# Tatort Betrieb

**Wie kann deliktischem Verhalten von Mitarbeitern begegnet werden? Wie weit darf die Überwachung des Arbeitnehmers am Arbeitsplatz gehen?**

Laut dem Einzelhandelsinstitut entstand durch kriminelle Handlungen von Mitarbeitern im Jahr 2007 in Deutschland ein Gesamtschaden von einer Milliarde Euro. Schätzungen beziffern den durch Mitarbeiter verursachten Schaden zwischen einem und fünf Prozent des Umsatzes, und eine Befragung von 1.700 Managern in Europa ergab, dass zehn Prozent der Trennungsverhandlungen Unehrlichkeit als Hintergrund haben.

**Diebstahl gehört zu den „klassischen" Mitarbeiterdelikten – neben Veruntreuung, Korruption, Betrug und Untreue.**

**Die „klassischen" Mitarbeiterdelikte** sind Diebstahl und Veruntreuung (Laptops, Büromaterial, Waren), Korruption (Vorteilsannahme, rechtswidrige Begünstigung), Betrug und Untreue (Scheinaufträge an Briefkastenfirmen, Buchführungsmanipulationen, falsche Spesenabrechnungen), Computerkriminalität, Verrat von Geschäftsgeheimnissen und Diebstahl von Know-how, Zeitdiebstahl, Schwarzarbeit, Sabotage, Vandalismus, Spionage, Nötigung und Erpressung.

Ziel eines von der *Simedia GmbH,* Bonn *(www.simedia.de),* am 16. Juli 2008 in Stuttgart unter dem Titel „Mitarbeiterkontrolle" abgehaltenen Forums war es, Möglichkeiten zur Aufklärung von Mitarbeiter-Delikten darzustellen und die rechtlichen Grenzen aufzuzeigen.

Den gängigen Einstellungen zu deliktischem Verhalten von Mitarbeitern stellte Dkfm. Harald Seiffert *(Von zur Mühlen'schen GmbH)* die Antithesen gegenüber: „Wir vertrauen unseren Mitarbeitern – aber Vertrauensschäden werden naturgemäß durch Vertrauenspersonen verursacht. Bei uns ist noch nie etwas Spektakuläres passiert" – Wollen Sie darauf warten? In gewissem Umfang sind Diebstähle und Schwund oder Inventurdifferenzen normal – sind Kontrollen also unwirtschaftlich?"

**Innerbetrieblichen Ermittlungen** sind Grenzen gesetzt. Einschränkungen ergeben sich aus Gesichtspunkten des Datenschutzes, des Telekommunikationsrechts, des Arbeitsverfassungsrechts und aus Persönlichkeitsrechten des Mitarbeiters selbst. Die Missachtung dieser Bestimmungen kann nicht nur zu strafrechtlicher Verantwortlichkeit, sondern auch dazu führen, dass die erhobenen Beweise vor Gericht nicht verwertet werden können, beispielsweise in einem arbeitsrechtlichen Verfahren.

Während es rechtlich unproblematisch ist, im Verdachtsfall schriftliche Dokumente wie Rechnungsbelege oder Geschäftspapiere auszuwerten oder Aussagen von Kollegen oder Geschäftspartnern einzuholen, ist die Verfolgung von Datenspuren im ITK-Breich für die Ermittlung von Innentätern praktisch immer mitbestimmungspflichtig, bedarf also der Zustimmung des Betriebsrats, erläuterte Gabriela Krader, Konzerndatenschutzbeauftragte bei der *Deutschen Post AG*. Das gilt für die Auswertung von Daten und Datenspuren im PC oder Notebook des Verdächtigen, auf den firmeneigenen Servern, den firmeneigenen Firewall- und Intrusion-Detection-Systemen, in Einbruchmelde- und sonstigen Alarmierungssystemen, in Zugangskontroll- und Videoüberwachungssystemen oder in TK-Anlagen. Bereits die objektive Eignung eines Systems zur Überwachung reicht aus, die Zustimmungspflichtigkeit zu begründen.

Das heimliche Mitschneiden von Gesprächen oder das Belauschen von nicht öffentlichen Äußerungen ist nach deutschem wie österreichischem Strafrecht verboten (§ 201 dStGB bzw. § 120 StGB; Missbrauch von Tonaufnahme- oder Abhörgeräten). Verboten ist nach deutschem Recht (§ 201a dStGB; Verletzung des höchstpersönlichen Lebensbereiches durch Bildaufnahmen), die unbefugte Herstellung oder Übertragung von Bildaufnahmen einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet. Für die „Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung)" gilt in Deutschland § 6b BDSG, wonach die Beobachtung grundsätzlich offen zu erfolgen hat und erkennbar zu machen ist.

Für die (offene oder verdeckte) Überwachung nicht öffentlicher Räume gilt, dass eine Speicherung und Auswertung der Daten im Rahmen der Verhältnismäßigkeit und unter Beachtung der Mitbestimmungsrechte des Betriebsrats zulässig ist. Eine permanente Beobachtung der Beschäftigten ohne besondere Gefahrenlage für den Arbeitgeber oder die Überwachung besonders geschützter Bereiche (Aufenthalts- und Umkleideräume, Duschen oder auch von Toiletten einschließlich der Vorräume – etwa, weil wiederholt die Toilette verstopft wurde) verstößt gegen die Persönlichkeitsrechte des Arbeitnehmers, ist generell verboten und kann auch nicht über eine Betriebsvereinbarung legalisiert werden. Es empfiehlt sich in den meisten Fällen

FOTO: EGON WEISSHEIMER

ANKER frisch!
SNACK COFFEE
IM FRANZ JOSEFS-BAHNHOF
9., Julius Tandler-Platz 3
Tel. 01/315 32 26
Wir sind für Sie hier: Mo bis Fr 6.00-18.00 Uhr · Sa 6.00-12.00 Uhr
WIR SIND STETS BEMÜHT „FRISCHE" WARE FÜR SIE BEREIT ZU HALTEN UND NEHMEN GERNE GRÖSSERE VORBESTELLUNGEN ENTGEGEN.
WÄHRINGER STRASSE 49 • TEL. 01/405 02 47
Öffnungszeiten: Mo bis Fr 6.30-18.00 Uhr

Dr. Markus Koller
FA f. Zahn-, Mund- u. Kieferheilkunde
ALLE KASSEN
1040 Wien, Schelleingasse 21/14
(U-Bahnstation Südtirolerplatz)
Tel. 01/505 35 73
Mo u. Mi 13-18 Uhr
Di u. Do 8-13 Uhr
und nach Vereinbarung

DAVID HALMER
EVA-MARIA HALMER
CHRISTIAN HALMER
BEHÖRDL. KONZ. GEBÄUDEVERWALTUNG
GESELLSCHAFT BÜRGERL. RECHTS
1170 WIEN, ELTERLEINPLATZ 8
TELEFON (01) 486 14 66 • FAX (01) 489 43 75
email: office@halmer.net

ARCHITEKTEN NEHRER+MEDEK UND PARTNER
ZT GmbH PROF. DI M. NEHRER DI H. POHL 1060 WIEN, GETREIDEMARKT 11
EMAIL: NEHRER.MEDEK.PARTNER@CHELLO.AT TEL. 01/581 58 00-0 FAX 33 DW

DI. RICHARD ANZBÖCK
STAATLICH BEFUGTER UND BEEIDETER ZIVILINGENIEUR FÜR SCHIFFSTECHNIK
ALLGEMEIN BEEIDETER UND GERICHTLICH ZERTIFIZIERTER SACHVERSTÄNDIGER FÜR WASSERFAHRZEUGE UND SCHIFFBAU
1190 WIEN, GUGITZGASSE 8/29
TEL.: 01/320 88 93
MESSBRIEFE
TECHNISCHE BERATUNG

EDV WRUHS
IT DIENSTLEISTUNGEN GMBH
Lenaugasse 9 1080 Wien
T +43 1 5220434
F +43 1 5220434 40
E office@edv.wruhs.at
http://www.edv.wruhs.at

**Harald Seiffert: „Vertrauensschäden werden durch Vertrauenspersonen verursacht."**

**Gabriela Krader: „Betriebsrat muss Verfolgung von Datenspuren im Computer zustimmen."**

der Abschluss von Betriebsvereinbarungen, in denen die zu speichernden und auszuwertenden Daten einschließlich der Zwecke der Auswertung exakt festgelegt werden.

Wenn trotz eines Verbots privater Nutzung von ITK-Anlagen die Einhaltung dieses Verbots nicht kontrolliert wird, kommt dies einem Dulden der privaten Nutzung gleich, wodurch die Verfolgung von Innentätern, etwa durch Auswertung von Verbindungsdaten, stark eingeschränkt ist. Krader empfiehlt auch in diesen Fällen den Abschluss von Verträgen mit den Beschäftigten. Die verdeckte Videoüberwachung am Arbeitsplatz ist nach Ausschöpfung aller anderen Möglichkeiten, das letzte Mittel („ultima ratio"), um einen Täter zu überführen, mitunter auch das einzige. Ein Allheilmittel gegen Straftaten ist der Einsatz von Videotechnik nicht, denn: „Was nützt das beste Videobild vom Tatablauf, wenn der Täter nicht zu erkennen ist."

**Tor- und Taschenkontrollen.** An Werkszugängen und -zufahrten Tor- und Taschenkontrollen durchzuführen, leitet sich aus dem Hausrecht und dem rechtlichen Anspruch des Unternehmens auf Schutz seiner Güter und Werte ab, gegenüber Mitarbeitern zudem aus dem Arbeitsvertrag. Es besteht ein Spannungsverhältnis mit den Persönlichkeitsrechten des Kontrollierten. Auch hier ist es anzuraten, Betriebsvereinbarungen über die Art und Weise der Kontrollen abzuschließen, betonte Manfred Jilg, Leiter des Werkschutzes der *BASF AG,* Ludwigshafen. Auf dieser Basis wird ein Handlungsrahmen für die Sicherheitsorganisation geschaffen, innerhalb dem präventive Maßnahmen und Kontrollen durchgeführt werden können. Im Unternehmen

Fotos: Kurt Hickisch

**Manfred Jilg: „Taschenkontrollen an Werkszugängen müssen geregelt sein.“**

**Carsten Klauer: „Eingriffe in die Intimsphäre eines Mitarbeiters sind unzulässig.“**

besteht die Pflicht, den Betriebsausweis sichtbar zu tragen. Besucher (Geschäftskunden, Mitarbeiter von Fremdfirmen) erhalten einen temporär gültigen Betriebsausweis sowie ein Sicherheitsmerkblatt, in dem unter anderem angeführt wird, dass Kontrollen durchgeführt werden und auch Videoüberwachung erfolgt. Durch die Unterschrift wird die unwiderrufliche Zustimmung zu diesen Kontrollmaßnahmen erklärt, die sich auf Personen, Fahrzeuge, die Ladung und Behältnisse erstreckt. Die Personenkontrolle kann auch eine körperliche Durchsuchung beinhalten, die nur in geschlossenen Räumen und ausschließlich von Personen des gleichen Geschlechts durchgeführt werden darf.

**Berufsdetektive.** „Der Einsatz von Detekteien gegen Mitarbeiter ist ein hartes Mittel, das wohl überlegt werden sollte“, sagte Dipl.-Kfm. Carsten Klauer, Vizepräsident des Bundesverbandes deutscher Detektive (BDD). Die Möglichkeiten, die Detekteien zur Verfügung stellen, reichen vom Testdiebstahl und Testkauf über offene und verdeckte Videoüberwachung, Ermittlung, Observation, Einschleusung, Einsatz von GPS zur Produktverfolgung, Diebsfallen, Mitarbeiter-Screening bis zum Einsatz von Tarnfirmen und Fahrzeugverfolgung über GPS. Welche Mittel eingesetzt werden, ist nicht nur eine Frage der Wirtschaftlichkeit und der rechtlichen Zulässigkeit, sondern auch einer Abwägung zwischen dem zu schützenden Rechtsgut und der Schwere des Eingriffs in die Persönlichkeitsrechte des Tatverdächtigen sowie unbeteiligter Personen. Absolut unzulässig sind Eingriffe in die Intimsphäre (z. B. Lesen eines Tagebuchs). Als Auskunftsmittel kommen auch öffentliche Quellen in Betracht, wie Zeitungen oder über In-

Fotos: Kurt Hickisch

EBCONT
electronic business consulting team
A-3040 Neulengbach
Hauptplatz 62
Tel.: 02772 / 51 269
Fax: 02772 / 51 269-9
Internet: www.ebcont.com

Dreicher Otto vorm. A. Szekely
Fliesenlegermeisterbetrieb
Hafner
Verkauf
Verlegung
Reparaturen
Service und
Instandhaltung
v. Kachelöfen
1160 Wien, Ottakringer Str. 43/6 (Eingang Huberg.)
Tel./Fax 01/403 85 47, Mobil 0664/394 77 30
E-Mail: otto.dreicher@aon.at
Homepage: members.aon.at/ottodreicher

B·R·A·H·M·S
Austria GMBH
Der Spezialist in der Labordiagnostik für:
Infetktiologie, Schilddrüse, Tumormarker,
Pränatalscreening
A-1050 Wien, Schönbrunnerstrasse 45/2/4
Tel.: 0043 1 585 66 67
Fax: 0043 1 585 66 67 9
e-mail: office@brahms.at

**Im Gegensatz zur Polizei kann eine Detektei in enger Zusammenarbeit mit dem Auftraggeber die Ermittlungen gegen einen Mitarbeiter in jedem Stadium abbrechen.**

ternet-Suchmaschinen eingeholte Auskünfte. Um Abnehmer für Diebsgut zu finden, wird vielfach über Internet inseriert, sodass auch Tauschbörsen in Erhebungen einzubeziehen sind.

Im Gegensatz zur Polizei, die zur Führung eines Ermittlungsverfahrens und zur Anzeigeerstattung verpflichtet ist, kann eine Detektei in enger Zusammenarbeit mit dem Auftraggeber die Ermittlungen in jedem Stadium abbrechen und sie ist auch nicht zu einer Anzeigeerstattung verpflichtet. Vielfach wollen Unternehmen nicht, dass deliktisches Verhalten ihrer Mitarbeiter durch Gerichtsverfahren publik wird, um das Image des Unternehmens nicht zu schädigen, was bis zu Kursverlusten an der Börse führen könnte. Mitunter wird von einer Auflösung des Dienstverhältnisses abgesehen, um dem Täter die Möglichkeit zu geben, den Schaden im Unternehmen abzuarbeiten.

Die Detektei hat die – „gerichtsfest" ermittelten – Beweisergebnisse vorzulegen, die in weiterer Folge für zivil- und strafrechtliche Verfahren sowie für disziplinäre Maßnahmen erforderlich sind. Ein notarielles Schulderkenntnis bildet die Basis für die Durchsetzung von Schadenersatzansprüchen. Auf Grund der gewonnenen Erkenntnisse werden auch Empfehlungen zu präventiven Maßnahmen gegeben, wie sich überhaupt die Tätigkeit von Detekteien zunehmend über die repressive Aufklärung hinaus zur Sicherheitsberatung weiterentwickelt.

**„Fraud Management".** Regeln aufzustellen, wie innerbetrieblich mit Verdachtsfällen in einem Unternehmen verfahren werden soll, ist eine Verpflichtung für die Unternehmensleitung. Entsprechenden Hinweisen nicht nachzugehen, könnte Haftungsfolgen für die Verantwortlichen auslösen. Bei Korruptionsdelikten fehlt die klassische Täter-Opfer-Beziehung; keiner zeigt den anderen an. Die „Schweigekartelle" können meistens nur über Insider mit einer Nahebeziehung zum Täter (Sekretärin, Mitarbeiter, enttäuschte Lebenspartner/Geliebte) aufgebrochen werden, die allerdings oft aus Angst vor Repressalien schweigen. Hinweisgeber brauchen Vertraulichkeit und Schutz. Es sind entsprechende Einrichtungen zu installieren, wo derartige Hinweise deponiert werden können, etwa von „Whistleblowing"-Hotlines, wie sie der *Sarbanes-Oxley-Act (SOX)* der USA vorsieht. Das „Whistleblowing" stößt allerdings an seine Grenzen, wenn es um den Schutz des Informanten geht. Letztlich kann zivil- und strafrechtlich erzwungen werden preiszugeben, von wem die Informationen stammen, die zu Nachforschungen geführt haben. Wenn andererseits der Hinweisgeber, aus Furcht vor Aufdeckung seiner Identität, in der Anonymität verbleibt, werden seine Angaben von vornherein als weniger glaubwürdig angesehen.

Rechtsanwälte sind zur Verschwiegenheit verpflichtet und haben das Recht, die Aussage zu verweigern über das, was ihnen in dieser Eigenschaft bekannt geworden ist. Es liegt daher nahe, Rechtsanwälte als externe Vertrauenspersonen für Hinweisgeber einzuschalten. Über die diesbezüglichen Erfahrungen als Ombudsmann berichtete Rechtsanwalt Dr. Rainer Buchert, im Ruhestand befindlicher Polizeipräsident von Stadt und Kreis Offenbach, der für eine Reihe von Unternehmen tätig ist.

Ombudsleute nehmen vertraulich Informationen auf korruptionsverdächtige Sachverhalte entgegen und geben Informationen nur nach Entbindung von ihrer Verschwiegenheitspflicht mit ausdrücklicher Zustimmung des Hinweisgebers weiter. Sie schirmen ihn nach außen ab. Für ergänzende Nachfragen bilden sie die Kontaktstelle.

Die *Deutsche Bahn AG* hat erstmals im Jahr 2000 zwei Ombudsleute berufen. Andere große Unternehmen sind dem Beispiel der Deutschen Bahn gefolgt. *Kurt Hickisch*

Foto: Picturedesk