

Revision und Internet – Überlegungen zur missbräuchlichen Nutzung im Unternehmen

Von Dipl.-Betriebswirt Christoph Wildensee, CISM, Hannover¹

1. Einleitung

Das Internet ist zu einem alltäglichen Instrument der Kommunikation und der Datenrecherche geworden - es gehört zum üblichen Erscheinungsbild am Arbeitsplatz. Doch mit Einzug dieses Mediums ist auch die Verunsicherung der Mitarbeiter gestiegen - einerseits hinsichtlich der dahinterliegenden Technologien und andererseits hinsichtlich der erlaubten Nutzung. Auf jeder Internet-Seite sind Links zu anderen Seiten platziert, Werbe-Banner und automatische Pop-Ups sind überall präsent, viele Seiten besitzen Links und Banner zu rechtlich fragwürdigen Inhalten.

Viele deutsche und auch internationale Unternehmen verfolgen bei der Überwachung des Internet-Einsatzes die Strategie eines ‚Laissez-faire‘, doch z.T. wird der Einsatz auch stark reglementiert und - mehr oder weniger effektiv - überprüft. Doch geht es meist weniger um den Wunsch des Überwachens, sondern vielmehr um das ‚Wie‘.

2. Regelungsbedarf als Schutz für den Mitarbeiter

Problematisch ist grundsätzlich, dass der Einsatz im Unternehmen gewünscht, jedoch das fachliche Know-how sowohl der Führungsebene als auch der Administratoren nicht in dem Maße vorhanden ist, wie dies erwartet wird. Oftmals kommen daher externe Dienstleister zum Einsatz, die bei der Konzeption, Realisierung und Implementierung die Fäden in der Hand halten. Dem eigenen Know-how-Aufbau wird vielfach erheblich zu wenig Aufmerksamkeit geschenkt. Aus wirtschaftlicher Sicht ist dies jedoch auch kaum verwunderlich, da die Situation in den Unternehmen selten den Aufbau von detaillierten Kenntnissen und versierten Mannschaften begünstigt. Der Einsatz der über Know-how-Bündelung optimierten Externen ist meist die einzige Alternative.

Entsprechend ist oft zu beobachten, dass zwar Einsatzkonzeptionen und Betriebsvereinbarungen in den Unternehmen erarbeitet werden, der Endanwender jedoch alleingelassen wird. Dabei ist gerade in diesem gefährdeten Bereich ein ‚Code of Conduct‘, also der Aufbau von Verhaltensrichtlinien für den üblichen Gebrauch, um zum einen den Mitarbeiter zu sensibilisieren, zum anderen aber auch zu schützen (Fürsorgepflicht) und verbindliche Verfahren für die Nutzung sowie den Fall des Missbrauchs zur Verfügung zu stellen, notwendig.

Beispiele für Regelungspunkte eines solchen Verhaltenskodex sind:

- Dienstliche Zweckbindung und Hinweis auf Eigenverantwortlichkeit jedes Benutzers
- Ausschluss des Ausprobierens weiterer, nicht freigegebener Dienste und Funktionen, Nutzung fremder Identitäten und Einbrüche ins System (Hacker-Mentalität)
- Ausschluss der Weitergabe von eigenen Benutzerkennungen und dazugehörigen Authentifizierungshilfsmitteln für eine Benutzung durch Dritte
- Untersagen des Ausspähöns der Systeme und Netze nach Sicherheitslücken und das bewusste Verschweigen vorgefundener, sicherheitsrelevanter Lücken und Inhalte durch Mitarbeiter
- Ausschluss des aufrührerischen, belästigenden oder diffamierenden Verhaltens gegenüber anderen Kommunikationspartnern

¹ Herr Wildensee ist bei der Stadtwerke Hannover AG als IV-Revisor tätig.

- Untersagen des bewussten Abrufens oder Anbietens von weltanschaulicher, politischer oder nicht dienstlich relevanter kommerzieller Werbung sowie des bewussten Abrufens oder Anbietens von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen oder pornographischen Äußerungen oder Abbildungen (Bilder, Schriften, Tondokumente etc.)
- Informationspflicht der Mitarbeiter über Verbote und insbesondere strafrechtlich relevante Umstände / Gegebenheiten (Holschuld des Mitarbeiters) und Informationsangebot des Arbeitgebers
- Regelung zu Verschlüsselung, digitaler Signatur, Newsgroups, Mailinglisten, Aufrufen von / Senden an nur bekannten Seiten und EMail-Adressaten, Firewall-/Gateway-Einstellungen / Sicherheitspolicy, Freigabe von Anschlüssen/Ports, Virenschanner-Einsatz (Attachement), Spamming, Bombing, Beschaffung über das Internet (Zahlungsrichtlinien), B2B / eCommerce / eProcurement-Regelungen, Java, ActiveX-Komponenten, Protokollierung, Einschränkung von Zugriffen (URL-Blocker) [Teile hiervon als geheime Dokumentation im Bereich IT-Sicherheit / IT-Infrastrukturmanagement]
- Ausschluss privater Software (auch Spiele), Download, auch Shareware, Freeware, Treiber etc.
→ solche Aufgaben zentralisieren → Hinweis: Wirkung auf Bestands- und Lizenzmanagement, Anlagenbuch, Inst.kosten etc.
- Einrichtung einer zentralen Meldestelle für den Endanwender mit z.T. befreiender Wirkung [...]

Bereits dieser Streifzug beinhaltet eine Vielzahl von Problemfeldern, die insbesondere auch dem Endanwender negativ ausgelegt werden können, wenn sie nicht geregelt sind. Daher sollte grundsätzlich bereits bei der Entwicklung solcher Regelungen darauf Wert gelegt werden, den Betriebsrat, die Interne Revision, den Datenschutz und die IT-Sicherheit zu beteiligen. Dies bedeutet jedoch auch z.T. eine Neudefinition der Aufgaben für die hier genannten Bereiche.

3. Abhängigkeit von schwer zu durchschauender Technologie

Problematisch ist weniger, dass eine erhebliche Menge an Daten aufläuft, sondern dass der Endanwender nicht weiß, was über ihn gespeichert wird, wo dies erfolgt und wer diese Daten zu welchem Zweck analysieren kann.

Bei einer Bereitstellung der Internet-Dienste als Server-Dienst durch Fachabteilungen des eigenen Hauses werden die Zugangs- und Abrechnungsdaten meist zentral gehalten. Dabei werden pro Mitarbeiter (oft maschinenabhängig) nicht nur die Zugangsdaten (Zeiten, Verweildauer), sondern auch die Inhalte/Nutzungsprofile gespeichert. Doch meist hat der Betriebsrat bereits im Vorfeld die Nutzung dieser Daten ausgeschlossen und nur bei konkreten Verdachtsmomenten die Auswertung von Protokollaten freigegeben. Eine solche Hürde als Revisor zu nehmen, ist nahezu unmöglich. Dies gilt auch für stand-alone-Konfigurationen.

Sofern ein externer Provider als Dienstleister des Server-Dienstes Internet genutzt wird, können sogar erheblich mehr Daten pro Nutzer anfallen. Dies bezieht sich insbesondere auf die inhaltliche Ausprägung. Hier kommt dem Betriebsrat und auch der Internen Revision eine sehr wichtige Rolle zu, denn sie müssen bereits bei den Vertragsverhandlungen einbezogen werden, um darauf hinzuwirken, dass die Daten nicht artfremd verwendet werden (es handelt sich um Auftragsdatenverarbeitung) und nicht zuletzt auch, um das Recht des Betriebsrates und der Internen Revision zur Prüfung beim externen Dienstleister auf Einhaltung bestehender Vertragsbestandteile und auf Sperrung kritischer Seiten fixieren zu lassen (Einstellungen Firewall, URL-Block, Bandbreite, Verfügbarkeit, Nachweisregelungen, QS etc.). Hier bestehen für Revisoren erheblich mehr Möglichkeiten, vertiefte Prüfungen durchzuführen. Entscheidend sind die ‚Agreements‘, die mit dem Provider und der Mitarbeitervertretung geschlossen werden.

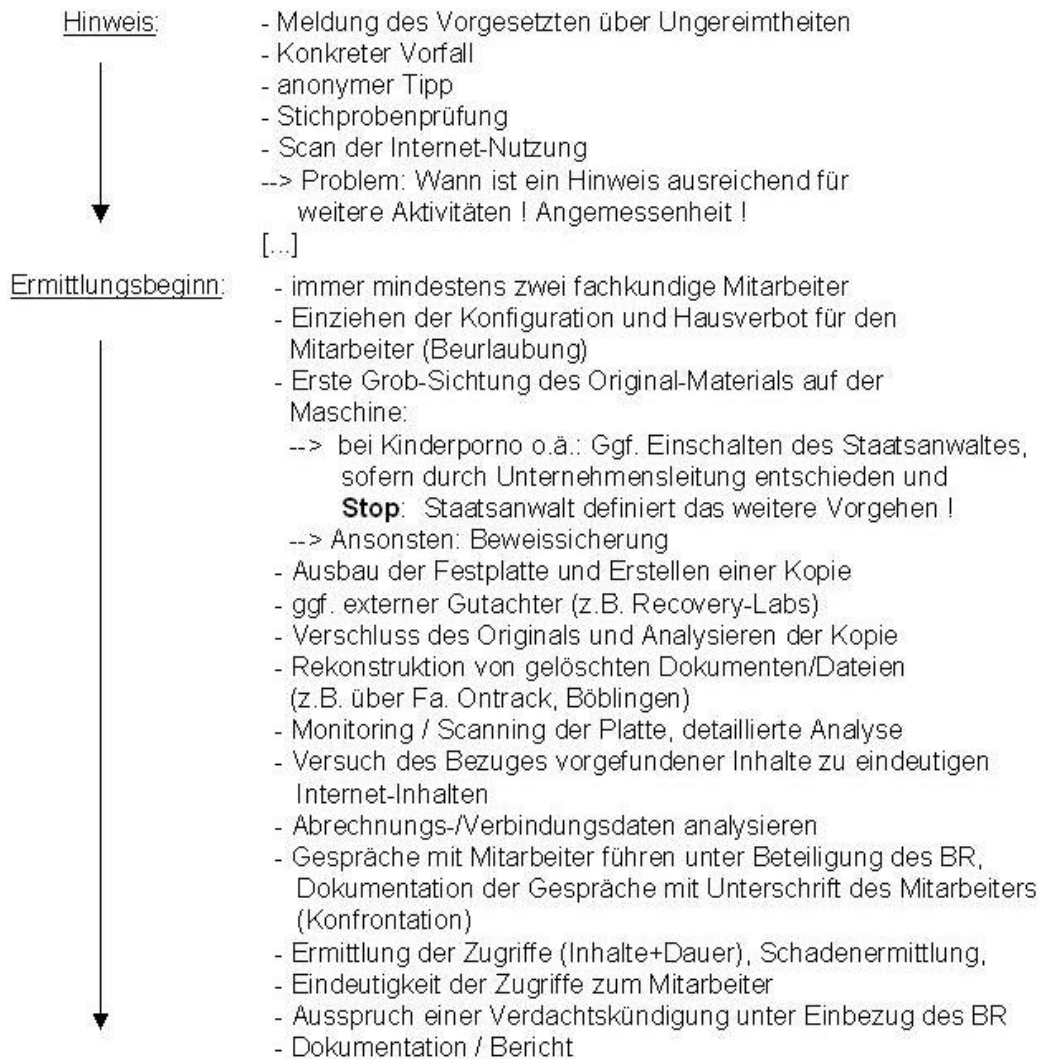
4. Besonderheit fragwürdiger Inhalte

Jedem Nutzer muss heute bewusst sein, dass er beim Surfen nicht nur Spuren in anderen Systemen hinterlässt, sondern auch auf seinem Arbeitsplatzrechner und in der IT-Infrastruktur (z.B. Internet-Gateway). Die Möglichkeit, verbotene / fragwürdige Inhalte aufzurufen (bewusst oder unbewusst), sind durch die dahinterliegenden Technologien erheblich gestiegen.

Fundstücke dieser inhaltlichen Ausprägung auf Arbeitsplatzrechnern sind somit differenziert zu betrachten. Da sie grundsätzlich personalrechtliche Konsequenzen nach sich ziehen können, ist ein besonderes Maß an Vertraulichkeit und Sorgfalt bei der Ermittlung notwendig.

4.1 Ermittlungsvorgehen

Das Vorgehen für die Revision in einem Fall der missbräuchlichen Nutzung ist komplex und nicht unbedenklich. Der folgenden Graphik ist der Ablauf detailliert zu entnehmen.



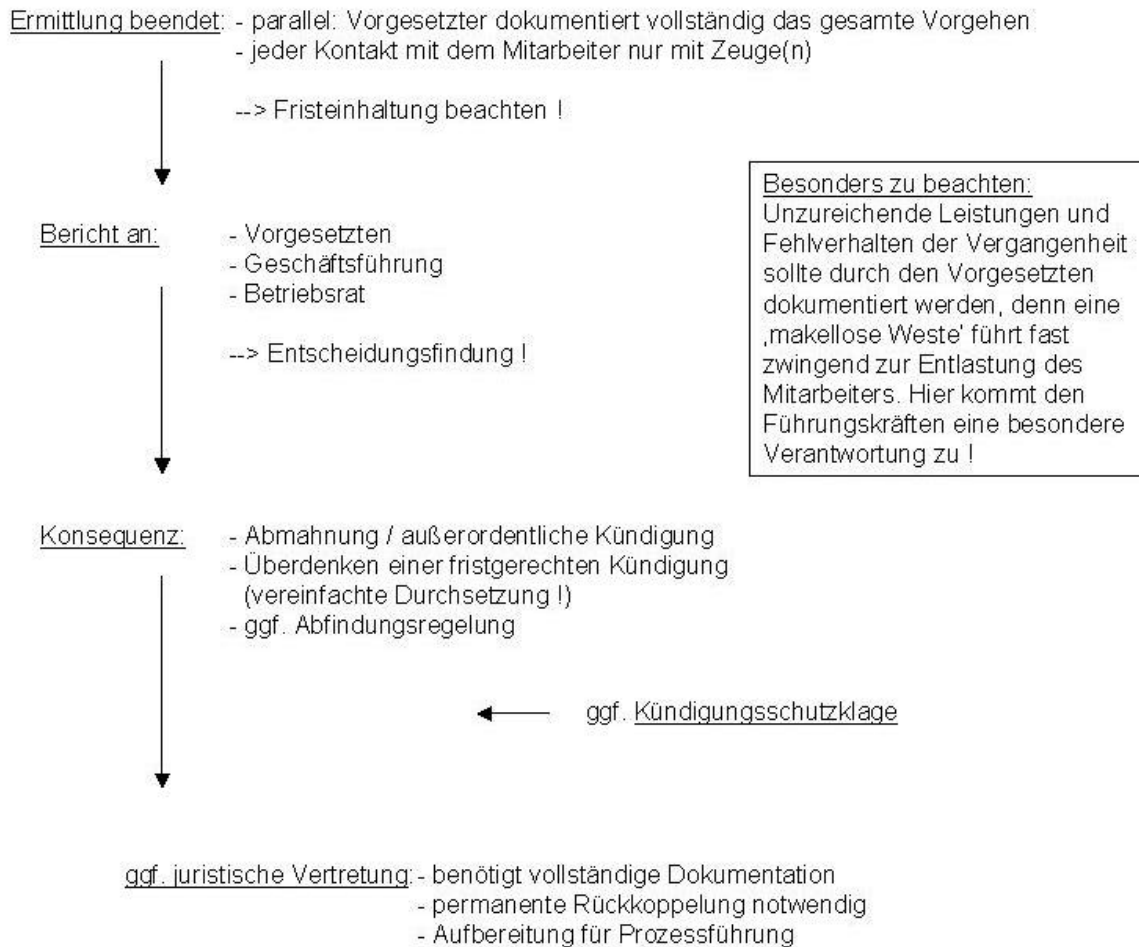


Abb. 1: Recherche-Vorgehen

Grundsätzlich gilt dieses Vorgehen sowohl in Unternehmen mit erlaubter (bzw. nicht verbotener) privater Nutzung als auch in Unternehmen, in denen die private Nutzung untersagt ist. Auswirkungen hat die Erlaubnis der privaten Nutzung lediglich auf die Schärfe der gerichtlichen Sanktionierung, die Ausgestaltung der Aufbewahrung und Weitergabe von ‚Connection-Daten‘ und die Möglichkeit der Einsichtnahme in mitarbeiterbezogene Postfächer.

Während in Unternehmen mit Verbotsregelung für das private Surfen und die Privat-Mailnutzung die Einsichtnahme durch Unternehmensinstanzen jederzeit möglich ist (es handelt sich in dem Fall um ein ausschließlich betrieblich bereitgestelltes Medium, das auch vollständig kontrolliert werden kann, denn es beinhaltet aus der Definition heraus nur betrieblich relevante Inhalte), besteht für Unternehmen ohne Verbotsregelung ggf. ein Verwertungsausschluss von Analyseergebnissen. Evtl. kommt es für solche Unternehmen noch schlimmer: Sofern das private Surfen und Mailen dezidiert erlaubt ist, kann sich hieraus ergeben, dass zukünftig das Unternehmen im Bereich der Nachweispflicht/Beweissicherung analog einem Telekommunikationsdienstleister gewertet wird. Dies hat zur Folge, dass die Connection-Daten der Mitarbeiter personenscharf und mit tiefgehenden Inhalten ermittelt und erheblich länger aufbewahrt werden müssen. Dies hat zwar keine unmittelbare Auswirkung auf eine evtl. stattfindende IT-Infrastruktur- und Verhaltensanalyse, kann jedoch dazu führen, dass im Fall einer unrechtmäßiger Nutzung durch einen Mitarbeiter und dem Fehlen solch tiefgehenden Inhalte das Gericht zum Ergebnis kommt, dass das Unternehmen seiner Sorgfaltspflicht nicht nachgekommen ist.

Dienstliche Zweckbindung	Erlaubte (oder nicht verbotene) private Nutzung
Analyse der Internet- und Mailnutzung (auch im Rahmen technischer Anpassungen o.ä.) jederzeit möglich	Analyse ist an Auflagen gebunden, hier wird häufig auf die Angemessenheit der Mittel und die Abwägung der Deutlichkeit der Sanktionierung für den Mitarbeiter verwiesen
Kein Verwertungsausschluss durch klaren dienstlichen Bezug	Evtl. Verwertungsausschluss bei geringsten Auflagenverletzungen im Kündigungsverfahren
Vorgehen bei ‚Personellen Maßnahmen‘ in beiden Fällen identisch, innerbetriebliche Sanktionierung (Ermahnung, Abmahnung, Stellenumbesetzung) ist meist unkritisch.	
Geringere Datenschärfe und Protokollierung nötig, sofern der eindeutige Bezug zum Mitarbeiter hergestellt ist	Evt. schärfere Datentiefe gefordert und somit Anforderungserhöhung im Bereich der Nachweispflicht/Beweissicherung
Erfolgsaussichten vor Gericht sind höher	Erfolgsaussichten vor Gericht sind gering, insbesondere im öffentlichen Dienst durch das Dienstrecht und die Kündbarkeitsregelungen

Tab. 1: Auswirkungen unterschiedlicher Nutzungsregelung ²

Juristische Gutachten und Urteile zu diesem Themenkomplex werden kaum nachvollziehbar-detailliert veröffentlicht. Folgende markante Punkte können jedoch beispielhaft als wichtige Vorarbeiten/Aktivitäten aufgezeigt werden:

- Grundsätzlich ist vorbehaltlich des endgültigen Ermittlungsergebnisses innerhalb der gesetzlichen Frist zur außerordentlichen eine Verdachtskündigung u/o eine fristgerechte Kündigung zu erwägen, als Zeitpunkt des Bekanntwerdens gilt anerkannt das Berichtsdatum der Internen Revision oder des externen Gutachters
- Der Mitarbeiter ist umgehend mit Hausverbot zu belegen, die Konfiguration ist einzuziehen
- Die Analyse ist mindestens durch zwei fachkundige Mitarbeiter mit computerforensischen Methoden zeitnah und vollständig durchzuführen (Zeuge), eine Ermittlungsprotokollierung/-dokumentation ist anzufertigen (plausibles und stringentes Vorgehen), sinnvoll kann auch die Nutzung von Dienstleistern zur Rekonstruktion von Datenstrukturen sein (z.B. Data Recovery - Ontrack), wenn ein methodisches Ermittlungsvorgehen durch eigene Mitarbeiter unzureichend ist
- Hatte der Mitarbeiter eine besondere Vertrauensstellung (DV-Koordinator, Administrator, Vorgesetzter), ist dies gesondert herauszustellen (für die Zumutbarkeit einer Weiterführung der Beschäftigung)
- Eine Schadenermittlung muss vorliegen. Einzubeziehen sind hier Nutzungsentgelte, aber auch besonders (vor Gericht anerkannte) entgangene bewertete Arbeitszeit !
- Sofern eine Betriebsvereinbarung vorliegt, in der die private Nutzung nicht ausdrücklich ausgeschlossen ist, sollte man es bei einer Abmahnung belassen, denn eine außerordentliche Kündigung geht in einem solchen Fall nahezu sicher zulasten des Arbeitgebers aus (BV-Nacharbeiten).
- Sofern eine Betriebsvereinbarung vorliegt, in der die private Nutzung ausgeschlossen ist, sind weitere Hürden zu nehmen. Beliebte Fragen vor Arbeitsgerichten sind: Trotz Vorlage der BV hätte der Mitarbeiter mit einer solchen Konsequenz rechnen müssen ? Gab es vergleichbare bekannte Fälle, die Signalwirkung ausstrahlen (z.B. Kündigungen bei Nutzung von Telefon-Hotlines) ? Sind Mitarbeitern generell die Konsequenzen bei Verstoß bekannt ? Haben die Mitarbeiter die BV zur Kenntnis genommen, möglicherweise sogar zur Kenntnis unterschrieben ? Gibt es Ausführungsbestimmungen und Erklärungen zur BV (s.o., Code of Conduct‘), denn von einem Mitarbeiter wird vor dem Arbeitsgericht nicht zwangsläufig erwartet, dass er die Technologie versteht, die er täglich nutzen soll ? Gibt es eine zentrale Institution/Meldestelle im Unternehmen, die dem Nutzer als Ansprechpartner dient ? Ist das Angebot an Zusatzinformationen für den Nutzer ausreichend ?

[...]

² Dem Autor ist ein Fall bekannt, bei dem in einem Unternehmen ohne Verbotsregelung Mitarbeiter in Pausen und nach Feierabend den dienstlich bereitgestellten Internet-Zugang nach Belieben nutzen durften. Dies taten einige Mitarbeiter in der Form, dass diese als ebay-Power-Seller agierten. Bedenklich !

4.2 Revision im Zwielficht

Nachvollzugsarbeiten durch Mitarbeiter der Revision erhalten eine besondere Brisanz, wenn die Inhalte strafrechtliche Relevanz aufweisen. Eine Beweissicherung kann beispielsweise bei vorgefundener Kinderpornographie kaum erfolgen, da bereits der Besitz strafbar ist. Wenn z.B. Beweisdokumente / Bilder für einen Bericht als Kopie in einem zentralen Revisionsystem gespeichert werden, macht sich der Revisor einschließlich seiner Führung evtl. bereits durch Einstellen dieser Inhalte des Verdachts der Verbreitung strafbar (vgl. hierzu §184(3) StGB) ? Sollte man das Finden solcher Inhalte überhaupt melden ? Besteht eine Meldepflicht ? Vorsicht ist somit geboten, da bereits die Klassifizierung dieser Inhalte und die Konsequenzabwägung problematisch ist, denn die Unternehmensleitung hat grundsätzlich kein Interesse einer öffentlichen Diskussion.

Für den Revisor bedeutet also das Finden solcher Inhalte unter Umständen das Betreten eines Terrains, das ihn selbst in Schwierigkeiten bringt. Zumindest innerhalb des Unternehmens scheint es notwendig, dass Revisionsmitarbeiter für den Fall der Ermittlung - gerade durch den Aspekt der Nachvollzugsarbeiten, bei denen sie selbst möglicherweise Zugriff auf die gefundenen Inhalte nehmen - durch die Unternehmensführung eine Entlastung erfahren, um nicht plötzlich selbst personalrechtlichen Maßnahmen ausgesetzt zu sein.

5. Abschluss

Generell bewirken die Komplexität, Undurchschaubarkeit und ‚Anonymität/Mobilität der Daten‘ einerseits und die schwer nachzuvollziehenden Technologien andererseits, dass der Mitarbeiter an sich in einen rechtlich fragwürdigen Raum gedrängt wird, den er selten überschauen kann. Es ist notwendig, dass Rahmenbedingungen durch das Unternehmen definiert werden, um einerseits den Mitarbeiter hinsichtlich der möglichen Konsequenzen zu informieren, zu schulen und ggf. zu entlasten, aber auch ansatzweise Rechtssicherheit in der Unternehmenskultur zu schaffen.

Dies bedeutet aber auch, dass sich der Revisor im Fall einer forensischen Ermittlung streng an zuvor zu definierende Regularien hält, um nicht selbst ins Zwielficht zu geraten. Diese sind durch die Revisionsabteilung mit der Führungsebene und der Personalvertretung abzustimmen, denn nur über ein solches Vorgehen kann eine Entlastung für den Revisor und somit eine angstfreie Zielerreichung erfolgen.

Literaturbeispiele

Tischer, M./ Jennrich, B.

Internet intern
Paderborn, 1997

Raepple, M.

Sicherheitskonzepte für das Internet
Heidelberg, 1998

Beispiele für Internet-Seiten:

<http://www.bsi.bund.de>

<http://www.annoyances.org>

<http://www.wildensee.de/veroeff.htm>