Einzelinformationen zusammengeführt (aggregiert) werden?
- Wie gross ist der Aufwand, um die Informationen auszuwerten?
- Wie kann die Qualität der ausgewerteten Informationen z.B. durch Quervergleiche, Plausibilisierungen usw. sichergestellt werden?

3.2.3.3 Darstellen

Die Resultate der Auswertungen müssen sinnvoll gruppiert und dargestellt werden. Auch wenn letztlich die Detailbewertungen vorliegen müssen, sind diese Zahlenlandschaften kaum geeignet, um darauf basierend einfach und schnell die richtigen Schlussfolgerungen zu ziehen.

Folgende Fragen sind wichtig:

- Wer ist das Zielpublikum (Spezialist / Management)?
- Was ist der maximal zumutbare Umfang der Darstellung?
- Was ist der Zweck der Darstellung?
- Welche Art Reaktion soll ausgelöst werden?
- Was muss unternommen werden, um eine Lösung der verschiedenen Probleme herbeizuführen?
- Was ist der Aufwand, um die ausgewerteten Informationen in der gewünschten Form darzustellen?

Die nachfolgenden Darstellungsmethoden werden mit ihren Vor- und Nachteilen vorgestellt und erklärt. Wichtig ist, dass ein bestimmter Sachverhalt mit unterschiedlichen Darstellungstechniken vermittelt jeweils verschiedene Reaktionen auslösen kann. Es ist daher vom Zielpublikum abhängig, welche Darstellungsmethode die geeignetste ist.

Zielpublikum	Umfang	Zweck	optimale Reaktion	Darstellungsform
Geschäftsleitung	klein, < 5 Seiten	Awareness	Budget freistellen; Projekt-Sponsoring	Grafiken
Sicherheitsfachstelle	egal	Risikoanalyse	Berichte, Projekte, Sicherheitsmassnahmen, …	Grafiken, Zahlen, Details
Oberes Management (Abteilungsleiter, oft Direktionsrang)	klein, < 5-10 Seiten	Überwachung	Korrektur	Grafiken, Zahlen

Tabelle 5: Darstellungsmethoden

Beispiel Radardiagramm

Radardiagramme eignen sich sehr gut dazu, Risikoprofile aufzuzeigen. Ideal sind mindestens 5 (besser 7) bis 30 verschiedene Faktoren, welche entweder direkt in der Grafik oder mittels einer separaten Legende bezeichnet werden.

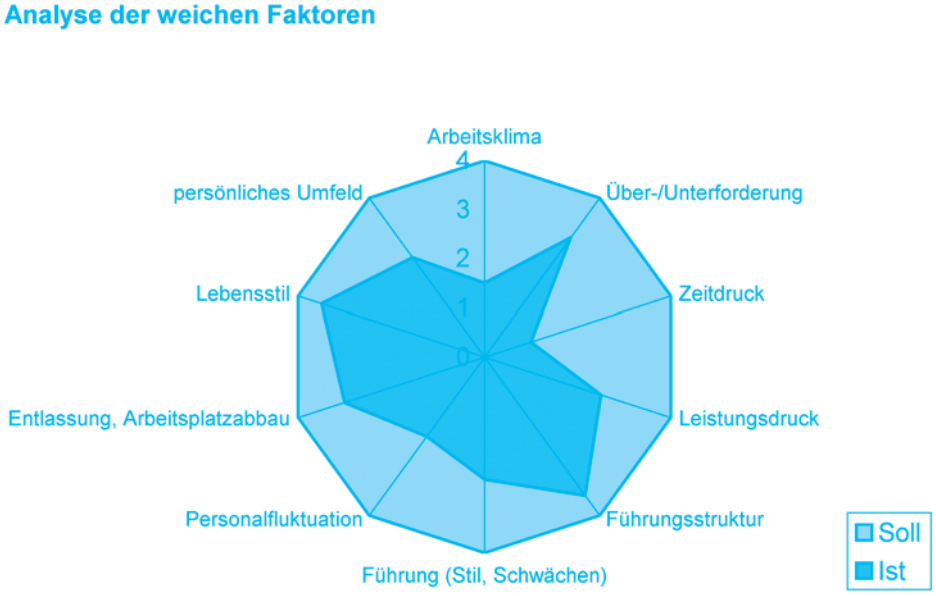


Abbildung 1: Radardiagramm

Beispiel XY-Diagramm

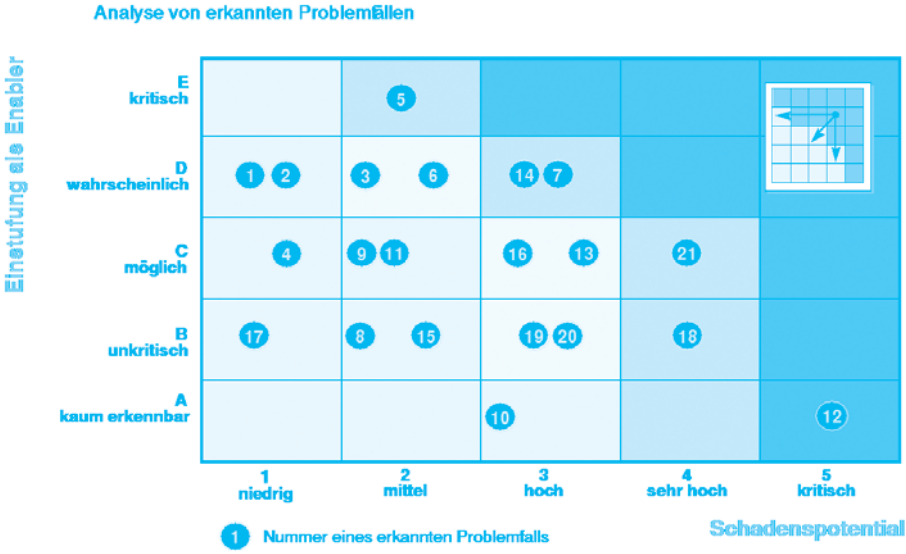


Abbildung 2: XY-Diagramm

Die obige Darstellung stammt aus dem Bereich Risikoanalysen/Risikomanagement. Diese Darstellungsart eignet sich sehr gut, bestimmte Problemfälle (im Beispiel Nr. 1 – 21) auf ihre Einstufung als "Enabler" sowie ihr Schadenspotential zu bewerten, so dass für den sachkundigen Betrachter klar ist, welche Problemfälle kritisch sind und daher mit erster Priorität angegangen werden müssen (im Beispiel Nr. 12, dann 5, 14, 7, 21, und 18 usw.).

Beispiel Histogramm

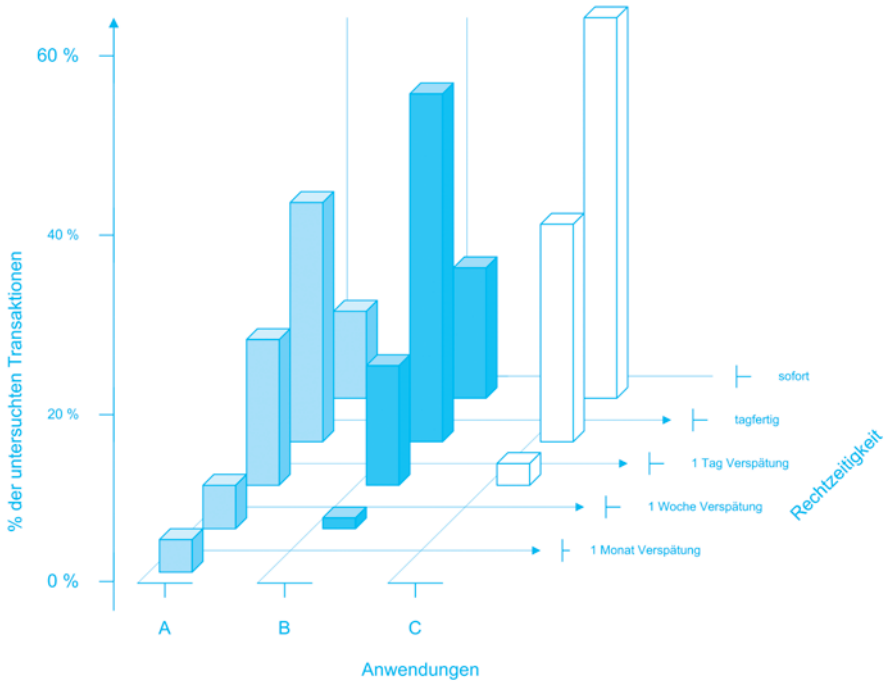


Abbildung 3: Histogramm

Das Säulendiagramm eignet sich für wenige Faktoren (im Beispiel drei Anwendungen), welche bezüglich mehrerer Ausprägungen klassifiziert wurden (im Beispiel bezüglich der Dauer bis zur korrekten Verbuchung der Transaktionen. Offensichtlich sind die Anwendungen A und B nicht ganz optimal, da doch zahlreiche Transaktionen verspätet abgeschlossen werden).

Beispiel "flächige" Darstellung

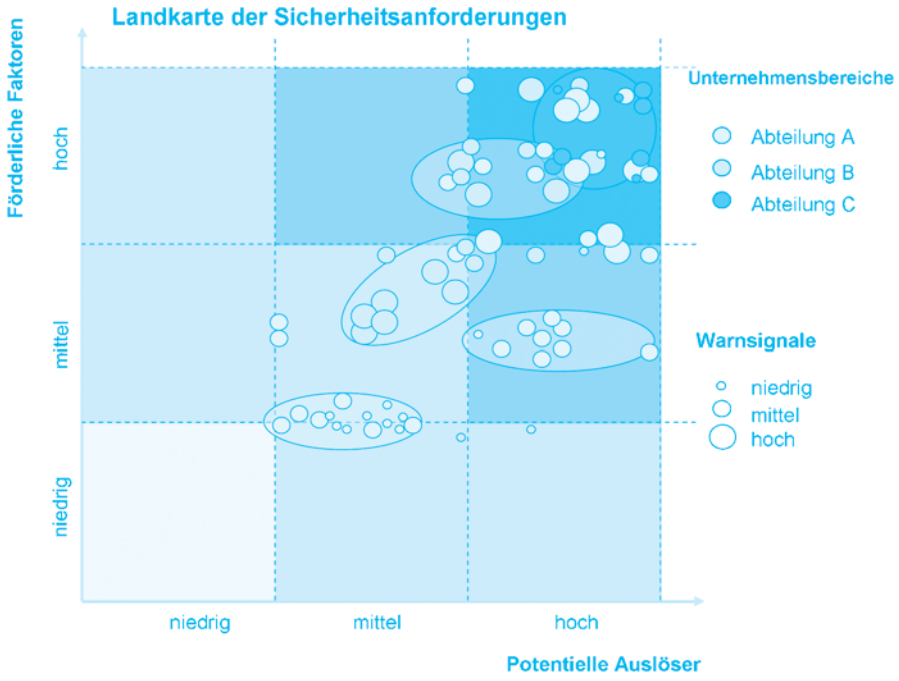


Abbildung 4: "flächige" Darstellung

Die "flächige" Darstellung eignet sich dazu, viele Faktoren auf letztlich zwei Dimensionen zu reduzieren und mittels der Flächengrösse noch eine zusätzliche Aussage über eine dritte Dimension (z.B. das Auftreten von Warnsignalen) zu machen. Das obige Beispiel zeigt auf, dass vor allem in der Abteilung C einerseits viele förderliche Faktoren sowie potentielle Auslöser vorhanden sind auf der anderen Seite aber die Warnsignale noch nicht detektiert wurden.

Weitere Darstellungsmöglichkeiten

Die aufgeführten Beispiele zeigen nur einen kleinen Ausschnitt aus den möglichen Darstellungstechniken. Interessant und besonders geeignet für eine Gefährdungsanalyse sind insbesondere alle Techniken, welche die Veränderung der Gefährdungslage über eine bestimmte Zeit darstellen können und damit eine Trendanalyse ermöglichen.

3.2.3.4 Kommunizieren

Die Darstellung der Auswertungsergebnisse muss separat zur Kommunikation betrachtet werden. Im Vordergrund von Darstellungen liegt die Überlegung, wie man die zahlreichen gesammelten und ausgewerteten Informationen so präsentiert, dass die darin enthaltene Aussage vom Zielpublikum erfasst werden kann. Bei der Kommunikation geht es nun um Fragen wie:

- Werden die Ergebnisse präsentiert (Zweiwegkommunikation) oder müssen diese vom Zielpublikum selber gelesen und verstanden werden (Einwegkommunikation)?
- Wieviel Zeit steht zur Verfügung?
- Wie häufig müssen die Ergebnisse kommuniziert werden? Einen täglichen Bericht wird man kaum persönlich präsentieren sondern per Mail schicken.

Die Darstellungsart und die Form der Kommunikation stehen in einem engen Zusammenhang. Es lohnt sich dennoch, diese beiden Fragestellungen (möglichst) getrennt zu betrachten.

Folgende Kommunikationsarten sind denkbar und sinnvoll :

- persönliche Berichterstattung
- Kurzbericht per Post oder Mail
- Bericht mit Management-Summary
- kurze Präsentation als Teil eines regelmässigen Meetings
- Präsentation als eigenes Meeting
- Webseite mit aktuell nachgeführten Informationen

Die nachfolgende Tabelle zeigt die Eignung dieser Kommunikationsarten in Abhängigkeit von der Häufigkeit der Berichterstattung.

Kommunikationsart	täglich	wöchentlich	monatlich	bei Ereignissen
persönliche Berichterstattung	+	+++	+	+++
Kurzbericht per Post oder Mail	++			++
Bericht mit Management-Summary	-	+	+++	+
Kurzpräsentation als Teil eines regelmässigen Meetings	-	++	++	-
Präsentation als eigenes Meeting	-	+	++	+++
Webseite mit aktuell nachgeführten Informationen	++	++	-	+

Tabelle 6: Kommunikationsarten in Abhängigkeit der Häufigkeit der Berichterstattung

3.2.3.5 Handeln

Darstellungsart und Kommunikationsweg hängen davon ab, welche Ziele verfolgt werden. Folgende Fragen sind in diesem Zusammenhang zu beantworten:

- Soll eine rasche Reaktion (z.B. Sperren eines Accounts) ausgelöst werden? Mit welchem Ziel?
- Soll eine vertiefte Untersuchung (z.B. Audit) ausgelöst werden?
- Soll eine Management-Reaktion (z.B. Anpassung des IKS) ausgelöst werden?

Die Erkenntnisse aus der Gefährdungsanalyse sollten in einem Risk Management Prozess zusammengefasst werden, welcher die Risiken systematisch ermittelt und die notwendigen Verbesserungsmassnahmen entwickelt und implementiert (siehe Kapitel 6. Prävention).

3.2.4 Hilfsmittel

Bei den Überlegungen zur Gefährdungsanalyse sollte man sich nicht scheuen, bereits vorhandene Resultate in den Auswertungsprozess einfliessen zu lassen (z.B. Erkenntnisse aus Revisionsberichten, Statistiken des Help Desk / Problem Management). Das Problem dabei ist, dass derartige Informationen oft nicht in die Struktur der ansonst erhobenen Informationen passen.

Gerade im Bereich der Informationssicherheit gibt es eine ganze Serie von anerkannten Methoden und Tools, welche zur generellen oder spezifischen Beurteilung der Verletzlichkeiten (Risiken) oder für ein eigentliches Sicherheitsbenchmarking eingesetzt werden können (z.B. Tools für Vulnerability Assessments wie ISS, CyberCop usw., Risikoanalysetools wie CRAMM, Marion etc.).

Die meisten dieser Tools beinhalten für die Darstellung der Untersuchungsergebnisse vordefinierte Berichtsformate. Diese Berichte sollten an die eigenen Darstellungsstandards angepasst werden.

3.2.5 Unternehmensspezifische Auswahl von Faktoren

Eine sinnvolle Auswahl der Faktoren ist wichtig, damit ein aussagekräftiges Urteil gebildet werden kann. Es zeigt sich, dass verschiedene Faktoren ähnliche Aussagen zulassen. Eine Reduktion auf den am besten messbaren Faktor von mehreren ähnlichen kann einen besseren Überblick verschaffen als die Gesamtheit aller Faktoren.

3.2.5.1 Auswahl pro Kunde/Unternehmen

Die Auswahl der Faktoren ist vor allem abhängig von der Grösse des Unternehmens und der Branche. Davon leiten sich Ausbildung der Mitarbeitenden, Kultur, Technologie, Vorhandensein eines IKS, Notwendigkeit der Einhaltung spezieller Gesetze und deren Überwachung implizit ab.

3.2.5.2 Auswahl/Bestimmung der Faktoren

Die Faktoren können z.B. mit einem pragmatischen Lösungsansatz (siehe Abbildung 5: Wirkungskreis), mit dem mathematischen Ansatz der linearen Optimierung (also der mathematischen Reduktion eines n-dimensionalen Raums auf einen übersichtlicheren m-dimensionalen Raum, wobei m sehr viel kleiner sein sollte als n) oder durch die Entwicklung eines Wirkungskreises in Analogie Probst/Gomez "Vernetztes Denken" bestimmt werden.

Aus einem solchen Wirkungskreis für eine Gefährdungsanalyse kann man z.B. in mehreren Schritten positive und negative Wirkungen darstellen und z.B. für eine genauere Analyse auch mathematisch berechnen. Eine solche mathematische Diskussion würde aber den Rahmen dieses Papiers sprengen (vergleiche hierzu aber Kapitel 6. Prävention).

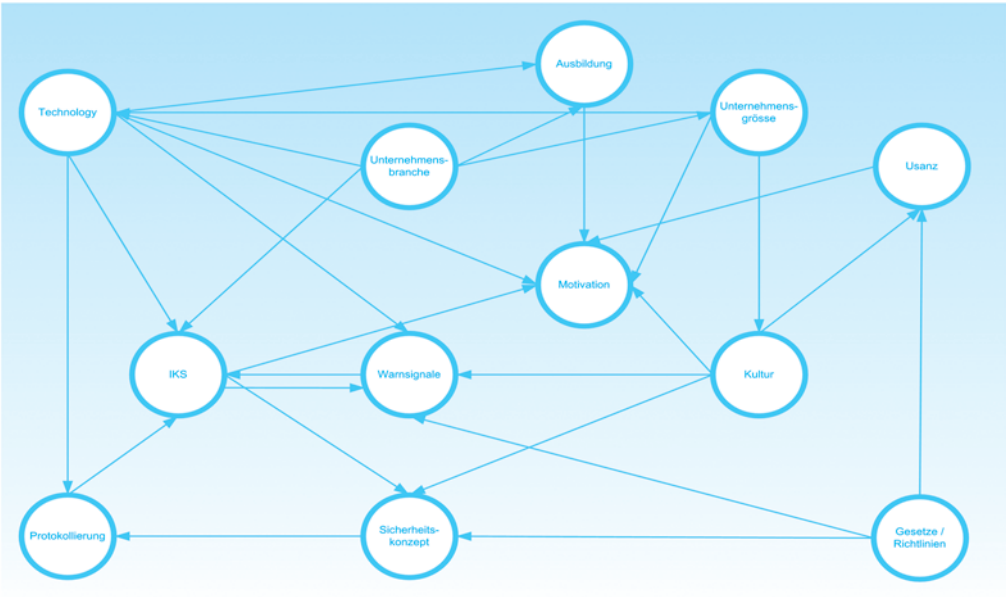
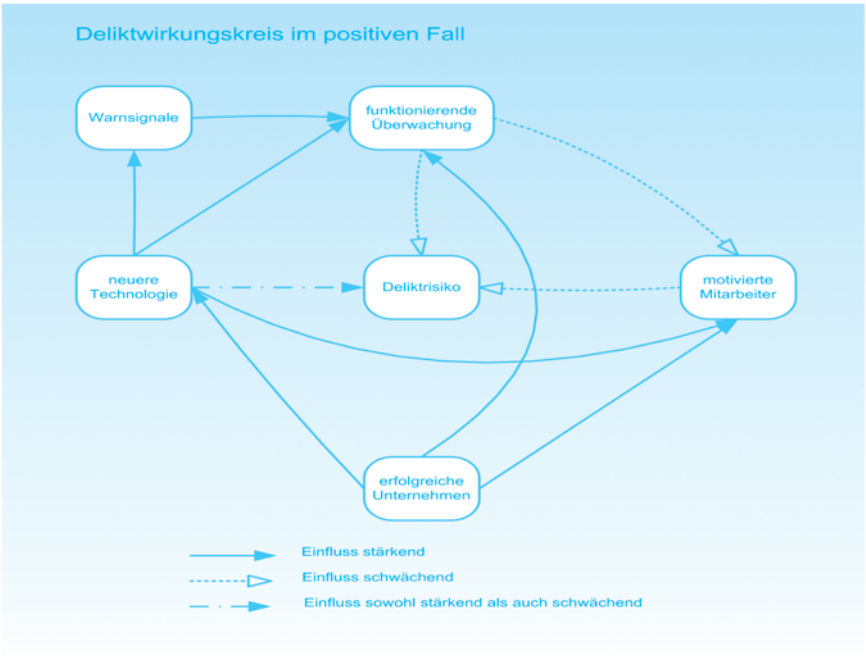


Abbildung 5: Wirkungskreis



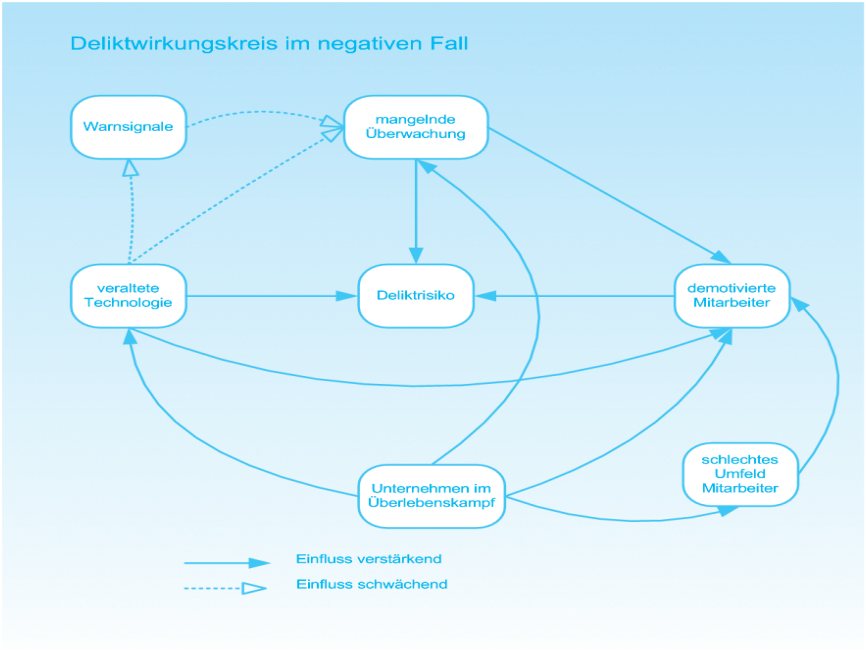


Abbildung 6 und Abbildung 7: Deliktwirkungskreise

3.2.6 Für KMU geeignete Faktoren

Möchte man für ein kleineres oder mittleres Unternehmen (KMU) eine Gefährdungsanalyse durchführen, sind nicht alle der aufgeführten Faktoren geeignet wie dies für ein Grossunternehmen der Fall ist. Grundsätzlich können für kleine Unternehmen die gleichen Faktoren wie bei Grossunternehmen untersucht werden. Je nach Branche des KMU's fehlen aber entsprechende Strukturen und Normen (IKS, interne Standards, Konzepte), z.B. eine sinnvolle Funktionentrennung. Eine Gefährdungsanalyse würde dies als eine Gefahrenquelle ausweisen.

Die "Tabelle 7: Auslöser deliktischer Handlungen" gibt Auskunft über Faktoren und ihre Eignung in Abhängigkeit von der Unternehmensgrösse. Die Einstufung geht von "---" für komplett nicht geeignet bis zu "+++" sehr geeignet. Zu beachten ist, dass unterschieden wurde zwischen Unternehmen mit einer kleinen Bedrohung (Unternehmen ohne grossen Geldfluss) oder solchen mit einer grossen Bedrohung (z.B. Banken, Unternehmen mit grossem Warenumsatz).

1. Faktoren, welche Auskunft über die Einfachheit zur Ausführung von deliktischen Handlungen geben (enabler):	KMU (kleine Bedrohung)	KMU (grosse Bedrohung)	Grossunternehmen (kleine Bedrohung)	Grossunternehmen (grosse Bedrohung)
Komplexität	+	++	+	+++
Volumen	-	+	+	+++
Qualität der Sicherheitskonzepte	+	++	++	+++
Richtlinien und Standards	+	++	++	++
Sicherheitsmassnahmen	++	+++	++	++
Qualität des IKS	+	+++	++	+++
Grad der Funktionentrennung	-	+	+	+++
Grad der Nachvollziehbarkeit	++	+++	++	+++
Qualität der Überwachung	++	+++	++	+++
Vertrauen in Technik	++	+	++	+++
Vertrauen in Einzelpersonen	-	+	++	+++
Grad des Sicherheitsbewusstseins	++	+++	++	+++

2. Faktoren, welche Hinweise zu möglicherweise erfolgten delik-tischen Handlungen geben (red flags) :	KMU (kleine Bedrohung)	KMU (grosse Bedrohung)	Grossunternehmen (kleine Bedrohung)	Grossunternehmen (grosse Bedrohung)
Stornorate	+	+++	++	+++
Korrekturbuchungen	+	+++	++	+++
Kundenreklamationen	++	+++	++	+++
Medienanfragen	++	+++	++	+++
Überstunden	-	++	++	+++
Wochenendarbeit	-	+	++	+++
tageweise Ferien	-	+	++	+++
Schlüsselpersonen	-	++	++	+++
Lebensstil und Einkommen	++	+++	-	++
unkooperatives Verhalten	+	++	-	+

3. Faktoren, welche deliktische Handlungen auslösen können (trigger) :	KMU (kleine Bedrohung)	KMU (grosse Bedrohung)	Grossunternehmen (kleine Bedrohung)	Grossunternehmen (grosse Bedrohung)
Arbeitsklima	+	++	+	++
Über-/Unterforderung	+	++	+	++
Zeitdruck	-	+	+	++
Leistungsdruck	+	++	+	++
Führungsstruktur	-	+	++	+++
Führung (Stil, Schwächen)	+	++	++	+++
Personalfluktuation	+	++	++	+++
Entlassung, Arbeitsplatzabbau	+	++	++	+++
Lebensstil	++	+++	+	++
Alkoholsucht, Drogensucht, andere Krankheiten	++	+++	+	+
persönliches Umfeld	++	+++	+	++

Tabelle 7: Auslöser deliktischer Handlungen

4 Durchführung einer Ermittlung

4.1 Grundsätzliche Aspekte

4.1.1 Ziel einer Ermittlung

Für ein Unternehmen stehen immer die eigenen Ziele und Interessen im Vordergrund. Aus diesem Grund ist es von zentraler Bedeutung, die bevorzugten Vorgehensweisen bei Computerdelikten aufgrund der Geschäftsziele zu definieren. Es geht also nicht a priori darum, mögliche Täter zur Rechenschaft zu ziehen, auch wenn dies sehr wünschenswert ist und im Interesse eines Unternehmens sein kann. Es kann jedoch durchaus sein, dass erlittene Verluste beziehungsweise die Wahrscheinlichkeit, dass davon wieder etwas zurückgewonnen werden kann, die Kosten für die Ermittlung und den Gang vor Gericht nicht rechtfertigen. Die genaue Bestimmung sowie die Priorisierung der Ziele sind grundsätzlich die Aufgaben des Managements. Der folgende Ablauf zeigt die wesentlichen Schritte auf, welche selbstverständlich von Fall zu Fall unterschiedlich sein können:

1. Schaden begrenzen

Das erste Ziel ist es, den Schaden zu begrenzen, d.h. zu verhindern, dass sich der erlittene Schaden noch weiter vergrössert.

2. Erlittene Verluste zurückgewinnen

Falls es der benötigte Aufwand rechtfertigt, wird versucht, erlittene Verluste wieder zurückzugewinnen. Z.B. über die Täterschaft oder die Versicherung, sofern vorhanden.

3. Künftige Schäden vermindern

Aufgrund einer Risikoanalyse werden angemessene Massnahmen getroffen, welche die Wiederhol-Wahrscheinlichkeit und/oder die potentiellen Schäden eines vergleichbaren künftigen Vorfalles auf ein vertretbares Mass reduzieren.

4. Täterschaft zur Rechenschaft ziehen

Das konsequente Erstatten einer Strafanzeige hat klar präventive Wirkung, kann aber je nach Sachlage negative Publizität nach sich ziehen. Die Reputations-Risiken müssen von Fall zu Fall beurteilt werden.

Die folgenden Erläuterungen gehen von der Annahme aus, dass ein Unternehmen über die entsprechenden Personen und ihren assoziierten Funktionen verfügt. Sollten bei kleineren und mittleren Unternehmen einzelne, hier erwähnte Funktionen nicht direkt besetzt sein oder existieren, dann ist es trotzdem wichtig, entsprechende Rollen und Aufgaben, sofern sinnvoll, an verfügbare und qualifizierte Personen interimistisch zu delegieren.

4.1.2 Zusammensetzung des Ermittlungsteams

4.1.2.1 Zentrale Ermittlungsverantwortung

Um eine professionelle, qualitativ hochstehende Ermittlung durchführen zu können, muss eine zentrale Ermittlungsverantwortung definiert und auch kommuniziert werden. Vor allem sollte verhindert werden, dass ein Führungsverantwortlicher bei Verdachtsmomenten auf eigene Faust gegen seine Mitarbeiter ermittelt. Die Erfahrung hat gezeigt, dass einerseits die Versuchung besteht, die Sache selbst in die Hand zu nehmen und anderseits diese Eigeninitiativen, aufgrund mangelndem Ermittlungswissen des jeweiligen Führungsverantwortlichen, oft in einem Desaster enden.

4.1.2.2 Kernteam

Das Kern-Ermittlungsteam besteht im optimalen Fall aus den folgenden Personen:

- *Ermittler:* Die Verantwortung betreffend des Vorgehens, im Speziellen die Einvernahme von Mitarbeitern, liegt bei den Ermittlern. Für diese Funktion eignen sich besonders Personen mit professioneller Erfahrungen in diesem Bereich, z.B. ehemalige Polizisten.
- *Computer-Ermittlungsspezialist:* Die Computer-Ermittlungsspezialisten unterstützen die Ermittler auf der technischen Ebene. Sie sichern und analysieren elektronische Beweismittel. Für diese Funktion eignen sich besonders Personen mit IT-Sicherheits- und Revisionskenntnissen sowie vertieften und umfassenden IT-Kenntnissen.
- *Kommunikationsverantwortlicher:* Bei grösseren und zeitkritischen Fällen empfiehlt es sich, einen Kommunikationsverantwortlichen zu bestimmen, der die unter Druck stehenden Ermittler entlastet. Diese Person sollte nicht selber ermitteln, aber überall als Beobachter dabei sein und die interne Kommunikation übernehmen. Für diese Funktion eignen sich vor allem Personen mit Erfahrung im Management Reporting und einem guten technischen IT-Verständnis.

4.1.2.3 Erweitertes Team

Je nach Situation und den vorhandenen Bedürfnissen wird das Kernteam um folgende Funktionen erweitert:

- Juristen
  Es empfiehlt sich zu Beginn einer Untersuchung, juristische Unterstützung in Anspruch zu nehmen. Von Vorteil sind interne Juristen, welche über die nötigen Strafrechtsangelegenheiten Bescheid wissen. Beim Beizug von externen Juristen für eine Untersuchung ist immer der Kostenfaktor im Auge zu behalten.

- Controller
  Insbesondere wenn es sich um eine Untersuchung handelt, bei der Finanztransaktionsanalysen durchgeführt werden müssen, ist die Hilfe durch einen Controller unerlässlich. Er wird der Ansprechpartner sein, wenn bei der Ermittlung die entsprechenden Zusammenhänge innerhalb des Unternehmens eine tragende Rolle spielen.

- Interne Revisoren
  Ebenso wie der Controller ist die interne Revision von grossem Nutzen. Sie kennt in den allermeisten Fällen eine Unternehmung sehr gut und verfügt über das notwendige Wissen, einzelne Bereiche detailliert analysieren zu können. Sofern eine interne Revision vorhanden ist, sollte sie unbedingt in die Ermittlungen einbezogen werden, da auch sie über einen grossen Erfahrungshintergrund aus den einzelnen Bereichen verfügt.

- Pressesprecher
  Es zeigt sich immer wieder, dass es sehr wichtig ist, wie ein Vorfall kommuniziert wird. Um Imageschäden vorzubeugen, sollte sich jedes Unternehmen Gedanken machen, ob und zu welchem Zeitpunkt und mit welchen Informationen an die Öffentlichkeit getreten werden soll.

- Managementvertretung
  Es empfiehlt sich einen direkten Kontakt zum Management aufrecht zu erhalten, um bei schwierigen, zeitkritischen Situationen innert kürzester Zeit die Autorisation für wichtige Entscheidungen zu erhalten.

- Technische Spezialisten
  Unter Umständen ist es auch notwendig, neben IT-Spezialisten, weitere Experten konsultieren zu können. Diese zusätzlichen Know-how-Träger sind bei Bedarf hinzuzuziehen.

- Externe Berater
  Qualitativ gute, externe Berater sind bei Ermittlungen in vielen Fällen unerlässlich. Sie verfügen über die notwendige Erfahrung in kritischen Situationen, entsprechend strukturiert und zielgerichtet vorzugehen. Gerade KMU's haben in den wenigsten Fällen eine interne "Eingreiftruppe", welche bei Wirtschaftsdelikten, bei denen der Computer das Tatwerkzeug darstellt, sprich bei computerkriminellen Handlungen, die notwendigen Untersuchungen führen können.

4.1.3 Interne Kommunikation

Eine funktionierende, angemessen kontrollierte, zeitgerechte interne Kommunikation ist das Fundament jeder erfolgreichen, professionellen Ermittlung. In diesem Bereich existieren die meisten Fallgruben und es geschehen demnach die meisten Fehler; oft mit irreparablen Folgen.

4.1.3.1 Technische vs. Managementkommunikation

Die hohe Komplexität von IT-Vorfällen führt oft zu Missverständnissen und Fehlinterpretationen des Management. Aus diesem Grund ist es meistens sinnvoll, die technische Kommunikation von der Management-Kommunikation zu trennen.

4.1.3.2 Führungs- & Informations-Rhythmus

Ein klarer Führungs- und Informations-Rhythmus verbessert die Kommunikationseffizienz. Bei jedem Meeting wird abgemacht, wann man sich das nächste Mal trifft und bei jedem Informationsmail wird angegeben, wann das nächste Mal informiert wird.

Vor allem für Bereiche mit regelmässigen Vorfällen (z.B. Virenabwehr, e-Services etc.) bewährt es sich, im Voraus e-Mail-Verteiler zu definieren.

4.1.3.3 Ermittlungsbezogene Interaktion mit Externen

Bei ermittlungsbezogener Interaktion mit externen Stellen, z.B. für externe Abklärungen oder bei Anzeigen durch Externe, besteht ein erhöhtes Reputationsrisiko. Folgende Punkte sollten unbedingt beachtet werden:

- Betroffene bzw. anzeigeerstattende Externe sollten immer über psychologisch erfahrene Personen angesprochen werden.
- Werden Kunden oder indirekt betroffene Externe in die Ermittlungen als Quellen miteinbezogen, dann können bescheidene finanzielle Abgeltungen an Externe sinnvoll sein. Sie sollten aber, um Missinterpretationen (z.B. Bestechungsversuch) zu vermeiden, klar als Entschädigung für Aufwände, Spesen, Umtriebe etc. deklariert werden.
- Es sollte vermieden werden, Details im schriftlichen Verkehr mit betroffenen Kunden oder Dritten aufzuführen, da solche Stellungnahmen leicht missbraucht werden können.

- Unter allen Umständen ist es zu vermeiden, Geschäfts- oder Bankgeheimnisverletzungen zu begehen.
- Unabhängig der Branche sollte jedes Unternehmen, welches mit externen Leistungserbringern zusammenarbeitet, eine entsprechende Vertraulichkeitsvereinbarung abschliessen. Ein Beispiel hierzu ist unter A. Beispiel Vertraulichkeitsvereinbarung auf Seite 164 aufgeführt.

4.1.3.4 Journalführung

Für grössere Fälle mit vielen Einzelereignissen bewährt es sich, ein Journal im Sinne eines Logbuches zu führen, d.h. Zeitpunkt eines Ereignisses, das Ereignis, die getroffenen Massnahmen und die involvierten Personen sequentiell festzuhalten. Der Eintrag in einem solchen Journal könnte wie folgt aussehen:

Datum / Zeit	Journalführung	Was ist geschehen
31.07.03 / 16:30	Arthur Honegger (AH)	Meldungseingang durch: Alberto Giacometti …
17:12	AH	FiBu Server wurde auf Antrag von AH vom Netz genommen.
21:15	AH	Daten des Verdächtigen Charles F. Ramuz sichergestellt, Auswertung …
01.08.03 / 08:15	Jacob Burckhardt (JB)	Hinweis durch die Personalabteilung, Sophie Taeuber: …
10:35	JB	Management-Meeting: Entscheid…
etc	etc	etc

Tabelle 8: Journal

Aufgrund der Komplexität von forensischen Fällen empfiehlt es sich, Erkenntnisse zu visualisieren: Systemübersicht, Geldströme, Angriffspfade, Transaktionswege etc.

4.1.4 Presse

Für die Pressekommunikation ist, falls vorhanden, die interne Pressestelle oder andernfalls die Geschäftsleitung verantwortlich. Falls keine geeignete und im Umgang mit der Presse geübte Person zur Verfügung steht, sollte auf die schriftliche Einreichung der Fragen bestanden werden. Ein allfälliges Presse-Interview benötigt entsprechende Vorbereitung – korrekte und ausgewogene Antworten auf die erwarteten Fragen sollten vor dem Interview zur Verfügung stehen. Das Eingestehen begangener Fehler in der Öffentlichkeit nimmt der Presse oftmals den Wind aus den Segeln. Es gibt nichts Rufschädigenderes, als ein über Monate andauernder Skandal mit immer wieder neuen Enthüllungen und Schlagzeilen.

4.1.5 Unabhängigkeit der Ermittler

Die Unabhängigkeit der Ermittler muss sichergestellt werden. Ein Ermittler muss einen Fall ablehnen, falls er befangen ist oder seine Unabhängigkeit berechtigterweise angezweifelt werden kann.

4.1.6 Schutz der Privatsphäre in der Praxis

Eine Überprüfung von Personen durch Zugriff und Auswertung von Daten in persönlichen Verzeichnissen stellt einen bedeutenden Eingriff in die Privatsphäre dar und soll nur bei konkretem Verdacht zugelassen werden. Von generellen Überprüfungen ohne konkrete Verdachtsmomente ist aufgrund von datenschutzrechtlichen Bedenken abzusehen. Ein bestehender Verdacht soll, vor dem Zugriff auf Daten in persönlichen Verzeichnissen, schriftlich begründet und festgehalten werden. Auch soll vorher definiert werden, wonach gesucht werden soll. Eine unabhängige Stelle, welche den verdächtigen Personenkreis nicht kennt oder zumindest keinen persönlichen Bezug dazu hat, soll aufgrund von klar definierten Rahmenbedingungen diese Daten bezüglich Relevanz auswerten. Um den Eingriff in die Privatsphäre so gering wie möglich zu halten, sollen nur die relevanten Daten für Ermittlungszwecke zur Verfügung gestellt werden. Im Weiteren ist zu beachten, dass in den entsprechenden Weisungen und Richtlinien der Unternehmung die Rahmenbedingungen für einen solchen Datenzugriff definiert sein sollten.

4.2 Ablauf einer Untersuchung

Nachfolgend wird der eigentliche Ablauf einer Untersuchung im Detail erläutert. In diversen Fällen mögen einzelne Schritte überflüssig sein. Es ist somit in der Verantwortung eines Ermittlers situationsbedingt zu entscheiden, ob die unten aufgeführten Schritte (vergleiche dazu nachfolgende Abbildung 8: Ablauf einer Ermittlung) notwendig sind. Die nachfolgenden Aktivitäten gelten sowohl für Ermittler öffentlicher Behörden als auch für firmeninterne Ermittler.

Die Strafverfolgungsbehörden nehmen erst durch das Vorliegen einer Strafanzeige bei Antragsdelikten oder durch die Tat selbst (Offizialdelikt) ihre Ermittlungsaufgaben wahr. Das bedeutet, dass je nach Zeitpunkt – seit dem Begehen der Straftat – die forensischen Spuren auf den inkriminierten Datenbeständen und Hardwarekomponenten intakt oder bereits teilweise vernichtet sind. Je länger der Vorgang zurückliegt, desto weniger können die notwendigen Beweismittel beschafft werden.

Um gerichtsverwertbare Daten zu erlangen ist – je nach Policy des Unternehmens – eine frühzeitige Einbindung der Strafverfolgungsbehörden angezeigt.

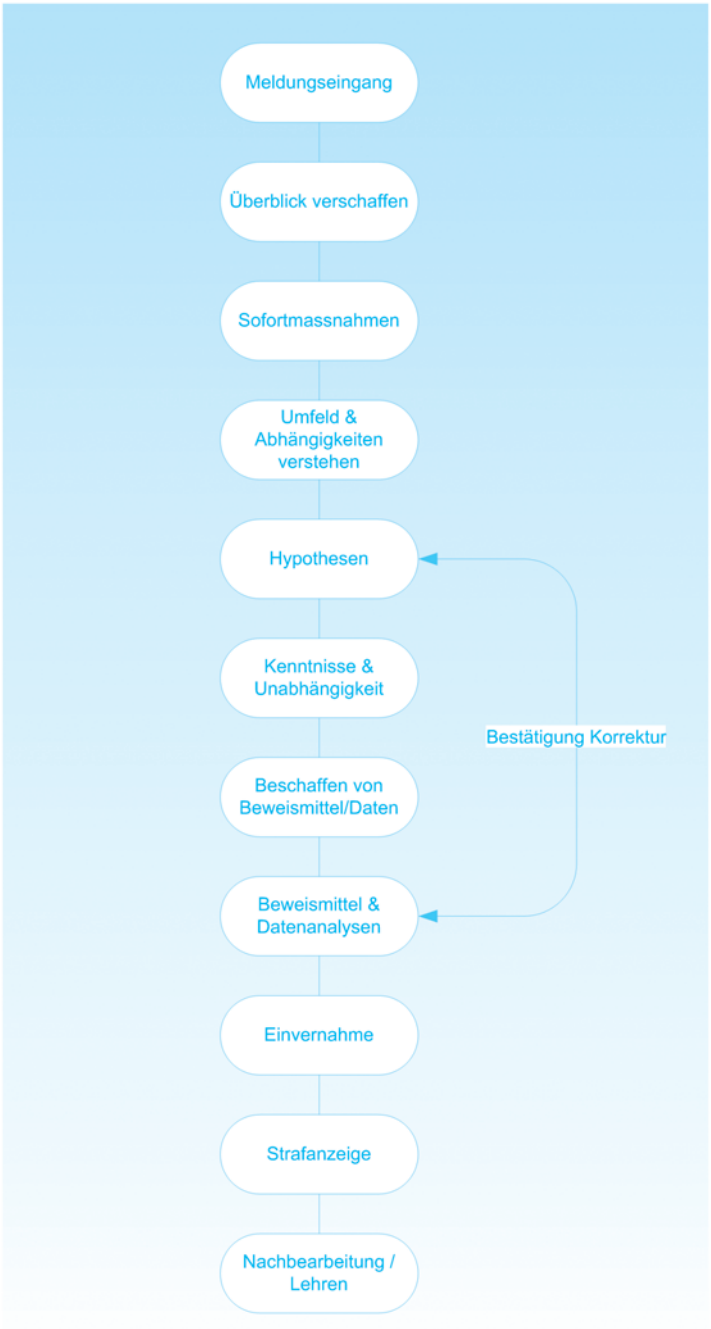


Abbildung 8: Ablauf einer Ermittlung

4.2.1 Meldungseingang

Der Fall beginnt in den meisten Fällen mit einem Meldungseingang: Eine Person oder Gruppe von Internen oder Externen bemerkt einen ungewöhnlichen resp. verdächtigen Vorfall. Um eine funktionierende, zentrale Bearbeitung von Fällen realisieren zu können, müssen die Meldewege und Verantwortlichkeiten in einer Unternehmung klar definiert und kommuniziert sein. Vor allem sollten Personen in Abteilungen, welche aufgrund ihrer Tätigkeit am ehesten Vorfälle entdecken könnten, ausgebildet und sensibilisiert sein. Z.B. interner IT Help-Desk, Kundenberater, Kunden Help-Desk, e-Services Help-Desk, IDS-Verantwortliche, Monitoring- und Firewall-Team, Top-Management, Personen im Bereich der Datenvernichtung, internes Controlling, interne und externe Revision, Rechtsdienst sowie weitere. Die Etablierung von Kommunikationskanälen für den Meldungseingang, z.B. das Einrichten einer eMail-Adresse sowie einer 24h-Sicherheits-Hotline zur Triage von Meldungen etc. ist für grössere Unternehmungen auf jeden Fall empfehlenswert.
Die e-Mail-Adresse abuse@eigenes_unternehmen.ch sollte für Internet-Meldungen eingerichtet sein, sie gilt international als "Best Practice" Standard.

Doppelter Nutzen einer Fraud Hotline

Eine sogenannte "Fraud Hotline" bietet jedem Mitarbeiter oder Vorgesetzten die Möglichkeit, Auffälligkeiten, Unregelmässigkeiten oder Verdachtsmomente telefonisch oder über andere Kanäle der Ermittlungsstelle zu melden. Je nach Situation ist der Mitarbeiter dabei auf die vertrauliche Behandlung seiner Meldung angewiesen. Eine solche Hotline mit Ermittlungsstelle kann sowohl von einem Unternehmen selbst als auch von einem externen Partner betrieben werden. Beim internen Betrieb eignen sich dafür besonders der interne Sicherheitsdienst, die interne Revision oder die Compliance-Abteilung. Beim externen Betrieb ist es wichtig, dass ein vertrauenswürdiger Partner gewählt wird, welcher sich durch den Erhalt von geschäftsgeheimen Informationen den Informanten nicht in die Lage eines Vertrauensmissbrauchs gegenüber seinem Arbeitgeber manövriert.

Präventive Wirkung

Die Existenz einer Betrugsmeldestelle hat klar präventive Wirkung, da dies impliziert, dass intern eine Ermittlungsstelle existiert, welche bei Betrug oder Verstössen gegen interne Weisungen ermittelt. Zudem wird dadurch ein klares Zeichen gesetzt. Unredlich arbeitende Mitarbeiter und Vorgesetzte müssen damit rechnen, dass ihr Handeln, falls es bemerkt wird, gemeldet wird. Dies kann entsprechende Konsequenzen nach sich ziehen. Der Gefahr, dass Mitarbeiter ungerechtfertigt angeschuldigt werden können und somit

der Entstehung einer Denunziation der Weg geebnet wird, muss entgegengewirkt werden. Dies wird erreicht, indem die entgegennehmende Fraud Hotline eine adäquate Triage des vorliegenden Tatbestandes durchführt.

Zuerst müssen zusätzliche Informationen zur Verifizierung der Anschuldigungen beschaffen werden. Im Weiteren müssen die richtigen Personen und Funktionsträger des Unternehmens kontaktiert werden, damit diese den Vorfall intern begleiten oder übernehmen können. Zum Schutz der Informanten und der Verdächtigten ist es wichtig, dass Untersuchungen und daraus entstehende Prozessveränderungen oder Anpassungen von Kontrollen mit der notwendigen Professionalität und ohne grosses Aufsehen durchgeführt werden.

Verbessern von Reputation und Unternehmenskultur

Das Betreiben einer Fraud Hotline vermittelt zudem sowohl gegenüber den Internen als auch gegenüber den Externen ein positives Bild. Es wird signalisiert, dass Betrug und Verstösse gegen interne Weisungen nicht akzeptiert werden sowie ethische und Compliance Aspekte ernst genommen werden. Dies stärkt die interne und externe Glaubwürdigkeit der Firma und damit die Reputation nach aussen wie auch die Loyalität und Zufriedenheit der Mitarbeiter. Wirtschaftsdelikte beeinträchtigen auch die Zufriedenheit von Mitarbeitern, welche selbst nicht direkt am Vorfall beteiligt waren.

Im Allgemeinen ist es auch eine Frage der Unternehmenskultur, wie eine solche Meldestelle eingeführt und betrieben wird. Wesentlich ist dabei, dass sich die obersten Organe eines Unternehmens mit dem Betrieb einer Fraud Hotline identifizieren können, ohne einen "Überwachungsstaat" zu schaffen, unter welchem letztendlich die Produktivität leidet.

Bei kleineren und mittleren Unternehmen empfiehlt es sich, sich zumindest im Klaren zu sein, wer für das eigene Unternehmen als Erstes eine solche Triage durchführen kann. Diese Anlaufstelle kann sowohl von einer internen als auch von einer externen Stelle übernommen werden. Des Weiteren ist es immer hilfreich, wenn bereits Ansätze im Umgang mit forensischen Tätigkeiten diskutiert und entsprechend erarbeitet werden.

4.2.2 Überblick verschaffen

Nach dem Eingang einer Meldung geht es in erster Linie darum, sich einen Überblick zu verschaffen, zu verstehen was geschehen ist und abzuschätzen, wie (zeit)kritisch der Vorfall möglicherweise sein könnte. Die folgende Checkliste soll die wesentlichen Aspekte aufzeigen, über welche man Bescheid wissen sollte, bevor irgendwelche Aktionen in die Hand genommen werden:

Checkliste: Überblick verschaffen nach Meldungseingang

Was ist passiert?	
Weshalb wurde etwas bemerkt?	
Welche Daten, Systeme, Applikationen sind involviert? Welche sind direkt betroffen?	
Gibt es im betroffenen Umfeld erhöhte Anforderungen an die Vertraulichkeit oder an die Verfügbarkeit?	

Personen & Kommunikation	
Wer hat den Vorfall wann gemeldet?	
Wer ist involviert?	
Wer wird verdächtigt?	
Ist der Vorgesetzte informiert? Muss der Vorgesetzte informiert werden?	
Ist der Personaldienst informiert? Muss der Personaldienst informiert werden?	
Ist das Management informiert? Muss das Management informiert werden?	

Schaden	
Ist ein Schaden entstanden? Finanziell? Verfügbarkeit? Vertraulichkeit? Integrität?	
Besteht das Risiko, dass ein Schaden entsteht?	
Besteht das Risiko, dass sich der Verlust vergrössert?	

Beweismittelbeschaffung & Sofortmassnahmen	
Wo liegen die kritischen Beweismittel?	
Könnten Beweismittel zerstört werden, wenn nicht sofort gehandelt wird?	
Ist der Fall zeitkritisch?	
Besteht die Gefahr, dass der Täterkreis versucht, Beweismittel zu zerstören?	
Könnte eine Ermittlungsperson direkt oder indirekt (als Mittelsperson des Täters) involviert sein?	
Besteht die Gefahr, dass sich der Täterkreis im zu ermittelnden Umfeld befindet? Wem kann in diesem Umfeld vertraut werden?	
Kann offen ermittelt werden oder muss verdeckt ermittelt werden?	
Steht der Fall in einem Gesamtkontext von Vorfällen oder ist es ein Einzelfall?	
Hat man genügend Informationen erhalten um A) die Schwere des Falles und die Risiken abschätzen zu können? B) angemessene Sofortmassnahmen anzuordnen? C) das weitere Vorgehen zu definieren?	

4.2.3 Sofortmassnahmen

Auch wenn Sofortmassnahmen so schnell als möglich ergriffen werden müssen, ist es unabdingbar die Folgen und Risiken vorher zu beurteilen, um die Verhältnismässigkeit der Massnahmen sicherzustellen. Je nach Situation sind unterschiedliche Sofortmassnahmen notwendig:

- System herunterfahren (Vergleiche hierzu Kapitel 5.4.1)
- System physisch oder logisch vom Netz nehmen
- Monitoring verstärken (z.B. temporäre Videoüberwachung einrichten)
- Logging aktivieren bzw. nach gewünschten Kriterien (Muster) anpassen
- Logische und physische Autorisationen sperren oder einschränken
- Beweismittel jeglicher Art vor Zerstörung schützen
- Im betroffenen Umfeld allfällige Gruppen-Passwörter oder Einzelpassworte ändern

Nach den getroffenen Sofortmassnahmen erfolgt eine erste interne Kommunikation mit der Beschreibung des Falles, den getroffenen Massnahmen, den nächsten Schritten und Anträgen an das Management. Von einer Einvernahme der Verdächtigen zu diesem Zeitpunkt ist in den allermeisten Fällen dringend abzuraten. Die Erfahrung hat gezeigt, dass gerade nach den Sofortmassnahmen immer wieder Einvernahmen durchgeführt werden, welche sich zu einem späteren Zeitpunkt als verfrüht herausgestellt haben.

4.2.4 Umfeld und Abhängigkeiten verstehen

Im nächsten Schritt geht es darum, die gewonnenen Erkenntnisse durch ein besseres Verständnis für das Umfeld und die Abhängigkeiten zu vertiefen und bestehende Vermutungen zu verifizieren und falls notwendig anzupassen. Durch vertrauliche Befragungen von Personen (z.B. Vorgesetzte auf höherer Stufe, Personaldienstverantwortliche etc.), welche das betroffene Umfeld und die involvierten Personen kennen und aufgrund der Sachlage nicht als Täter in Frage kommen, soll ein besseres Verständnis für Umfeld und Abhängigkeiten auf technischer sowie auf Beziehungs- und Arbeitsebene erlangt werden.

Checkliste: Umfeld und Abhängigkeiten	
Was macht die betroffene Abteilung?	
Wie sind die Verantwortlichkeiten und Kompetenzen in dieser Abteilung?	
Gibt es bekannte Seilschaften in der betroffenen Abteilung?	
Wie ist die Zusammenarbeit mit anderen Abteilungen?	
Könnten Personen aus anderen Abteilungen involviert sein?	
Was macht die verdächtigte Person?	
Was sind die Verantwortlichkeiten und Kompetenzen der verdächtigten Person?	
Wie zuverlässig sind die benützten Informationsquellen? Können die Aussagen verifiziert bzw. plausibilisiert werden?	
Welche Technologien, Plattformen und Applikationen werden verwendet?	
Kommunikations-, Datenfluss- und Transaktionskonzepte?	
Abhängigkeiten von anderen IT Systemen, Vernetzung?	

Checkliste: Hintergrundabklärungen	
Finanzlage der Involvierten (Personalabteilung einbinden)?	
Sind Lohnzessionen bekannt?	
Werden Lohnbestandteile direkt verwaltet?	
Ist eine Scheidung bekannt?	
Ist die Zugehörigkeit zu einer extremistischen Religionsgemeinschaft bekannt?	
Falls das Unternehmen selbst den Mitarbeitenden ein Lohnkonto vorschreibt. Wie verhält sich der Kontostand des Mitarbeitenden?	
Ist der Betroffene bereits polizeilich bekannt?	
Was weiss allgemein das mitarbeitende Personal über den Mitarbeitenden (Abhängigkeiten, Suchtverhalten, sexuelle Neigungen, Freizeitbeschäftigungen usw.)?	
Wie ist die Stimmung allgemein in der Organisationseinheit?	
Über welche Fahrzeuge verfügt die Person?	
Dienstreisetätigkeiten vor dem Vorfall?	
Welche Kontakte hatte der Mitarbeitende?	
Sind Vorfälle bei anderen im gleichen Wirtschaftszweig tätigen Organisationen bekannt?	
Inwiefern könnte sich der Mitarbeitende mit technischen Massnahmen Backdoors, Trojaner, Zeitbomben etc. abgesichert haben?	
Sind Resultate einer Potentialanalyse, eines Assessment oder ähnliches über die Person vorhanden?	
Ist der Einbezug eines Profilers notwendig? Ist Schadenssumme hoch genug?	

4.2.5 Hypothese

Aufgrund aller vorhergehenden Abklärungen ist man nun in der Lage, Hypothesen bezüglich des Vorfalls aufzustellen, und kennt die Orte, wo relevante Beweismittel liegen könnten. Diese Hypothesen sollten immer aufgrund des wahrscheinlichsten Szenarios aufgestellt werden. Wobei auch mögliche weniger wahrscheinliche "Worst Case"-Szenarios und damit auch die Konsequenzen von Ermittlungsaktivitäten im Fall von falschen Hypothesen berücksichtigt werden sollten. Die einzelne Hypothese muss getestet werden, indem alle Fakten und Voraussetzungen, welche diese Hypothese definieren, akkurat verifiziert werden. Nach der Prüfung der Hypothese ist es in den meisten Fällen notwendig, die Hypothese zu verfeinern und somit zu präzisieren. Anschliessend müssen die zusätzlich gewonnen Erkenntnisse wieder auf ihre Plausibilität hin geprüft werden. Mehrfach wird es notwendig sein, die Hypothese auszubauen und in einen grösseren Kontext zu bringen. Hierbei kann es hilfreich sein zu versuchen, die entsprechende Hypothese mit anderen Hypothesen oder Ansätzen zu verknüpfen.

Auf dem Markt gibt es einige Softwaretools, welche zur Visualisierung von Ermittlungsergebnissen entwickelt wurden. Oftmals sind diese Programme sehr kostenintensiv und sollten aus diesem Grund, bei vorliegender Notwendigkeit einer Anschaffung, angemessen auf die entsprechenden Bedürfnisse evaluiert werden. Es sollte aber auf jeden Fall versucht werden, alle Erkenntnisse, Beziehungen, Zugehörigkeiten, Besitzverhältnisse, Profile etc. zu visualisieren. Dafür sind Methodiken wie Mindmaps, Ursachen-Wirkungsdiagramme, Morphologische Kästen, Brainstormings etc. z.B. auf Flipcharts geeignet.

4.2.6 Fachkenntnisse und Unabhängigkeit

Genügend Fachkenntnisse, Ressourcen, die technischen Mittel für die gerichtlich verwendbare Aufbereitung der Beweismittel und eine angemessene Unabhängigkeit sind notwendige Vorraussetzungen für einen aussichtsreichen Fall. Wenn diese Bedingungen nicht erfüllt sind, besteht das Risiko, dass eine Anklage zu einem späteren Zeitpunkt wegen Verfahrensfehlern fallen gelassen werden muss. Der Beizug von externen Experten muss in Erwägung gezogen werden. Der Entscheid basiert im Wesentlichen auf einer Kosten-/Nutzenrechnung. Das Budget, der erlittene Verlust, die Wahrscheinlichkeit, dass ein Teil des Verlustes wieder zurückgewonnen werden kann, müssen im Hinblick auf die Notwendigkeit, derartige Ereignisse in Zukunft vermeiden zu können, abgewogen werden.

4.2.7 Beschaffung von Beweismitteln/Daten

Es besteht eine erhebliche Gefahr, dass die Beweismittel zu einem späteren Zeitpunkt nicht mehr korrekt gesichert werden können, da sie inzwischen verloren gegangen sind (z.B. aufgrund knapper Backup-Zyklen) oder verändert wurden und deshalb die Gerichtsverwendbarkeit nicht mehr gegeben ist. Aus diesem Grund ist es essentiell, dass bei jeder Beweismittelsicherung professionell vorgegangen wird, auch wenn in diesem Zeitpunkt noch nicht feststeht, ob es am Ende der Ermittlung zu einer Strafanzeige kommt oder nicht.

Eine Angestellte wird in einem Unternehmen verdächtigt, deliktische Handlungen zu begehen. Das Unternehmen fokussiert ihre Ermittlungen und Beweismittelbeschaffung auf den persönlichen Bereich dieser Mitarbeiterin.

Das Unternehmen möchte den persönlichen Schubladenstock der Verdächtigen unbemerkt durchsuchen:

> Dieser Schritt ist aufgrund des Persönlichkeitsrecht fraglich. (Doch unter gewissen Voraussetzungen zulässig.) Art. 328 Abs. 1 OR verweist bei der Erläuterung der Pflichten des Arbeitgebers auf die Wahrung der Persönlichkeitsrechte nach Art. 28 ZGB. Das Durchsuchen eines Schubladenstocks kann, sofern private und intime Gegenstände des Arbeitnehmers darin gefunden werden, eine Beeinträchtigung des Privatlebens darstellen. Die Widerrechtlichkeit liesse sich allerdings vertraglich ausschliessen, sofern der Arbeitnehmer im Arbeitsvertrag zustimmt, dass sein Büromaterial (Bürotisch und Schubladen) gegebenenfalls durchsucht werden könne. Eine solche Einwilligung sollte vor Art. 27 ZGB standhalten, denn es ist dem Arbeitnehmer zumutbar, private oder intime Sachen nicht am Arbeitsplatz zu hinterlegen.
>
> Ohne vertragliche Einwilligung findet Art. 328 Abs. 1 OR seine Grenze bei den Erfordernissen des Arbeitsverhältnisses (Art. 328 Abs. 2 OR). Man kann argumentieren, dass es aus unternehmerischer Sicht teilweise notwendig sein kann, Schränke oder Schubladen eines Mitarbeiters zu öffnen, um Dokumente oder Gegenstände zu finden, welche aus unternehmerischen Gründen dringend benötigt werden. Der Arbeitgeber sollte folglich auch in Schubladen oder Schränke Einsicht nehmen können. Ziel darf aber nicht das Auffinden persönlicher Gegenstände sein.

Das Unternehmen möchte ein verschlossenes Couvert aus diesem Schubladenstock unbemerkt öffnen:

> Ein solches Vorgehen ist strafrechtlich unzulässig, denn das Öffnen einer Schrift, ohne dazu berechtigt zu sein, stellt eine strafbare Handlung dar (Art. 179 StGB, Verletzung des Schriftgeheimnisses). Das Bundesgericht hat im Entscheid BGE 114 IV 17 ff jedoch konkretisiert, dass an ein Unternehmen adressierte Briefe (erste Zeile des Couverts mit Bank AG, Seestrasse 23, 8000 Zürich) mit dem Zusatzvermerk "zu Handen von Herrn Charles F. Ramuz " als an das Unternehmen adressiert zu gelten haben und nicht zum Ausdruck bringen, dass die betreffende Person ausschliesslich zur Öffnung der Schrift berechtigt ist. Vorgesetzte können ebenfalls den Brief öffnen. Sofern jedoch der Vermerk "Persönlich" angebracht wurde, ist die Schrift eindeutig ausschliesslich an die betreffende Person adressiert und darf daher nicht geöffnet werden.
>
> Private Briefe, die in keiner Weise an das Unternehmen adressiert sind, z.B. ein Brief, den ein Mitarbeiter zu Hause im Briefkasten erhielt und zur Arbeit mitnahm und dann verschlossen liess, sind jedenfalls durch Art. 179 StGB geschützt und dürfen nicht geöffnet werden.

Das Unternehmen möchte die Handtasche der Verdächtigen unbemerkt durchsuchen:

> Die Frage lässt sich nach denselben Überlegungen wie beim ersten Fall bereits angestellt beantworten. In diesem Falle gelingen jedoch die zwei Ausschlussmöglichkeiten der Widerrechtlichkeit (eine vertragliche Einigung oder der Arbeitszweck) nicht. Eine vertragliche Vereinbarung, heimliche Durchsuchungen der eigenen privaten Tasche zu erdulden, sind nach Art. 27 ZGB übermässige Bindungsverträge, bei welchen die Freiheit des Arbeitnehmers in einem die Sittlichkeit verletzenden Grade eingeschränkt wird. Ausserdem kann das Durchsuchen von privaten Taschen kaum durch den unternehmerischen Arbeitszweck gerechtfertigt sein. Allerdings sind Leibesvisitationen bei der Torkontrolle (z.B. Taschenkontrolle zur Verhinderung von Diebstählen) nach diversen Gerichtsentscheiden zulässig (z.B. OGer. ZH JAR 1985, 209).

Die oben beschriebenen Handlungen sind grundsätzlich von Strafuntersuchungsbehörden vorzunehmen und nicht von firmeninternen Personen. Die Bestimmungen des Strafprozessrechts über zulässige Hausdurchsuchungen durch die Untersuchungsbehörden sind hierbei anwendbar. Um die Verletzung der obig erläuterten Normen (Persönlichkeitsrechte nach ZGB 28 und die Verletzung des Schriftgeheimnisses nach Art. 179 StGB) zu legalisieren, müsste eine konkrete Notwehrsituation oder eine Wahrung höherer Interessen vorliegen.

Sofern das Unternehmen erheblichen Verdacht schöpft (z.B. ein Gegenstand wurde gestohlen und nur ein Mitarbeiter hatte Zugang zum Ort, wo sich der Gegenstand befand), kann von einem im Gange befindlichen Angriff gesprochen werden, der eventuell, durch Notwehrrecht gerechtfertigt, mit den erwähnten Massnahmen abgewehrt werden kann. Stellt sich die Vermutung danach als falsch heraus, beurteilt sich dies nach den Fragen des Sachverhaltsirrtums (Art. 19 StGB). Derjenige, der gestützt auf eine Fehlvorstellung das Notwehrrecht beansprucht hat, wird gegebenenfalls nach dem Sachverhalt gestellt, den er sich vorgestellt hat. Hätte er jedoch den Irrtum bei pflichtgemässer Vorsicht vermeiden können, so ist er wegen Fahrlässigkeit strafbar (Art. 19 Abs. 2 StGB). Deswegen sind sehr hohe Verdachtsanforderungen zu stellen und zur Absicherung des Unternehmens auch zu archivieren, um nach Feststellung eines Fehlverdachts nicht in Anspruch genommen zu werden.

Eine Wahrung höherer Interessen kann vorliegen, wenn ein im öffentlichen Interesse stehendes Gut geschützt werden soll. Dem Arbeitgeber in einer Waffenfabrik (denkbares Beispiel) könnte es in Einzelfällen, aufgrund hohen Verdachts, gestattet sein, in die Privatsphäre des Arbeitnehmers durch die erwähnten Handlungen einzugreifen, um das höherstehende öffentliche Interesse, die Sicherheit der Bevölkerung, zu wahren.

4.2.7.1 Grundsätze für die Erlangung beweiskräftiger elektronischer Informationen

1. Integrität der Daten bewahren

Die von Ermittlern durchgeführten Tätigkeiten dürfen keine Veränderungen an denjenigen Daten verursachen, die in der Folge eventuell vor Gericht verwendet werden. Beschlagnahmte Gegenstände sind vor Änderungen jeglicher Art zu schützen. Dabei muss auch die Möglichkeit äusserer Einflüsse wie Magnetismus oder Funkwellen in Betracht gezogen werden. Die Erfahrung hat hierbei gezeigt, dass es immer wieder Täter gibt, welche über ausgeklügelte Schutzmechanismen für ihre Infrastruktur verfügen.

Ein Beispiel: Ein PC soll in einem Büro beschlagnahmt werden. Der Türrahmen zum Raum, in welchem der entsprechende PC steht, wird mit einem starken Magnetfeld gespiesen. Falls der erwähnte PC durch dieses Magnetfeld, zur Türe hinaus, getragen wird, besteht die Gefahr, dass Daten auf der Festplatte dieses PCs unleserlich gemacht werden. Durch den Transport der Harddisk in einem Faradayschen Käfig könnte diese vor der Wirkung des Magnetfeldes geschützt werden.

In Fällen, bei denen es schwieriger und auch aufwändiger ist, die Integrität der gespeicherten Daten zu garantieren, da keine Festplatten vorhanden sind, z.B. bei (mobilen) Telefonen oder digitalen Assistenten, müssen alle Aktivitäten, die für die Gewinnung der Informationen getätigt wurden, für andere nachvollziehbar festgehalten werden.

Die Integrität der Daten wird durch den Einsatz einer forensisch korrekten, nicht invasiven Software sichergestellt, welche von den sichergestellten Datenträgern mittels eines speziellen Verfahrens vor Ort, ein identisches Abbild (Image) erstellt, ohne dabei Originaldaten zu verändern. Es dürfen grundsätzlich keine Untersuchungsarbeiten direkt an Originaldatenträgern vorgenommen werden. Für die Abbild-Erstellung und spätere Untersuchung der auf diese Weise erhobenen Daten werden Methoden angewandt, die erprobt und anerkannt sein müssen. Während der Abbild-Erstellung werden automatisch, in einer für Dritte nachvollziehbaren Art und Weise, Prüfsummen (file integrity) der untersuchten Daten erstellt. Diese Prüfsummen stellen elektronische Siegel der untersuchten Daten dar, die Manipulationen jeglicher Form nach der Beweismittelsicherung erkennen lassen.

Um die Integrität und somit auch die Nachvollziehbarkeit zu gewährleisten, ist es von enormer Wichtigkeit, dass die Systemzeit des zu untersuchenden Systems protokolliert und in das erwähnte Prüfsummenverfahren miteinbezogen wird. Vergleiche hierzu Kapitel 5.4.3.

2. Vieraugenprinzip

Alleiniges Agieren eines Ermittlers vor Ort ist, wenn möglich, zu vermeiden. Um später verlässliche Aussagen machen zu können, empfiehlt es sich, im Minimum zu zweit am "Tatort" zu ermitteln.

3. Protokollierung

Alle Tätigkeiten, welche auf dem elektronischen Beweismaterial durchgeführt werden, sind zu protokollieren bzw. aufzuzeichnen und aufzubewahren. Ein unabhängiger Dritter sollte in der Lage sein, diese Tätigkeiten nachzuvollziehen und dabei dasselbe Ergebnis zu erhalten. Die Nachvollziehbarkeit ist einer der wichtigen Aspekte, besonders im Hinblick auf ein mögliches Gerichtsverfahren.

4. Rechtmässigkeit

Die rechtlichen Rahmenbedingungen für den Zugriff auf Daten müssen eingehalten werden, so z.B. die Gewährung des Bankgeheimnisses.

4.2.7.2 Arten der Sicherstellung

Grundsätzlich bestehen vier Möglichkeiten zur Sicherstellung elektronischer Informationen. Bei allen Möglichkeiten sind unbedingt Experten und Firmenangehörige z.B. als Zeugen für die korrekte Abwicklung der Sicherstellung beizuziehen. Des Weiteren können solche Personen, bei Bedarf, als technische Unterstützung oder in Notfällen, bei unbeabsichtigten Beeinträchtigungen des Betriebes, dienen.

1. Sicherstellung und Beschlagnahmung

Folgende Aspekte sind bei der Sicherstellung und Beschlagnahmung von elektronischen Geräten und Datenträgern relevant:

Vorteile:

- Das gesamte Beweismaterial wird unter Kontrolle gebracht.
- Auswertung findet in einer kontrollierten Umgebung statt. Die allenfalls notwendige Sorgfalt bei der Auswertung der Daten kann somit ungestört angewendet werden.

Nachteile:

- Gefahr einer Beschädigung der Hardware.
- Mögliche Beeinträchtigung anderer nicht in Verbindung mit dem Ermittlungsfall stehender Aktivitäten.

Anwendungsempfehlung:

- Bei Einzelcomputern oder kleinen Netzwerken in kleinen Unternehmungen. Der Zeitfaktor erscheint hier als wichtigster Gradmesser. Können Resultate im Netzwerk ohne weiteres erlangt werden, so erübrigt sich die Beschlagnahme der Geräte.
- Wenn die Beschlagnahmung aufgrund des Vorfalles erforderlich erscheint oder wenn strafrechtlich relevante Daten vorhanden sind, deren Besitz in sich bereits eine Straftat darstellt. Oder wenn die Komplexität der Datenbestände einen Überblick über die Vollständigkeit der Daten vor Ort verunmöglicht.
- Wenn die vorhandenen IT-Komponenten nicht mehr auf dem üblichen Weg auf dem Markt beschafft werden können, um eine gleiche Umgebung nachzubauen.

Bei dieser Methode wird mit Hilfe von Spezialgeräten ein exaktes, beweisbar unverfälschtes Abbild des Speicherinhaltes einer Festplatte auf ein externes Speichermedium kopiert, wo es anschliessend in einer geschützten Umgebung und mit geeigneten Werkzeugen ausgewertet werden kann. International wird dafür auch der Begriff Mirroring verwendet.

Vorteile:

- Keine Beschädigungsgefahr für die zu untersuchende Hardware.
- Geringes Risiko, andere Aktivitäten negativ zu beeinträchtigen. Der operative Betrieb des Systems selbst sowie umliegender Systeme wird kaum und wenn, dann nur kurz gestört.
- Die Datenanalyse kann in einer kontrollierten Umgebung erfolgen.

Nachteile:

- Spezielle Geräte und entsprechendes Fachwissen sind erforderlich.
- Zeitaufwändig (für 10 GB ca. 45')

Anwendungsempfehlung:

- Kleine bis mittlere Unternehmen.
- Bei erheblichen Abhängigkeiten vom betroffenen IT System.
- Bei Gefahr, dass einem Dritten "grosser" Schaden zugefügt werden könnte.
- Wenn eine Beschlagnahmung unverhältnismässig erscheint.

2. Beschlagnahmung von Backups

Bei grossen Netzwerken und Mainframe-Umgebungen kann die Sicherstellung und Analyse von Backup-Bändern zielführend sein. Dieser Vorgang darf aber den übrigen Betrieb nicht beeinträchtigen.

Vorteile:

- Minimale Beeinträchtigung der betroffenen Systeme und Umgebung.
- Kleiner Aufwand.

Nachteile:

- Es besteht ein erhebliches Risiko, dass Beweise übersehen werden.
- Die Beweiskraft, d.h. Integrität der gewonnenen Informationen muss speziell sichergestellt werden (Time stamp, Beglaubigung etc).

Anwendungsempfehlung:

- Bei bekannten Stichworten, mit denen in Dateien gesucht werden kann.
- Falls eine Beschlagnahmung oder ein Imaging des Systems nicht möglich oder unangemessen ist. Wobei zu beachten ist, dass der Begriff "unangemessen" bezüglich Zeitaufwand und verfügbare Speichermedien verwendet wird.

3. Selektives Kopieren von Daten

Eine weitere Möglichkeit besteht auch darin, Dateien selektiv zu suchen, zu kopieren und anschliessend auszuwerten. Die Suche nach solchen Dateien erfolgt mittels Stichworten und wird auf alle vorhandenen Dateien angewendet, da Daten, durch Umbenennung von Dateiendungen, versteckt werden können. Die Auswahl von geeigneten Stichworten steht somit bei dieser Vorgehensweise im Zentrum des Erfolges.

4.2.7.3 Lagerung von elektronischen Beweismitteln

Informatiksysteme und elektronische Beweismittel müssen unter bestimmten Bedingungen gelagert werden, um die Hardware und die gespeicherten Daten vor Zerstörung zu schützen. Die Einhaltung folgender präventiver Massnahmen wird dringend empfohlen:

- Physisch gesicherter Lagerraum mit Zutrittskontrolle
- Brandschutzvorrichtungen, Brandmelder, keine unnötigen brennbaren Materialien, striktes Rauchverbot
- Temperatur sollte bei ca. 21°C liegen und es muss trocken sein
- Keine, über das normale Mass hinausgehende, elektromagnetische Einstrahlung (Sendeantennen, Hochspannungsanlagen etc.)
- Antistatische Bodenbeläge
- Keine wasserführenden Leitungen in Decke und Boden

4.2.7.4 Orte von elektronischen Beweismitteln

Die nachfolgende Auflistung zeigt mögliche Orte von elektronischen Indizien und Beweismitteln:

Mögliche Orte für Logfiles & Daten
Client Software
e-Mail-Client (Sent-Items, Inbox, Archive, Deleted Items, Adressen, Headers)
Office-Daten (lokal, privates Drive, Gruppendrive)
Online-Agenden
Logische Schlüssel zu Daten/Applikationen (Passworte, Private Keys, Dongles)
Internet, Internet-Suchmaschinen (Daten)
Internet-Browser (Surf-History, Temporäre Dateien, Cookies etc.)
Server Software
Applikationen
Datenbanken
e-Mail-Server (Logs, e-Mail-Daten-Backups, Disaster-Recovery Ausrüstungen)
e-Mail-Gateway (Logs)
Internet-Gateways (Logs)

Hardware	
	Platinen (CMOS-Informationen, z.B. Passwort)
	Festplatten
	Speicherkarten
	PCMCIA-Karten
	Physische Schlüssel zu Geräten
	Chipkarten (Passworte, Daten)

Systeme	
	Client / Server / Middleware / Host
	Transaktionssysteme /-server
	Backup-Medien (Bänder, Roboter)
	Videoaufzeichnungs-Systeme
	Kopierer mit Festplatte
	Faxgeräte, e-Mail-Faxsysteme
	Zutrittssysteme, (Logs, Berechtigungen)

Peripherie	
	Drucker
	Scanner
Telefone / PBX (Gespeicherte, gewählte Telefonnummern, Adressen, Namen, Logs)	

Mobile Geräte	
	Personal Digital Agents
	Mobiltelefone
	Pager

Mobile Speichermedien	
	Disketten (3_", Jaz- und Zip-Disketten)
	CDs/DVDs
	Speicherdongles

Umfeld-Überprüfungen

- Hat jemand im verdächtigen Personenkreis psychische, beziehungs- oder finanzielle Probleme oder einen Lebensstil, welcher mit den Einkommensverhältnissen nicht übereinstimmt?
- Mit Daten aus der Personalabteilung verifizieren.
- Wie sehen die Beziehungsnetze aus? Bestehen Abhängigkeiten?

Interviews

- Personaldienst, Abteilungsleiter, lokale Sicherheit etc.
- Vorsicht, keine Interviews mit den Verdächtigen zum Sammeln von Beweismitteln führen und keine Interviews mit Personen führen, die aufgrund von Beziehungen mit den Verdächtigen befangen sein könnten.

Geschichte

- Gibt es bereits ähnliche Vorfälle im Unternehmen?
- Gibt es weitere Vorfälle im betroffenen Umfeld oder mit den verdächtigen Personen?

4.2.8 Beweismittel- und Datenanalyse

Ziel der Analysephase ist es herauszufinden, was wirklich geschehen ist, d.h. die Hypothese aufgrund von Indizien mit hoher Beweiskraft zu bestätigen, zu korrigieren oder zu widerlegen.

4.2.8.1 Analyse der Beweismittel

Die Beweismittel müssen bezüglich Relevanz für den Tatbestand beziehungsweise den Vorfall analysiert werden. Ferner ist es hilfreich, den Modus Operandi zu verstehen, um so Aussagen über die typische Vorgehensweise der Täter zu machen oder um bekannte Tatmuster zu erkennen. Die Beweismittel müssen auf Plausibilität und Nachvollziehbarkeit überprüft werden. Als Ergebnis der Analyse von Beweismitteln sollte auch das Tätermotiv herausgearbeitet werden. Bei der Überprüfung der Beweismittel muss immer in Erwägung gezogen werden, dass technische Probleme, eine Viren- oder Trojanerverseuchung oder ähnliches vorgelegen haben könnten. Ferner ist auch denkbar, dass sich eine Drittperson die Rechte der verdächtigen Person verschafft und missbraucht hat. Mögliche Indikatoren dafür sollten unbedingt abgeklärt werden. Dabei sollte spezifisch nach installierter Spionage-Software oder aufgeschriebenen Passwörter gefahndet werden. Das Hacking- beziehungsweise IT Know-how der verdächtigen Person und in deren Umfeld sollte, sofern möglich, eruiert werden. Wichtig zu wissen ist auch, wer während des Vorfalles anwesend war und ob der Vorfall auch von einem anderen "Ort" über das Netzwerk ausgelöst worden sein könnte.

Hat man alle Beweismittel zusammengetragen, sollte abgeklärt werden, ob Lücken oder Widersprüche in der Beweiskette existieren. Ansonsten sollte es möglich sein, den Vorfall aufgrund der Aufzeichnungen (Logs) zeitlich lückenlos nachzuvollziehen. Aufgrund der Analyse sollte die These mit einer hohen Wahrscheinlichkeit bewiesen werden können. Ansonsten muss die These angepasst und es müssen allenfalls weitere Spezialisten beigezogen werden, welche weitere Beweismittel zur Analyse sammeln können. Zu diesem Zeitpunkt ist es auch notwendig, die gesammelten Beweise explizit mit Personen zu verknüpfen, um so allenfalls zusätzliche Erkenntnisse zu gewinnen. Sollte dies nicht den gewünschten Erfolg bringen, dann müssen die Ermittlungen aufgrund mangelnder Beweise eingestellt werden.

4.2.8.2 Kriterien für eine hohe Beweiskraft der Beweismittel

Nachfolgende Kriterien garantieren für eine hohe Beweiskraft von Informationen (Log-Files, Dateien, Aussagen).

Allgemein kann festgehalten werden, dass die Aussagekraft von Beweismittel sich vergrössert, je grösser die Vertrauenswürdigkeit (Integrität) der Beweismittel beziehungsweise des Interviewpartners ist.

Log-Files sollten auf verschiedenen Systemen, Plattformen und Applikationen, welche von unterschiedlichen Administratoren betreut werden, gesammelt werden. So z.B. stimmt der Login-Zeitpunkt des Täters mit den effektiven Präsenzzeiten überein? Des Weiteren sollten Log-Files durch unterschiedliche Benutzerkonten mit unterschiedlichen Login-Passwörter generiert worden sein. Der logische Zugriff auf die Log-Files sollte eingeschränkt sein. Ferner ist es von eminenter Bedeutung, die Integrität von Log-Files nachweisen zu können. Die Vorraussetzungen dafür werden stark limitiert, falls Benutzer berechtigte Zugriffe mit Administrationsrechten auf ein solches System haben. Als Beweismittel benützte Dateien müssen mit den Dateien auf Backupbändern verglichen werden, um so die Integrität verifizieren zu können. Diese Dateien sollten auf verschiedenen Systemen liegen z.B. e-Mail-Servern und Datenservern.

4.2.9 Einvernahme

Falls die These mit grosser Wahrscheinlichkeit bewiesen und der Verdacht erhärtet werden konnte, kann eine Einvernahme der verdächtigen Personen in Betracht gezogen werden. Je nach Schwere des Falles muss entschieden werden, ob eine interne Einvernahme durchgeführt oder ob direkt die Polizei eingeschaltet werden soll. Insbesondere bei der internen Einvernahme ist zu berücksichtigen, dass die arbeitsrechtlichen Rahmenbedingungen eingehalten werden. Die Einschaltung der Polizei kann angebracht und notwendig sein, hat aber den Nachteil, dass die Kontrolle über den weiteren Verlauf der Ermittlung aus den Händen gegeben wird. Spätestens vor der Einvernahme sollte das lokale Management informiert werden. Folgende grundsätzliche Aspekte sollten bei einer internen Einvernahme (Konfrontation eines Verdächtigten mit vorliegenden Beweismitteln) berücksichtigt werden.

Die Aufnahme der Einvernahme auf Tonträger oder Videobänder kann kontraproduktiv wirken und dazu führen, dass keine Aussagen gemacht werden. Besser ist eine schriftliche Protokollführung, da sie auf den Verdächtigen weniger aggressiv wirkt und der Angeschuldigte am Ende der Einvernahme dieses Protokoll durchlesen und korrigieren kann, bevor er es anschliessend unterzeichnet.

Die Einvernahme sollte niemals alleine durchgeführt werden. Optimal sind zwei Personen: der Ermittler und der Computer-Ermittlungsspezialist. Der Ermittler hat dabei die Leitung und der Computer-Ermittlungsspezialist eine Kontroll- und Unterstützungsfunktion. Mehr als zwei Personen können bedrohlich und dadurch wiederum kontraproduktiv wirken.

Die Erfahrung hat gezeigt, dass die verdächtige Person für die Befragung aus dem gewohnten Umfeld herausgenommen werden sollte. Dies wirkt verunsichernd und führt eher zu einem Geständnis. Die Befragung sollte auf jeden Fall fair erfolgen und der verdächtigen Person soll trotz eines begründeten Verdachtes Respekt entgegengebracht werden. Falls sich der Verdacht schlussendlich nicht bestätigen sollte oder sich durch die Befragung der Vorfall plausibel klären lässt, muss es für diesen Mitarbeiter ohne schlechten Nachgeschmack oder befürchtete Nachteile möglich sein, weiter für das Unternehmen zu arbeiten.

Aufgrund der Resultate der Einvernahme werden je nachdem die Verdachtsmomente fallengelassen, entsprechende Massnahmen durch den Personaldienst getroffen (Verweis, Entlassung) oder eine Strafanzeige erstattet.

4.2.10 Strafanzeige

Ob ein betroffenes Unternehmen eine Strafanzeige bei der zuständigen Instanz einreichen sollte oder ob es gar besser ist darauf zu verzichten hängt von den Umgebungsvariablen des vorliegenden Falles ab. Es müssen Risikoüberlegungen in die Abwägung miteinbezogen werden, da die Reputation des Unternehmens in Mitleidenschaft gezogen werden könnte. Generell sollte die Reaktion des Umfeldes nicht vernachlässigt werden. In einem zweiten Schritt sollten die Kosten den Nutzen gegenübergestellt werden, denn ein Verfahren ist immer für alle Beteiligten eine zeitaufwändige und insbesondere eine kostenintensive Angelegenheit. Diese Prozessrisiken beinhalten auch die Wahrscheinlichkeit auf einen Prozesserfolg, der unter anderem stark von der Beweiskraft der Beweismittel abhängig sein kann. Sollte das Schadensausmass grosse Dimensionen annehmen, empfiehlt es sich, auf eine Strafanzeige hinzuarbeiten.

Es ist in der Vergangenheit auch schon vorgekommen, dass in gewissen Fällen aufgrund von ethischen und menschlichen Überlegungen von einer Anzeige abgelassen wurde. Dies birgt jedoch das Risiko in sich, Nachahmungstäter zu provozieren.

Eine Anzeige hat zumindest für das betroffene Unternehmen eine signalisierende Präventionswirkung, so dass so schnell kein potentieller Delinquent mehr zum effektiven Täter wird. Oft wird auch von einer Strafanzeige abgesehen, wenn die Wahrscheinlichkeit sehr gross ist, dass zumindest ein Teil der Verluste wieder zurückerhalten werden kann. Alle diese Aspekte sollten im jeweiligen Fall berücksichtigt werden.

4.2.11 Nachbearbeitung und Lehren

Ziel der Nachbearbeitung ist es, die Gründe für den Vorfall zu analysieren und daraus Lehren zu ziehen. Zu diesem Zweck soll erörtert werden, mit welchen Massnahmen der Vorfall hätte verhindert werden können. Hierbei ist es wichtig die Wirksamkeit des internen Kontrollsystems zu verifizieren. Dies soll wie folgt ablaufen: In einem ersten Schritt wird analysiert, welche internen Kontrollen überhaupt existieren und in einem zweiten Schritt, bei welchen Ausnahmen die internen Kontrollen nicht greifen. Aus den Erkenntnissen der Nachbearbeitung sollte ein Massnahmenkatalog entstehen, der unter anderem auch eine Neugestaltung einzelner Prozesse beinhalten kann. Zuletzt stellt sich für jedes Unternehmen aber die Frage: "Können die bestehenden Risiken, welche zu diesem Vorfall geführt haben mit vertretbarem Aufwand eliminiert oder verringert werden oder sollen die bestehenden Risiken akzeptiert werden?"

5 Technische Aspekte

Im Anschluss an die prozessorientierte Betrachtungsweise der forensischen Analyse im Kapitel 4 Durchführung, beleuchtet dieses Kapitel die technischen Aspekte bei der Suche nach elektronischen Beweismitteln. Es wird empfohlen, zuerst das Kapitel 4 durchzulesen, da technische Handlungen nur im Kontext eines strukturierten Gesamtvorgehens vorgenommen werden sollten.

Angesichts der komplexen und stets sich weiter entwickelnden IT-Welt ist es eine Herausforderung, das bei der Abwicklung eines konkreten Vorfalls notwendige technische Know-how verfügbar zu haben, sei es firmenintern oder durch externe Partner. Aus demselben Grund können in diesem Dokument nicht alle Betriebssysteme oder Applikationen diskutiert werden. Das Ziel ist vielmehr, dem Leser allgemein aufzuzeigen, wo und wieso elektronische Spuren entstehen können, die zur Rekonstruktion beziehungsweise zur Beweisführung eines Tathergangs verwendet werden können. Bei konkreten Beispielen werden Schwerpunkte im Arbeitsplatzbereich bei Windows- und im Serverumfeld bei Windows- und Unixsystemen gebildet. Grossrechner werden nicht spezifisch betrachtet.

Um dem Leser die Materie zu vereinfachen, wird zwischen Spurenarten und deren Fundorten unterschieden. Die Art beschreibt den Inhalt der elektronischen Spuren, die je nach involvierten Systemen und Anwendungen an verschiedenen Orten vorgefunden werden können. So können beispielsweise Protokolldateien (Art) vom Benutzerarbeitsplatz sowie von mehreren Servern (Ort) zur Beweisführung herangezogen werden.

Dieses Kapitel beginnt entsprechend mit der Einführung in die diversen Spurenarten. Anschliessend werden konkrete Beispiele bei Windows-Arbeitsplätzen sowie bei verbreiteten Anwendungen vorgestellt. Während einer forensischen Analyse wichtige Punkte wie auch technische Hilfsmittel und Werkzeuge werden zum Schluss dieses Kapitels diskutiert.

5.1 Arten von elektronischen Spuren

In den folgenden Kapiteln werden Arten von Spuren allgemein erklärt. Die Erklärung bleibt allgemein, weil solche Spuren grundsätzlich in verschiedenen Typen von Systemen, wie Arbeitsplatz, Server, Netzwerkkomponenten etc., mit unterschiedlichen Betriebssystemen und Anwendungen vorkommen können. Die Auflistung erhebt keinen Anspruch auf Vollständigkeit, sondern soll einen guten Überblick verschaffen.

Die Struktur richtet sich nach den verschiedenen Ursprüngen der beschriebenen Spuren:

- von Benutzern willentlich erstellte Dokumente
- Daten von Anwendungen und Betriebssystem
- Rückstände aus systemnahen Daten
- Flüchtige, d.h. auf der Festplatte nicht gespeicherte, Informationen
- Physisch verbliebene Daten auf einer beschädigten oder überschriebenen Festplatte.

5.1.1 Benutzerdateien

Benutzerdateien sind alle Dateien, die der Anwender durch bewusstes Abspeichern selber erstellt. Oft handelt es sich hier um Dateien, die zu einer spezifischen Applikation, wie beispielsweise einem Textverarbeitungsprogramm, einer Tabellenkalkulation oder einem Mailprogramm, gehören. Oft stellen diese Dateien konkrete Willensäusserungen eines Benutzers dar, weshalb das Auffinden von solchen Files sehr nützlich für die Beweisführung sein kann.

Bei passwortgeschützten oder verschlüsselten Dateien ist durch deren Unlesbarkeit vorerst noch kein Informationsgehalt gegeben. Weitere Anstrengungen sind notwendig, entweder um die zur Entschlüsselung notwendigen Passwörter zu finden oder um sie mit speziellen Passwort-Knackprogrammen zu bestimmen. In einigen Fällen (namentlich bei schwacher Verschlüsselung) ist der Zugriff auch ohne Kenntnis der Passwörter möglich.

5.1.2 Nutzbare Daten von Anwendungen und Betriebssystem

Jedes Betriebssystem und jede Anwendung führt in irgendeiner Form eigene Daten. Diese Art von Daten wird meist im Hintergrund und ohne Benutzerinteraktion verwaltet, sie äussert sich meist nur in Form von spezifisch gestalteten Standardfunktionen. Gerade deshalb können diese Daten im Rahmen einer Spurensuche wertvolle Informationen liefern. Sie werden nämlich mangels Kenntnissen der Benutzer oft nicht aktiv gelöscht. Eine bewusste Löschung ist allerdings bei entsprechendem Wissen und teilweise unter Einsatz geeigneter Hilfssoftware in vielen Fällen möglich. Je nach Anwendung oder System können Einstellungen zum Voraus verhindern, dass solche Spuren überhaupt angelegt werden.

5.1.2.1 Protokolldateien

Betriebssystem und Applikationen können in unterschiedlichem Masse Vorgänge protokollieren. Dazu schreiben sie vordefinierte Vorkommnisse je nach Konfiguration in dedizierte Logfiles. Logfiles dienen der Nachvollziehbarkeit von applikations- und systemspezifischen Vorgängen und Zuständen.

Protokolldateien werden heutzutage vorwiegend geführt, um im Rahmen eines Troubleshooting Hinweise auf Problemursachen ausfindig machen zu können. Sie sind meist nicht auf forensische Ermittlungsarbeiten ausgerichtet und bieten deshalb im schlechteren Fall lediglich Anhaltspunkte über aus forensischer Sicht relevante Vorgänge und Zustände.

Die Protokollierung sollte aus oben den genannten Gründen während dem normalen Betrieb so konfiguriert sein, dass alle relevanten Aktivitäten möglichst lückenlose nachvollziehbar sind.

Es gilt zu berücksichtigen, dass Logfiles relativ einfach manipuliert werden können: So haben Administratoren und zum Teil Benutzer auf ihren Rechnern die Rechte, Protokolldateien und damit wertvolle Spuren zu löschen. Werden diese Dateien als einfach editierbare Files, z.B. Textdateien, geführt, so ist mit den entsprechenden Rechten auch eine Änderung des Inhalts möglich. Dem kann entgegengewirkt werden, indem die Zugriffsrechte entsprechend restriktiv vergeben werden. Die Glaubwürdigkeit von Protokolldateien wird erhöht, wenn deren Inhalt durch Protokolldateien anderer Systeme (und anderer Administratoren) bestätigt wird.

5.1.2.2 Temporäre Files

Diverse Programme legen Dateien auf dem Disk ab, um eine Wiederherstellung der Daten im Falle von Programmfehlern zu erlauben. Microsoft Word, als verbreitetes Beispiel, erzeugt automatisch solche Dateien, ohne dass der Benutzer dies bemerkt. Ist der Vorgang abgeschlossen, löscht die Anwendung die temporären Dateien automatisch.

Temporäre Dateien werden auch dann erzeugt, wenn Daten sequenziell durch verschiedene Programme verarbeitet werden. Ein gängiges Beispiel dafür ist das Ausdrucken von vorbereiteten Reports vom Internet: Hier wird oft eine PDF-Datei im Acrobat Reader angezeigt, und anschliessend über die Druckfunktion des Acrobat Readers ausgedruckt. Dabei erzeugt zuerst der Acrobat Reader eine temporäre Datei. Anschliessend wird die Datei dem Drucker Spooler übergeben, der sie bis zum Senden an den Drucker wieder temporär ablegt. Wird eines der betroffenen Programme durch eine unerwartete Situation (z.B. infolge eines Programmfehlers) beendet, so werden die temporären Dateien nicht mehr automatisch gelöscht und bleiben erhalten.

Auch wenn temporäre Dateien automatisch wieder gelöscht werden, so wurden sie doch auf die Festplatte geschrieben. Wie im Kapitel 5.1.3.1 beschrieben, können gelöschte Dateien unter bestimmten Umständen wieder hergestellt werden.

5.1.2.3 Eingabehilfen

Betriebssystem und Applikationen speichern oftmals ohne Zutun des Benutzers Informationen zuletzt getätigter Aktivitäten, um den Benutzer bei der wiederholten Ausführung derselben Aktion zu unterstützen. Die häufigste Form der Eingabeerleichterung ist die so genannte History, das Auslösen einer bereits getätigten Aktion per "Shortcut". Beispiele solcher Historien sind:

- *Zuletzt aufgerufene Dateien im Windows Explorer oder in MS Office Applikationen*. Diese Aufzeichnung ermöglicht ein schnelles Starten desselben Files über einen Shortcut innerhalb Windows oder der Applikation. Die Informationen sind in Form eines Links auf die Originaldatei mit zugehörigem Pfad, unabhängig, ob sie lokal auf der Festplatte oder auf irgendeinem Server auf einem Netzwerk abgespeichert war, in einem benutzerbezogenen Order abgelegt. Die Informationen können auch dann noch unverändert vorhanden sein, wenn die Originaldatei, auf die der Link zeigt, in der Zwischenzeit gelöscht wurde.
  Interessant ist, dass sogar Dateien, die in ein Officeprogramm der Firma Microsoft (Winword, Excel, Access, Powerpoint etc.) importiert werden, also nie als alleinstehende Datei vom Benutzer geöffnet werden, ebenfalls Niederschlag finden in der Windows History. Beispiele hierfür sind Grafiken oder Objekte aus anderen Dokumenten.
- *Internet Browser History*. Vereinfacht das wiederholte Browsen zu denselben Websites. Zu der Webadresse sind abhängig vom Browser noch übergebene Parameter, Zugriffszeiten sowie Anzahl der Besuche vorhanden. Dadurch ist es möglich zu sehen, wonach beispielsweise gesucht wurde oder welche Daten abgefragt wurden.
- *Shell-History*. Sowohl in der Unix- wie in der Windows-Umgebung werden die in einer Shell ausgeführten Kommandos in Form einer History abgespeichert.

Weitere Eingabehilfen können zum Beispiel sein:

- *AutoComplete im Internet Browser*. Einige Internet Browser bieten die angenehme Funktion, dass sie sich Benutzereingaben beim Ausfüllen eines Internetformulars merken. Wird später ein erneutes Formular ausgefüllt, so müssen nicht mehr alle Daten komplett eingegeben werden (z.B. Suchbegriffe bei www.google.com).
- *Cookies*. Die so genannten Cookies können von aufgerufenen Webseiten je nach Sicherheitseinstellungen auf dem Computer hinterlassen werden, um bestimmte Informationen zu speichern und bei einem nächsten Aufruf wieder abzufragen. Damit können Websites mit benutzerspezifischem Inhalt gefüllt werden, ohne die Benutzerdaten jedes Mal interaktiv abfragen zu müssen.

Eingabehilfen helfen dem Benutzer sich wiederholende Aktionen vereinfacht auszuführen. Da für diesen Zweck bestimmte Daten gespeichert werden müssen, stellen sie eine nützliche Informationsquelle dar, um im Rahmen einer forensischen Analysen, Vorgänge und Zustände zu reproduzieren.

Häufig verwendete Funktionen werden auch über "Shortcuts" in Form von Symbolen aufgerufen. Beispiele dafür sind Icons auf dem Windows-Arbeitsplatz. Die Art der Shortcuts kann Informationen über die Arbeitsweise und Gewohnheiten der Benutzer geben.

Da Eingabehilfen dem Benutzer dienen, sie aber nicht immer erwünscht sind, werden häufig Einstellungen durch die Anwendung zur Verfügung gestellt, die eine Deaktivierung oder ein Löschen der Daten aus der Eingabehilfe ermöglichen.

5.1.2.4 Konfigurationsdateien, Registry

Konfigurationsdateien beziehungsweise die Registry eines Windows-System enthält installationsspezifische Einstellungen der verwendeten Programme. Beispiele für solche Einstellungen sind die Pfade für die Ablage von Daten oder Parametrisierung der Darstellung auf dem Bildschirm. Beim Entfernen von Programmen von einem Rechner (Deinstallation) werden häufig nicht alle Einträge in der Registry angepasst. Aus diesem Grund gewährt die Registry häufig Einblick in die Geschichte eines Rechners, auch wenn der Benutzer versucht hat, diese zu verschleiern.

Einige Programme legen auch Zugriffscodes zu geschützten Daten in der Registry ab. Zugang zu diesen Daten können Möglichkeiten zur Entschlüsselung von verschlüsselten Daten eröffnen.

5.1.2.5 Zeitangaben zu Dateien

Wichtige Informationen über Dateien sind deren so genannten MAC-Zeiten. MAC steht hier für letzte Modification, letzter Access und Creation Zeit, also für die letzte Veränderung und den letzten Zugriff sowie für das Erstellungsdatum der entsprechenden Datei. In der Sprache von Windows sind das die Dateiattribute LastWriteTime, LastAccessTime und CreationTime. Mit ihrer Hilfe können Vorgänge (teilweise) zeitlich nachvollzogen werden. Trotzdem ist Vorsicht geboten, da Betriebssysteme unterschiedlich mit MAC-Zeiten umgehen. So kann es beispielsweise aus Systemsicht korrekterweise vorkommen, dass das Erstellungsdatum jünger ist als das letzte Modifikationsdatum. Aus Gründen der Logik, ist dieser Fall ja gar nicht möglich. Der Ermittler sollte deshalb genau wissen, in welchen Fällen welche Zeit gespeichert wird, um deren Aussagekraft beurteilen zu können. Zudem werden keine Historydaten gespeichert, so dass nur die Zugriffs- und Veränderungszeiten der unmittelbar letzten Aktion sichtbar sind.

5.1.2.6 Zwischenspeicher (Cache)

Zur Erhöhung von Performance sowie Verfügbarkeit kennen Anwendungen und Betriebssysteme die Technik der temporären Speicherung von Daten. So speichert beispielsweise ein Internet Server die aufgerufenen Seiten, damit bei erneutem Zugriff nicht mehr die gesamte Seite über das Internet transportiert werden muss. Dadurch lässt sich die Performance erhöhen. Weiter werden die innerhalb der letzten Zeit aufgerufenen Seiten durch den Browser lokal zwischengespeichert. Ihr Inhalt (inklusive den grafischen Inhalten) steht deshalb lokal, ohne Zugang zum Netzwerk, auf dem Arbeitsplatzrechner zur Verfügung.

Bei lokalen Zwischenspeichern steht dem Benutzer häufig die Möglichkeit zur Verfügung, diese Dateien zu löschen.

5.1.3 Rekonstruierbare, systemnahe Datenrückstände

Aufgrund der Funktionsweise von Betriebssystemen ist es unter bestimmten Umständen möglich, nicht mehr zugängliche Daten zu rekonstruieren. Hierzu werden allerdings spezielle Hilfswerkzeuge benötigt. An dieser Stelle speziell erwähnenswert sind die Wiederherstellung gelöschter Dateien sowie Datenfragmente aus alten Dateien.

5.1.3.1 Gelöschte Dateien

Gelöschte Dateien können unter bestimmten Umständen wiederhergestellt werden. In welchem Masse hängt vom installierten Dateisystem ab. In der Funktionsweisen betreffend Löschen und Wiederherstellen von Dateien gibt es allerdings grosse Ähnlichkeiten zwischen den meisten Dateisystemen.

Die Daten werden grundsätzlich irgendwo auf der physischen Festplatte gespeichert. Damit sie das Betriebssystem finden kann, führen die gängigen Dateisysteme ein Inhaltsverzeichnis, das so genannte Indexfile, welches auf die physische Speicheradresse der effektiven Daten zeigt. Beispiele sind der File Allocation Table bei FAT, der Master File Table (MFT) bei NTFS.

Der Löschvorgang findet im Normalfall im Indexfile und nicht auf der physischen Festplatte statt, da die Löschung einer grossen Datei zu viel Zeit in Anspruch nehmen würde. Da die Daten auf der Festplatte physisch nicht gelöscht, sondern nur der entsprechende Eintrag im Indexfile markiert wird, bleiben die Daten weiterhin bestehen. Deshalb kann eine gelöschte Datei mit geeigneter Software ganz oder teilweise wiederhergestellt werden, solange die einzelnen Sektoren nicht durch neue Daten überschrieben worden sind.

Folgende Abbildung beschreibt den Zusammenhang zwischen Indexfile und physischer Festplatte bei der Löschung einer Datei.

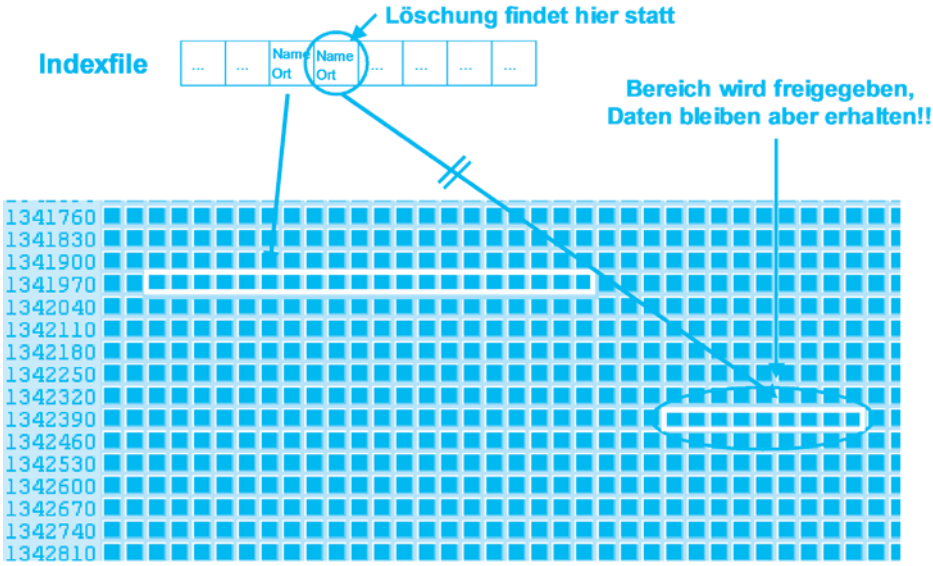


Abbildung 9: Zusammenhang zwischen Indexfile und physischer Festplatte bei Löschung

Grundsätzlich sind alle Arten von Dateien wiederherstellbar, so auch für den Benutzer unsichtbare Systemdateien, die nur temporär erstellt und dann automatisch wieder gelöscht wurden.

Diverse Recovery-Tools, zum Beispiel DOS undelete für FAT oder Restorer2000 für NTFS, können ganze Dateien wiederherstellen. Für die Datensuche in den einzelnen Sektoren werden spezielle Forensic-Programme, zum Beispiel EnCase[118], benötigt.

Interessant ist auch die Tatsache, dass auch bei der Formatierung eines Datenträgers, bei der Löschung einer Partition oder bei einer gesamten Neupartitionierung die Daten physikalisch nicht gelöscht werden. Eine Wiederherstellung ist dadurch mit Spezialprogrammen möglich.

118 Forensic Software, http://www.encase.com

5.1.3.2 Freier Speicherbereich (Slack Space)

Beim freien Speicherbereich, dem so genannten Slack Space, verhält es sich ähnlich wie bei gelöschten Dateien: Aufgrund technischer, für den Benutzer nicht sichtbarer Vorgänge können viele Informationen auf der Festplatte zurückbleiben, auch nachdem der Benutzer sie zu löschen glaubt. Slack Space kann deshalb, im Rahmen von Ermittlungsarbeiten, von grossem Interesse sein. Es ist allerdings anzumerken, dass es sich bei solchen Daten eher um Datenfragmente als um vollständige Dokumente handeln wird.

Der freie Speicherbereich ist derjenige Platz auf der Festplatte, der zur Verfügung steht, um Daten abzuspeichern. Ausser bei neuen Festplatten ist die Wahrscheinlichkeit gross, dass aufgrund des zeitoptimierten Löschvorganges (siehe Kapitel 5.1.3.1) Daten aus alten Dateien in diesem Bereich liegen. Diese Datenreste werden, da sie ja als gelöscht gelten, bei der nächsten Schreiboperation auf diesen Sektor überschrieben. Bei dieser Überschreiboperation bleiben unter Umständen Daten zurück und können mit geeigneten Werkzeugen ausgelesen werden.

Grundsätzlich gibt es drei Typen von freien Speicherbereichen:

1. *Nicht allozierter Speicherplatz* ist jener Bereich auf dem Datenträger, der gegenwärtig nicht in Verwendung ist. Hier können hauptsächlich gelöschte Daten gefunden werden (siehe Kapitel 5.1.3.1).

2. *RAM Slack* ist der Fachausdruck für Daten auf *Sektor*resten. Ein Disksektor ist die kleinste *physisch b eschreibbare* Einheit auf einem Datenträger (typischerweise 512 Bytes). Auch wenn die zu speichernde Datei kleiner als 512 Bytes sind, so müssen beim Speichervorgang 512 Bytes geschrieben werden. Die fehlenden Bytes werden mit Zufallsdaten aus dem Arbeitsspeicher gefüllt, was sich RAM Slack nennt.

3. *Drive Slack* ist der Fachausdruck für Daten auf *Block*resten. Ein Block, im Englischen Cluster, ist die kleinste *adressierbare* Einheit auf einem Datenträger. Ein Cluster besteht, je nach Dateisystem und Formatierung, aus einem oder mehreren Sektoren. Ist diese so genannte Allocation Unit, beispielsweise zwei Sektoren pro Block, also 1024 Bytes, so werden auch dann zwei Sektoren, nämlich ein Block, von einer Datei belegt, wenn diese auch nur 10 Bytes gross ist. Der zweite Sektor wird in diesem Fall beim Speichervorgang der Datei gar nicht beschrieben und enthält weiterhin die bisherigen Daten, den Drive Slack.

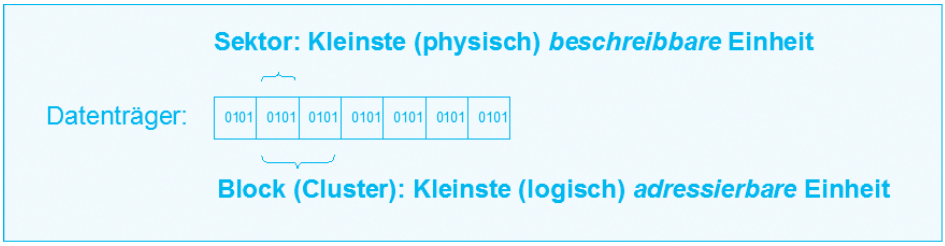


Abbildung 10: Drive Slack

Alle Informationen, die in irgendeiner Weise auf der Festplatte gespeichert waren, auch wenn nur temporär, können sich in freiem Speicherbereich befinden. Weiter kommt hinzu, dass sich per Zufallsprinzip ausgewählte Daten aus dem Arbeitsspeicher im Slack befinden können. In diesem Bereich können durchaus sensitive Daten, wie zum Beispiel verschlüsselte Daten oder Passwörter im Klartext, liegen.

Für das Aufspüren von Daten im Slack werden hohe Anforderungen an die Software gestellt. Mit kommerziellen Forensic-Produkten, wie EnCase[119], können Slacks durchsucht werden.

Sowohl verbliebene Daten von gelöschten Dateien als auch Slack Space können mit Werkzeugen definitiv gelöscht werden, so dass sie auch mit Forensic-Werkzeugen nicht wieder herstellbar sind. Es existieren zum Teil auch Einstellungen bei Betriebssystemen, welche die Entstehung von Slack Space verhindern (Beispiel: High Water Marking bei VMS).

119 Forensic Software, http://www.encase.com

5.1.4 Flüchtige Spuren

Spuren sind dann flüchtig, wenn sie durch das Abschalten des Rechners verloren gehen. Als solche gelten u.a. Informationen im Arbeitsspeicher und laufende Prozesse. Damit Spuren nicht unabsichtlich vernichtet werden, muss bei einer Untersuchung darauf geachtet werden, ob und wie man einen Rechner abstellt (siehe dazu Kapitel 5.4.1 Rechner stoppen).

5.1.4.1 Arbeitsspeicher (RAM)

Der Arbeitsspeicher ist ein flüchtiger Speicher. Das heisst, die Informationen gehen grundsätzlich mit dem Runterfahren des Rechners verloren.

Um die physische Begrenzung des Arbeitspeichers, des so genannten RAM (Random Access Memory) zu erweitern, können heutige Betriebssysteme Teile davon auf die Festplatte auslagern. Der ausgelagerte Teil wird Swap- oder Pagefile genannt. Die meisten Daten, die das System im Arbeitsspeicher hält, können je nach Speicherverfügbarkeit in das Swap-/Pagefile ausgelagert werden.

Der Arbeitsspeicher bzw. das Swap-/Pagefile sind aus forensischer Sicht deshalb interessant, weil dort auch speziell geschützte Daten in einer "verwertbaren" Form liegen können. So können beispielsweise auf der Festplatte verschlüsselte Daten oder auch Passwörter im Klartext gefunden werden. Weiter können Daten vorgefunden werden, die durch den Benutzer nur am Bildschirm bearbeitet, aber nie aktiv abgespeichert wurden.

Grundsätzlich kann das Swap-/Pagefile mit jedem Texteditor durchsucht werden, der mehrere hundert Megabyte grosse Dateien anzeigen kann. Zuerst muss allerdings auf die Datei zugegriffen werden können, da beispielsweise Windows 2000 das Pagefile exklusiv verwendet und dadurch während dem Betrieb Zugriffe durch andere Prozesse verweigert. Das kann umgangen werden, indem beispielsweise von einem Unix-Rechner auf das Windows-Filesystem zugegriffen wird, oder indem der Computer direkt mit einer Unix- oder DOS-Bootdiskette[120] gestartet wird. Die kommerzielle Ermittlungssoftware EnCase erlaubt die Analyse des virtuellen Speichers sogar im laufenden Betrieb.

Einstellungen im Betriebssystem erlauben es, ein Pagefile während dem Herunterfahren des Rechners zu löschen beziehungsweise mit Zufallsdaten zu überschreiben. Ein Auslesen von (alten) RAM-Daten ist dann nicht mehr möglich.

---

120 Unter Verwendung des Tools ntfsdos (www.sysinternals.com/ntw2k/freeware/NTFSDOS.shtml), damit der Zugriff auf NFTS Dateien aus dem Betriebssystem DOS möglich ist.

5.1.4.2 Laufende Prozesse

Die Liste der laufenden Prozesse in einem Rechner kann Informationen über Aktivitäten eines Angreifers, über installierte Hintertüren oder über die Gewohnheiten eines Benutzers geben. Die Prozessliste eines Rechners enthält neben den laufenden auch inaktive Prozesse und solche, welche durch Ereignisse aktiviert werden. Diese können weitere Informationen darüber geben, welche Art von Arbeiten in der letzten Zeit auf einem Rechner durchgeführt worden sind.

Die Prozessliste muss noch vor dem Herunterfahren eines Rechners ausgelesen werden, da diese Information ansonsten verloren geht.

5.1.5 Physische Speicheranalyse

Alle bisher beschriebenen Spurenarten sind logischer Natur. Das bedeutet, dass sie mittels Software-Tools auffindbar sind. Es ist ferner auch möglich, durch eine physikalische Analyse an Daten auf der Festplatte zu gelangen, wenn der logische Zugang verhindert ist.

Einerseits können physisch beschädigte Datenträger, zum Beispiel durch Feuer oder Wasser, in dafür ausgestatten Labors untersucht werden. So ist es möglich, Daten von einer Festplatte zu lesen, welche stark beschädigt ist.

Andererseits sind die physikalischen Löschvorgänge auf den magnetischen Medien (Festplatte) nicht perfekt in dem Sinne, dass nicht alle magnetischen Partikel neutralisiert werden. Spezielle Geräte erlauben die Analyse solcher Restmagnetisierungen. Dies erlaubt ein Lesen von bereits überschriebenen Daten.

Solche Analysen können allerdings nur in spezialisierten Labors durchgeführt werden. Sie sind sehr teuer und werden meist nur in Notsituationen angewendet.

5.2 Fundorte elektronischer Spuren bei Services

Bei der Suche nach Spuren wird man zwangsläufig Zugriff auf persönliche Daten haben. Dies kann Verdächtige betreffen. Es kann aber auch Unbeteiligte betreffen. Das Rechtssystem verlangt einen Schutz dieser Daten. Details zu den einschlägigen Gesetzen finden sich in Kapitel 2.3 Persönlichkeits- und Datenschutzrecht.

5.2.1 eMail mit Mail-Protokollen

Die folgende Abbildung zeigt die typische, technische Situation für den Zugang zum Mail über die eigentlichen Mail-Protokolle (z.B. SMTP und POP).

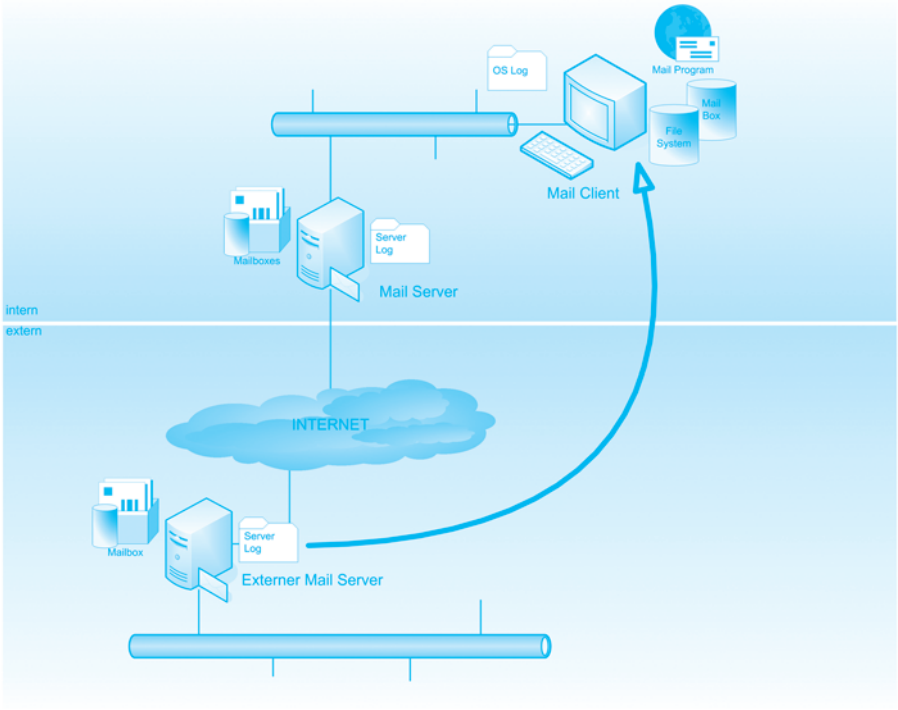


Abbildung 11:Mail mit Mail-Protokollen

Mails werden grundsätzlich über Mail Server übermittelt. In professionellen Installationen wird intern ein solcher Mail Server unterhalten. In kleineren Umgebungen wird ein Mail Server eines Anbieters (z.B. ISP) verwendet.
Der Anwender verwendet ein Mail Programm (Outlook, Outlook Express etc.), welches die Kommunikation mit dem Mail Server vornimmt, und welches die Meldungen verwaltet.

Spuren der Aktivitäten finden sich natürlich auf den Mail Servern (beim Sender und beim Empfänger bzw. bei den betreffenden ISPs). Spuren finden sich aber auch in den Mail Programmen der Endbenutzer. Solche Spuren können in den eigentlichen Speichern der Programme sein (Mail Boxen, Server Logs). Sie finden sich aber auch im Bereich der Infrastruktur der betreffenden Rechner (File System, System Log Dateien).

Im Hinblick auf mögliche forensische Untersuchungen empfiehlt es sich, die angebotenen Log-Mechanismen der eigenen Systeme so weit wie möglich zu aktivieren.

5.2.2 eMail über Web

In diesem Fall wird ein Mail Server verwendet, welcher nicht lokal installiert ist. Dieser Server ist so ausgerüstet, dass seine lokal gespeicherten Daten über einen speziell eingerichteten Web Server zugänglich gemacht werden. Der Anwender greift über einen Standard Browser auf diesen Web Server zu und liest/schreibt seine Meldungen.

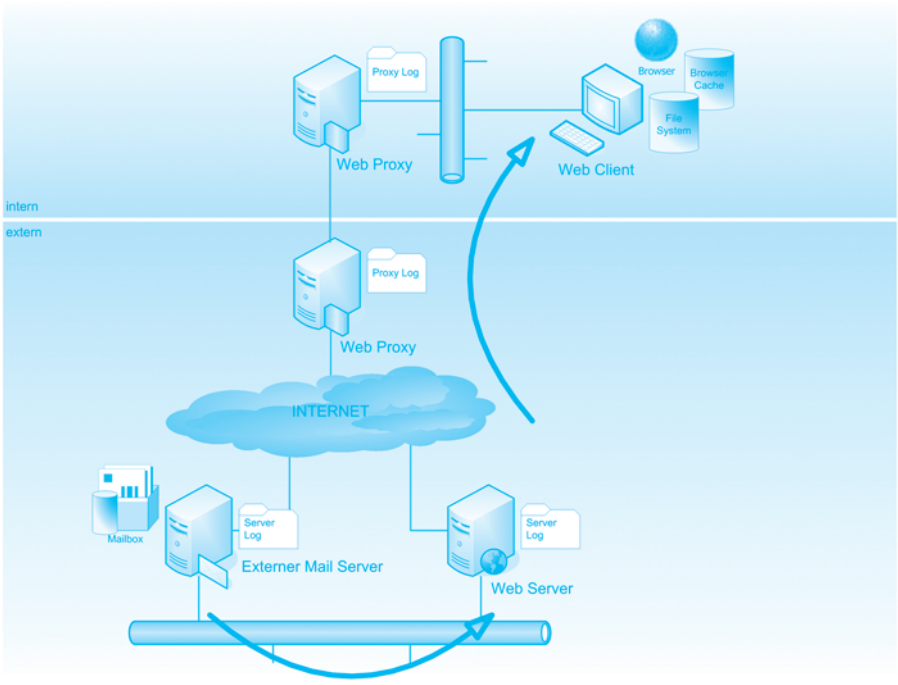


Abbildung 12: Mail über Web

Abbildung 12 zeigt den Zugang zu Mail über ein Browser Interface.

Spuren der Arbeit finden sich natürlich nach wie vor auf allen beteiligten Mail Servern. Zusätzlich können Spuren im Web Server gefunden werden (Log Dateien). Der Zugriff auf den Web Server geschieht über die vorhandenen Mittel des Netz- (Internet) Zugangs. Falls aktive Elemente verwendet werden (z.B. Internet Proxy), so sind auch hier Spuren zu erwarten. Schliesslich finden sich auch Spuren im Browser des Anwenders bzw. in der Infrastruktur der verwendeten Arbeitsstation.

Neben den absichtlich abgespeicherten Daten sind auf dem File System temporäre Dateien zu erwarten (z.B. durch das Ausdrucken von Daten).

Im Hinblick auf mögliche forensische Untersuchungen empfiehlt es sich, die angebotenen Log-Mechanismen der eigenen Systeme so weit wie möglich zu aktivieren.

5.2.3 Web Server

Die Situation ist hier analog zu derjenigen des Surfens (s. Abbildung 14: Surfer) Es ist lediglich "intern" und "extern" vertauscht.

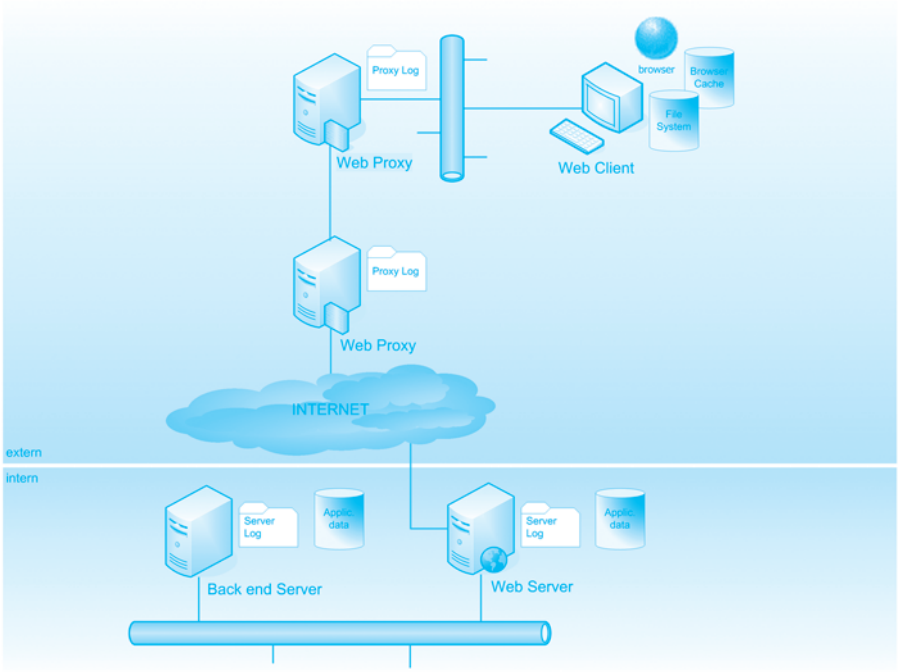


Abbildung 13: Web Server

Der Anwender benutzt seinen Browser, um auf die Daten eines Web Servers zuzugreifen. Spuren finden sich im Browser selbst sowie auch im Bereich der Infrastruktur des verwendeten Rechners. Schliesslich können auch Spuren auf aktiven Elementen der Internet-Infrastruktur lokal gefunden werden.

Häufig beziehen die Web Server ihre angebotenen Daten von einem Back End Server innerhalb der anbietenden Organisation. Auch diese Server können Spuren von Zugriffen enthalten.

Im Falle von Point to Point Netzen (z.B. Morpheus) muss die oben skizzierte Situation allgemeiner betrachtet werden. Im Client wird eine spezielle Anwendung eingesetzt, welche eine eigene Datenverwaltung im lokalen File System vornimmt und diese auch auf dem Netz zur Verfügung stellt. Jeder teilnehmende Client fungiert damit als Server im betreffenden Netz. Interessante Informationen finden sich in diesem Fall auf allen Installationen der am Netz teilnehmenden Partner, insbesondere auch über Verweise auf shared Dateien des untersuchten Teilnehmers.

Im Hinblick auf mögliche forensische Untersuchungen empfiehlt es sich, die angebotenen Log-Mechanismen der eigenen Systeme so weit wie möglich zu aktivieren.

5.2.4 Surfen

Die Situation ist hier analog zu derjenigen des Server-Anbieters (s. Abbildung 13: Web Server). Es ist lediglich "intern" und "extern" vertauscht.

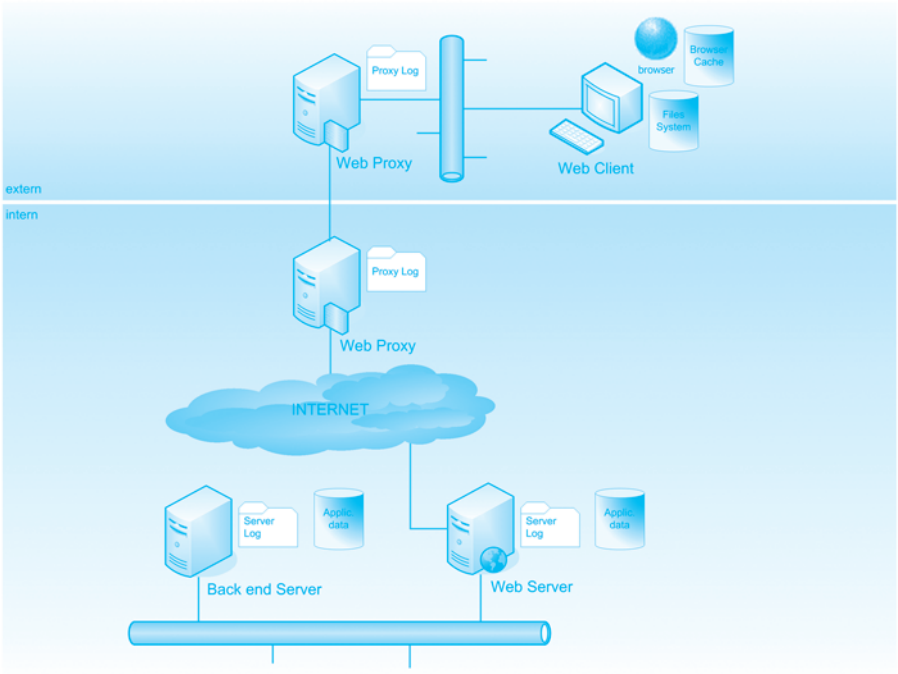


Abbildung 14: Surfer

Im Hinblick auf mögliche forensische Untersuchungen empfiehlt es sich, die angebotenen Log-Mechanismen der eigenen Systeme so weit wie möglich zu aktivieren. Insbesondere die Logs der Proxy Server können hier gute Dienste leisten.

5.2.5 Teilnahme in Foren/Chats, etc.

Die Situation ist grundsätzlich ähnlich wie beim "normalen" Surfen. Folgende Punkte sind speziell zu beachten:

- Im Fall von Chat sind immer mehrere Clients beteiligt. Alle diese Clients können interessante Daten enthalten.
- Falls der Client spezielle Programme verwendet, so sind auch im Umfeld dieser Programme spezielle Spuren zu erwarten (history, logs).
- Im Fall von Foren müssen die, vom Server abgelegten Daten, speziell beachtet werden.

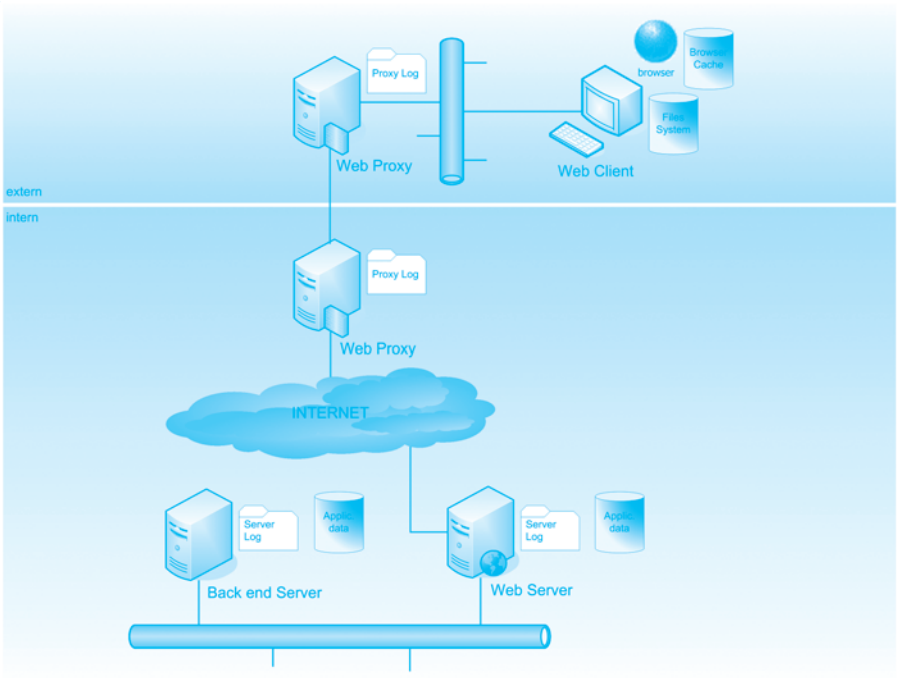


Abbildung 15: Foren / Chats

Da hier immer die Rechner und Daten mehrerer Personen beteiligt sind, sei hier noch einmal auf den gesetzlich vorgeschriebenen Schutz der Persönlichkeit und der persönlichen Daten verwiesen (s. Kapitel 2.3 Persönlichkeits- und Datenschutzrecht).

5.2.6 Drucken/Scannen/Faxen

Neben den offensichtlichen Spuren im Client und in den involvierten Server-Systemen ist den lokalen File-Systemen der Peripherie-Geräte und den betreffenden Queues Beachtung zu schenken. Insbesondere Drucker bieten in vielen Fällen ausgebaute Möglichkeiten zur Speicherung und Verwaltung von Druckdateien an. Es ist üblich, dass die Warteschlange von Druckern nach Beenden des Druckauftrags nicht vollständig gelöscht wird.

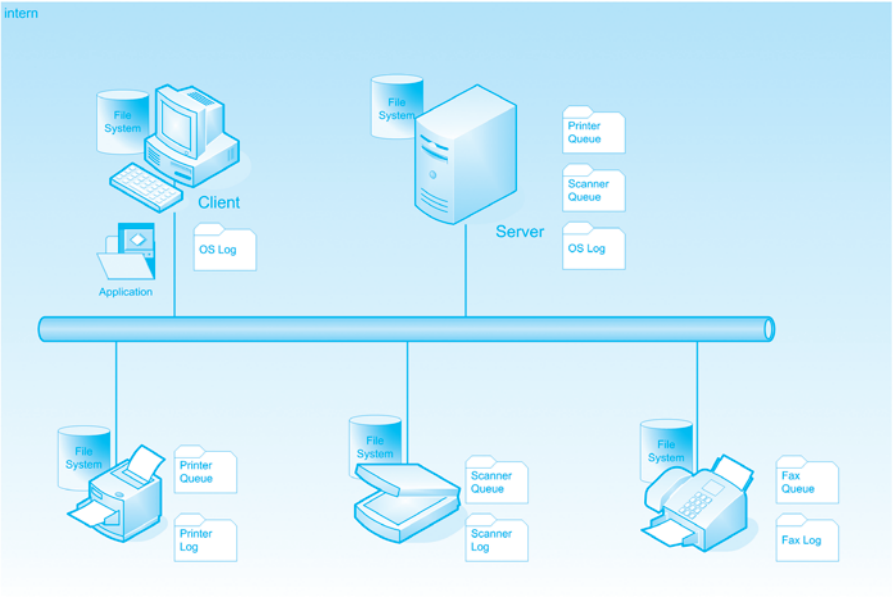


Abbildung 16: Printer und Scanner

Da Drucker und Scanner im Normalfall von mehreren Benutzern verwendet werden, wird der Ermittler hier häufig Daten von verschiedenen Personen einsehen können. Aus diesem Grund sei hier speziell auf den gesetzlichen Schutz der Persönlichkeit und von persönlichen Daten verwiesen (s. Kapitel 2.3 Persönlichkeits- und Datenschutzrecht).

5.3 Fundorte bei speziellen Aktionen und Ereignissen

Neben Standard-Diensten können auch spezifische Aktivitäten von Benutzern und Benutzergruppen das Ziel von Untersuchungen sein.

Bei einer Untersuchung müssen alle zum Zugriff auf das System verwendeten, aktiven Elemente betrachtet werden. Insbesondere sind dies:

- Internet Zugang (Router beim Provider)
- Router
- Lastverteiler (loadbalancer)
- Switches
- Firewalls
- Proxy Server (cache proxy, reverse proxy)
- Web Server
- Anwendungsserver
- Back End Systeme (Datenbanken)

Neben den Hauptzugängen sind auch allfällige Nebenzugänge (Wartungszugänge, Remote Access Systeme) zu beachten.

Auch hier können die Hilfssysteme des Netzes Informationen liefern:

- DNS Server
- Server mit Links auf die betreffenden Dienste
- Systeme von eingebundenen, externen Dienstanbietern
- Verbindungstabellen in den Routers
- ARP Tabellen in Switches

5.3.1 Server Faking, man-in-the-middle

Es wird davon ausgegangen, dass für das Vorspielen eines Servers die DNS- und/oder Routing Informationen verändert werden müssen. Deshalb sind die betreffenden Daten in DNS Systemen, Routern und evtl. auch Switches zu analysieren.

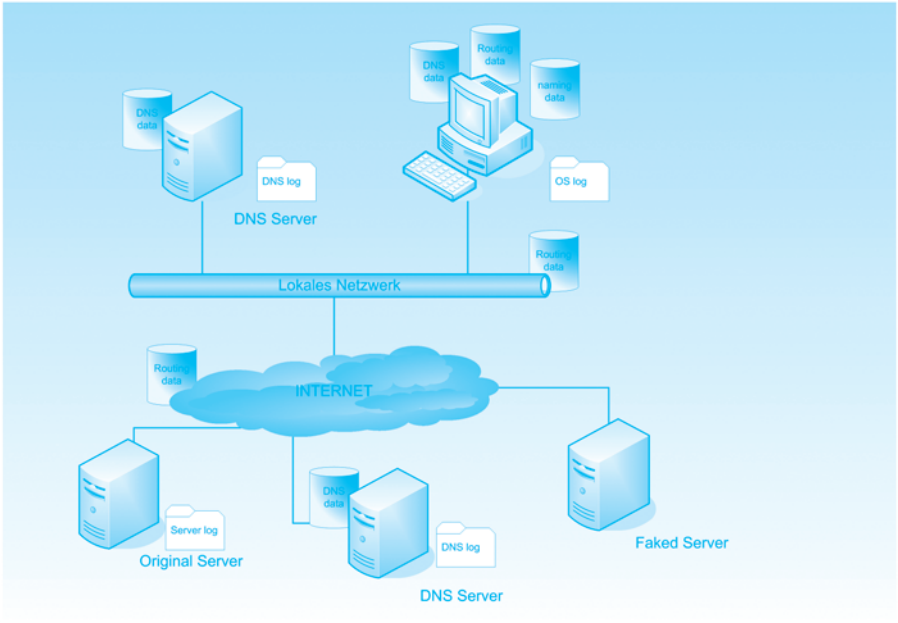


Abbildung 17: Server faking

Auch die Server logs des Original-Server werden Informationen (Spuren) enthalten, da der Angreifer diesen Server vor einem erfolgreichen Faking eingehend analysieren muss.

5.3.2 Trojaner, Viren

Bei der Untersuchung von Trojanern und Viren ist insbesondere der Ausbreitungspfad von Interesse. Je nach verwendeter Technologie muss die Situation unterschiedlich behandelt werden. Bei der Ausbreitung über Mail kann Abbildung 11 als Basis verwendet werden. Bei Web-basierten Viren kommt eher Abbildung 14 zur Anwendung.

Weitere Informationen sind natürlich aus den involvierten Virenscannern zu gewinnen, insbesondere in denjenigen Systemen, welche die betreffenden Viren erkennen konnten.

5.4 Knackpunkte in der Praxis

Wie anderorts, unterscheiden sich auch bei einer forensischen Analyse Theorie und Praxis relativ stark. Insbesondere wird man mit technischen Problemen konfrontiert, für die Standardempfehlungen kaum gemacht werden können. Das genaue Vorgehen ist von Fall zu Fall verschieden und hängt stark von der vorgefundenen Situation beziehungsweise der Umgebung ab.

Es sei hier noch einmal speziell auf die, in Kapitel 2 Rechtliche Rahmenbedingungen für Forensic Computing ausgeführten, technischen Grundlagen, verwiesen. Nicht alles was technisch machbar ist, ist auch gesetzlich erlaubt. Insbesondere ist zu beachten, dass widerrechtlich erlangte Informationen in einem Gerichtsverfahren nicht oder nur am Rande berücksichtigt werden können. Ausnahmen von der Strafbarkeit können in einzelnen Fällen durch "Notwehr" und "Notstand" begründet werden oder sind im Rahmen von Unterstützungsarbeiten für Strafverfolgungsbehörden möglich (s. Kapitel 2.6.1 Beweismittel, Ziffer b).

Die folgenden Kapitel weisen auf einige solcher Knackpunkte hin und diskutieren mögliche Vorgehen.

5.4.1 Rechner stoppen

(Vergleiche generell hierzu Kapitel 4.2.3 Sofortmassnahmen)

Grundsätzlich gibt es zwei Zustände eines Rechners entweder er ist in Betrieb oder er ist abgestellt, z.B. ein Arbeitsplatzsystem über Nacht. Der erste technische Schritt am System selbst ist oftmals das Ein- oder Ausschalten des Rechners. Im Rahmen von forensischen Analysen sind auch andere erste Schritte denkbar, wie beispielsweise die Serverisolation oder das Ausbauen der Festplatte.

Diese erste Aktion am System ist ziemlich kritisch, da bei falschem Vorgehen wertvolle Daten überschrieben oder gelöscht werden können. Jeder der folgenden Schritte ist denkbar und keiner kann pauschal favorisiert werden. Es muss situationsabhängig entschieden werden:

- System starten (sofern es abgestellt ist)
- System ausschalten
  - Cold Shutdown oder Stromstecker raus
  - Warm Shutdown über normale Funktion des Betriebssystems
- System isolieren
  - Logisch, z.B. Trennung vom Netzwerk oder Entfernen aus der Domäne
  - Physisch, d.h. Verhinderung des physischen Zugangs
- Punktuelle Veränderungen am System, z.B. das Ausschalten einzelner Dienste
- System weiter laufen lassen

System starten	Beschreibung
	Ein abgestelltes System wird neu gestartet
	Vorteil
	-
	Nachteil
	Durch die Aktivitäten auf der Festplatte während des Hochfahrens werden u.U. wertvolle Spuren überschrieben. Daten könnten manipuliert werden, was die Beweisführung später erschweren wird. System ist erneut für Angriffe erreichbar.

Cold Shutdown	Beschreibung
	Abstellen des Rechners über den Shutdown-Knopf oder durch Unterbrechung der Stromzufuhr.
	Vorteil
	"friert" den Zustand der Disks ein, d.h. praktisch 1:1-Zustand der gespeicherten Daten zu diesem Zeitpunkt. Keine ungewollten Datenveränderungen durch das System mehr. System ist für einen Angreifer nicht mehr erreichbar.
	Nachteil
	Inhalt des Arbeitsspeichers geht verloren.

Warm Shutdown	Beschreibung
	Runterfahren des Rechners über die Betriebssystemfunktion.
	Vorteil
	"friert" den Zustand der Disks ein. System ist für einen Angreifer nicht mehr erreichbar.
	Nachteil
	Durch den Shutdown-Prozess können wertvolle Spuren verloren gehen (Festplattenaktivitäten) Inhalt des Arbeitsspeichers geht verloren. (Moderne Notebook-Installationen bieten oft "Standby" Zustände, welche auch den Zustand des Arbeitsspeichers konservieren)

System logisch isolieren	
	Beschreibung
	Runterfahren des Rechners über die Betriebssystemfunktion.
	Vorteil
	Verhindert Veränderungen der Daten von aussen. Beeinflussung von Umsystemen (z.B. durch unerwünschten Verkehr) wird gestoppt. Arbeitsspeicher oder laufende Prozesse bleiben erhalten.
	Nachteil
	Dadurch, dass das System weiter läuft, können ungewollt Spuren verloren gehen (Festplattenaktivitäten oder Programme eines Angreifers).

System physisch isolieren	
	Beschreibung
	Ein System wird durch physische Massnahmen, wie das Einschliessen in einem Raum physisch isoliert.
	Vorteil
	Unterbindet physische Eingriffe und damit auch die Manipulation an Daten.
	Nachteil
	-

Punktuelle Veränderungen	
	Beschreibung
	Beispielsweise das Stoppen einzelner Services oder das Löschen von Malware.
	Vorteil
	Arbeitsspeicher oder laufende Prozesse bleiben grösstenteils erhalten.
	Nachteil
	Grosse Gefahr der Spurenverwischung.

System weiter laufen lassen	
	Beschreibung
	Vorderhand keine Aktionen.
	Vorteil
	Arbeitsspeicher oder laufende Prozesse bleiben grösstenteils erhalten. Attacke wird nicht unterbunden, so dass durch die weiteren Schritte des Angreifers weitere Beweisstücke gesammelt werden.
	Nachteil
	System bleibt nach wie vor angreifbar. Attacke wird nicht unterbunden.

Grundsätzlich ist darauf zu achten, dass das System möglichst schnell einer Attacke entzogen wird, und dass möglichst wenig Spuren vernichtet werden. Deshalb ist einem erneuten Systemstart bzw. dem Weiterlaufenlassen sowie von punktuellen Veränderungen in den meisten Fällen abzuraten. Die wohl in den meisten Fällen sinnvollen Massnahmen sind der Cold Shutdown bzw. die Systemisolation.

5.4.2 Schutz vor absichtlicher und unabsichtlicher Veränderung

(Vergleiche generell hierzu Kapitel 4.2.7.1 Grundsätze für die Erlangung beweiskräftiger elektronischer Informationen)

Falls Spuren als Beweismittel verwendet werden sollen, müssen sie spezielle Kriterien erfüllen. Eine allgemeine Charakterisierung aus juristischer Sicht findet sich in Kapitel 2.5 Gesellschafts- und Bankenrecht und speziell im Kapitel 2.5.1 Gesellschaftsrechtliche Zuständigkeit für IT-Infrastruktur.

Der Schutz vor Veränderung ist wesentlich für die Qualität aller Spuren. Bei der Verwendung von Spuren im Rahmen einer Beweisführung muss die Echtheit nachweisbar sein. Veränderungen sind möglich durch logischen und/oder physischen Zugang zu den betreffenden Systemen.

Es geht darum, jederzeit garantieren zu können, dass Spuren bei und nach deren Erfassung nicht verändert wurden. Dazu sind zwei wesentliche Massnahmen notwendig: Einerseits wird vom Datenträger bzw. vom gesamten System ein vollständiges Abbild mit digitaler Signatur erstellt (z.B. Disk Imaging-Methode siehe Kapitel 4.2.7.2 Arten der Sicherstellung). Andererseits sind die Originalsysteme sicher aufzubewahren.

Speziell Wert muss deshalb darauf gelegt werden, dass der Zugang zu den Systemen auf ausser verdachtstehende Personen beschränkt ist, und dass diese Tatsache im Nachhinein auch zweifelsfrei nachgewiesen werden kann.

Grundsätzlich wird auf dem Originalsystem keine Untersuchung durchgeführt. Die Gefahr von Datenveränderungen oder -zerstörungen ist viel zu gross. Forensische Analysen sollten nur auf Kopien durchgeführt werden.

5.4.3 Rechnerzeit

Bei der Verwendung von Spuren sind verschiedene Zeiten wichtig, insbesondere

- die Zeit der Entstehung der Spuren
- die Zeit der Erfassung (Sicherung) der Spuren.

Im Allgemeinen kann man nicht davon ausgehen, dass die lokale Zeit der untersuchten Rechner (interne Uhr) mit der physikalischen Zeit übereinstimmt. Damit jedoch im Rahmen eines Rechtsverfahrens Zeitangaben, zum Beispiel aus Protokolldateien, als verlässlich angesehen werden können, ist es wichtig, deren Authentizität zu kennen. Es ist deshalb unabdingbar, dass zur Zeit der Datensicherung die Systemzeit mit der effektiven Zeit verglichen und eine Abweichung festgehalten wird. Vergleiche hierzu Kapitel 4.2.7.1 Grundsätze für die Erlangung beweiskräftiger elektronischer Informationen.

5.4.4 Grosse Datenmengen

Bei grösseren Installationen stellt sich das Problem der Datenmenge. Die relevanten Daten müssen aus einer Vielzahl von Aufzeichnungen herausfiltriert werden. Zu diesem Zweck müssen im Normalfall grosse Datenmengen erfasst, gespeichert und durchsucht werden, was immense Ressourcen an Diskspace bzw. CPU voraussetzt. Werkzeuge von Standard-Systemen sind hier nur beschränkt einsetzbar (z.B. Suchfunktionen).

5.4.5 Zeitdruck

Wie bereits weiter oben erwähnt ist die Integrität der analysierten Spuren massgeblich für deren Wert. Da jede Art von Arbeiten (unter Umständen auch nur das Laufenlassen des Systems) an einem System potentiell Veränderungen an Spuren vornimmt, besteht insbesondere ein Zeitdruck bei der Sicherung von Spuren.

5.4.6 Identifikation der relevanten Systeme

Bei Untersuchungen in grösseren Organisationen (Rechenzentren) ist die Identifikation der relevanten Systeme nicht trivial. Auch Art und Umfang der Interaktionen der verschiedenen Systeme sind für einen Aussenseiter nicht ohne weiteres ersichtlich. Eine effiziente Analyse wird im Normalfall nicht möglich sein ohne die Mithilfe von (vertrauenswürdigen) Insidern.

Eine ungenaue Identifikation der relevanten Systeme kann dazu führen, dass die Systeme Unbeteiligter analysiert werden. Aus juristischer Sicht muss gewährleistet werden, dass der Ermittler sich nicht des "unerlaubten Eindringens in ein Datensystem" (s. Kapitel 2.2.4.2 Unlauterer Wettbewerb) oder der "unerlaubten Datenbeschädigung (s. Kapitel 2.2.4.3 Verletzung von Schweigepflichten) strafbar macht.

5.4.7 Passwortschutz

Moderne Systeme sind fast durchgängig durch Passwörter geschützt. Insbesondere in vernetzten Systemen (z.B. NT Domänen) ist ein Zugang auf Ressourcen ohne Kenntnis entsprechender Passwörter aufwändig. Der Zugang zu Passwörtern erleichtert auf der andern Seite die Arbeit des Ermittlungs-Teams. Hier ist im Normalfall die Hilfe von Insidern notwendig.

Passwörter können in vielen Fällen auch über "Passwort Cracker" ermittelt werden. Man beachte dabei, dass Passwörter in vielen Fällen als "schützenswerte Daten" betrachtet werden, welche aus Gründen des Datenschutzes nicht ohne weiteres zugänglich gemacht werden dürfen (s. Kapitel 3.2.3 Vorgehen zum Analysieren der Gefährdungsfaktoren).

5.4.8 Verschlüsselung

Die Verschlüsselung mit starken Methoden gewährt einen hohen Schutz gegen unberechtigten Zugriff auf Daten. In solchen Fällen ist ein Zugriff ohne Kenntnis der verwendeten Schlüssel (Passwörter) sehr aufwändig und deshalb in der Praxis kaum möglich.

5.4.9 Alte Datenträger

Bei der Analyse von älteren Datenträgern stellt sich möglicherweise das Problem, dass keine geeigneten Lese-Geräte mehr zur Verfügung stehen.

Zu beachten ist ferner, dass die meisten Datenträger (Bänder, Disketten etc.) durch die natürliche Alterung Datenverlust erleiden (typisch nach einigen Jahren). Damit wird der Zugang mittels Standard-Werkzeugen erschwert und evtl. sogar verunmöglicht.

5.4.10 Defekte Datenträger

Defekte Datenträger können einerseits Quellen von wertvoller Information sein (z.B. wenn sie unbedarft entsorgt wurden). Anderseits können solche Datenträger, im Normalfall, nicht mittels Standardgeräten bearbeitet werden.

Spezialisierte Unternehmen bieten die Analyse solcher Datenträger an. Diese Arbeiten sind aber zeitintensiv und mit vergleichsweise hohen Kosten verbunden.

5.4.11 Verschiedenste Hardware

Eine Untersuchung kann den Zugang auf Informationen auf verschiedensten Plattformen und auf unterschiedlichen Datenträgern verlangen. Dies verlangt einen hohen Grad an Flexibilität der verwendeten Geräte und Programme.

Ein Zugang zu Disks, ohne diese zu verändern, kann auf unterschiedliche Arten geschehen. Beispiele für Zugangsarten sind das Booten des betreffenden Rechners von einem mobilen Datenträger (Diskette, CD Rom) und der anschliessende Zugang über das Netzwerk, oder der Ausbau der relevanten Datenträger und deren Einbau in einen Test-Rechner.

5.4.12 Treiberproblematik

Falls fremde Datenträger und/oder Geräte auf einem Untersuchungsrechner analysiert werden müssen, so müssen geeignete Treiberprogramme zur Verfügung stehen. Dies ist insbesondere dann schwierig, wenn unübliche Geräte betroffen sind, und wenn die Untersuchungsarbeiten unter Zeitdruck stehen (Spurensicherung).

5.5 Hilfsmittel und Werkzeuge

5.5.1 Produkte

Nachfolgend sei eine unvollständige Auswahl an Tools und Produkten, die für eine technische Untersuchung eingesetzt werden können, geboten:

Produkt	Anwendungsbereich	kommerziell	Anbieter
Encase	Komplette Palette: Datensicherung, -aufbereitung und -analyse	kommerziell	www.guidancesoftware.com
Maresware: the suite	Datenanalyse	kommerziell	www.maresware.com
Norton Ghost	Datensicherung	kommerziell	www.symantec.com
Safeback	Datensicherung	kommerziell	www.forensics-intl.com
The Coroner's Toolkit	Komplette Palette: Datensicherung, -aufbereitung und -analyse	nicht kommerziell	www.fish.com/forensics
Unix dd Com-mand	Datensicherung	nicht kommerziell	Unix Kommando
Vogon	Komplette Palette: Datensicherung, -aufbereitung und -analyse	kommerziell	www.vogon.de

Tabelle 9: Forensische Tools

6 Prävention

6.1 Ziel der Prävention und grundsätzliches Vorgehen

Übergeordnetes Ziel der Prävention ist, die effektive oder latent vorhandene Gefährdung durch vorbeugende Massnahmen zu reduzieren. Dies kann auf mehrere verschiedene Arten erfolgen, welche gleichzeitig und grösstenteils unabhängig voneinander verfolgt werden können, so z.B.:

- konsequente Implementierung von (IT-) Grundschutz
- Risk-Management basierend auf Gefährdungsanalyse
- konsequentes Vorgehen bei Verdachtsfällen und Strafanzeige bei Delikten
- ausgewählte präventive Informatik-Massnahmen
- systemischer Ansatz, basierend auf den erkannten Faktoren aus Kapitel 2

6.2 Konsequente Implementierung von Grundschutzmassnahmen

Grundschutz heisst, diejenigen Massnahmen zu implementieren, welche in der Praxis allgemein als nützlich anerkannt sind. Grundschutzmassnahmen sind in der Regel von allen (Sicherheits-) Experten empfohlen, werden jedoch nicht von allen Unternehmen oder in allen Bereichen umgesetzt. Am Beispiel des Automobils lässt sich der Stellenwert von Grundschutzmassnahmen gut illustrieren: Alle Experten sind sich einig, dass ein Fahrer und auch die Mitfahrer sich im Auto anschnallen sollten, weil dies das Risiko einer schweren Verletzung bei Unfällen drastisch senkt. Aber nicht alle Fahrer und noch weniger die Beifahrer schnallen sich an, befolgen also die Grundschutzmassnahme auch wirklich.

Im Geschäftsumfeld gelten z.B. die konsequente Funktionentrennung, die lückenlose Protokollierung relevanter Informationen oder die systematische Überwachung insbesondere der Ausführung erteilter Aufträge als Grundschutzmassnahmen. Mögliche Quellen solcher Grundschutzmassnahmen sind die Ordnungsmässigkeitskriterien in Deutschland oder der Schweiz, oder z.B. das COSO-Framework, welches heute teilweise als Vorläufer von Corporate Governance Standards betrachtet wird.

Auch im Informatikumfeld gibt es, aus unterschiedlichsten Quellen, ähnliche, teilweise weit präzisere Kataloge von Grundschutzmassnahmen, welche gesamtheitlich implementiert werden sollten (z.B. ISO 17799, CobiT). Es kann gezeigt werden, dass durch die konsequente Umsetzung von solchen IT-Grundschutzmassnahmen einerseits die Eintretenswahrscheinlichkeit von gravierenden Ereignissen um bis zu einem Faktor 5 gesenkt werden kann und anderseits auch das Schadenpotential entsprechend abnimmt.

6.3 Risk-Management basierend auf Gefährdungsanalyse

Der klassische Risk-Management-Ansatz führt eine Risikoanalyse durch – idealerweise anhand der im Kapitel 3 Gefährdungsanalyse aufgeführten Faktoren – und versucht dann, die erkannten Gefährdungen mittels sinnvoller Massnahmen zu reduzieren. Während die Grundschutzmassnahmen einen allenfalls sehr umfassenden Katalog an Sicherheitsmassnahmen darstellen, versucht das Risk-Management die wirklich kritischen Bereiche zu identifizieren und diese dann mit gezielten Massnahmen zu verbessern. Dies ist zwar sehr kostenintensiv, jedoch ist der Aufwand für die Durchführung einer umfassenden Gefährdungsanalyse noch grösser.

Das Risk-Management ist in zahlreichen Büchern bereits beschrieben. Wendet man die darin veröffentlichten Verfahren auf die im Kapitel 2 vorgestellten Faktoren (Indikatoren) an, können Defizite frühzeitig erkannt und behoben werden.

Es ist offensichtlich sehr wichtig, dass die relevanten Faktoren für die Gefährdungsanalyse sorgfältig herausgearbeitet werden. Fast noch wichtiger ist es, die Relevanz dieser Faktoren periodisch zu überprüfen, da sich die Aussagekraft und Verlässlichkeit eines bestimmten Indikators mit der Zeit ändern kann.

6.4 Konsequentes Vorgehen bei Verdachtsfällen und Strafanzeige bei Delikten

Eine sehr wirkungsvolle präventive Methode zur Verringerung des Risikos von unerwünschten und kriminellen Handlungen ist die systematische und mit hoher Professionalität durchgeführte Analyse sämtlicher Verdachtsfälle und die konsequente Strafanzeige bei erkannten Delikten. Sowohl die Analyse sämtlicher Fälle wie auch die Strafanzeige führen bei potentiellen Tätern zur Erkenntnis, dass sich ein Delikt in diesem Unternehmen nicht lohnt, weil jeder Verdacht sofort und professionell abgeklärt wird und alle Delikte angezeigt werden.

Wenn man diese Tatsachen bekannt macht (oder bekannt werden lässt), wird ein "unsicherer" Täter auf das Delikt verzichten. Die abschreckende Wirkung einer Strafanzeige ist so gross, dass er sicherlich nicht mehr nur aus purer Neugierde oder Leichtsinn eine Tat begehen wird. Den Fällen, bei denen der Täter aus einer Notlage heraus ein Delikt begeht, kann damit zwar nicht entgegengewirkt werden, doch dürfte die Gesamtzahl von Delikten demnach deutlich abnehmen.

Ein solches Vorgehen hätte für das Unternehmen noch den weiteren Vorteil, dass (trotz der allfälligen Verunsicherung im Einzelfall) sich eine "Kultur der Ehrlichkeit" durchsetzt und nicht "eine Kultur der persönlichen Bereicherung".

6.5 Ausgewählte präventive Informatik-Massnahmen

Im breiten Spektrum möglicher Informatik-Grundschutzmassnahmen gibt es einige wenige, welche einen überdurchschnittlich grossen Einfluss auf (möglicherweise) deliktische Handlungen haben. Die nachfolgende Tabelle zeigt für drei ausgewählte Bereiche Eingabe-Verarbeitung-Ausgabe, Programme und Hacking/Spionage einige der wirksamsten präventiven Massnahmen auf.

Gegen Manipulation von Eingabe/Verarbeitung/Ausgabe
Funktionentrennung resp. Vieraugenprinzip (segregation of duties)
Zugriffsschutzsysteme mit restriktiver Vergabe von Berechtigungen für den direkten Zugriff auf Dateien und Programme (access control systems)
periodische Überprüfung von Stammdaten (wirksam aber aufwändig)
Protokollierung wesentlicher Transaktionen und regelmässige Auswertung
von Benutzern unabhängige Abstimmkreise
Gegen Manipulation von Programmen
konsequentes Änderungswesen (change management)
Abnahmetests durch Fachbereiche (user acceptance/approval)
Einsatz von Prüfsummen über produktive Programme
restriktiver direkter Zugriff auf produktive Programme
restriktiver Einsatz von Dienstprogrammen (system utilities)
starke Zugriffsschutzsysteme, sichere Betriebssysteme, …
Gegen Hacking/Spionage
Logon mit starker Authentisierung (strong authentication)
gut administrierte Zugriffsschutzsysteme, insbesondere an den Netzeingängen
Verschlüsselung von gespeicherten und übermittelten Daten (encryption)
permanente real-time Überwachung der Netzwerke und Zugriffsschutzsysteme

6.6 Prävention basierend auf systematischem Ansatz

6.6.1 Anwendung des Wirkungskreis-Modells in der Prävention

Im Abschnitt 3.2.5 wurde ein Wirkungskreis basierend auf einigen ausgewählten Faktoren der Gefährdungsanalyse vorgestellt. Im Zentrum dieses Wirkungskreises steht der Mitarbeiter resp. die Motivation des Mitarbeiters. Zahlreiche Faktoren haben eine direkte oder indirekte Wirkung auf den Mitarbeiter. Wenn irgendwo im Wirkungskreis ein Einfluss ausgeübt wird, werden einige der benachbarten Faktoren sich direkt verändern, diese wiederum ihre Nachbarn usw., bis das gesamte System wieder mehr oder weniger im Gleichgewicht ist. Dieses Prinzip eines kybernetischen Modells benutzt man in diesem Ansatz, um die richtigen präventiven Massnahmen zu bestimmen. Um zu einem solchen Wirkungskreis-Modell zu kommen, bestimmt man – wie im Kapitel 3.2 "Durchführung der Gefährdungsanalyse" aufgezeigt – die, für das Unternehmen möglichst aussagekräftigen Faktoren, und wählt dann in einem zweiten Schritt diejenigen aus, welche am besten ausgewertet oder beeinflusst werden können.

6.6.2 Konkretes Anwendungsbeispiel

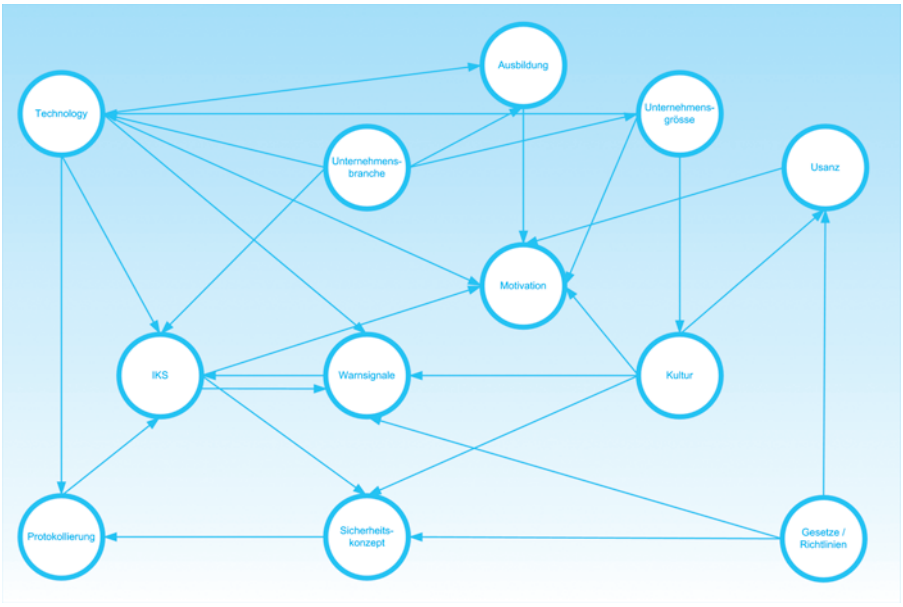


Abbildung 18: Anwendungsbeispiel eines Wirkungskreises

Im obigen Beispiel eines Wirkungskreises sieht man, wie das Interne Kontrollsystem (IKS) beeinflusst wird von Faktoren wie Technologie, der Branche resp. der Art der Geschäftstätigkeit des Unternehmens, der Sammlung (Protokollierung) von Informationen, dem Erkennen von Warnsignalen usw. Diametral gegenüber steht die Ressource Mensch resp. dessen Motivation, Delikte und andere unerwünschte Handlungen zu begehen. Diese Motivation hängt von zahlreichen Faktoren ab, welche teilweise dem Mitarbeiter eigen sind (also Veranlagung, Charakter, Geltungsdrang usw.) oder von aussen auf den Mitarbeiter einwirken (z.B. Unternehmenskultur, Ausbildung, Internes Kontrollsystem usw.).

Angenommen der illustrierte Wirkungskreis ist typisch für ein Unternehmen, wird nun versucht in diesem Wirkungskreis diejenigen Faktoren zu beeinflussen, welche die beste (stärkste, schnellste) positive Auswirkung auf das Gesamtsystem haben.

Ein aus diesem Modell herauslesbares Beispiel möglicher Prävention wäre eine sorgfältig getroffene Wahl von neuen Mitarbeitern. Es gibt mehrere nationale und internationale Standards, welche die Überprüfung eines Mitarbeiters bei der erstmaligen Anstellung (oder allenfalls periodisch in bestimmten Abständen) fordern, so z.B. sollten Mitarbeiter vor Stellenantritt einen Strafregisterauszug vorlegen, man holt Betreibungs- und Leumundsauskünfte über sie ein, verifiziert eingereichte Schulabschlüsse, Diplome oder Titel beim ausstellenden Institut auf ihre inhaltliche Richtigkeit und generell auf die tatsächliche Bedeutung usw. Mit diesem Ansatz wird verhindert, dass offensichtlich unerwünschte Personen eine Vertrauensposition erhalten, welche sie zu einem späteren Zeitpunkt ausnutzen könnten. Man schaltet sich somit direkt in den Wirkungskreis ein. Dadurch wird dort "geschraubt", wo ein direkter Effekt erzielt werden kann, nämlich beim Mitarbeiter selber.

Immer noch basierend auf der Annahme, dass der oben gezeigte Wirkungskreis typisch für ein Unternehmen ist, kann man auch an anderen Stellen viel (positiven) Einfluss geltend machen: beim Internen Kontrollsystem (IKS). Wenn ein gut funktionierendes IKS vorhanden ist, können Gefährdungen wirksam vermindert oder zumindest rechtzeitig erkannt werden.

6.6.3 Weitere präventive Massnahmen im Personalbereich

Wenn das kybernetische Modell wirklich für die Prävention angewendet werden soll, muss die folgende Überlegung angestellt werden: Wie kann man jedes einzelne Element im Wirkungskreis am besten beeinflussen? Wendet man diese Frage z.B. auf den Faktor Mensch an, so wird schnell klar, dass der Mensch, also der Mitarbeiter über sein Umfeld, seine Arbeit, seine Kollegen, generell die Firmenkultur und – ganz wichtig – auch durch seinen Vorgesetzten beeinflusst wird. Hier muss also die Prävention einsetzen!

Trotz dieser allseits bekannten und anerkannten Erkenntnis wird der wesentliche Einfluss von ganz generellen Personalmassnahmen (Führung, Ausbildung, Karriereplanung etc.) auf die Gesamtgefährdung eines Unternehmens oft zu gering eingeschätzt. Mit Hilfe des Wirkungskreises können solche Zusammenhänge erkannt, dargestellt und letztlich beeinflusst werden.

Zusätzlich zu diesen generellen Massnahmen im Personalbereich gibt es noch eine Reihe von Massnahmen, welche direkt auf die Mitarbeiter oder ihre Vorgesetzten wirken:

Prävention bei Mitarbeitern
Regelungen aufstellen und von Mitarbeitern unterschreiben lassen (z.B. Nutzung von Internet, E-Mail, …)
Mitarbeiter im Rahmen ihrer Arbeit schulen auf was tolerierbar und was verboten ist (z.B. ab und zu private E-Mails ist ok, Download von Porno ist klar verboten).
Verstösse und entsprechende Sanktionen definieren und bekannt machen ("Bussenkatalog")

Prävention bei Vorgesetzten
Erkennung und Interpretation typischer Warnsignale schulen
korrektes Vorgehen bei Verdacht vermitteln (wen kontaktieren, was nicht machen)
Führungstechniken und Führungsverhalten schulen
Überwachung/Kontrolle von angeordneten Massnahmen als persönliche Aufgabe der Vorgesetzten betrachten

A. Beispiel Vertraulichkeitsvereinbarung

Vereinbarung

zwischen

.....
.....
.....

(im folgenden "PartnerFIRMA" genannt)

und

IhreFirma AG
Postfach
8000 Zürich

(im folgenden "IhreFIRMA" genannt)

betreffend

Gegenseitige Geheimhaltepflicht

(Confidentiality /Data Protection)

Die vorliegende Vereinbarung bezweckt allein die abschliessende Regelung der **gegenseitigen** Verschwiegenheit, um damit zu ermöglichen, im Rahmen des geplanten Gedankenaustausches bzw. der beabsichtigten Gespräche über das XYZ Projekt (nachstehend Projekt), uneingeschränkt vertrauliche Informationen/Dokumente auszutauschen bzw. einen freien Gedankenaustausch zu pflegen.

Entsprechend vereinbaren die PartnerFirma und die IhreFirma was folgt:

1. Vertrauliche Informationen

Unter "Vertrauliche Informationen" versteht man vorliegend **sämtliche** Informationen/Dokumente (nachstehend "Informationen"), die **im Rahmen des Projekts** von einer Partei oder einem von ihr Bevollmächtigten (gemeinsam: nachstehend "Informant") der anderen Partei oder einem von ihr Bevollmächtigten (gemeinsam: nachstehend "Adressat") **nach Inkrafttreten der vorliegenden Vereinbarung** zugänglich gemacht bzw. übergeben werden. Darunter fallen insbesondere sämtliche Informationen über das XYZ Projekt. Nicht vorausgesetzt ist, dass die einzelnen Informationen mit "Vertraulich" oder "Geheim" speziell gekennzeichnet sind. Miterfasst ist auch der spezifische Inhalt des Projektes selbst. Sodann ist die Form und das Medium belanglos, in der/dem die Informationen dem Adressaten zugänglich gemacht bzw. übergeben werden – d.h., ob schriftlich (original oder in Kopie), mündlich (inkl. Aufzeichnungen davon) oder mittels irgendeinem Wiedergabemedium.

Demgegenüber entfällt die Vertraulichkeit einer einzelnen Information, falls sie:

a) dem Adressaten, seinen Mitarbeitern oder einem für das Projekt beigezogenen Berater bereits vorher bekannt war; oder
b) vom Adressaten, seinen Mitarbeitern oder von einem für das Projekt beigezogenen Berater unabhängig von den erhaltenen Informationen entdeckt wurde.

2. Rechte an den Informationen; Wahrung der Vertraulichkeit

Die Parteien sind sich einig, dass sämtliche Rechte (insb. Eigentums-/Schutzrechte) an den Informationen, die dem Adressaten unter der vorliegenden Vereinbarung zugänglich gemacht werden, beim Informanten verbleiben. Gleichzeitig sichern sie sich gegenseitig zu, dass die künftige Preisgabe der Informationen keine Rechte Dritter (insb. Schutzrechte sowie obliegende Geheimhaltepflichten) verletzt.

Zur Wahrung der Vertraulichkeit hat der Adressat mindestens diejenige Sorgfalt zu üben, die er zum Schutz eigener, vergleichbar vertraulicher Informationen trifft; dabei ist jedenfalls eine sachgerechte, der Vertraulichkeit entsprechende Sorgfalt als Mindestanforderung zu gewährleisten.

3. Verwendung der Informationen; erlaubte Weitergabe

Den Parteien ist es untersagt, die Informationen ausserhalb des Projektes bzw. des mit dieser Vereinbarung verfolgten Zwecks zu benützen; jeglicher anderweitige Gebrauch ist m.a.W. unstatthaft. Insbesondere dürfen die Informationen weder gesamthaft noch auszugsweise Dritten zugänglich gemacht bzw. Dritten zur Nutzung überlassen werden. Eine erweiterte Nutzung der Informationen setzt eine vorausgehende schriftliche Zustimmung des Informanten voraus.

Als Dritte im vorstehenden Sinne gelten auch Tochter-, Beteiligungs- und Konzerngesellschaften der Parteien, ungeachtet des Grades der Beteiligung.

Der Adressat hat die Weitergabe von vertraulichen Informationen auf Mitarbeiter zu beschränken, die für das Projekt Kenntnis von den Informationen haben müssen – m.a.W. dürfen sie intern nicht unnötig verbreitet werden. Eine Weitergabe an Berater, die für das Projekt beigezogen werden, bedarf einer vorausgehenden Anzeige. Sowohl im einen wie im anderen Fall wird vorausgesetzt, dass die Informations-Empfänger über den Inhalt der vorliegenden Vereinbarung nachweislich informiert und sie zu deren Einhaltung verpflichtet worden sind; auf Verlangen des Informanten ist eine separate Geheimhalteerklärung vom Mitarbeiter/Berater unterzeichnen zu lassen, in die der Informant jederzeit Einsicht nehmen darf.

4. Behördliche Verfügungen

Wird der Adressat von einem Gericht oder von einer Behörde verpflichtet, die Informationen (oder Teile davon) offenzulegen oder gar auszuhändigen, so hat der Adressat den Informanten umgehend schriftlich (via Fax und per Post) darüber zu informieren, damit dieser sich bestmöglichst zur Wehr setzen kann. Auf Verlangen und auf Kosten des Informanten ist der Adressat verpflichtet, zwecks Abwehr der Verfügung mit dem Informanten zusammenzuarbeiten bzw. gemeinsam geeignete Massnahmen zu treffen, um die Geheimhaltung der Informationen bestmöglich zu schützen.

5. Haftung bei Vertragsbruch

Der Adressat haftet dem Informanten unbeschränkt für jeden, durch Vertragsbruch schuldhaft verursachten direkten Schaden, inkl. Anwaltshonorar und Gerichtsgebühren. Verletzt der Informant mit der Preisgabe von Informationen an den Adressaten Rechte Dritter, so hat der Informant den Adressaten für sämtliche Verpflichtungen schadlos zu halten, die diesem gegenüber dem Dritten erwachsen sollten. Jede weitere Ersatzpflicht ist ausgeschlossen.

6. Richtigkeit der Informationen (Gewährleistung/Haftung)

Unter der vorliegenden Vereinbarung übernimmt der Informant keinerlei Gewähr für die Richtigkeit und Vollständigkeit der Informationen. Damit trifft ihn auch keine Ersatzpflicht für Schäden, die sich aus der Nutzung der überlassenen Informationen ergeben könnten.

7. Inkrafttreten, Dauer, Kündigung

Die vorliegende Vereinbarung tritt mit beidseitiger, rechtsgültiger Unterzeichnung in Kraft. Diese Vereinbarung kann durch beide Parteien schriftlich und unter Einhaltung einer Kündigungsfrist von zehn (10) Tagen gekündigt werden

8. Dauer der Geheimhaltepflicht; Wirkungen der Beendigung der Vereinbarung

Die Parteien sind sich einig, dass nach Beendigung der Vereinbarung die bisher überlassenen Informationen während einer Periode von drei (3) Jahren weder vom Adressaten selbst noch von seinen Mitarbeitern, Beratern oder den vom Adressaten beherrschten Gesellschaften (Ziff. 3) weiter genutzt oder Dritten gar offengelegt werden dürfen, ohne dass nicht eine schriftliche Zustimmung vom Informanten vorliegen würde – es sei denn, die Informationen würden mittlerweilen als öffentlich bekannt gelten. Somit dauern sämtliche Rechte und Pflichten unter der vorliegenden Vereinbarung entsprechend fort.

Bei personenbezogenen Informationen, bei denen ein Dritter Geheimnisherr der Informationen ist, gilt die Geheimhaltepflicht zeitlich unbefristet (Bankgeheimnis, Datenschutz).

Mit (a)Ablauf oder Kündigung der Vereinbarung, (b)Rückruf des Informanten, oder (c)Erreichung des mit der vorliegenden Vereinbarung verfolgten Ziels (vorbehältlich anderweitiger Absprache), wird der Adressat verpflichtet, die Informationen (inkl. Kopien und anderweitiger vollständiger oder auszugsweiser Aufzeichnungen) umgehend (jedenfalls nicht später als fünf (5) Tagen ab Beendigung bzw. Erhalt des Rückrufs in physischer Form dem Informanten zurückzugeben (ungeachtet, ob vom Adressaten oder Informanten erstellt) bzw. auf Computersystemen, die im Herrschaftsbereich des Adressaten oder einem von ihm beauftragten Dritten stehen, nicht rekonstruierbar zu löschen. Der Adressat hat dem Informanten in Schriftform zu bestätigen, den vorstehenden Anforderungen entsprochen zu haben.

9. Schlussbestimmungen

Die Vereinbarung enthält sämtliche Abreden der Parteien im Zusammenhang mit der vorliegend geregelten Geheimhaltepflicht. Sie geht früheren Äusserungen sowie Bedingungen aus Korrespondenz und Verhandlungen vor. Alle späteren Änderungen und Ergänzungen bedürfen zu ihrer Gültigkeit der Schriftform.

Keine der Parteien ist aufgrund dieser Vereinbarung verpflichtet, während oder nach Ablauf der Geltungsdauer mit der anderen Partei eine neue Vereinbarung einzugehen – auch nicht in Zusammenhang mit dem Projekt.

Die Geheimhaltepflicht hindert keine der Parteien daran, ihre Mitarbeiter, die mit Aufgaben aus dem Projekt betraut waren, jederzeit frei für neue Arbeiten einzusetzen.

Sollten Teile der Vereinbarung (oder eines Nachtrags/Anhangs) nichtig, unwirksam oder sonst aus irgendeinem Grund nicht vollstreckbar sein oder werden, so wird die Gültigkeit dieser Vereinbarung bzw. eines Nachtrags/Anhangs im übrigen nicht berührt. Die Parteien werden dann die Vereinbarung so auslegen und gestalten, dass der mit den nichtigen oder rechtsunwirksamen Teilen angestrebte Zweck soweit als möglich trotzdem erreicht wird.

Diese Vereinbarung oder einzelne Rechte und Pflichten daraus dürfen nur nach vorgängiger schriftlicher Zustimmung der Gegenpartei auf Dritte übertragen werden.

Als **Erfüllungsort** und **ausschliesslicher Gerichtsstand** wird **Zürich vereinbart.**

Die vorliegende Vereinbarung sowie die Beurteilung der Gültigkeit des vereinbarten Gerichtsstandes unterstehen schweizerischem Recht.

..... PartnerFirma

(Ort, Datum)

....

..... IhreFirma

(Ort, Datum)

....

B. Literaturverzeichnis

BARRELET DENIS/EGLOFF WILLI, Das neue Urheberrecht, Kommentar zum Bundesgesetz über das Urheberrecht und verwandte Schutzrechte, 2. Aufl. Bern 2000 (zit. BARRELET/EGLOFF)

VON BÜREN ROLAND/MARBACH EUGEN, Immaterialgüter- und Wettbewerbsrecht, 2. Aufl. Bern 2002 (zit. VON BÜREN/MARBACH)

HUGUENIN CLAIRE, Obligationenrecht, Besonderer Teil, Zürich 2002 (zit. HUGUENIN)

JANAL DANIEL S., Internet-Sicherheit für Unternehmen, New York, Frankfurt/Main 1999 (zit. JANAL)

JÖRG FLORIAN S., Vertragsgestaltung und Rechtsmodelle, in: ARTER OLIVER/JÖRG FLORIAN S. (Hrsg.), Internet-Recht und Electronic Commerce Law, Lachen/St. Gallen 2001, 3 (zit. JÖRG)

KIKINIS MICHAEL, Internet und Geistiges Eigentum, in: ARTER OLIVER/ JÖRG FLORIAN S. (Hrsg.): Internet-Recht und Electronic Commerce Law, Lachen/St. Gallen, 2001, 217 (zit. KIKINIS)

REHBERG JÖRG, Schweizerisches Strafgesetzbuch, Zürich 1999 (zit. REHBERG, Schweizerisches Strafgesetzbuch)

REHBERG JÖRG/DONATSCH ANDREAS, Strafrecht I, Verbrechenslehre, 7. Aufl. Zürich 2001 (zit. REHBERG/DONATSCH, Strafrecht I)

REHBERG JÖRG/ECKERT ANDREAS/FLACHSMANN STEFAN, Tafeln zum Strafrecht, Besonderer Teil, 3. Aufl. Zürich 1998 (zit. REHBERG/ECKERT/FLACHSMANN, Tafeln)

REHBERG JÖRG, Strafrecht IV, Delikte gegen die Allgemeinheit, 2. Aufl. Zürich 1996 (zit. REHBERG, Strafrecht IV)

REHBINDER MANFRED, Schweizerisches Urheberrecht, 3. Aufl. Zürich 2000 (zit. REHBINDER, Urheberrecht)

REHBINDER MANFRED, Schweizerisches Arbeitsrecht, 15. Aufl. Zürich 2002 (zit. REHBINDER, Arbeitsrecht)

RIEMER HANS MICHAEL, Personenrecht des ZGB, 2. Aufl. Bern 2002 (zit. RIEMER)

ROSENTHAL DAVID, Projekt Internet, Zürich 1997 (zit. ROSENTHAL)

SCHATZMANN ROLF, E-Forensic – ein erster Überblick, digma 2001, 186 (zit. SCHATZMANN)

SCHLAURI SIMON, Die Digitale Signatur: Basistechnologie des elektronischen Geschäftsverkehrs, in: ARTER OLIVER/JÖRG FLORIAN S. (Hrsg.), Internet-Recht und Electronic Commerce Law , Lachen/St. Gallen 2001, 57 (zit. SCHLAURI)

SCHMID NIKLAUS, Computer- sowie Check- und Kreditkarten-Kriminalität, Zürich 1994 (zit. SCHMID, Computerkriminalität)

SCHWARZENEGGER CHRISTIAN, E-Commerce – Die strafrechtliche Dimension, in: ARTER OLIVER/JÖRG FLORIAN S. (Hrsg.), Internet-Recht und Electronic Commerce Law, Lachen/St. Gallen 2001, 333 (zit. SCHWARZENEGGER, E-Commerce)

SCHWARZENEGGER CHRISTIAN, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001, in: DONATSCH ANDREAS/FORSTER MARC/SCHWARZENEGGER CHRISTIAN (Hrsg.), Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift für Stefan Trechsel zum 65. Geburtstag, Zürich 2002, 305 (zit. SCHWARZENEGGER, FS Trechsel)

SCHWENZER INGEBORG, Schweizerisches Obligationenrecht, Allgemeiner Teil, 2. Aufl. Bern 2000 (zit. SCHWENZER)

SENN, MISCHA CHARLES, Werbung mit E-Mails, sic! 2002, 85 (zit. SENN)

STRATENWERTH GÜNTER, Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 5. Aufl. Bern 1995 (zit. STRATENWERTH)

THOT NORMAN B./GIMMY MARC ANDRÉ, Vertragsabschluss im Internet, in: KRÖGER DETLEF/GIMMY MARC A., 2. Aufl. Berlin/Heidelberg/New York 2002, 4 (zit. THOT/GIMMY)

TRECHSEL STEFAN, Schweizerisches Strafgesetzbuch, Kurzkommentar, 2. Aufl. Zürich 1997 (zit. TRECHSEL)

WEBER ROLF H., Art. 394 – 411, 419 – 424 OR, in: HONSELL HEINRICH/VOGT NEDIM PETER/ WIEGAND WOLFGANG (Hrsg.): Kommentar zum Schweizerischen Privatrecht, Obligationenrecht I, 3. Aufl. Basel 2003 (zit. OR-Weber)

WEBER ROLF H., E-Governance im Unternehmen, in: Neuere Tendenzen im Gesell-

schaftsrecht, Festschrift für Peter Forstmoser zum 60. Geburtstag, Zürich 2003, 347 (zit. WEBER, E-Governance)

WEBER ROLF H., E-Commerce und Recht, Zürich 2001 (zit. WEBER, E-Commerce)

WEBER ROLF H., Informatik und Jahr 2000, Zürich 1998 (zit. WEBER, Informatik und Jahr 2000)

WEBER ROLF H./JÖHRI YVONNE, Vertragsschluss im Internet, in: WEBER ROLF H. et al. (Hrsg.): Geschäftsplattform Internet, Rechtliche und praktische Aspekte, Zürich 2000, 39 (zit. WEBER/JÖHRI)

WEBER ROLF H./UNTERNÄHRER ROLAND, Wirtschaftsterrorismus im Internet, in: Festschrift für Niklaus Schmid zum 65. Geburtstag, Zürich 2001, 365 (zit. WEBER/UNTERNÄHRER, Wirtschaftsterrorismus)

WIDMER URSULA/BÄHLER KONRAD, Rechtsfragen beim Electronic Commerce, 2. unveränd. Aufl. Zürich 2001 (zit. WIDMER/BÄHLER)

Mit zunehmendem Einsatz von IT-Mitteln in der Wirtschaft, Verwaltung, Wissenschaft und anderen Bereichen steigt deren Bedeutung sowohl als Ziel wie auch als Mittel der kriminellen Bedrohung.
Der Ausdruck "forensisch" bedeutet übersetzt "vor Gericht/für das Gericht". Demzufolge bedeutet "Computer Forensics" die Sicherstellung von digitalen Beweismitteln zur Überführung eines Straftäters. Dabei werden Methoden angewendet, die der Analyse, der Auswertung, der Sichtbarmachung und der Sicherung dieser Beweismittel zugute kommen und deren Beweiskraft vor Gericht unterstreichen und verstärken.

Die Arbeitsgruppe "Forensics" der Fachgruppe Security der SI hatte zum Ziel, ein Vademecum zum Bereich "Computer Forensic" zu erstellen.

Es behandelt die Themen

- Rechtliche Rahmenbedingungen für Forensic Computing
- Gefährdungsanalyse
- Durchführung einer Ermittlung
- Technische Aspekte
- Prävention

Das Vademecum soll sowohl den KMU's als auch den grossen Unternehmen als Entscheidungsgrundlage dienen, die sich durch ihre Geschäftsaktivitäten mit forensischen Belangen konfrontiert sehen.

Arbeitsgruppe "Forensics"

Diese Publikation wurde unterstützt durch

Information Systems Audit and Control Association®

InfoSurance
Information zählt immer