Inhaltsverzeichnis

1. Einleitung

news 25.04.2006 17:17

<< Vorige | Nächste >>

Studie: Sicherheitsvorfälle in UK kosten 10 Milliarden Pfund

Der durch Viren, Spyware und Hackerangriffe verursachte Schaden in britischen Unternehmen beträgt jährlich rund 10 Milliarden Pfund. Das ist das Ergebnis einer von PricewaterhouseCoopers unter rund 1000 britischen Firmen durchgeführten Umfrage "DTI Information Security Breaches Survey". Laut der heute auf der Infosec-Konferenz in London vorgestellten Umfrage ist der Schaden im Vergleich zur 2004 erstellten Studie damit um 50 Prozent gestiegen, obwohl die Unternehmen ihre Investitionen in IT-Sicherheit von drei Prozent in 2004 auf vier bis fünf Prozent ihres IT-Budgets in 2006 erhöht haben.

Quelle :(Heise 06)

IT-Sicherheit ist seit der Vernetzung von Computern eines der wichtigsten Themen der Informatik. Nachrichten wie die oben aufgeführte, stoßen daher nicht auf Überraschung und zählen schon fast zu Alltagsbild der Informatik. Mittlerweile ist bekannt, dass die Sicherheit des System eine herausragende Rolle spielt. Im Zeitalter des Internets ergeben sich Angriffspotenziale von allen Seiten. Hinzu kommt die immer größer werdende Abhängigkeit von der IT, die soweit geht, das Unternehmen ohne ein funktionierendes IT-System nicht mehr marktfähig sind. Die Wichtigkeit von Sicherheit eines Systems ist also jedem Unternehmer klar. Umso verwunderlicher, dass trotz gestiegenem Bewusstseins, die Sicherheit von Systemen immer noch nicht gewährleistet ist.

Im Zuge dieser Ausarbeitung soll auf die Fragestellung wie IT-Sicherheit aus einem nicht ausschließlich technischen Standpunkt erklärt werden kann, eingegangen werden. Zunächst wird die Gegenwärtige Situation in einer Bestandsaufnahme aufgeführt. Anschließend sollten die konkreten Herausforderungen, vor denen die IT-Sicherheit heute steht aufgezeigt werden. Um ein tieferes Verständnis zu erzeugen, sollen hier die Vielfalt und die

Unkontrollierbarkeit von Angriffen dargestellt werden. Am Ende des zweiten Kapitels wird gezeigt, dass trotz ausreichend funktionierender Technik, IT-Sicherheit alles andere als selbstverständlich ist. Der „menschliche Faktor" spielt eine große Rolle und darf in einem Sicherheitskonzept nicht vernachlässigt werden.

Aus den Schlussfolgerungen des zweiten Kapitels wird klar, dass dem bisherigen IT-Sicherheitsansatz ein entscheidender Ansatz fehlt. Im dritten Kapitel wird eine Verbindung zur Ökonomie hergestellt. Hier geht es zunächst um den Begriff der Institutionen, aus welchem heraus die Entwicklung der Prinzipal – Agenten Theorie dargelegt wird. Diese Theorie, die auf der Informationsasymmetrie zwischen Unternehmensführung und Mitarbeitern begründet ist, lässt sich auch auf die Problematik der IT-Sicherheit anwenden.

Im vierten Kapitel werden die Lösungsmöglichkeiten der Prinzipal - Agenten Theorie vorgestellt und kritisch hinterleuchtet. Wie kann es gelingen die Mitarbeiter eines Unternehmens trotz Informationsasymmetrie dazu zu bringen, verantwortlich mit der Sicherheit der Unternehmens-IT umzugehen?

Die Ausarbeitung schließt mit dem Fazit, in dem die gewonnenen Erkenntnisse nochmals zusammen gefasst werden.

2. IT-Sicherheit heute

Um eine Einführung in die Problematik zu geben, werden im folgenden die Rahmenbedingungen in denen sich IT-Sicherheit heute bewegt, beschrieben. Insbesondere soll gezeigt werden, von welcher globalen Bedeutung IT-Sicherheit im Wirtschaftsleben ist.

2.1 Eine Bestandsaufnahme

In der Studie des britischen „Departement of Trady & Industry" , dem so genannten „Information Security Breaches Survey", werden IT-Sicherheitsspezifische Daten und Zahlen erhoben und analysiert. Untersucht werden britische Unternehmen, diese werden hinsichtlich ihre Einstellung zu IT-Sicherheit, sowie bezüglich Sicherheitsvorfällen und Risiken in diesen Unternehmen befragt. Sowohl große als auch mittelständische Unternehmen sind Bestand der Analyse. Die Ergebnisse sind zum Teil überraschend.

Laut dem „Information Security Breaches Survey 2006" hatten 62 % aller Unternehmen und 87% der großen Unternehmen im Jahre 2005 mindestens einen Sicherheitsvorfall. Die Gesamtkosten pro Jahr belaufen sich für die Unternehmen auf ca. 10 Mrd. Pfund (DTI 2006).

Im Vergleich zu der selben Studie aus dem Jahr 2004 ist das eine Kostensteigerung von 50 % zu beobachten. Auffällig ist dabei, dass die Kosten bei großen Unternehmen um 50 % zurückgegangen sind, die größten Kostensteigerungen also in kleinen und mittelständischen Unternehmen zu verzeichnen sind(DTI 2004).

Bezüglich des Stellenwerts der IT-Sicherheit in den Unternehmen zeigt die Studie, dass im Jahre 2002 73% aller Unternehmen der IT-Sicherheit eine sehr hohe Priorität einräumen(DTI 2002).

War vor einigen Jahren noch zu beklagen, dass IT-Sicherheit von Seiten der Unternehmen vernachlässigt wurde, ist die Problematik nun auch bis ins Top-Management vorgedrungen. Drei mal so viele Unternehmen wie 6 Jahre zuvor haben nun ihre eigenen Sicherheitsvorgaben. 4 – 5 % der Unternehmensausgaben beziehen sich auf IT-Sicherheitsinvestitionen. Fast jedes Britische Unternehmen konsultiert Sicherheitsexperten.

Auch in die Technik wird ständig investiert. 98 % aller Unternehmen nutzen Antivirus-Software, 88 % installieren wöchentlich neue Patches für ihre Betriebssysteme. Spamfilter sind bei 86 % der Unternehmen ein fester Bestandteil.

Obwohl ein deutlicher Trend hin zu mehr Sicherheit zu verzeichnen ist, ist die Anzahl der Sicherheitsvorfälle paradoxer Weise in den letzten Jahren deutlich gestiegen, wie die folgende Grafik belegt.

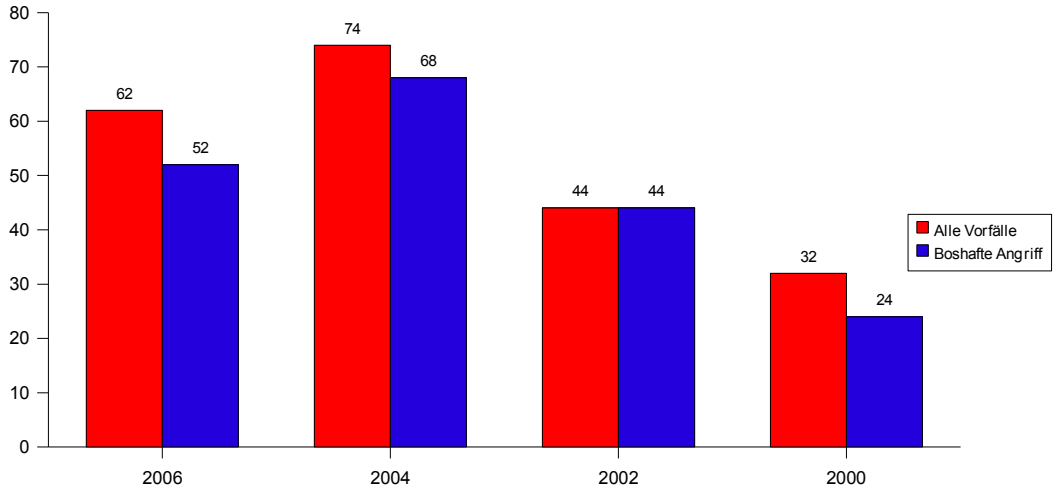


Abbildung 1:Angriffe auf Unternehmen, Quelle : (DTI 2006)

Trotz gestiegener Ausgaben in Technik und Organisation und trotz dem hohen Stellenwert den IT-Sicherheit in den Unternehmen einnimmt, scheinen Angriffe mehr denn je eine sehr große Gefahr darzustellen. Die Sicherheitsvorfälle in den Unternehmen sind bis 2004 stetig gestiegen. Zwar gab es einen leichten Rückgang zwischen 2004 und 2006, trotzdem beklagen 2005 immer noch 62 % aller Unternehmen mindestens einen Sicherheitsvorfall.

Die Erklärungsansätze für dieses Phänomen sind vielseitig. Der Anstieg ist sicherlich zum einen durch den verstärkten Einsatz von Computern in den Unternehmen zu erklären. Spätestens seit 2002 arbeiten die

meisten Unternehmen mit vernetzter IT-Technik. Mit vermehrter Nutzung von Technik steigt auch das Angriffspotential. Viele der Angriffe in 2004 wären 2000 in den meisten Unternehmen nicht vorstellbar gewesen. Zudem ist zwischen den Jahren 2004 und 2006 ein leichter Rückgang zu verzeichnen. Ein Grund hierfür dürfte das steigende Bewusstsein für die Problematik bei vielen Beteiligten sein. Unternehmen sind sich bewusster geworden, dass sich IT-Security durchaus erfolgskritisch auf den Unternehmenserfolg auswirken kann. Sicherlich spielt auch Microsofts „Trustworthy Computing" - Initiative eine große Rolle welche zumindest die Microsoft Betriebssysteme sicherer gemacht hat. Es bleibt abzuwarten, ob sich der Trend auch in der Zukunft fortsetzt.

Trotz des Rückgangs der Vorfälle in den letzten zwei Jahren bleiben die Ausgaben für IT-Sicherheit hoch. Bei einem angenommenen Bruttoinlandsprodukt von 1,2 Millionen Pfund in Großbritannien, kosten IT-Sicherheitsvorfälle die Unternehmen umgerechnet ca. 1 % des BIP. Und dies trotz einem gestiegenen Bewusstsein für Sicherheit und die Einführung von „Security Policies" in vielen Unternehmen. Es stellt sich die Frage, wie dies zu erklären ist. Warum rechnen sich die riesigen Investitionen und die Bereitschaft der Management-Ebenen über IT-Sicherheit nachzudenken, nicht?

Die Antwort auf diese Frage kann aufgrund der guten Ausstattung der Unternehmen nicht nur technischer Natur sein. Die meisten Unternehmen, verfügen bereits über gute Technologien. Schon 2002 gibt der „Information Security Breaches Survey" Handlungsempfehlungen für das Management, die über die reine technische Seite des Problems weit hinaus gehen. Als wichtiger Punkt wird das schaffen einer sicherheitsbewussten Kultur im Unternehmen empfohlen. Dies soll durch Bildung der Mitarbeiter über die Themen Sicherheitsrisiken und Verantwortlichkeit entstehen.

2.2 Was ist IT-Sicherheit?

„In theory, there is no difference between theory and practice. But, in practice, there is."
Jan L. A. van de Snepscheut

Der Begriff IT-Sicherheit wird seit jeher sehr verallgemeinernd benutzt, etwa als Beschreibung von einem Produkt. „Unser Produkt ist sicher!" oder „Unsere Firewall macht sicher!", dies sind die Zusammenhänge in denen der Begriff IT-Sicherheit auftritt. Obwohl diese Slogans in den Bereich der IT-Sicherheit gehören, umfasst IT-Sicherheit ein weitaus größeres Gebiet. Zur IT-Sicherheit gehören Fragen wie: „Wozu brauchen wir IT-Sicherheit? Vor wem wollen wir uns absichern? Was wollen wir absichern? Wie können wir es absichern?".
Ein wichtiges Merkmal von IT-Sicherheit ist, dass diese nie als absolut begriffen werden sollte. Es gibt kein System, welches über eine lückenlose Sicherheit verfügt. Das bedeutet nicht, dass das Sicherheitssysteme schlecht sind oder keine Sicherheiten bietet. Es bedeutet eben nur, dass Sicherheit immer nur partiell gilt.
Ein weiterer wichtiger Punkt der IT-Sicherheit ist, dass die Technologie immer mit Menschen interagiert. Solange diese Schnittstelle vernachlässigt wird, kann ein Sicherheitssystem keinen langfristigen Erfolg haben.
Der menschliche Faktor spielt bei der IT-Sicherheit eine große, wenn nicht sogar die tragende Rolle. Wie kann man Individuen dazu bringen sich um IT-Sicherheit zu kümmern? Wie kann man dafür sorge tragen, dass es daran denkt die Sicherheitsregeln einzuhalten? Und wie kann man verhindern das dieses Individuum vielleicht sogar absichtlich eben diese Regeln missachtet, da es keinen Angriff erwartet?

IT-Sicherheit ist offensichtlich mehr als eine bloße Eigenschaftsbeschreibung eines Systems. Sie muss sich mit der globalen Sicherheit des Systems beschäftigen und möglichst alle Akteure die in Interaktion mit dem System sind miteinbeziehen. Es stellt sich die Frage, wer die Akteure, wer die Angreifer und wer die Opfer sind. Der Folgende Abschnitt widmet sich diesen Fragen.

2.3 Protagonisten der IT-Sicherheit

"*Das was aus Bestandteilen so zusammengesetzt ist, dass es ein einheitliches Ganzes bildet, nicht nach Art eines Haufens, sondern wie eine Silbe, das ist offenbar mehr als bloß die Summe seiner Bestandteile.*" Aristoteles , Metaphysik 1041 b 10 (VII. Buch (Z))

Die Ursprünge der Systemtheorie gehen zurück bis auf Aristoteles und waren seit jeher ein wichtiger Ansatzpunkt um komplexe Systeme zu verstehen. „Das Ganze ist mehr als die Summe seiner Teile". Dieser Satz beschreibt, dass es für das Verständnis von komplexe Phänomene nicht ausreicht Einzelteile und Einzelprozesse zu betrachten, viel mehr geht es um die Organisation dieser Einzelteile. Jedes System hat Grenzen. Innerhalb dieser Grenzen befinden sich Systemelement. In dem Fall eines großen Unternehmens sind dies die Mitarbeiter und Prozesse die innerhalb des Unternehmens ablaufen. Außerhalb der Grenze befinden sich externe Elemente, zum Beispiel andere Unternehmen, aber auch externe Angreifer. Sowohl interne-, als auch externe Elemente sind für IT-Sicherheit von Belang.

2.3.1 Angreifer

Es wäre ein fataler Fehler Angreifer nur außerhalb der Unternehmensgrenzen zu suchen.

Welche Typen von Angreifern gibt es? Hier wären zunächst Hacker zu nennen. Darunter sind Computer-Profis zu verstehen, deren Spezialität es ist Software-Systeme zu kompromittieren. Dies kann aus monetären Anreizen, etwa dem Ausspähen von Kontodaten, oder aus Prestigegründen, um in der entsprechenden Szene Anerkennung zu ernten, geschehen.

Dieser Angreifer-Typus stellt eine erhebliche Gefahr dar. Jeder der möglichen Angriffsarten die weiter unten beschrieben werden, können und werden von Hackern verübt. Allerdings gibt es noch andere Gefahrenherde, die beachtet werden sollten.

Laut dem „Information Security Breaches Survey" des britischen „Departement of Trade and Industry" sind 21 % der Sicherheits-vorfälle in großen Unternehmen den Mitarbeitern des Unternehmens selbst zuzuschreiben. Allein das Öffnen von E-Mails die die Würmer „WORM_NACHI.A" und „WORM_MSBLAST.A" enthielten hat 43,9 % der gesamten Virenvorfälle bei Schering im Jahr 2003 ausgelöst. Die Nachlässigkeit vieler Mitarbeiter führt dazu, dass viele von ihnen als potentielle Gefahr für die IT-Sicherheit eines Unternehmens angesehen werden müssen.

Der dritte Typus von Angreifern sind Mittelsmänner und Unwissende. Sie sind zwar nicht die direkten Angreifer, bieten dem Angriff aber eine Plattform, etwa durch das verteilen von virenverseuchten E-Mails. Auch sie stellen eine Gefahr dar, die man in der IT-Sicherheit nicht unterschätzen darf. Ein Mittelsmann unterscheidet sich dabei von dem Unwissenden dadurch, dass er weiß, dass er einen Angriff unterstützt und dies trotzdem zulässt. Die Motivation eines solchen Handelns kann monetärer Natur sein, wenn er eine finanzielle Entlohnung für seine Handlungen erwarten darf. Er kann aber auch auf Motiven wie Rache heraus handeln, wenn er z.B. unzufrieden mit der Unternehmensführung ist.

Der unwissende Angreifer stellt ein großes Problem dar. Im Allgemeinen kann ihm nichts vorgeworfen werden. Im speziellen gibt es allerdings den Vorwurf der Fahrlässigkeit. Der durchschnittliche Mitarbeiter erwartet von seinem Computer, dass er ihn hindert Dinge zu tun, die sicherheitsgefährdend sind. Er erwartet, dass wie bei Microsofts Service Pack 2 ein Fenster in der Art : „Warnung! Sie sind im Begriff einen sicherheitsgefährdenden Schritt zugehen. Bitte klicken sie auf WEITER, wenn sie diese Meldung ignorieren wollen" erscheint.

Hierzu ein Beispiel. Stellen wir uns ein Unternehmen vor, dass seine Mitarbeiter mit WLAN bestückten Laptops ausstattet. Mitarbeiter Müller ist auf einer Dienstreise in Rom gewesen und möchte jetzt die Wartezeit am Flughafen nutzen um seine E-Mails zu abzurufen.

Um an dem Flughafen ins Internet gehen zu können, muss er allerdings zunächst ein Anmeldeverfahren durchlaufen, in welchem er sich authentifiziert und seine Kontodaten angibt. In der kurzen Zeit die er nach dem Anmeldeverfahren seine E-Mails prüft, schleust sich ein Wurm auf den Laptop ein. Am nächsten Tag betritt Müller das Firmengebäude, loggt sich in das Firmennetzwerk ein, wo sich der Wurm verbreiten kann und einen schwerwiegenden Sicherheitsvorfall auslöst.

Sowohl Mittelmänner als auch Unwissende können ein wichtiges Glied bei einem Angriff sein. Sei es ein Mitarbeiter der bewusst (aus Frust oder aus Eigeninteresse) die Installation eines bestimmten Wurms auf seinem System zulässt und damit den Weg ebnet für einen großflächigen, unternehmensweiten Angriff. Oder der Mitarbeiter, der unbedacht am Flughafen surft und aufgrund von Fahrlässigkeit Viren in das Unternehmen trägt.

Beide sind nicht selten schwer voneinander zu unterscheiden. Die Grenzen zwischen Fahrlässigkeit und Vorsatz sind häufig wenig deutlich.

Im Laufe dieser Arbeit soll geklärt werden, wie der Mitarbeiter Müller dazu gebracht werden kann, seinen Laptop abzusichern und sich verantwortlich zu verhalten. Wie am an den Zahlen der Firma Schering deutlich wird, stellt die soeben beschriebene Form von Sicherheitslücken für die Unternehmen ein erhebliches Schadenspotential dar.
Die soeben geschilderten Angriffe können auch genutzt werden um einer dritten Person Informationen zukommen zu lassen, z.B. einem Konkurrenzunternehmen. Ein Hacker kann beispielsweise damit beauftragt werden ein Konkurrenzprogramm anzugreifen, oder einem Mitarbeiter wird Geld oder eine Abwerbung im Tausch gegen sensible Informationen angeboten. Derartige Praktiken lassen sich unter dem Stichwort Industriespionage beschreiben.
Angreifer können aber auch Institutionen sein, von denen man illegales Verhalten nicht erwarten würde. Zum Beispiel die Presse auf der Suche nach unsauberen Geheimnissen oder aber auch die Regierung oder die Polizei. In Zeiten in denen der Bürger zunehmend durchsichtig wird, stellt sich die Sicherheit und Vertraulichkeit der sensiblen Informationen als enorm großes Problem heraus.
Angriffe auf die IT-Systeme von Unternehmen weisen das Problem auf, das sie schwer zu verfolgen und zu bestrafen sind. Nicht selten dürfte der Fall auftreten, das ein Angriff auf Seiten des Angegriffenen gar nicht bemerkt wird. Vor allem in Zeiten des Internets, wo Angreifer direkt im Büro nebenan oder auf der anderen Seite des Erdballs sitzen können, stößt das nationale und europäische Recht an seine Grenzen.

2.3.2 Opfer und Angriffsarten

Opfer eines Angriffs kann in der heutigen Welt jeder Mensch sein, dessen Computer an das Internet angeschlossen ist. Da dies heute für so gut wie jeden Computer gilt entsteht ein enorm breites Angriffsfeld.

In dieser Ausarbeitung sollen private PC-Anwender unberücksichtigt bleiben, außer wenn sie nicht als Mittelsmänner oder Unwissende an dem Angriff beteiligt sind. Schwerpunktmäßig soll der unternehmerische Bereich beleuchtet werden, der ein weitaus kritischeres Angriffsfeld darstellt.

Da heute fast alle Unternehmen und beinahe jede öffentliche Einrichtung an das Internet angeschlossen ist, sollte sich jedes Unternehmen und jede öffentliche Einrichtung kritisch mit ihrer IT-Sicherheit auseinander setzen. Waren früher Angriffe über Diskette oder andere Datenträger leicht zu kontrollieren (indem man die Nutzung von Disketten untersagte), so lässt sich eine solche Kontrolle auf den Internetverkehr nicht mehr anwenden.

Die Angriffe auf die sich ein solches Unternehmen vorbereiten muss sind vielschichtig. Sie betreffen jeweils eine oder mehrere der folgenden Zielsetzungen eines Unternehmens: Vertraulichkeit, Verifikation, Authentifikation und Integrität. Ein für das Unternehmen kritisches Risiko entsteht, wenn es eine konkrete Schwachstelle im System gibt. Diese Schwachstelle muss gefährdet sein, d.h. Angreifer wollen sich die Schwachstelle zu nutze machen und die Ausnutzung der Schwachstelle muss ein gewisses Schadenspotenzial mit sich bringen. Wenn dann noch die Häufigkeit eines solchen Angriffs, sehr hoch sein kann, besteht ein großes Risiko für das Unternehmen. Das Risikomanagement eines Unternehmens muss sich mit der Suche nach Schwachstellen beschäftigen ihre Gefährdung, Schadenspotenzial und die Häufigkeit eines möglichen Angriffs abschätzen. Eine abschließende Aufzählung aller potentiellen Angriffsformen würde den Rahmen dieser Semesterarbeit sprengen, grundsätzlich kann man diese jedoch den folgenden Kategorien zuordnen:

Kriminelle Angriffe sind Angriffe bei denen es um Betrug, Diebstahl von Daten oder anderem wertvollen Eigentum, Zerstörung, Spionage oder Manipulation geht. Unter Vertraulichkeitsverletzungen werden alle

datenschutzkritischen Angriffe eingestuft aber auch das Abhören von Datenverkehr oder elektronische Überwachung. Eine vor allem in großen Unternehmen häufig auftretende Angriffsart ist der „Publicity-Angriff" (vgl. Bruce) heutzutage häufig durch DOS (Denial-of-Service) Attacken ausgeführt. Die Angreifer haben hier kein anderes Ziel als die Schwachstellen des Unternehmens an die Öffentlichkeit zu bringen, bzw. ihren eigenen Namen (meisten nicht verfolgbare Hackernamen) in der Szene bekannt zu machen. Diese Angriffe stellen aus Unternehmenssicht ein erhebliches Risiko dar, wie wie im Laufe dieser Ausarbeitung dargelegt werden soll.

2.4 Technische Mittel der Angreifer

Die technischen Möglichkeiten, auf die Angreifer zurückgreifen können, sind nahezu unerschöpflich. Zu den neusten Angriffstools oder Algorithmus bestehen praktisch keine Zugangsbarrieren, diese können von jedem beliebigen Computer im Internet eingesehen werden. In den Fällen, in denen der Angreifer über ausreichende finanzielle Mittel verfügt, meist handelt es sich hier um Fälle der organisierten Kriminalität bzw. um Unternehmensspionage, kann das nötige Fachwissen von Spezialisten eingekauft werden.

Angriffe finden dabei auf unterschiedlichen Ebenen statt. Sie können durch Emails, das Ausnutzen einer unsicheren Browserimplementierung oder einer Sicherheitslücke im Betriebssystem eines Servers eingeleitet werden.

Eine zweite Folge der Vernetzung ist die Automatisierung von Angriffen, die vor allem bei DOS und „Dynamic" - DOS-Attacken zum Tragen kommt. Ist eine Schwachstelle in einem System erst einmal gefunden, wird der Angriff von Hackern und anderen Angreifern automatisiert und in ein Skript oder ein kleines Stück Software eingebettet. Nun kann jeder Computerbesitzer mit minimalen Grundkenntnissen selbst den Angriff durchführen, indem er die Scripte benutzt ohne sie kennen, oder

programmieren zu müssen. Das früher notwendige Fachwissen für einen weit angelegten Angriff entfällt. Es entstehen so genannte „Skript-Kiddies" die sich mit ihren Skripten von einem Angriff zum nächsten hangeln.

Der Ablauf der Angriffe ist meist ähnlich. Viren sind nicht mehr sonderlich weit verbreitet aber immer noch von großer Brisanz. In allgemeinen sind Viren nicht mehr als Programmcode der sich an ein Anwendungsprogramm hängt oder sich selbst in den Bootsektor schreibt. Beim Ausführen des Programms oder beim Booten wird der Code des Virus mit ausgeführt und er „infiziert" andere Programme. Dies bedeutet, dass der Virus seinen Code in denen andere Programme schreibt . Makroviren sind Scripte, zum Beispiel in der Skriptsprache Visual Basic geschrieben, die sich im Internet schnell verbreiten können, weil sie sich an E-Mail anhänge und Webseiten-Contents heften.

Würmer treten im Gegensatz zu Viren nur in vernetzten Computersystemen auf. Sie verstecken sich nicht wie Viren in anderen Programmen, sondern sind eigenständige Programme die sich selbstständig über das Netzwerk hinweg reproduzieren um den maximalen Schaden an möglichst vielen Orten anzurichten.

Ein Trojaner ist einem Wurm sehr ähnlich. Es ist ein Stück schädlicher Code, der in einem Programm eingebettet ist, welches gutwillig wirkt. Das trojanische Pferd ist dabei meist eine Software von der man nicht erwarten würde, dass sie sich schädlich verhält, etwa ein Bankmanagement-Programm dass nach ein paar Monaten Nutzung dem User ohne sein Wissen Geld auf ein Konto in Indien überweist. Dies geschieht nicht aktiv durch das Programm selbst. Der Trojaner installiert sich aus dem Programm heraus in den Computer und überwacht zum Beispiel den Transaktionsverkehr und übermittelt dann Kreditkartennummer oder Online-Banking PIN an seinen Schaffer. Trojaner können sich auch im Netzwerk reproduzieren.

Ein Trojaner ist besonders heimtückisch, weil der Nutzer ihn nicht als boshafte Software erkennt. Er ist also wieder ein Unwissender in der Angriffskette.
Weitere böswillige Software, wie etwa schädliche Java-Scripte oder ActiveX Controls können ebenfalls Gegenstand eines Angriffs sein.

Alle diese Angriffe werden durch die Nutzung des Internets erst ermöglicht. Angriffsmethoden können im Internet entdeckt, benutzt, weiterentwickelt und automatisiert werden. Die Unternehmen stehen somit vor einem globalen Problem, dass sich allein durch technische Maßnahmen nicht mehr lösen lässt.

2.5 Potentielle Fehler auf der Anwenderseite

Wie kommt es, dass IT-Systeme nach 20 Jahren Software Entwicklung immer noch so unsicher sind?
Um einen Angriff zu ermöglichen bedarf es einer Angriffsfläche. Angriffsflächen können vielfältig sein, lassen sich meist aber auf Sicherheitslücken oder fehlerhafte Implementierung von Software oder Betriebssystemen zurückführen. Die Ariane 5 Rakete der ESA explodierte aufgrund eines Überlaufs bei dem Versuch eine 64-Bit-Zahl in eine 16-Bit-Zahl zu konvertieren. Die meisten Würmer und Viren machen sich Sicherheitslücken im Windows Betriebssystem zu nutze. Viele Applets können überhaupt nur deswegen schädlich werden, weil die Browser-Implementierung unverantwortlich verlief.
Usability ist ein wichtiges Stichwort: Wie bereits erwähnt, erwartet der Nutzer von seinem System informiert zu werden, wenn er im Begriff das System durch seine Handlungen zu gefährden. Das System sollte also mit dem User in einen Dialog treten, in dem es ihm die ablaufenden Prozesse verdeutlicht und Handlungsempfehlungen liefert. Trotz dem

seit Jahren gestiegenem Bewusstsein für Usability in der Software Entwicklung gibt es immer noch Systemlücken, die selbst bei vorsichtiger Nutzung einen Angriff von außen ermöglichen.
Daher stellt sich die Frage warum Software so anfällig für Sicherheitslücken ist. Warum ist es augenscheinlich nicht möglich eine sichere Software auf den Markt zu bringen?
Die Antwort auf diese Frage ist für Informatiker nicht neu: Software ist Komplex. Das Windows-Betriebssystem besteht aus mehreren Millionen Zeilen Code. Unzählige Module interagieren miteinander, senden wechselseitig Daten oder machen Einträge auf den Speichermedien. Die Kontrolle über ein solch komplexes System ist allein schon aufgrund der enormen Komplexität unmöglich. James Bessen bemerkt treffend:

„Because the features in a complex software program interact with each other, each use-product must be individually teste to ensure it works. Yet firms cannot feasibly test all possible use-products because the number of possible combinations is astronomical”(Bessen 2005)

Er geht von einem hoch stilisierten Modell aus, dass für unsere Ansprüchen genügt: Für jedes “Feature”, d.h. für jede besondere Funktion eines Programms gibt es zwei Nutzungsmöglichkeiten: Entweder es wird in Interaktion mit anderen Features benutzt, oder nicht. Die Nutzung eines Programms ließe sich also in einer binären Form fassen. Ein Programm mit 4 features hat also 2^4 = 16 mögliche Nutzungsarten. Geht man von einem Programm aus, welches 100 Features besitzt, wessen Software mit verschiedenen Hardware-Herstellern kompatibel sein soll und welches auf eine verschiedene Speichergrößen oder Grafikkarten angepasst sein muss, dann ergeben sich Nutzungsarten für ein Stück Software, die die Testbarkeit eines solchen Produktes nahezu unmöglich machen. Laut Bessen treffen Entwickler zwar Annahmen, welche Kombinationen am

wahrscheinlichsten sind und diese werden dann getestet. Trotzdem bleibt es eine unmögliche Aufgabe ein Stück Software für alle möglichen Umstände bzw. Angriffsarten zu testen und abzusichern.
Dies gibt eine Erklärung warum Software immer einen gewissen Unsicherheitsfaktor mit sich bringt. Aber es erklärt noch nicht, warum fehlerhafte Software immer häufiger genutzt wird. Es scheint fast so als würde fehlerhafte und unsichere Software die sicheren Produkte vom Markt verdrängen. Eine Erklärung hierfür ist die Marktpenetrations-Strategie.

"*The huge first-mover advantages that can arise in economic systems with strong positive feedback are the origin of the so-called Microsoft philosophy" of `we'll ship it on Tuesday and get it right by version 3'. Although sometimes attributed by cynics to a personal moral failing on the part of Bill Gates, this is perfectly rational behaviour in many markets where network economics apply.*"
(Anderson 2001)

Große Softwarefirmen scheinen kein Interesse für sichere Software zu haben, die Entwicklung würde viel zu lange dauern. Es geht vielmehr darum die Produkte möglichst rasch am Markt anbieten zu können, um schnell eine kritische Anwendergröße zu erreichen. Anschließend erst widmen sich diese Unternehmen dann den Sicherheitsaspekten. Dieses ex post Verfahren gilt in der IT- Sicherheit als überholt und unzweckmäßig. Allerdings ist diese Verhalten in sich logisch und folgt den Gesetzen des freien Marktes.
Obwohl die Technik allein niemals ein absolut sicheres System schaffen kann, ist diese heute soweit ausgereift, dass die Auslöser für Sicherheitsvorfälle in den seltensten Fällen in der Technik zu finden sind. Der Information Protection Officer von der Schering AG, Alexander Göbel sagt dazu : „Es ist ganz klar, dass die Angriffspotentiale auf

einem viel niederem Niveau befinden. Ein Angreifer wird nicht versuchen unsere Firewall zu durchbrechen, weil diese zu ausgereift ist und es nahezu unmöglich ist da durch zu kommen. Die Angriffspotenziale um die wir uns heute kümmern sind eher im unternehmensinternen Bereich angesiedelt. Wir müssen uns verstärkt mit Fragen über Verantwortlichkeit und Vertraulichkeit der Mitarbeiter auseinander setzen".

2.6 IT-Sicherheit heute – ein Zwischenstand

Aus den beschriebenen Schwierigkeiten und Problemen lässt sich schlussfolgern, dass die absolute Sicherheit eines Systems Utopie ist. Im Gegensatz dazu wird durch Automatisierung von Angriffen und durch leichteren Zugang zu Computern und zur Technik jeder denkbare Angriff möglich und es wird für die Angreifer immer leichter diese auszuführen.
Unbemerkt ist es in den letzten Jahren jedoch zu einer schleichenden Veränderung bei Angriffen auf IT-Systeme gekommen. Stand früher noch die Technik im Visier der Angreifer, so ist es heute der Anwender, der die größte potentielle Sicherheitslücke darstellt. Die Angriffe müssen auf einer anderen Ebene durchgeführt werden.
Aus Sicht der Autoren ist daher für einen Umgang mit dem Problem eine ganzheitliche Sichtweise erforderlich. Der technische Aspekt spielt hier eine äußerst wichtige Rolle, auch in Zukunft dürfte es von außerordentlicher Bedeutung sein, das sich Unternehmen durch den Einsatz modernster Technik vor Angriffen von innen und außen schützen. Da in der allgemeinen Diskussion zum Thema IT-Sicherheit jedoch vor allem auf die technologischen Gesichtspunkte hingewiesen wird, soll dieser Bereich in dieser Arbeit ausgespart werden. Dem interessierten Leser seien hier die diversen Artikel und Bücher empfohlen, die sich mit dieser Thematik beschäftigen. Will man IT-Security jedoch ganzheitlich betrachten, ist eine nur auf die technische Seite beschränkte Sichtweise nicht ausreichend, der technische Aspekt

ist eine notwendige, nicht aber eine hinreichende Bedingung für Sicherheit. Erst durch die Einbeziehung der Menschen fügt sich der Kreis zusammen, selbst die Leistung des besten Computer der Welt ist von der Qualifikation seines Nutzer abhängig.

2.7 Praxis der IT-Sicherheit

„*Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit dem Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.*" *Aktiengesetz (AktG), § 91 (2)*

Wie bereits erläutert wurde, ist die wahrgenommene Bedeutung von IT-Sicherheit in den letzten Jahren durchaus gewachsen. Sowohl Gesetze als auch Unternehmensverträge schreiben ein gewisses Maß an Sicherheit vor. So etwa das Aktiengesetz, welches zwar recht allgemein gehalten, aber doch unmissverständlich postuliert, dass sich der Vorstand einer Aktiengesellschaft mit dem Thema Sicherheit zu beschäftigen hat (vgl. GmbH-Gesetz, § 43, (1)).
Die „First wave of information security" mit der Professor Basie von Solms die technische Herangehensweise von Unternehmen Anfang der 80er betitelt, beendigt. Auch nach von Solms, hat sich der Management-Ansatz mittlerweile durchgesetzt (second wave) und die Institutionalisierung von IT-Sicherheit in den Unternehmen hat begonnen (Solms 2000, S. 615-620).
Der technische Weg allein kann dabei aufgrund der Komplexität der Technik und der Unberechenbarkeit der Protagonisten keinen Erfolg garantieren. Die Statistiken aus dem ersten Teil dieser Ausarbeitungen belegen, dass viele Angriffe, durch unachtsames Verhalten von Mitarbeitern ermöglicht werden. Es gibt sogar Angriffe die von den Mitarbeitern bewusst von innerhalb des Unternehmens initiiert werden.

Gerade solche Angriffe können mit den heutigen technischen Möglichkeiten nicht verhindert werden, da Angreifer die von innen kommen (seien es Unwissende, Mittelsmänner oder tatsächliche Saboteure) immer hinter dem Sicherheitswall sitzen. Von ihnen wird erwartet, dass sie mit verantwortlichem Handeln die Sicherheit des Systems unterstützen. Die kryptographische Verschlüsselungsfunktion für die Passworte eines Unternehmenssystems kann noch so ausgeklügelt sein: Wenn ein Mitarbeiter das Passwort aufschreibt weil er es sich nicht merken kann, kann diese Information unter Umständen in falsche Hände gelangen und erheblichen Schaden auslösen.

Die Betrachtung von IT- Sicherheit in der Praxis erfordert also neben dem technischen Ansatz eine intensive Betrachtung des menschlichen Faktors, ohne muss IT-Sicherheit langfristig scheitern.

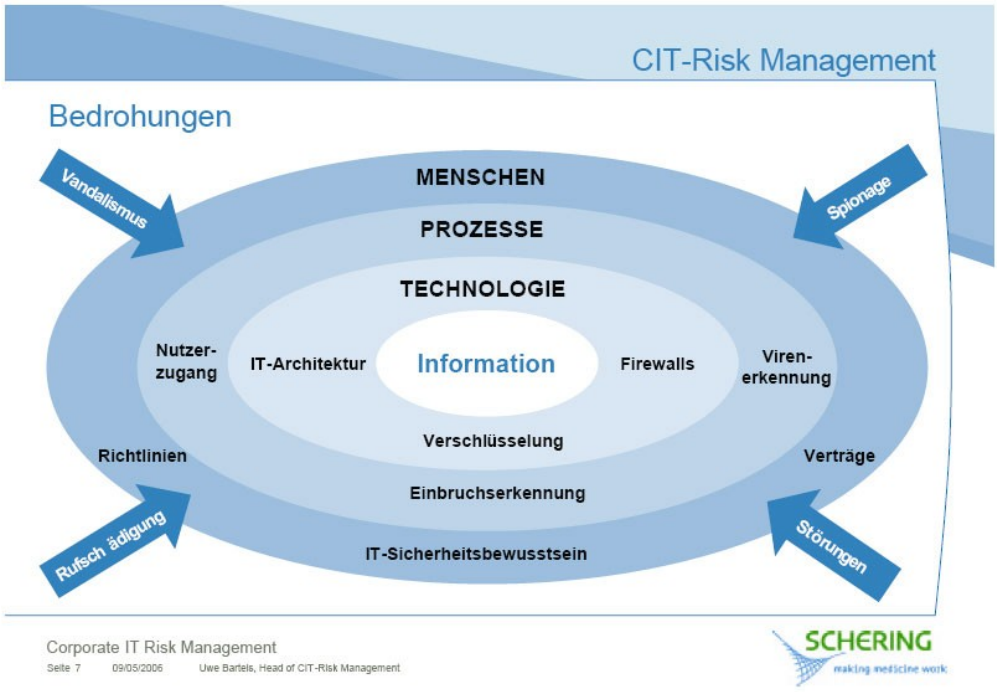


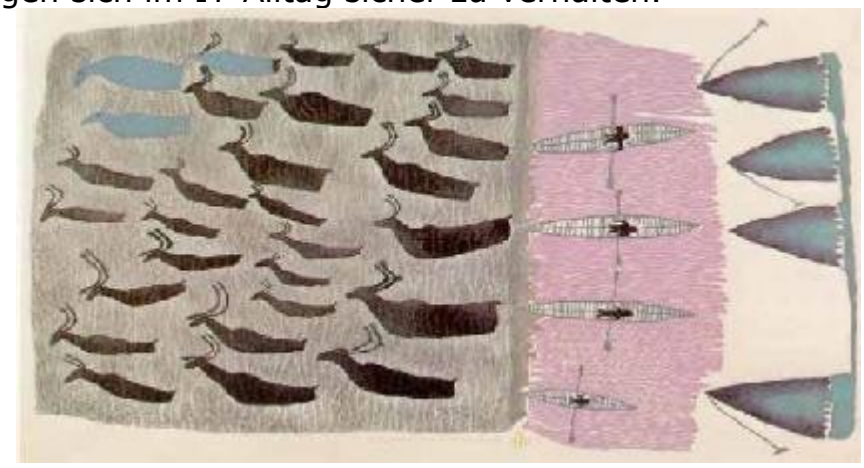
Abbildung 1: Risk Management, Quelle: (Schering 2006)

Wie muss ein Unternehmen konkret handeln? Wie kann man Mitarbeiter dazu überreden, sich mit ihrem Laptop nicht am Flughafen ins Internet einzuwählen? Wie kann man sie dazu bringen sich sein Passwort zu merken anstatt es sich aufzuschreiben?
Bei der Betrachtung dieser Fragen wird schnell deutlich, dass diese Probleme aus Perspektive der heutigen Informatik nicht gelöst werden können. Eine Betrachtung der IT-Sicherheit unter ökonomischen Gesichtspunkten wird notwendig.

3. IT-Sicherheit unter ökonomischen Gesichtspunkten

„Schöne mathematische Werke wurden durch schlechte Programmierung, durch ein miserables Betriebssystem oder durch eine unglückliche Passwortwahl irrelevant."*(Schneier 2004)*

Der Mensch ist, wie schon beschrieben, selbst mit der besten IT-Verschlüsselung und noch so ausgeklügelten Sicherheitsmechanismen, als Sicherheitsrisiko nicht völlig auszuschließen. Hier stellt sich demnach nicht die Frage nach noch besserer Technik. Fraglich ist viel mehr, warum es für die Firmen so schwierig ist, ihren Mitarbeitern beizubringen sich im IT-Alltag sicher zu verhalten.



«Hunting Caribou by Kajaks» Bild der Kanadischen Inuit Luke Anaguhadluq von 1976

Diese Problematik gibt es schon seit Urzeiten. Als man sich damals zur Jagd auf so genannte Karibus zusammen schloss stellte sich die Frage, wie sichergestellt werden kann, das alle Individuen die gleiche Arbeit für gleichen Lohn leisten? Man kann versuchen diese Frage unter einem psychologischen Hintergrund zu erklären, wobei man in diesem Fall nur die Handlungen eines Einzelnen beschreibt bzw. versucht vorher zusagen. Dies reicht in einem so komplexen Umfeld wie es in einem Unternehmen der Fall ist, nicht aus. Auch die Ökonomie beschäftigt sich erst seit kurzem mit dieser Problematik und seinem vielleicht wichtigsten Aspekt, den internen und externen Institutionen. Doch gerade diese sind in vielen Situationen die wichtigen Entscheidungsparameter.

3.1 Die institutionelle Ökonomie

„Wachstum und Entwicklung hängen entscheidend von den jeweils gültigen Institutionen ab."(Voigt 2002)

Die neue Teildisziplin, der neuen Institutionen Ökonomie(NIÖ), beschäftigt sich mit der oben aufgeworfenen Fragestellungen. Sehr großen Wert wird die Institutionen gelegt, die das Handeln aller Akteure maßgeblich beeinflussen. Mit Institutionen sind nicht allein vom Staat oder andern öffentlichen Einrichtungen gegebenen Gewaltinstanzen gemeint. Vielmehr werden neben den gesetzlichen Verboten und Pflichten auch Normen, Sitten, Traditionen unter diesem Begriff zusammengefasst. Die verschiedenen Ebenen von Institutionen kann folgendermaßen klassifizieren:

Regel	Art der Überwachung	Institutionenkategorie	Beispiel
1. Konvention	Selbstüberwachung	intern vom Typ 1	grammatikalische Regeln
2. Ethische Regel	Imperative Selbstbindung	intern vom Typ 2	Dekalog, kategorischer Imperativ

Regel	Art der Überwachung	Institutionenkategorie	Beispiel
3. Sitte	Spontane Überwachung durch andere Akteure	intern vom Typ 3	gesellschaftliche Umgangsformen
4. Formelle private Regel	Geplante Überwachung durch andere Akteure	intern vom Typ 4	Selbst geschaffenes Recht der Wirtschaft
5. Regel positiven Rechts	Organisierte staatliche Überwachung	extern	Privat- und Strafrecht

Quelle: Stefan Voigt, S. 39

Betrachtet man Institutionen aus gesellschaftlicher Perspektive, bietet es sich an Institutionen deren Missachtung von der Gesellschaft selbst sanktioniert werden, wie zum Beispiel gesellschaftliche Umgangsformen, als intern zu bezeichnen. Im Gegensatz hierzu, werden externe Institutionen durch den Staat durchgesetzt, also durch eine außerhalb des Modells stehende Machtquelle. Interne und externe Institutionen stehen normalerweise in einer Wechselbeziehung. (Voigt 2002) Vorstellbar ist jedoch auch eine neutrale Beziehung, bei der externe und interne Institutionen nicht gleichstark auf die Handelnden einwirken. Wenn externe- und interne Institutionen auf gleicher Weise das Handeln von Individuen beschränken und die Einhaltung durch beide überwacht wird, so spricht man von einer komplementären Beziehung. Bei Überwachung durch nur eine Instanz, also entweder privat oder staatlich, handelt es sich um eine substitutive Beziehung. Besonders ineffizient ist es, wenn sich interne und externe Institutionen gegenseitig korrigieren, blockieren oder aufheben. Ist dies der Fall, so ist es für das Individuum unmöglich eine Institution zu befolgen ohne dabei die andere Institution zu verletzen.

3.2 Chancen und Risiken von Kooperationen

Nun zurück zu der Jagd auf Karibus. Einem einzelnen Individuum fällt es schwer ein wesentlich größeres und schwereres Tier wie ein Karibu allein zu erlegen. Darum schlossen sich schon damals die Menschen zu Gemeinschaften zusammen, da sie auf diese Weise zusammen ein

besseres Ergebnis erzielten, als wenn jede Person alleine auf die Jagd gegangen wäre. Ökonomisch betrachtet legen die Individuen ihre Fähigkeiten und Ressourcen zusammen, um die Summe des Outputs, nämlich die erlegten Herde Karibus, im Verhältnis zu der Summe der einzelnen Teile, nämlich gar keinen, oder nur wenige Karibus, zu vergrößern.

Dieses nutzenmaximierende Verhalten birgt ein ökonomisches Problem, für welches bisher keine zufriedenstellende Lösung gefunden wurde. Sobald die Handelnden einmal ihre Ressourcen zusammengelegt haben, gibt keine Möglichkeit mehr den Beitrag der einzelnen Individuen zu messen und dadurch zu einer „gerechten Verteilung" zu finden. Diese Problematik kann dazu führen, dass jedes Mitglied der Gruppe bestrebt ist seine persönliche Leistung zu minimieren und dadurch seine Kosten-Nutzen-Rechnung zu verbessern. Das führt im schlimmsten Fall zu einer Einstellung jeglicher Kooperation zwischen den Gruppenmitgliedern. Folge ist eine suboptimale Lösung.

Ökonomisch lässt sich somit festhalten: Wenn Individuen bei Kooperationen versuchen ihren persönlichen Nutzen zu maximieren, führt das zu nicht optimalen Ergebnissen. Als Lösung dieses Problems bedarf es einer Institution die verhindert das Individuen bei gemeinschaftlichen Aktivität als Trittbrettfahrer agieren. Es gibt eine Reihe an Möglichkeiten eine solche Institution zu schaffen, beispielsweise durch eine Art Ehrenkodex auf den sich die Gruppenmitglieder verständigen.

Eine andere Möglichkeit, die nunmehr in den Vordergrund dieser Ausarbeitung treten soll, ist eine Organisationsform der Hierarchien. Teammitglieder werden hier mit besonderen Rechten ausrüstet die es ihnen erlauben Gebote und Verbote aufzustellen und diese durch Sanktionen durchzusetzen. Dieses, im folgenden als Vorgesetzter bezeichnete Mitglied, darf in der Hierarchie untergebene Individuen

(Arbeitnehmer) aufnehmen und freisetzen. Der Vorgesetzter sorgt dafür das alle Mitglieder die geforderte Arbeit erbringen bzw. bestraft Mitglieder die dies nicht tun.
Als problematisch stellt sich bei einer immer größer werdenden Gruppe heraus, dass der Vorgesetzte immer mehr seiner Ressourcen (Zeit, Kraft...) dafür aufbringen muss seine Arbeitnehmer zu kontrollieren. Zusätzlich erschwerend kommt hinzu, das die Arbeitnehmer teilweise versuchen ihre Untätigkeit zu verschleiern. Es handelt sich um eine Informationsasymmetrie die nur mit Einsatz zusätzlicher Ressourcen abgebaut werden kann. Dieser Problematik, dass der Auftraggeber (=Vorgesetzter) die Handlungen seines Untergebenen kaum oder gar nicht kontrollieren kann, ist in der Ökonomie unter dem Begriff der Prinzipal-Agenten-Theorie bekannt.

3.3 Die Prinzipal-Agenten-Theorie

„Whenever one individual depends on the action of another, an agency relationship arises. The individual taking the action is called the agent. The affected party is the principal."
(Pratt/Zeckhauser 1985)
Der Prinzipal, im gewählten Beispiel der Vorgesetzt verfolgt bestimmte Interessen, diese könnten zum Beispiel in einer Steigerung der Unternehmensgewinne liegen. Zu diesem Zweck delegiert er Aufgaben an die Agenten (die Arbeitnehmer). Diese wiederum verfolgen ebenfalls Interessen, jedoch stimmen diese nicht unbedingt mit denen des Prinzipals überein. Beispielsweise kann der Agent versuchen seinen persönlichen Nutzen dadurch zu erhöhen, dass er für die gleiche Entlohnung weniger arbeitet. Hinzu kommt, das der Prinzipal nicht alle Agenten überwachen kann und dadurch nicht das gleiche Wissen hat wie die Agenten. Es liegt somit zum einen ein Interessenkonflikt zum anderen eine Informationsasymmetrie vor.

Diese Problematik existiert nicht allein bei Firmen, sondern auch beispielsweise bei Aktionären und Vorstandsmitgliedern, zwischen Generälen und untergeordneten Offizieren oder zwischen Wählern und Politikern. Immer wird der Agent vom Prinzipal mit Aufgaben betraut, die er im Interesse des Prinzipals ausführen soll. Der Agent versucht jedoch, im Handlungsspielraum der ihm gegeben wurde, seine eigenen Interessen durchzusetzen. Ständige Kontrollen durch den Prinzipal sind aus Gründen der Effizienz nicht möglich.

Für den Prinzipal gibt es allerdings die Möglichkeit mit dem Agenten Verträge abzuschließen, welche den Agenten den Anreiz geben, möglichst optimal für den Prinzipal zu handeln. Die Verträge müssen so gestaltet sein, dass der Agent den Nutzen den er aus dem Vertrag ziehen kann maximiert und gleichzeitig der Nutzen für den Prinzipal, quasi als Nebenbedingung, maximiert. Die Kosten die hieraus für den Prinzipal entstehen werden Agenturkosten genannt, sie beinhalten alle Kosten, die der Prinzipal aufwenden muss, um dem Agenten seinen „Eigennutzen ab zukaufen". Dieses Vorgehen kann zu zwei Problemen führen, die sich durch den Zeitpunkt ihres Eintretens unterscheiden lassen lassen. Die Adverse Selection beschreibt die Informationsasymmetrie vor Vertragsschluss. Das Problem, des Moral Hazard entsteht im Gegensatz dazu erst nach dem Vertragsschluss.

3.3.1 Adverse Selection

Bei der Adverse Selection kommt es durch ein Informationsdefizit beim Prinzipal vor Vertragsschluss zu einer ganzen Reihe möglicher negativer Effekte.

Um bei dem bereits erwähnten Beispiel der Karibu-Jagd zu bleiben: Angenommen die Karibu-Jäger wählen einen Anführer bzw. Prinzipal. Dieser stellt aus der Gruppe von Stammesmitgliedern seine Jagdgruppe zusammen. Er möchte die stärksten und fähigsten Männer aufnehmen, um möglichst viele Karibus zu fangen. Handeln die Mitglieder

(=Agenten) nicht aus altruistischen Motiven, so müsste er ihnen nach dem Jagen eine höhere Entlohnung zukommen lassen. Obwohl die übrig bleibende Summe die unter den restlichen Stammesmitgliedern verteilt werden kann, geringer ist, kann dieses Verhalten durchaus rational sein. Angenommen der Anführer würde einem starken und fähigem Mann drei Karibus geben, einem mittelmäßig fähigem Mann zwei Karibus und einem schwachen Jäger einen Karibu. Der Anführer, kann jedoch nicht auf Anhieb erkennen und beurteilen welcher Jäger zu den starken und fähigen gehört. Die Jäger wissen allerdings ganz genau um ihre Fähigkeiten und können ihren Wert gut abschätzen. Um dieses Problem zu lösen bietet der Häuptling allen potentiellen Jägern den durchschnittlichen Lohn von zwei Karibus. So kann er eventuelle Verluste die ihm ein zu hoch bezahltes Mitglied bringt, durch ein etwas niedriger bezahltes, gutes Mitglied ausgleichen. Allerdings hat diese, auf den ersten Blick durchaus vernünftige Regelung, erhebliche Nebenwirkungen. Der Lohn ist aus Sicht der schlechten Jäger durchaus attraktiv, er liegt über dem, was diese normalerweise für ihre Arbeit erhalten würden. Für die guten Jäger liegt der Lohn jedoch erheblich unter ihrem Produktivitätsniveau, unter Umständen sind sie nicht bereit, auf Grundlage dieser Entlohnung auf die Jagd zu gehen. Sie werden versuchen abzuwandern oder einfach nicht mehr ihre Fähigkeiten trainieren, da sie ja auch mit weniger Jagderfahrung genauso gut bzw. schlecht bezahlt werden. Letztendlich kommt es dazu das die weniger fähigen Männer die fähigen verdrängen. Der Prinzipal hat beim nächsten Jagdausflug nur noch die Auswahl zwischen den Männern die ihn zwei Karibus und denen die ihn ein Karibu kosten würden. Er setzt natürlich wieder einen durchschnittlichen Lohn von diesmal 1,5 Karibus fest. Dies führt wiederum dazu, das nun auch die durchschnittlichen Jäger nicht mehr bereit sind, für den Prinzipal auf die Jagd zu gehen. Die Negativauslese setzt sich fort bis nur noch die schlechten Jäger übrig sind.

Dieser Teufelskreis lässt sich durchbrechen. Der Anführer könnte, bevor er Jäger auswählt von ihnen eine Arbeitsprobe verlangen, bei der sie ihre Fähigkeiten unter Beweis stellen müssen. Dies ist für den Anführer allerdings mit so genannten Agenturkosten verbunden.

3.3.2 The Market for 'Lemons'

„But the bad cars sell at the same price as good cars since it is impossible for a buyer to tell the difference between a good and a bad car; only the seller knows."
(Akerlof 1970)

George Akerlof hat 1970 bereits mit seinem Artikel " The Market for 'Lemons' " den soeben beschriebenen Mechanismus aufgezeigt. Im deutschsprachigen Raum ist das Dilemma auch als das 'Saure-Gurken-Problem' bekannt. Das Ergebnis eines derartigen Marktumfeldes ist, dass völlige Systemversagen nach relativ kurzer Zeit. Diese These steht im völligen Widerspruch zur neoklassischen Theorie, nach der sich jeder Markt selbst reguliert.
Akerlof beschreibt die Problematik am Beispiel des amerikanischen Gebrauchtwagenmarkt. Um das Beispiel so einfach wie möglich zu halten, gibt es nur gute oder schlechte Autos. In den USA werden qualitativ schlechte Gebrauchtwagen auch 'lemons' (Zitronen) genannt. Die zentrale Rolle bei der Betrachtung spielt die Informationsasymmetrie oder auch hidden characteristics zwischen Käufer und Verkäufer. Der Prinzipal, in diesem Fall der Käufer, möchte ein qualitativ gutes Auto kaufen und ist auch bereit einen höheren Preis dafür zuzahlen. Dem Prinzipal ist es jedoch nicht möglich, kostenlos festzustellen ob das Auto eine 'Zitrone' ist oder nicht. Der Agent (der Verkäufer) wiederum kennt die Qualität seines Automobils ganz genau und hat eine genaue Vorstellungen vom Preis den er für das Auto verlangen kann. Um seine persönlichen Nutzen zu vergrößern, versucht

der Agent ein möglichst schlechtes Auto zu einem möglichst hohen Preis zu verkaufen. Da dem Käufer nun wichtige ausschlaggebende Informationen fehlen, geht er von einer durchschnittlichen Wahrscheinlichkeit aus, ein gutes Auto zu bekommen. Dies schlägt sich im Preis nieder, den der Käufer maximal zu zahlen bereit ist, er muss eventuelle Risiken die mit einer Zitrone verbunden sind, einkalkulieren. Angenommen, der Prinzipal wäre bei vollständiger Informations-Symmetrie bereit für eine Zitrone 200 Dollar und für ein gutes Auto 1000 auszugeben. Da Informationsasymmetrie vorliegt, bildet der Käufer einen Mittelwert, also 600 Dollar, die er bereit ist für ein Auto zu bezahlen, dessen genaue Beschaffenheit er beim Kauf nicht beurteilen kann. Die Folge der Preisvorstellung des Prinzipals ist, das sich alle Agenten mit gute Autos vom Markt zurück ziehen, da der Durchschnittspreis nicht ihren Erwartungen entspricht. Andererseits freuen sich die Agenten die Zitronen verkaufen, sie können ihre Produkte weit über dem tatsächlichen Wert verkaufen. Der Prinzipal dagegen hat keine Chance mehr an ein gutes Auto zu kommen, obwohl er eigentlich bereit gewesen wäre mehr Geld für ein gutes Auto auszugeben.

Es gibt zwei Möglichkeiten um die eben beschriebene Informationsasymmetrien abzubauen. Durch Screening versucht der Kunde als schlechter informierter Seite, das Auto durch unabhängige Sachverständige wie die Dekra oder den TÜV begutachten zu lassen. Beim Signaling versucht der Händler als besser informierte Seite durch saubere Scheckheft pflege und Probefahrten, dem Käufer die Qualität des Autos nachzuweisen.

Bei diesem streng abgegrenzten Markt von gut und schlecht, sind die guten Autos nach dem „ersten Durchlauf" quasi nicht mehr am Markt vertreten, da sie von niemandem gekauft werden. Bei differenzierten Märkten, wie sie im realen Leben vorkommen, dauert es einige Zeit und mehrere Durchläufe bis nur noch die Lemons übrig bleiben.

3.3.3 'Lemons' in der IT-Sicherheit?

„Clearly they write it as well as they can, and then test it as much as they can afford. Yet, it always ships with bugs in it, and in time those bugs are exploited [...]"(Grigg 2005)

Die " The Market for Lemons " Problematik soll im folgenden auf ein bereits bekanntes und sehr umstrittenes Beispiel aus der IT-Sicherheit übertragen werden.

Das meist benutzte Client-Betriebssystem der Welt ist Microsoft Windows. Gerade das Betriebssystem sollte als Fundament für alle anderen Anwendungen eigentlich eine stabile und sichere Plattform bieten.

Auch Microsoft selbst müsste eigentlich ein besonderes Interesse daran haben, seine Kunden zu befriedigen und besonders sichere Software auf den Markt zu bringen. Die Realität sieht anders aus: Beinahe täglich werden neue Meldungen über neue Sicherheitslöcher von den Medien verbreitet, diese erreichen häufig kritische Ausmaße. Diese negative Presse kann selbst für ein selbst für einen quasi-Monopolisten wie Microsoft nicht von Interesse sein, so möchte man meinen. Warum also ist es so schwer sichere Software zu schreiben?

Die These, das ein derartiges Verhalten aus Sicht von Microsoft ökonomisch durchaus sinnvoll ist, mag auf den ersten Blick überraschen. Dafür gibt es zwei mögliche Begründungen. Die erst, von Microsoft Gegnern gern zitierte Grund ist, dass Microsoft durch dieses Verhalten immer einen Grund hat, die Kunden zum Umstieg auf die neueste Windows Version zu überzeugen. Diese Begründung ist wissenschaftlich und auch logisch von keiner großen Bedeutung, schließlich dürften die meisten Kunden mittlerweile verstanden haben das ein neues Betriebssystem nicht zwingend mit mehr Sicherheit verbunden ist, im Gegenteil weisen neu eingeführte Produkte häufig im besonderen Masse Geburtsfehler auf, die erst in den folgenden

Versionen behoben werden. Was aber wenn hinter diesem Vorgehen ein ökonomisches Prinzip steckt? Wie würde ein „Market for unsafe Operation Systems" aussehen?

Zunächst zu den Akteuren. Der Prinzipal will in diesem Fall ein sicheres Betriebssystem besitzen und delegiert den Auftrag an einen Agenten. Der Kunde ist also der Prinzipal und der Agent wäre Microsoft bzw. ein beliebig anderes Software Unternehmen. Die Unternehmen wissen, dass sie für absolut sichere Software, mindestens 1000 Dollar pro verkauften Stück verlangen können. Diese Entwicklungskosten entstehen vorrangig durch ein so genanntes ex post Verfahren bei dem jede Zeile Code geprüft und evaluiert werden muss.

Für ein System gleichen Funktionsumfangs, jedoch ohne Evaluierung und dementsprechend unsicherer, veranschlagt das Unternehmen 200 Dollar. Der Kunde würde bei vollständiger Informationssymmetrie für ein wirklich sicheres Betriebssystem 1000 Dollar zahlen, für ein weniger sicheres Programm liegt seine Zahlungsbereitschaft bei 200 Dollar. Der Hersteller ist daran interessiert seinen persönlichen Nutzen zu optimieren. Dem Kunde wiederum fehlen die nötigen Informationen um zu entscheiden, ob die Software wirklich sicher ist oder nicht. Der Hersteller jedoch weiß relative genau wie sicher bzw. unsicher sein Produkt ist. Der Kunde wird versuchen einen durchschnittlichen Preis von 600 Dollar zu zahlen, der er nicht weiß sein kann eine wirklich sichere Software zu bekommen. Das Endergebnis das aus den jeweiligen Versuchen der Akteure den persönlichen Nutzen zu maximieren entsteht, ist identische mit dem Beispiel der Karibu Jäger. Die teureren und sicheren Betriebssysteme verschwinden vom Markt, da der Kunde nur noch 600 Dollar statt der erforderlichen 1000 Dollar zahlt. Die Hersteller produzieren immer billigere und unsichere Softwaresysteme, da sie nur so ihren Nutzen maximieren können.

Als Beschleuniger stellt sich ein falsch verstandener Innovationsdruck heraus, der die Softwarehersteller zu immer neuen unerprobten, unsicheren und „evaluierbaren" Funktionen zwingt, welche das System immer komplexer und fehleranfälliger machen.

3.3.4 Moral Hazard

Moral Hazard Probleme entstehen zwischen Prinzipal und Agenten nach dem Vertragsschluss. Die Problematik besteht darin, das der Prinzipal die unerwünschte, opportunistische Handlungen des Agenten nachdem der Vertrag geschlossen ist, nur schwer verhindern kann. Gerade wenn die Beziehung zwischen Prinzipal und Agenten zeitlich begrenzt ist, hat Letzterer unter Umständen keinen Anreiz, sein vollständiges Leistungspotential abzurufen.

Auch dieses Problem kannte schon der Anführer der Karibu Jäger. Die Gruppe, die er zusammen gestellt hat, ist inzwischen so groß, dass er nicht mehr jeden Einzelnen kontrollieren kann, ob er auch wirklich sein Bestes gibt. Da Karibus immer in kleinen Teams zu je drei Leuten gejagt werden, bilden sich nach und nach bestimmt Teams heraus. Der überwiegende Teil der Teams ist recht erfolgreich bei der Jagd. Da jedes Team am Ende der Jagd den gleichen Anteil an der Beute bekommt, kommt es wieder zu dem Problem, dass die Teams ihren Nutzten maximieren können, in dem sie ihre Mitarbeit verringern. Sie begrenzen den Ressourceneinsatz und erhalten dennoch den gleichen Anteil am Gesamtergebnis.

Für den Prinzipal ist es nur schwer möglich, das Moral Hazard Problem zu lösen, da er den Einsatz, den eine Person zu erbringen bereit ist, erst nach Vertragsschluss beobachten kann.

3.3.5 Moral Hazard und das mobiles Internet

„[E]xisting security protocols assume that nothing moves. The allowed assumption is that the security problem is just about solved for things that don't move."
(Needham 2002)

In vielen Unternehmen wird versucht jeden Mitarbeiter möglichst Effektiv einzusetzen. Dazu gehört auch unproduktive Zeitnutzung, wie zum Beispiel auf Dienstreisen, so kurz wie möglich zu gestalten. Auch die ständige Erreichbarkeit ist für viele Firmen eine wichtige Grundanforderung die sie an ihre Mitarbeiter stellen. Aus diesem Grund hat der Trend zum mobilen Internet bzw. mobiles Emailing in den letzten Jahren einen regelrechten Boom erlebt. Mitarbeiter können oft zu jeder Tag- und Nachtzeit überall auf der Welt mit Informationen und neuen Aufgaben versorgt werden. So kommt es zu einer Minimierung der ungenutzte Arbeitszeit. Gerade der Trend zur zunehmenden Mobilität und weltweiten Vernetzung aber ist es, der für die Unternehmen auch ein erhebliches Sicherheitsrisiko darstellt. Das Unternehmen hat vielfach keinerlei Kontrollmöglichkeiten, in welchem Umfeld der Mitarbeiter die mobile Technik einsetzt. Um die Gefährdung in Grenzen zu halten, werden häufig Richtlinien erlassen, die dem Mitarbeiter unter bestimmten sicherheitsbedenklichen Situationen untersagen das Internet zu nutzen. Inwiefern diese Regelungen eingehalten werden, ist indes für das Unternehmen kaum kontrollierbar.

Oft sind sich die Arbeitnehmer durchaus bewusst, dass sie in einer kritischen Situation sind und das die Quelle die sie im Begriff sind zu öffnen nicht unbedingt vertrauensvoll ist. Aufgrund der fehlenden Kontrollmöglichkeiten, über die sich auch der Agent völlig im klaren ist, sinkt jedoch die Hemmschwelle sicherheitsgefährdendes Verhalten zu unterlassen. Der Agent wird in diesem Fall versuchen, den Prinzipal

nicht über die, vielleicht sogar ausschließlich initiierte Nutzung, zu informieren. Da der Prinzipal (Unternehmen) von den Externalitäten keine Kenntnis hat, kann er auch nicht beurteilen, ob es die Situation erforderlich machte, den Laptop zu benutzen und ob die Internetverbindung wirklich notwendig war. Erneut ist eine Informationsasymmetrie und ein Interessenkonflikt zwischen Prinzipal und Agenten beobachtbar. Der Prinzipal will sein Unternehmensnetzwerk frei von Viren und Würmern halten, der Agent dagegen möchte sich auch eventuell kritische Dokumente ansehen.

Für die Unternehmen ist es wie schon beschrieben kaum möglich, das Verhalten seiner Angestellten zu kontrollieren. Ist dies schon im Büroalltag nur mit besonderen Anstrengungen zu bewältigen, so scheitert eine Überwachung der mobil arbeitenden Angestellten spätestens an den exorbitanten Kosten.

4. Lösungsmöglichkeiten der Prinzipal-Agenten-Theorie

Die Prinzipal-Agenten Theorie dreht sich um die Frage wie verhindert werden kann, dass sich der Mitarbeiter dem Unternehmen gegenüber opportunistisch verhält. Die Lösungsansätze bewegen sich dabei zwischen zwei Polen: Auf der einen Seite steht der Aufbau von Schutzmechanismen mit dem Ziel Kontrolle über den Mitarbeiter und seine Handlungen zu erlangen (zum Beispiel durch den Aufbau von bürokratischer Kontrolle). Auf der anderen Seite kann versucht werden, die Diskrepanz zwischen den Interessen des Prinzipals und denen des Agenten zu verringern. Die beiden Pole stellen dabei Extreme dar, die im heutigen Wirtschaftsleben in dieser Reinform nicht anzutreffen sind. Ein Unternehmen, welches jeden Schritt seiner Mitarbeiter überwacht und keinerlei Handlungsfreiräume zulässt, verliert die Flexibilität auf Veränderungen des Marktes schnell zu reagieren. Die ständige Kontrolle

führt zu erheblichen Transaktionskosten und dürfte auf Mitarbeiterebene erheblichen Widerstand erzeugen. Es dürfte zudem schwer sein, die Regeln in einer Weise aufzustellen, in der sie nicht unterwandert werden können, rein Gesellschaftlich betrachtet bestätigt sich diese Annahme: Gerade Länder mit strengen Regeln und diktatorischen Regierungsformen (wie z.B. Burma und Libyen) haben gleichzeitig mit einem hohen Maß an Korruption zu kämpfen (Patrik, bitte Quelle einfügen!!!).

Andererseits dürfte auch das andere Extrem, eine Homogenisierung der Agenten- und Prinzipalsinteressen, kaum realistisch sein. Eine Organisationsform, bei der auf jegliche Kontrollmechanismen verzichtet wird dürfte langfristig nicht lebensfähig sein. Der Begriff des „blinden Vertrauens" ist nicht umsonst im Volksmund mit negativen Assoziationen besetzt und Fälle wie Worldcom oder Enron zeigen auf, welche Folgen durch ein zu geringes Maß an Kontrolle entstehen können.

4.1 Motivation durch monetäre Anreize

Der Trend, den fixen Gehaltsanteil durch einen variablen Gehaltsanteil zu ersetzen, hat in den letzten Jahrzehnten ständig an Bedeutung hinzu gewonnen. Bestehende Systeme wurden durch differenzierte Prämiensysteme für individuelle Leistungen, oder Leistungen die eine Gruppe erbringt, ergänzt (Kappel 1989, S. 44). Die Formen dieser Prämiensysteme können vielfältig sein, und erstrecken sich von Geld und Prestige (z.B. die Auszeichnung „Mitarbeiter des Monats") bis hin zu zusätzlichen Urlaubstagen (Kohn 1994, S. 15).

In den USA ist der Anteil der Unternehmen, die ihren Mitarbeitern mindestens 20% des Lohns durch solche Anreizsysteme zukommen lassen von 38 Prozent im Jahre 1989 auf 50 Prozent im Jahre 1993 angestiegen (Pfeiffer 1998 S. 47). Doch diese so genannten Incentive Programme treffen keinesfalls auf uneingeschränkte Begeisterung.

Umfragen innerhalb der Firmen ergaben, dass 47 Prozent der Mitarbeiter dieses System der Belohnungen weder für fair, noch für vernünftig halten (Pfeiffer 1998, S. 47). Zudem ist zu beobachten, das ein Incentive Programm mit großem Aufwand verbunden ist, viel Zeit und Geld muss investiert werden, ohne sich dabei über das Ergebnis sicher sein zu können (Pfeiffer 1998, S. 47).

Der Nutzen solcher Entlohnungssysteme ist durchaus umstritten. So wurden in einer Studie junge Frauen aufgefordert, Kleinkindern festgelegte Spiele beizubringen. Ein Teil der Frauen wurde im Erfolgsfall eine Belohnung in Form von kostenlosen Kinokarten versprochen, der andere Teil der Frauen bekam keine Belohnung. Das überraschende Ergebnis war, das die Gruppe der mit Anreizen motivierten Frauen mehr Zeit für die Erfüllung der Aufgabe brauchte, zudem zeigten die Frauen ein höheres Unzufriedenheitslevel. Auch die Aufgabenerledigung war weniger erfolgreich, als dies bei der Vergleichsgruppe der Fall war: Die Frauen hatten es nicht geschafft allen Kindern die Spielregeln nachhaltig zu vermitteln (o.V. 1990, S. 10).

Im Zuge der Prinzipal-Agenten Theorie können monetäre Anreizsysteme, die von Seiten des Prinzipals initiiert werden, als eine Art Steuerungswerkzeug dargestellt werden. Ziel ist es, den Agenten von opportunistischen Handlungen, die einzig in seinem Interesse, nicht aber im Interesse des Unternehmens sind, abzuhalten. Dieser Grundgedanke kann auch auf das Problem der IT-Security angewendet werden. Mitarbeiter, die sich entsprechend „sicher" verhalten, könnten durch ein solches System belohnt werden, was wiederum Anreize für entsprechendes Verhalten erzeugen würde.

4.1.1 Historische Entwicklung von Incentive Systemen und deren zugrunde liegendes Menschenbild

Die Idee der Incentive Systeme stammt historisch betrachtet aus der Beobachtung von Tieren. Hier fand man heraus, dass Tiere durch entsprechende Belohnungen zu einem bestimmten Verhalten erzogen werden konnten, diese Erkenntnis wurde sodann auf die Theorie menschlichen Verhaltens übertragen (Kohn 1994, S. 15).
Um dies nachzuvollziehen, ist es wichtig das Menschenbild, welches sich hinter dieser Theorie verbirgt, zu erklären. Im Mittelpunkt steht hier der Homo Ökonomikus, ein Wesen, welches all seine Entscheidungen auf rationalen Überlegungen begründet, und jeweils auf Basis der besten erhältlichen Information handelt (Pfeiffer 1998, S. 44). Der Homo Ökonomikus verfolgt als einziges Ziel die Maximierung des eigenen Nutzens, Kriterium ob eine Stelle angenommen wird und in welcher Weise sich das Individuum für das Unternehmen engagiert ist abhängig von der finanziellen Gegenleistung, die ihm das Unternehmen dafür bietet (Pfeiffer 1998, S. 44). Entspricht die Bezahlung nicht der erwarteten Leistung, so wird das Individuum seine Leistung und Anstrengung so weit herunter fahren, bis sich zwischen Leistung und Entlohnung ein Gleichgewicht ergibt (Pfeiffer 1998, S. 44). Führt man diese Überlegung weiter, so gilt die Arbeit an sich in diesem System als harte und gräuliche Angelegenheit, zu der Menschen nur durch eine Kombination aus Belohnung und Bestrafung bewegt werden können (Pfeiffer 1998, S. 44).

4.1.2 Warum Incentive Systeme scheitern

Untersucht man Incentive Programme empirisch, so werden interessante Erkenntnisse ans Tageslicht befördert. Unter anderem fand man heraus, das Belohnungen tatsächlich eine Leistungssteigerung bewirken können. Die ernüchternde Erkenntnis war jedoch, das die Bereitschaft zu mehr Leistung schnell wieder abnimmt. Vor allem wenn

es darum geht Verhaltensveränderungen, zu bewirken, sind Belohnungen, wie auch Bestrafungen als unwirksam einzuschätzen (Pfeiffer 1998, 44).
Warum Belohnungssysteme in der Praxis scheitern, soll im folgenden differenzierter Betrachtet werden

4.1.2.1 Bezahlung wirkt nicht motivierend

Diese These mag im ersten Augenblick verwirren. Ist es doch gerade Geld, was eine allgegenwärtige Rolle in unserer Gesellschaft zu spielen scheint. Wir kaufen Güter und Dienstleistungen für Geld uns selbst in der täglichen Presse-Berichterstattung dreht sich alles ums Thema Geld. Mal ist es die Umsatzsteuer, die vor der Erhöhung steht um die Kassen des Finanzministers zu füllen, mal sind es die Klinikärzte, die Monatelang für ihre Forderung nach einer 30 Prozentigen Gehaltserhöhung auf die Straße gehen. Stellt man Menschen jedoch die Frage was sie beschäftigt, was für sie im Job wichtig ist, so kommt die Bezahlung immer erst am fünfter oder sechster Stelle (Kohn 1994, S. 18). Damit soll keineswegs behauptet werden, das Menschen nicht für Geld arbeiten, doch es sind schlussendlich andere Faktoren wie Sinn oder Spaß die als wahre Gründe für die Arbeit genannt werden (Pfeiffer 1998, S. 43). Geld wirkt als eine Art Hygienefaktor, es muss im ausreichenden Maße zur Verfügung stehen, macht per se aber nicht glücklich. Rutscht das Gehalt unter das als gerecht empfundene Maß, so hat dies jedoch durchaus Auswirkungen. Wenn ein Individuum nur die Hälfte des sonst üblichen Lohns verdient, wird dies sicherlich negative Auswirkungen auf die Arbeitsmoral haben, verdoppelt man den Lohn jedoch, so muss sich die Arbeitsleistung aber nicht unbedingt auch verbessern (Kohn 1994, S. 18).

4.1.2.2 Belohnungen wirken wie Strafen

Sowohl Belohnungen als auch Bestrafungen sind an bestimmte Bedingungen geknüpft, bei Belohnungen sind diese Bedingungen positiv formuliert, als „du sollst" Aussagen, bei Bestrafungen negativ, als „du sollst nicht", es handelt sich um zwei Seiten der selben Medaille (Kohn 1994, S. 18). Die Mitarbeiter sind sich dabei durchaus bewusst, dass sie durch Belohnung von außen gesteuert werden. Eben dieses Bewusstsein durch die Organisation und durch den Chef manipuliert zu werden weil man ihnen nicht vertraut, ist es was die Mitarbeiter die Belohnung als Bestrafung erleben lässt (Kohn 1994, S. 18).

Es ist ein Zeichen von organisationalem Misstrauen, solche Belohnungssysteme entstehen zu lassen. Ihnen liegt die Annahme zugrunde, das es im Unternehmen ein Motivationsgefälle gibt. Gerade den Menschen, die eher am unteren Ende der Befehlskette stehen wird dabei unterstellt, das sie eher zu wenig leisten, gerade diese Gruppe der „noch-nicht mobilisierten" soll durch Belohnung angetrieben werden (Sprenger 1994, S. 9).

Die Belohnung kann jedoch auch durch einen anderen Mechanismus zur Bestrafung werden. Wenn der Mitarbeiter schon mit dieser gerechnet hat, sie ihm aber aus welchen Gründen auch immer verweigert wird, wird dies vom Betroffenen wie eine Bestrafung wahrgenommen (Kohn 1994, S. 18).

4.1.2.3 Belohnungen untergraben das Interesse an der Arbeit

Menschen können aus verschiedenen Motiven handeln, diese Motive lassen sich in zwei Gruppen, die Gruppe der intrinsischen- und der extrinsischen Motivation einordnen. Während die intrinsische Motivation von der Person selbst, also etwa aus Freude an der Sache kommt, wird extrinsische Motivation, zum Beispiel die Zahlung von Prämienboni für ein bestimmtes Verhalten, von außen erzeugt. Es gilt als erwiesen, das Motivation von außen nie die Motivation, welche aus dem Inneren der

Seele kommt, erreichen kann. Menschen die außergewöhnliches vollbringen tun dies in der Regel nicht wegen der monatlichen Überweisung auf ihr Gehaltskonto, sondern wegen der inneren Erfüllung die sie durch die Aufgabe erlangen (Kohn 1994, S. 19).

Zahlt ein Unternehmen seinen Beschäftigten für ein bestimmtes Verhalten einen Bonus, so wird damit auch immer unterschwellig eine Botschaft kommuniziert. Der Sender versucht durch die Bonuszahlung das Verhalten des Empfängers zu steuern (Kohn 1994, S. 19). Hier kann schnell der Gedanke aufkommen, das die Arbeit - wenn derartige Bestechungen notwendig sind - wohl etwas Minderwertiges ist, etwas was der Mitarbeiter ohne Bestechung nicht tun würde (Kohn 1994, S. 19).

Je mehr ein Chef also betont, welche großartigen Verdienst-möglichkeiten der Arbeitnehmer durch gute Arbeit im Unternehmen hat, umso weniger wird sich diese Person für die Arbeit an sich interessieren (Kohn 1994, S. 19). In diesem Falle verschiebt sich der Fokus vom Interesse an der Arbeit als solches auf das Interesse an der Belohnung (Sprenger 1994, S. 19). Mitarbeiter werden in Zukunft bei jeder Tätigkeit nach äußeren Anreizen fragen (Kohn 1994, S. 21), was bei den Chefs wiederum die Überzeugung auslöst, nur noch durch Anreize motivieren zu können, ein Teufelskreis setzt sich fort…

4.1.2.4 Belohnung vergiftet das Klima

Häufig ist nach der Einführung eines Incentive Programms eine Veränderung des Betriebsklimas beobachtbar. War dies vorher durch Kooperation und gegenseitige Sympathien gekennzeichnet, entwickeln sich im Zuge der Konkurrenz um Belohnungen, Anerkennungen oder Rangstellungen häufig ein Klima des Misstrauens, des „den anderen ausstechen" wollens. Im Zuge dieser Entwicklung kommt es nicht selten zur Zerstörung von guten Beziehungen, diese fallen der Jagd nach dem

Geldtopf zum Opfer, jeder denkt nur noch an seinen eigenen Vorteil, statt das System für alle Beteiligten zu verbessern (Sprenger 1994, S. 10).

Andererseits ist häufig auch eine Unterwanderung des Systems zu beobachten. So ist es durchaus anzutreffen, das etwa bei der Prämierung von Verbesserungsvorschlägen, diese bereichsübergreifend ausgetauscht werden um möglichst viel Prämien kassieren zu können (Sprenger 1994, S. 12). Zum anderen schrecken einige Mitarbeiter selbst vor Manipulationen ihrer Tätigkeit, häufig sogar mit unmoralischen- oder sogar illegalen Mitteln, nicht zurück (Kohn 1994, S. 20).

Auch die Beziehung zwischen Chef und Mitarbeiter kann durch die Einführung eines Incentive Systems Schaden nehmen. Dem strafenden Chef, der Belohnungszahlungen verweigert, dürften keine all zu großen Sympathien entgegen schlagen (Kohn 1994, S. 19). Wer dann doch eine Zurückweisung erfahren hat ist gekränkt und wird sich rächen, jeden Tag ein bisschen, mal geht dort eine Unterlage verloren, mal wird da eine Deadline vergessen, das alles natürlich vollkommen unbeabsichtigt (Sprenger 1994, S. 13).

Damit sie erst gar nicht in diese Situation kommen, greifen die Mitarbeiter dann zu Tricks, Schwierigkeiten bei der Arbeit werden vor dem Vorgesetzten versteckt, jeder versucht sich selbst als ungeheuer kompetent zu verkaufen (Kohn 1994, S.19).

4.1.2.5 Belohnung missachtet Ursache und Wirkung

In einer dynamischen Wirtschaftsentwicklung sind Zielvereinbarungen oft schon einen Tag nach Verfassung nicht mehr das Papier wert, auf dem sie geschrieben sind, zu schnell Ändern sich die Rahmenbedingungen, oft genug ohne das das Unternehmen Einfluss darauf nehmen kann. Probleme die im täglichen Handeln der Wirtschaftsakteure auftreten verlangen meist differenzierte Lösungen,

Bonuszahlungen werden dann häufig als eine Allzweckwaffe eingesetzt, sie sollen als Substitut für die Dinge, die der Mitarbeiter wirklich braucht – zum Beispiel soziale Unterstützung oder Spielraum zur Selbstverwirklichung - herhalten.

4.1.2.6 Belohnungen schwächen die Risikofreude

Belohnungen sind an bestimmte Verhaltensweisen geknüpft, die exant von den beiden Vertragspartnern vereinbart werden müssen. Wie in dem vorhergehenden Abschnitt bereits erläutert, verändern sich die Rahmenbedingungen im Zeitverlauf jedoch teilweise unvorhersehbar. Auf diese Weise können sich neben Schwierigkeiten auch neue Chancen für das Unternehmen bieten, Chancen die in den Zielvereinbarungen nicht festgehalten wurde, da sie zu diesem Zeitpunkt den Akteuren nicht bekannt waren. Arbeitet der Mitarbeiter nun zielstrebig auf das Erreichen seiner Ziele hin, so ist es für ihn nicht sinnvoll diese neuen Herausforderungen anzunehmen, letztendlich könnte er damit das erreichen der vereinbarten Ziele verfehlen, er wird also versuchen jegliche Herausforderung zu minimieren (Kohn 1994, S. 20).

4.1.3 IT-Security durch monetäre Anreize

Anhand der soweit geschilderten Erkenntnisse kann bezweifelt werden, dass sich der Einsatz von Belohnungssystemen für die Verbesserung der IT-Security eignet. Gerade hier sind es ja nachhaltige Verhaltensänderungen und nicht kurzfristige Leistungssteigerungen, die zu bewirken sind. In diesem Kontext stellt sich zudem die Frage, wie ein solches System rein praktisch aufgebaut werden sollte. Die mangelnde Beachtung von Sicherheitsstandards lässt sich kaum prüfen, und kommt wenn überhaupt erst im Fall eines Security-Zwischenfalls ans Tageslicht. Es dürfte also schwierig sein einen geeigneten Maßstab für die Bezahlung von Prämien und für die Einhaltung von Sicherheitsregeln zu finden. Es ist zudem sicherlich nicht sonderlich glaubwürdig, ständig von

der Wichtigkeit aller Mitarbeiter für den Unternehmenserfolg zu sprechen, und gleichzeitig starke Differenzierungen innerhalb des Vergütungsgefüges durchzuführen (Pfeiffer 1998, S. 49).
Zwar soll hier nicht völlig ausgeschlossen werden, dass die Bezahlung von Boni durchaus eine höheres Sicherheitsbewusstsein bei den Mitarbeiter erzeugen kann, allerdings ist angesichts der hohen Kosten und der desaströsen Nebenwirkungen zu bezweifeln, das dies mit einem halbwegs vernünftigen Kosten-Nutzen Kalkül verwirklichbar ist.

4.2 Führung durch Vertrauen

Beckert definiert Vertrauen als „…Erwartung, das kooperatives Handeln nicht ausgebeutet wird" (Beckert 1998, S. 58). Nebst der unternehmerischen Steuerung durch Macht oder Befehl, bietet sich Vertrauen als drittes Steuerungselement an.
Bei der Betrachtung der Realität scheint eher das Gegenteil von Vertrauen, das Misstrauen, Einzug gehalten zu haben. Misstrauen lässt sich als „The unwillingness of individuals to take kooperative action that increases their vulnerability" definieren (Scott 1980, S. 158). Zeichen des Misstrauens sind allgegenwärtig, sie reichen von Zeiterfassungscomputern über Geheimnistuerei bezüglich der Gehälter bis zur „Können Sie mir das schriftlich geben" Mentalität in vielen Unternehmen (Sprenger 2005, S. 19). Es haben sich, so scheint es, zwei Lager gebildet, die sich unversöhnlich gegenüber stehen, auf der einen Seite die Arbeitgeber, die ständig die Wichtigkeit des Mitarbeiters zu betonen suchen, auf der anderen Seite die Angestellten, die hilflos miterleben, wie jede Restrukturierungsrunde zu ihrem Nachteil wirkt. Engagement für die Firma, zum Teil jahrzehntelang, scheint in den Zeiten der Globalisierung nichts mehr wert zu sein, die Mitarbeiter sehen sich als ständige Verlierer, eine Atmosphäre in der Vertrauen nicht entstehen kann (Sprenger 2005, S. 30). Ein weiterer Beleg für diese Frontenbildung ist die betriebliche Mitbestimmung, wie

selbstverständlich wird hier angenommen, das nur ein Betriebsrat aus dem eigenen Lager die Interessen der Arbeitnehmerschaft erfolgreich vertreten kann (Sprenger 2005, S. 30). Folge des gegenseitigen Misstrauens ist, dass beide Seiten beginnen Sicherungsmaßnahmen aufzubauen. Dabei werden häufig die Kosten, die mit solchen Sicherungsmaßnahmen verbunden sind, unterschätzt. Misstrauen, und die damit verbundenen Gegenmaßnahmen führen zum Aufbau von bürokratischen Strukturen im Unternehmen, dem keine geschaffenen Werte gegenüberstehen (Sprenger 2005, S. 43). Bei genauer Betrachtung ist sogar festzustellen, das die mit Monitoring-Aktivitäten und vertraglichen Sicherungsmaßnahmen verbundenen Kosten all zu oft die Verluste die ein Unternehmen aufgrund von Mitarbeiterbetrug erleidet, bei weitem übersteigen (Sprenger 2005, S. 45). Auf Seiten der Mitarbeiter führen die Zeichen des Misstraut werdens zu Demotivation, Angst und abnehmender Loyalität, durch die ständige Umstrukturierung und den Abbau von Arbeitsplätzen werden eingespielte Teams auseinander gerissen, organisch gewachsene Beziehungsstrukturen werden zerstört und am Schluss ist es sogar der Kunde, der durch den Verlust vertrauter Ansprechpartner unter den Umwälzungen zu leiden hat (Müller 1998, S. 237).

Aber nicht nur aus Kostengesichtspunkten scheint ein Umdenken in Richtung mehr Vertrauen sinnvoll. Im Rahmen der Globalisierung haben sich die Strukturen von Unternehmen grundlegend gewandelt. Es ist das Zeitalter der Internationalisierung, der Heimarbeit, der Netzwerkorganisation und des New Public-Managements, um nur einige Schlagwörter zu nennen (Sprenger 2005, S. 26). Gleichzeitig nehmen die Aufgaben der Mitarbeiter an Komplexität tendenziell zu, Menschen arbeiten Länder- und Kulturen übergreifend in virtuellen Netzwerken zusammen, die Vorgesetzten verstehen die Aufgaben ihrer Mitarbeiter häufig aufgrund der Komplexität nicht mehr. Wie als mit Vertrauen lässt sich unter diesen Umständen Leistung koordinieren? (Sprenger 2005, S.

52). Die Verbreitung von virtuellen Arbeitsgemeinschaften, so genannten Communities of Practice ist besonders bei den Global Playern längst zum Alltag geworden, Daimler-Chrysler verfügt momentan über 140 solcher Gemeinschaften, bei Siemens sind es nach letzten Zählungen sogar 345 (Sprenger 2005, S. 53).

Der Sinn von Befehlsketten und Kontrolleinrichtungen kann auch bezüglich seiner Wirksamkeit kritisch beurteilt werden. Es gibt keine Überwachung die hermetisch genug ist, keine Befehlskette die zu hundert Prozent geschlossen ist und keinen Vertrag in dem sich wirklich jedes Detail regeln ließe. Auf ein gewisses Maß an Vertrauen kann also niemals vollkommen verzichtet werden (Sprenger 2005, S. 96).

Aber auch in der Welt der Konsumenten ist Vertrauen zu einem wichtigen Faktor geworden. Beim Kauf von Produkten handelt es sich häufig um so genannte Vertrauensgüter, die Eigenschaften solcher Gütern sind weder vor, noch nach dem Kauf durch den Käufer überprüfbar, ob das Gemüse tatsächlich aus biologischen Anbau stammt, oder ob der Computer tatsächlich über einen Intel Chip verfügt ist für den Konsument nicht, oder nur mit erheblichen Kosten überprüfbar. In einer solchen Vertrauenswelt sind es vor allem Marken, die den Menschen Sicherheit geben können. Marken signalisieren Vertrauenswürdigkeit und geben ein Leistungsversprechen ab, sie dienen somit als eine Art Navigationshilfe und reduzieren die Komplexität alltäglicher Entscheidungen (Sprenger 2005, S. 33). In der normalen Alltagswelt ist Vertrauen ein wichtiges Element, obwohl es vielleicht nicht in jedem Augenblick bewusst wahrgenommen wird. Man vertrauen darauf das der Fahrstuhl nicht abstürzt, der Motor des Autos anspringt, oder das es hell wird, wenn der Lichtschalter umgelegt wird, um nur einige als völlig selbstverständlich wahrgenommene Beispiele zu nennen (Sprenger 2005, S. 57).

4.2.1 Der Wert von Vertrauen

Der Wert von Vertrauen lässt sich nicht in Euro und Cent wieder geben, zu schwierig scheint die Messung. Allerdings gibt es verschiedene Studien, die die Auswirkungen, die Vertrauen hat, untersuchen. Da wäre zum einen die Beziehung zwischen dem Top-Management und den Mitarbeitern: Untersuchungen ergeben hier einen signifikanten Zusammenhang zwischen dem Vertrauen, welches die Mitarbeiter dem Management entgegenbringen, und mit der Einstellung, die bei den Mitarbeitern entstehen wenn dieses Management Fusions-entscheidungen bekannt gibt (Scott 1980, S. 159). Scott weist zudem nach das Vertrauen einen entscheidenden Einfluss auf den Erfolg von Management by Objectives Programmen hat, verallgemeinernd kann man daraus schließen, das Vertrauen somit die Basis für die erfolgreiche Implementierung von Managemententscheidungen ist (Scott 1980, S. 171).

Auf der Mitarbeiterebene scheint Vertrauen ebenfalls eine wichtige Rolle einzunehmen. Gerade in Zeiten kurzfristiger und mobiler Zusammenarbeit steigt der Bedarf an Vertrauen stark an, in dieser Situation ist es für den Einzelnen nicht möglich sich anderweitig abzusichern (Sprenger, 2005, S. 64). Dies mag vor allem deshalb zunächst ungewohnt sein, da mit der Person, der vertraut werden sollen oft keine persönlichen Erfahrungen geteilt werden (Sprenger 2005, S. 64).

Aber weshalb ist Vertrauen zwischen den Mitarbeitern wichtig? Vertrauen fördert zum einen die effiziente und schnelle Zusammenarbeit, diese ist nur gewährleistet, solange sich die Individuen gegenseitig vertrauen (Sprenger 2005, S. 148). Symmetrische Interaktionsmuster können am ehesten entstehen, wenn zwischen den beteiligten Personen ein Klima der wechselseitigen Sympathie und des Vertrauens herrscht (Müller 1998, S. 244). Herrscht

in einem Unternehmen eine Kultur des Vertrauens, so ergeben sich Kreislaufeffekte. Vertrauen führt zu Kooperationsbereitschaft, Kooperationsbereitschaft führt zu Vertrauenszuwachs, was wiederum positive Verstärkungseffekte auf die Vertrauenskultur ausübt (Müller 1998, S. 244).

Je stabiler das Beziehungsnetz innerhalb der Organisation ist, umso mehr Interaktion findet zwischen den Mitgliedern statt. Solche Netzwerke erleichtern den Austausch und die Kombination von Wissen, die Zugangsbarrieren zu den Wissensquellen verringern sich (Müller 1998, S. 243). Zusammenfassend lässt sich also sagen, das ein hohes Maß an Vertrauen mit effizienten Gruppenfunktionen, Bereitschaft wichtige Informationen zu teilen und entsprechend zu handeln, mit der Zufriedenheit der Beteiligten und mit der Organisationseffektivität insgesamt positiv korreliert ist (Scott 1980, S. 158).

4.2.2 Was Vertrauen nicht ist

Aufgrund der teilweisen Romantisierung des Vertrauensbegriffs scheint es an dieser Stelle angebracht, Formen von Vertrauen zu definieren, die in der Unternehmenswelt wenig hilfreich sind.

Vertrauen wird all zu oft von passiven Führungskräften missbraucht. Wer nicht führen kann oder will, ummäntelt die eigene Passivität gerne mit dem Begriff des Vertrauens gegenüber den Untergebenen. Dabei sollte Vertrauen nicht dafür genutzt werden, sämtliche Führungsaufgaben aufzugeben. Wie später beschrieben werden soll, bedeutet „richtiges" Vertrauen auch keinesfalls die Aufgabe von Kontrolle, es ist im Gegenteil wichtig, das Vertrauen auch immer wieder durch Ergebnisse gerechtfertigt wird (Sprenger 2005, S. 79).

Ein Fall von Missbrauch des Vertrauensbegriffs ist dann zu beobachten, wenn andere Argumente ausgehen und Vertrauen als letzter rettender Stohhalm heran gezogen wird (Sprenger 2005, S. 85f.). Wer nicht mehr überzeugen kann wirbt nur all zu gerne um Vertrauen, dabei zerstört

gerade das „Geschönte" jegliches Vertrauen in die Sache (Werner 2002, S. 62). Wenn Misstrauen eingekehrt ist, gibt es dafür meist triftige Gründe, ein einfaches „Vertrauen Sie mir" kann diese Gründe nicht beiseite wischen, es erzeugt beim Adressaten oft eher Widerstand (Sprenger 2005, S. 86). Menschen werden von anderen Menschen vor allem dann als vertrauenswürdig angesehen, wenn sie nicht offensiv darum werben (Sprenger 2005, S. 87).

4.2.3 Wie Vertrauen gefördert werden kann

Wie kann es einem Unternehmen nach all diesen positiven Ausführungen nun gelingen Vertrauen herzustellen? Wer die Frage aus dieser Perspektive angeht, hat schon verloren, bevor er überhaupt begonnen hat. Vertrauen ist etwas, was sich aktiv nicht herstellen lässt, kein aktiv aufgelegtes Programm kann das Vertrauenslevel innerhalb des Unternehmens anheben, Vertrauen stellt sich allenfalls selbst her (Werner 2002, S. 62). Menschen sind nun mal nicht steuerbar, wohl aber sind sie beeinflussbar (Sprenger 2005, S. 158), es gibt also durchaus Maßnahmen die ergriffen werden können, um die Entstehung eines Vertrauensklimas zu begünstigen.

Grundlage hierfür ist zunächst die Definition eines gemeinsamen Ziels, ein Leitbild oder eine Vision, die möglichst von allen Mitarbeitern geteilt werden sollte (Beckert 1998, S. 64). Werden Probleme als gemeinsam Anerkannt, die nur im Kollektiv zu lösen sind, so entspannt sich das Netz der Zusammenarbeit. Dies gilt jedoch nur so lange, wie das zu lösende Problem als wichtiger angesehen wird, als der persönliche Vorteile, den das Individuum aus einer „karriereorientierten Selbstoptimierung" gewinnen kann (Sprenger 2005, S. 151). Grundvoraussetzung hierfür ist auch, dass das Unternehmen seinen Angestellten auch eine langfristige Perspektive bietet (Beckert 1998, S.

64), es dürfte nicht gerade vertrauensförderlich sein, wenn die Mitarbeiter befürchten müssen schon bei der nächsten Restrukturierungswelle ihren Arbeitsplatz zu verlieren.

Ebenso wichtig sind die formalen und informalen Kontakte der Organisationsteilnehmer untereinander. Darunter fällt die Ansprechbarkeit für Meinungen und Ideen und der freundliche, versöhnliche Umgang zwischen den Individuen. Auch Führungsentscheidungen sollten möglichst auf transparentem Wege zustande kommen (Beckert 1998, S. 64).

Ein weiterer Faktor der für die Entstehung einer Vertrauenskultur wichtig ist, ist die generelle Vorhersehbarkeit, Verlässlichkeit und Transparenz durch Kommunikation. Unberechenbares Verhalten und Gerüchte wirken wie Gift auf das Vertrauen (Beckert 1998, S. 65). Auch Aufrichtigkeit und Loyalität den Mitarbeitern gegenüber ist hier wichtig (Beckert 1998, S. 65).

Im Unternehmensalltag dürften diese Handlungsempfehlungen teilweise nur schwer zu realisieren sein. Der Alltag setzt sich häufig aus dem verfolgen mehrerer miteinander in Konkurrenz stehenden Zielen, dem Treffen von Entscheidungen die genauso gut andersherum getroffen werden könnten, oder dem zufrieden geben mit suboptimalen Kompromissen zusammen (Sprenger 2005, S. 87). Auch Aufrichtigkeit an sich wirkt sich nicht per se förderlich auf das Vertrauen aus. Gerade in Konfliktgesprächen kann all zu große Offenheit, z.B. dem Mitarbeiter mal so richtig die Meinung sagen, weitaus mehr Probleme schaffen als lösen (Sprenger 2005, S. 117).

Manchmal ist es notwendig die eigene Meinung zu ändern, dieses Verhalten kann auch treffend als Lernen bezeichnet werden. Ist das Vertrauenslevel innerhalb der Organisation ohnehin niedrig, besteht hier die Gefahr, das die Mitarbeiter derartige Inkonsistenzen als Unglaubwürdigkeit auslegen (Sprenger 2005, S. 88).

Wenn nun all diese Maßnahmen eingeleitet werden, wer garantiert dann, dass es sich der Mitarbeiter nicht doch anders überlegt und das Unternehmen betrügt? Die Antwort lautet: Niemand. Und genau hier wird eines der Grundprobleme von Vertrauen sichtbar. Wird Vertrauen bestätigt, so bleibt dies in den meisten Fällen unsichtbar, es wird von den Beteiligten als Selbstverständlichkeit wahrgenommen. Tritt allerdings das Gegenteil ein, Vertrauen wird missbraucht, so ist dies sofort für jedermann sichtbar, es wird sofort erlebt (Sprenger 2005, S. 169), der Aufschrei ist laut und man nimmt sich vor nie wieder derart „naiv" zu agieren. Doch gerade hier liegt die Gefahr: Die tatsächliche Existenz von einem oder auch mehreren Vertrauensbrüchen darf nicht dazu führen, dass ab sofort generalisiertes Misstrauen im Unternehmen einkehrt (Sprenger 2005, S. 168).

Trotzdem stellt sich die Frage, wie mit einem Vertrauensbruch umzugehen ist. Zunächst muss hier unterschieden werden, ob die betroffene Person nicht leisten will, oder nicht leisten kann, nur im ersten Fall kann von einem Vertrauensbruch die Rede sein (Sprenger 2005, S. 166). Sprenger schlägt als Maßnahme gegen Vertrauensbruch einen Abbruch jeglicher Kooperation auf Zeit vor. Damit einher geht ein bewusster, entschiedener und klarer Entzug von Vertrauen. Nach einiger Zeit sollte man dem Mitarbeiter eine zweite Chance geben, und ihm erneut das Vertrauen anbieten. Betrügt der Mitarbeiter aufs Neue, so sollte man sich möglichst rasch von ihm trennen, gibt man ihm eine dritte oder vierte Chance, so vermindert man den Wert von Vertrauen (Sprenger 2005, S. 172f.).

4.2.4 Vertrauen und Kontrolle

Obwohl sich Vertrauen und Kontrolle zunächst gegenseitig auszuschließen scheinen, sollten sie im Unternehmen eher als komplementär begriffen werden.

Von Walt Disney wir erzählt, das er ein Mensch mit geradezu manischer Kontrollsucht war. Unter den Mitarbeitern war bekannt, dass er des Nachts durch die dunklen Büros ging, um das Tageswerk seiner Zeichner zu begutachten. Allerdings wich er auf der anderen Seite positiv von den damaligen Praktiken anderer Studios ab, bei Disney gab es keine Zeiterfassungssysteme und die Mitarbeiter hatten keine festgelegte Zahl von Zeichnungen pro Tag abzuliefern. Ganz im Gegenteil wurden die Zeichner von Disney ermutigt, ihren eigenen Entwürfen kritisch gegenüber zu stehen und ungeeignetes Material wegzuwerfen (Oelsnitz 2001, S. 28).

Wie dieses Beispiel zeigt, ist es wichtig Kontrolle und Vertrauen sinnvoll zu balancieren. Je nachdem wie Kontrolle gelebt wird, kann es Vertrauen nicht nur untergraben, sondern auch helfen es zu sichern (Sprenger 2005, S. 71). Aufgaben sollten differenziert betrachtet werden, es gibt Teile, die durch Vertrauen gesichert werden sollten, andere Teile können und müssen über Kontrolle überprüft werden (Sprenger 2005, S. 73). Dabei sollte Kontrolle nicht als Misstrauen verstanden werden, sondern eher als eine Art „auf dem laufenden halten", was auch durchaus von der Person des zu kontrollierten ausgehen kann (Sprenger 2005, S. 73). Es ist wichtig das Vertrauen nicht blind ist, sondern auch immer wieder durch Ergebnisse gerechtfertigt werden muss (Sprenger 2005, S. 76).

Wie gefährlich solche blindes Vertrauen sein kann, belegen nicht zuletzt die Aussagen des Rennfahrers Alain Prost, über seinen Kollegen Ayrton Senna. In einem Interview erzählte Prost, das Senna „…sich aufgrund seines Gottvertrauens für unverletzlich hielt (Sprenger 2005, S. 74). Wie hinlänglich bekannt ist, starb Senna am 1. Mai in der als besonders gefährlich bekannten Tamburello-Kurve in Imola.

Vertrauen darf also nicht heißen, auf sämtliche Regeln der Vorsicht, der Sicherheit und der Kontrolle zu verzichten, vielmehr sollte die Kontrolle immer der Aufgabe angepasst sein (Sprenger 2005, S. 75), eine gefährliche Operation am Herzen verlangt andere Sicherheitsregeln als das Kopieren eines Reports.
Kontrolle sollte dabei systematisch und unabhängig von der kontrollierten Person erfolgen. Ein gutes Gefühl oder Sympathien gegenüber dem anderen sind keine ausreichenden Gründe um auf Kontrolle völlig zu verzichten. Um ein letztes Beispiel zu erwähnen sei hier die Äußerung von H. G. Wells genannt, welcher nach einem Besuch bei Josef Stalin über eben diesen zu Protokoll gab: „ Niemals zuvor habe ich einen so offenen, fairen und ehrlichen Menschen getroffen. Niemand fürchtet sich vor ihm, und er genießt das Vertrauen aller" (Sprenger 2005, S. 83).

4.2.5 IT-Security durch Vertrauen

Die vorhergehenden Ausführungen sollten deutlich gemacht werden, das eine Lösung der Prinzipal-Agenten-Theorie durch die Schaffung einer Vertrauensorganisation zumindest theoretisch möglich ist. Eine solche Organisation in der Realität zu schaffen, dürfte da schon schwieriger sein, Vertrauen ist bekanntlich eine verletzliches Gebilde, welches durch kleine Unachtsamkeiten schnell zerstört werden kann. Fraglich ist ob Vertrauen auch als Lösungsmöglichkeit für Probleme der IT-Sicherheit gelten kann. Diese Frage ist aus Sicht der Autoren nur teilweise zu bejahen. Es wäre sicherlich naiv zu behaupten, IT-Sicherheit gegenüber der externen Umwelt durch Vertrauen zu erreichen, anders sieht es jedoch für die unternehmensinterne IT-Sicherheit aus. Hier kann es durchaus sinnvoll sein, den eigenen Mitarbeitern Vertrauen entgegen zu bringen, unter Umständen bleibt den Unternehmen auch nichts anderes übrig. Gerade wenn virtuelle Teams über große Distanzen zusammenarbeiten ist Vertrauen wichtig,

um solch virtuelle Teams zielorientiert steuern zu können (Heimburg 2002, S. 1). Gerade die Überwachung von diesen, schon fast virtuellen Mitarbeitern, dürfte praktisch kaum durchzuführen sein, weshalb Vertrauen als einziges Steuerungsinstrument in Frage kommt. Abschließend sein hier aber auch nochmals betont, das auch und gerade beim Thema IT-Sicherheit die möglichen Kosten, die durch einen Vertrauensmissbrauch entstehen können, immer mitberücksichtigt werden müssen (Sprenger 1994, S. 75). Kann durch unachtsames Verhalten der Mitarbeiter unter Umständen die Existenz der ganzen Unternehmung aufs Spiel gestellt sein, so sollte Vertrauen spätestens hier durch Kontrolle komplimentiert werden.

Die Prinzipal-Agenten Theorie betont die unterschiedlichen Interessenlagen von Prinzipal und Agenten, am Beispiel IT-Sicherheit dargestellt durch das Unternehmen und seine Angestellten. Abschließend sei hier darauf hingewiesen, das es durchaus andere Ansätze gibt, die das Verhältnis zwischen Arbeitgebern und Arbeitnehmern beschreiben. Gerade im Hinblick auf Vertrauen als Steuerungselement sei hier kurz die Theorie der selbsterfüllenden Prophezeiung angesprochen. Nach dieser Theorie hängt das Verhalten anderer Menschen direkt von unseren Erwartungen, wie sich die andere Person verhalten wird ab. Unsere Handeln orientiert sich demnach daran, was wir von der anderen Person erwarten, und eben diese Handlungen lösen beim anderen genau diese Handlungen aus, die wir von ihm erwarten. Wenn eine Person eine andere Person nicht für vertrauenswürdig hält, so wird sie die Sicherungsmaßnahmen erhöhen, und der anderen Person somit signalisieren, das ihr nicht vertraut wird, was die misstraute Person auch prompt durch entsprechende Handlungen bestätigt (Pfeiffer 1998, S. 45).

4.3 Abbau von Informationsasymmetrien

Das Vorliegen von Informationsasymmetrien kann als das zentrale Problem der Prinzipal-Agenten Theorie bezeichnet werden. Die Informationsasymmetrien können vor- oder nach dem Vertragsschluss vorliegen und werden als Adverse Selection bzw. Moral Hazard bezeichnet. Eine genaue Beschreibung erfolgte im dritten Kapitel dieser Ausarbeitung, im Folgenden sollen die Lösungsmöglichkeiten zum Abbau dieser Informationsasymmetrien beschrieben werden.

4.3.1 Signaling

Signaling bezeichnet das Verhalten von Agenten, das sich dadurch auszeichnet, dass dieser für den Prinzipal „verborgene" Informationen von sich aus preisgibt (Laffont 2002, S. 167). Der Nutzen für den Agenten muss die Kosten übersteigen. Dies bedeutet, das es für den Agenten vorteilhaft ist, diese Informationen zu übermitteln. So könnte zum Beispiel bei einer Bewerbung ein herrausragendes Zeugnis oder ein bestimmter Abschluss die Wahrscheinlichkeit einer Einstellung erhöhen bzw. das Gehalt positiv beeinflussen. Signaling geht daher immer vom Agenten und seinen individuellen Zielen aus.
Eine weitere Möglichkeit Signaling einzusetzen, ist verschiedene Agenten miteinander in Beziehung zu setzen. So zeigte Bengt Holmström das die Leistung eines Agenten einen anderen zu besserer Leistung anspornen kann, auch wenn diese in keiner direkten Beziehung zueinander stehen(Holmström 1979,S.74-91).

4.3.2 Screening

Screening geht von der Person des Prinzipals aus. Bei dieser Methode werden die Agenten auf ihre Eigenschaften geprüft. Bei der Stellenvergabe kann dies durch Einstellungstests, Assessment-Center oder Gespräche erfolgen. Ein solches Screening ist mit Suchkosten

verbunden. Zum einem beim Prinzipal, der vielleicht hunderte Bewerber überprüfen lassen muss um eine Stelle zu besetzen, zum anderen für den Agenten der den Tests ausgesetzt wird.
Die Gefahr solcher Tests liegt in ihrer proklamierte Objektivität und Genauigkeit. Ob ein Screeningverfahren wirklich die Auswahl eines geeigneten Kandidaten begünstigt ist nicht garantiert. In der Wirtschaft setzt man diese meistens in einem mehrstufigen Verfahren ein, an dessen Ende der Kandidat ausgewählt wird.
Screening ist, insbesondere bei Personalentscheidungen im heutigen Wirtschaftsleben weit verbreitet. Oft wird mit Hilfe eines solchen Verfahrens aus einer hohen Anzahl von Bewerbern der Kandidat heraus gefiltert, der für die Stellenbesetzung am geeignetsten erscheint. Man hofft dank dieser Methode die individuellen Eigenschaften der Bewerber abschätzen zu können.

4.3.3 Self Selection

Ein weiterer Ansatz zur Verringerung der Informationsasymmetrien wird als Self Selection bezeichnet. Dem Vertragspartner werden hierbei verschiedene Verträge angeboten, unter denen er selbst wählen kann. So kann er, der ja sein Risiko etwa bei einer Versicherung, selbst am besten abschätzen kann, denjenigen Vertrag wählen seinen Nutzen am besten maximiert. Durch die Wahl des Vertrags offenbart der Agent dem Prinzipal Informationen, die sich im Zeitverlauf als nützlich erweisen können. Durch die geschickte Wahl von verschiedenen Kriterien, ist es dem Prinzipal zudem möglich, Agenten die bestimmte Eigenschaften haben abzuschrecken. So werden etwa im Versicherungsbereich hohe Sicherheitsrisiken nicht oder nur zu erhöhten Konditionen abgesichert. Damit kann sich der Versicherer im vorhinein davor schützen mit den für ihn „falschen" Agenten Verträge abzuschließen.

Des weiteren besteht die Möglichkeit einen mehrstufigen Auswahlprozess durchzuführen. In diesem können mögliche Vertragspartner effizienter ausgewählt werden und zufällige, das Ergebnis verfälschende Selektionen verhindert werden. Eine solche Vorauswahl der potentiellen Vertragspartner bietet relativ einfach die Möglichkeit eine Informationsasymmetrie zu vermeiden. Im Ergebnis führt diese Wahl zu einem guten Match zwischen den Vertragspartnern, da beide Informationen austauschen. Dem Agenten erscheint die Möglichkeit der Wahl positiv, da er so Einfluss auf den Prozessverlauf nehmen kann. Durch die Bestimmung der Wahlmöglichkeiten ist es jedoch eigentlich der Prinzipal, der den Auswahlprozess modelliert und steuert (Laffont 2002, S. 369).

4.3.4 Interessenangleichnung

Eine der Grundannahmen der Prinzipal-Agenten Theorie sind die kollidieren Interessen der Akteure. Wenn es gelingt diese Interessen zu homogenisieren, so wird der Agent genau die Handlungen ausführen, die der Prinzipal von ihm erwartet, nicht weil er dafür belohnt wird, sondern weil sie in seinem eigenen Interesse liegen.

Ein Unternehmen kann verschiedene Interessen haben, primär steht dabei jedoch das Erzielen von positiven Cash Flows im Vordergrund. Auch der Angestellte strebt nach Nutzenmaximierung, diese kann in seinem Fall darin bestehen den Arbeitsaufwand für ein gegebenes Gehalt möglichst zu minimieren.

Es gibt verschiedene Strategien die Ziele des Unternehmens auch zu den Zielen des Agenten zu machen. Da wäre zum Beispiel die Möglichkeit das Gehalt vom Erfolg der Firma abhängig zu machen (siehe 4. 1). Diese Möglichkeit wird von Konzerne vor allem im höheren Management, mittlerweile aber auch immer mehr auf den darunter liegenden Ebenen genutzt. Das der Nutzen solcher Anreizsysteme durchaus umstritten ist, wurde bereits erörtert.

Eine weitere Möglichkeit ist die Stärkung der Corporate Identity. Hierbei soll unter den unternehmensinternen Akteuren ein „Wir-Gefühl" erzeugt und gestärkt werden. Oft werden die Ziele des Unternehmens Top Down zu den Zielen der Angestellten erklärt, eine ebenfalls recht zweifelhafte Strategie, die teilweise an Gerhirnwäsche grenzt.

Als letzter Punkt ist die direkte Verbindung der persönlichen Interessen mit denen der Firma zu nennen. So kann man etwa den Angestellten dazu bringen, indem er sein eigenes Eigentum oder seine persönlichen Daten schützt auch das Eigentum bzw. die Firmendaten zu schützen.

4.3.5 IT-Security durch den Abbau von Informationsasymmetrien

Welche der soeben beschriebenen Instrumente sind auch für die Verbesserung der IT-Sicherheit auf Unternehmensebene anwendbar? Hier wäre zunächst das Signaling zu nennen. Die einzelnen Mitarbeiter dazu zu bringen ihre Fähigkeiten, Probleme und Intentionen zu kommunizieren dürfte sich allerdings als durchaus schwierig herausstellen. Man könnte Institutionen schaffen die ihnen die Möglichkeit erleichtern. So könnten Boards, Mailinglisten oder auch Treffen in bestimmten Abständen die Kommunikationsdichte erhöhen. Der Erfolg hiervon hängt jedoch stark von der Kooperationsbereitschaft der Belegschaft ab. Um diese zu fördern könnte man Anreize schaffen, die aber wieder ihre eigenen Probleme schaffen (siehe 4.1). Die andere Möglichkeit des Signaling, den Ehrgeiz der Mitarbeiter zu stärken ist ebenfalls interessant. So könnte man diejenigen Mitarbeiter, die am schnellsten auf eine potenzielle Bedrohung reagieren auf einer Rangliste eintragen. Die Mitarbeiter würden damit spielerisch dazu motiviert schnell auf Gefahren zu regieren. Dabei muss besonderer Wert darauf gelegt werden nicht eine zu kompetitive Atmosphäre zu schaffen. Beim Thema Sicherheit geht es nicht um individuelle Spitzenleistung, sondern darum das gesamte System sicher zu machen. Auch von einer zu

starken Fokussierung auf IT-Sicherheit ist abzuraten, die Mitarbeiter haben schließlich andere Aufgaben im Unternehmen, deren Performance nicht darunter leiden sollte.

Das Screening scheint weniger geeignet die Asymmetrie zu beheben. Menschen mögen es im allgemeinen nicht Testsituationen oder Befragungen ausgesetzt zu werden. Dabei kann es schnell dazu kommen das man lieber gar nichts oder wenig über seine wahren Probleme sagt, da man ja nicht als inkompetent gelten will. Bei einem Screening müsste daher eine möglichst unbefangene, kooperative Atmosphäre geschaffen werden. So könnten etwa die Vorgesetzten von ihren eigenen Problemen, Missgeschicken und Wissenslücken berichten um den Untergebenen die Angst zu nehmen über dies Themen zu sprechen. Dies könnte auch zur Teambildung und Corporate Identity beitragen. Ein automatisches Screening auch Überwachung genannt bietet eine weitere Möglichkeit Informationen zu erzeugen. Ein solches System hat verschiedenste Auswirkungen auf die Angestellten. Die Probleme die ein solches System verursacht sind Zahlreich. Da wären zunächst rechtliche Probleme, die Überwachen von Mitarbeitern ist zum Beispiel in Deutschland nur mit einem Beschluss des Betriebsrats erlaubt. Zudem kann es aufgrund der Datenmenge zu einer Informationsüberflutung kommen, auch die Mitarbeiter dürften einer derartigen Kontrolle ablehnend gegenüber stehen, bezeugt sie doch fehlendes Vertrauen der Unternehmensleitung gegenüber der Belegschaft. Daher stellt sich die Frage in wie weit ein solches System verlässliche Daten liefert und ob es einen solchen Aufwand wert ist.

Die Self Selection bietet ein interessantes Werkzeug zur Steuerung von Risiken. So könnten den Mitarbeitern verschiedene Sicherheitspakete angeboten werden, die von „Ich mache alles selbst!" bis „Hilfe, schützt mich!" reichen könnten. Dadurch könnte man sowohl die Einzelrisiken gut steuern als auch den individuellen Fähigkeiten gerecht werden. Ein weiterer Vorteil dieses Instruments ist die Wahlfreiheit, die man den

Angestellten damit vermittelt. Diese kommuniziert sowohl Vertrauen als auch Eigenverantwortung. Als Konsequenz einer solchen Herangehensweise wird sowohl die Verantwortung besser verteilt, als auch die IT-Sicherheit im Ganzen erhöht.

Die Interessenangleichung ist ein weiteres Mittel die IT-Sicherheit zu erhöhen. Diese kann schon mit relativ einfachen Mitteln gute Erfolge erzielen. So bekamen etwa bei Schering die Mitarbeiter Schlüssel zu ihren Büros. Wenn diese nun in die Mittagspause gehen, schließen sie ab, um ihre Wertgegenstände zu schützen. Dabei schützten sie natürlich auch die Computer vor unberechtigten Zugriffen und erhöhten somit das Sicherheitsniveau. Dieses Beispiel zeigt auf, wie selbst einfache Maßnahmen helfen können die Sicherheit zu erhöhen. Dies ist sicherlich ein Bereich der noch einiges an Entwicklungspotential aufweist. So kann mit der Verknüpfung von persönlichen Interessen mit denen der Firma eine Verbesserung der Sicherheit erzielt werden. Man kann sich dabei verschieden Maßnahmen vorstellen. So könnte jedem Mitarbeiter erlaubt werden, den Computer auch privat zu nutzen. Um die privaten Daten zu schützen wäre er vielleicht leichter dazu zu bewegen, Maßnahmen einzuleiten als wenn es „nur" um die Arbeitsdokumente ginge.

4.4 Bürokratische Kontrollen etablieren

Im Kontext der Prinzipal-Agenten Theorie stellt die Kontrolle über die Prozesse und die beteiligte Akteure einen Weg dar, die schon beschriebenen opportunistischen Interessen der Agenten zu verringern bzw. zu unterbinden.

4.4.1 Das etablieren von Kontrollsystemen

In der Ökonomie spielt die Kontrolle über Prozesse und Mitarbeiter eine nicht unerhebliche Rolle. Gemmy Allen unterteilt den Kontrollprozess dabei grob in vier Schritte. Zuerst müssen Standards etabliert werden.

Diese beziehen sich meistens auf spezifische Prozesse und werden in einem numerischen Wert angegeben. Dabei spielen Qualität, Quantität und die Zeit eine Rolle. Die Toleranzen in denen sich die Werte bewegen dürfen werden ebenfalls in diesem Schritt festgelegt.

Die Werte werden meistens von den Führungskräften des entsprechenden Bereichs festgelegt. Zur Entscheidungsfindung werden verschiedene Quellen herangezogen, diese können zum Beispiel mündliche und schriftliche Berichte, Zeitkarten oder Beobachtungen sein.

Anschließend werden die gemessenen Daten mit den festgelegten Standards verglichen und Abweichungen festgestellt, dabei werden die erwarteten Abweichung mit in Betracht gezogen. Die Daten werden dann ausgewertet und es werden Mittelwerte errechnet. Mit diesen können dann sowohl die positiven als auch die negativen Ausreißer ermittelt werden.

Im abschließenden Schritt werden dann die Maßnahmen festgelegt. Diese müssen die Schwachstellen beseitigen und den Fluss der Prozesse wieder herstellen. Kontrolle soll stets dazu dienen die Abweichungen von den Standards zu ermitteln und die daraus folgenden Probleme zu beheben. Im Laufe dieses Prozesses kann es auch dazu kommen, das die Wahl der Standards sich als falsch herausstellt. Dies muss dazu führen das die Standards dementsprechend angepasst werden und ein neuer Kontrollzyklus etabliert wird (Allen 2002).

Bei der Organisation von Arbeitsumfeldern kann man diese so gestalten, dass Kontrollinstanzen entstehen. Diese könnten sich in Form eines wöchentlichen Berichts oder Treffens bestehen. Durch eine solche Umgebung kann man dem einzelnen Mitarbeiter einen Rahmen bieten, der ihm sowohl Sicherheit als auch beständiges Feedback zu seiner Arbeit liefert.

4.4.2 Chancen und Risiken von Kontrollensystemen

Die Kontrolle kann ein hervorragendes Werkzeug sein die Effizienz und das Umfeld zu verbessern. Dabei muss auf einen angemessenen Rahmen geachtet werden. So muss die Art wie auch die Intensität der Kontrolle so gewählt werden, dass sich die Mitarbeiter wohl fühlen, eine Rückmeldung zu ihrer Leistung erhalten und dabei für den Vorgesetzten leichter zu beurteilen sind. Die Gefahr in die man sich bei der Etablierung von Kontrollmechanismen stets begibt ist einerseits, dass sich manche Mitarbeiter diesen vorsätzlich entziehen und andererseits dass sich das Betriebsklima erheblich verschlechtert. So sollte stets vermittelt werden, dass die Kontrolle sowohl dem Wohl der Firma dient, also auch jedem einzelnen Mitarbeiter. Dabei sollte man möglichst die Angestellten in die Prozesse einbeziehen und ihnen ihre persönlichen Vorteile aufzeigen.

4.4.3 IT-Sicherheit durch bürokratische Kontrollen

Das etablieren von Kontrollsystemen kann auch in der Informatik für die Schaffung von Sicherheit interessant sein. Die Kontrolle als Mittel zur Erhöhung der Sicherheit ist das Grundthema vieler Lehrbücher. Da Kontrolle in diesem Kontext meistens Überwachung und Einschränkung bedeutet sollten man hier genau differenzieren.

Die oben erwähnten Optionen sollen den einzelnen Mitarbeiter zu einer besseren Arbeitsleistung und einer besseren Reflexion eben dieser verhelfen. Kontrolle ist nicht dazu gedacht den Mitarbeiter zu entmündigen und zu überwachen wie das heute vielfach geschieht. Die Wirksamkeit solcher Überwachungssysteme als auch deren Auswirkungen sind zu hinterfragen. Dem Betriebsklima sind solche Systeme nicht förderlich. Zudem kann Sicherheit zu einer Erhöhung der

Kreativität der Mitarbeiter führen. Leider ist die Kreativität jedoch nicht auf die Schaffung von Werten, sondern auch das Umgehen der Kontrollsysteme gerichtet.

Dies hat zur Folge, dass eine neue Definition der Kontrolle notwendig erscheint. Eine mögliche Beschreibung sollte vor allem auf zwei Punkte eingehen. An erster Stelle steht die Zweckgebundenheit, die sich dadurch auszeichnet, dass jede Kontrollmaßnahme stets mit einem bestimmten Ziel verbunden seien sollte. Wenn sich herausstellt, dass dies nicht oder nicht mehr der Fall ist sollte Kontrolle überdacht bzw. beendet werden. Die Kontrollmechanismen dienen nicht dem Selbstzweck oder der Neugier der Vorgesetzten sondern sollen den Grad an Sicherheit für die Firma und der einzelnen Mitarbeiter erhöhen. Des weiteren muss jede Kontrollmaßnahme kommuniziert werden. Dies verringert die Informationsasymmetrie zwischen Agent und Prinzipal und erhöht das Vertrauen der Mitarbeiter in die Firma. So kann sich der einzelne Mitarbeiter sicher und informiert fühlen. Eine offene Informationspolitik führt zu einem besserem Betriebsklima als auch zu einer besseren Corporate Identity. Im Endeffekt bedeutet dies, dass sich alle Kontrollmechanismen durch Zweckgebundenheit und Offenheit auszeichnen sollten.

4.5 Verbesserung der Reputation

Der Ruf der Firma ist nicht nur nach außen, sondern auch nach innen wichtig. Die Möglichkeit mit Stolz auf die eigene Arbeit und den Arbeitgeber zu blicken ist vielen Menschen wichtig. Wie diese Reputation erhalten und verbessert werden kann wird im Folgenden betrachtet.

4.5.1 Externe und interne Reputation

Die Ökonomie bietet unterschiedliche Strategien zur Reputations-verbesserung an. Dies kann zum Beispiel durch Kampagnen oder Werbung geschehen. Hier bieten sich eine Vielzahl von Möglichkeiten.

Sie reichen von der Unterstützung sozialer, ökologischer aber auch sportlicher Projekte. Diese können die Meinung der Öffentlichkeit mit Hilfe der Medien entscheidend verbessern. Die öffentliche Wahrnehmung differenziert aber stark zwischen positiven und negativen Meldungen. So kann etwa die Entlassung von 10.000 Mitarbeitern nicht mit einem Hilfsprojekt in Afrika ausgeglichen werden. Die Menschen merken sehr schnell wenn Projekte nur der Publicity dienen und strafen die entsprechende Firma entsprechend ab.

Die Reputation nach innen zu verbessern ist ein schwieriges Unterfangen. Dies muss mit vielen kleinen Schritten versucht werden. Letztendlich geht es auch hier wieder um das Schaffen von Vertrauen, was bereits unter 4.1 diskutiert wurde. Das Betriebsklima ist ein weiterer Punkt der beachtet werden muss. So darf weder Ungleichbehandlung nach Willkür oder Machtmissbrauch geduldet werden, sonst entwickelt sich schnell die Meinung das nur unter Ausnutzung der eigenen Macht und ohne Rücksicht auf Verluste vorwärts zu kommen sei.

4.5.2 IT-Sicherheit durch die Verbesserung der Reputation

Die Steigerung der Reputation als Mittel zur Verbesserung der IT-Sicherheit kann in verschiedenen Variationen eingesetzt werden. Zum einen kann Reputation durch Institutionen erzeugt werden. Dies geschieht bereits vielfach mit der Ausgabe von Zertifikaten und der Zertifizierung durch vertrauenswürdige Stellen. Mit einer solchen Vorgehensweise sichern sich die Firmen auch nach außen hin ab und zeigen, dass sie internationale Richtlinien einhalten. Der institutionale Aspekt ist sicherlich nicht unwichtig, allerdings sollten auch die Menschen einbezogen werden. Wie im Abschnitt 4.1 bereits beschrieben ist Vertrauen ein entscheidender Punkt in einem ganzheitlichen IT-Sicherheitskonzept. Die Steigerung der Reputation trägt wiederum dazu bei dieses Vertrauen zu erhöhen. Reputation heißt hier vor allem

Steigerung von Ansehen durch Erhöhung der Transparenz, in der IT-Sicherheit gilt Offenheit als das beste Mittel um Schwachstellen zu finden.

5. Fazit

Aus der vorliegenden Arbeit soll ersichtlich werden, das die Gründe für die Unsicherheit von Informationstechnik tiefere Wurzeln hat, als dies auf den ersten Blick erkennbar ist. Eine singuläre Fokussierung auf die rein technische Komponente von IT-Sicherheit wird der Problematik nicht gerecht und kann zu keiner dauerhaften Lösung führen. Um Wirkungszusammenhänge besser verstehen zu können bietet sich die Ziehung von Parallelen zur Ökonomie, und hier im besonderen zur Prinzipal-Agenten Theorie an. Eine Abschließende Lösung dieser Problematik ist die Ökonomie bisher schuldig geblieben, insofern kann in der vorliegenden Arbeit auch kein Patentrezept für den Umgang mit dem Faktor Mitarbeiter im Zusammenhang mit IT-Sicherheit gegeben werden. Allerdings können verschiedene Möglichkeiten mit dem Dillema umzugehen beschrieben werden, sie alle haben ihre Stärken, aber eben auch ihre Begrenzungen.

Aus Sicht der Autoren ist eine Standartlösung aber auch aufgrund der großen Komplexität des menschlichen Wesens nicht möglich. Instrumente, wie das Belohnen sicherheitssensiblen Verhaltens von Mitarbeitern, mag auf einige Individuen durchaus eine Anreizwirkung entfalten, andere Individuen mögen ein solches System dagegen als Bevormundung und Ungerechtigkeit empfinden. So unbefriedigend dieses Ergebnis auch sein mag, so lässt sich doch sagen, das es ein einziges „richtiges" Verhalten nicht gibt. Viel mehr muss auf der Unternehmensebene situationsspezifisch und unter Berücksichtigung möglicher Neben- und Langzeitwirkungen gehandelt werden.

Literaturverzeichnis

Heise 06: Heise News, Tickermeldung, 2006, http://www.heise.de/newsticker/meldung/72366

DTI 2006: Department auf Trade and Industry, DTI Information Security Breaches Survey 2006, 2006, htp://www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullserveyresults_execsum06.pdf

DTI 2004: Department of Trade and Industry, DTI Information Breaches Survey 2004, 2004, http://www.pwc.com/uk/eng/ins-sol/publ/pwc_DTI-InfoSecutiry-Survey2004-Exec.pdf

DTI 2002: Department of Trade and Industry, DTI Information Security Breaches Survey 2002, 2002, http://www.pwc.com/images/gx/eng/about/svcs/grms/2002ExecSum.pdf

Bessen 2005: James Bessen, Open Source Software: Free Provision of Complex Public Goods, 2005, http://ssrn.com/abstract=588763

Anderson 2001: Ross Anderson, Why Information Security is hard - an econimic perspective, 2001, http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf

Solms 2000: Basie von Solms, Information Security - Third Wave, 2000, http://dblp.uni-trier.de

Schering 2006: Uwe Bartels, Alexander Göbels, Corporate IT Risk Management, 2006

Schneier 2004: Bruce Schneier, Secrets & Lies, 2004

Voigt 2002: Stefan Voigt, Institutionenökonomik, 2002

Pratt/Zeckhauser 1985: Pratt/Zeckhauser, Principals and Agents: The Structure of Business, 1985

Akerlof 1970: George Akerlof, The Market for 'Lemons': Quality Uncertainty and the Market Mechanism, 1970

Grigg 2005: Ian Grigg, Sicurity Signaling - The Market for Lemmings, 2005, https://www.financialcryptography.com/cgi-bin/mt/mt-tb.cgi/285

Needham 2002: Roger Needham, Keynote Address: Mobile Computing versus Immobile Security, 2002

Kappel 1989: H. Kappel, Neue Entlohnungsformen drängen!, 1989

Kohn 1994: A. Kohn, Warum Incentive-Systeme oft versagen, 1994

Pfeiffer 1998: J. Pfeifer, Sechs gefährliche Legenden über Arbeitsentgelte, 1998

o.V. 1990: Unbekannt, Belohnung motiviert nicht, 1990

Sprenger 1994: R. Sprenger, Ideen bringen Geld, 1994

Beckert 1998: J. Beckert, A. Metzner, h. Roehl, Vertrauenserosion als organisatorischer Faktor und wie ihr zu begegnen ist, 1998

Scott 1980: D. Scott, The Casual Relationship between Trust and the Assesesed Value of Management by Objectives, 1980

Sprenger 2005: R. Sprenger, Vertauen führt, 2005

Müller 1998: W. Müller, Welche Werte sollen gelten? - oder: Was ist der Mitarbeiter wert?, 1998

Werner 2002: J. Werner, Vertrauen, 2002

Oelsnitz 2001: D. v. d Oelsnitz, Walt Disney ein Lehrstück in Sachen Management, 2001

Heimburg 2002: Y. Heimburg, Führung in virtuellen Teams, 2002

Laffont 2002: Jean-Jaques Laffont, David Martimort, The Theorie of Incentives, 2002

Holmström 1979: Bengt Holmström, Moral Harazard and Observability, 1979

Allen 2002: Gemmy Allen, Supervision a Hyperlink Book, 2002, http://ollie.dcccd.edu/mgmt1374/book_intro.html