INTERVIEW

Die kontrollierte Krise – Erfolgreiche Maßnahmen bei Compliance-Verdachtsfällen

Interview mit Ass. jur. Paul H. Malberg

Ein Compliance-Verdachtsfall trifft Unternehmen meist unvorbereitet, doch besonders die ersten Entscheidungen sind prägent. Schnelles, aber dennoch überlegtes Handeln verhindert größere Schäden und sorgt für eine kontrollierte Aufklärung. Welche Maßnahmen sinnvoll sind, hängt vom jeweiligen Fall ab. Der Detektiv Paul H. Malberg zeigt, wie Unternehmen vorbereitet sein können, um Risiken zu minimieren und von Anfang an die richtige Strategie zu wählen.

Ass. jur. Paul H. Malberg
ist Geschäftsführer der Detektei PROOF-MANAGEMENT GmbH in Hamburg, Düsseldorf, Frankfurt/M. und Köln.

ZAU: Ein Unternehmen erhält über das interne Hinweisgebersystem eine anonyme Meldung: Ein leitender Mitarbeiter soll über Monate hinweg Geschäftsgeheimnisse an einen Wettbewerber weitergegeben haben. Die Anschuldigungen wiegen schwer, aber es gibt keine direkten Beweise – nur Indizien. Wie gehen Sie als Berater und Wirtschaftsdetektiv in einer solchen Situation grds. vor?

Malberg: Ein anonymer Hinweis beinhaltet zumeist einen ernstzunehmenden Sachverhalt, der ein strukturiertes, strategisches und besonnenes Vorgehen erfordert. Ohne direkte Beweise, aber mit belastenden Indizien, ist es entscheidend, die richtigen Maßnahmen einzuleiten, um den Verdacht zu prüfen, ohne voreilige Schlüsse zu ziehen. Hier kommt ein vorbereiteter Alarmplan ins Spiel – ein essenzielles Instrument, das Unternehmen auf solche Fälle vorbereitet und eine rechtskonforme, diskrete Aufklärung ermöglicht.

1. Sofortmaßnahmen & Ersteinschätzung

- **Sichtung des Hinweises:** Welche Details werden genannt? Gibt es spezifische Angaben zu Personen, Vorgängen oder Zeiträumen?
- **Erste Plausibilitätsprüfung:** Stimmen die Vorwürfe mit bekannten Sachverhalten überein? Gibt es Anzeichen für Insider-Wissen oder ist die Meldung vage und spekulativ?
- **Risikoabschätzung:** Besteht akuter Handlungsbedarf (z.B. drohender weiterer Geheimnisverrat) oder kann eine systematische Untersuchung erfolgen?

2. Kommunikation & Wahrung der Vertraulichkeit

- **Schutz der Hinweisgeber- und Beschuldigtenrechte:** Ein anonymer Hinweis ist keine Schuldzuweisung – sowohl der Hinweisgeber als auch der Verdächtige müssen vor voreiligen Konsequenzen geschützt werden.
- **Interne Steuerung der Kommunikation:** Nur ein enger, autorisierter Personenkreis sollte informiert wer-

„Besonders in Fällen eines schwerwiegenden Verdachts sollte verhindert werden, dass der Mitarbeiter noch in der Lage ist, sein Smartphone oder seinen Computer zurückzusetzen."

den, um Gerüchte und Unsicherheiten zu vermeiden. Eine Eskalation kann nicht nur rechtliche, sondern auch unternehmenskulturelle Schäden verursachen.
- **Dokumentation der Schritte:** Jeder Schritt vom ersten Tag an wird schriftlich und chronologisch festgehalten, um Transparenz und Nachvollziehbarkeit zu gewährleisten. Im Fall späterer Maßnahmen gegen Mitarbeiter sind Prüfungen der Verhältnismäßigkeit schriftlich zu fixieren.

3. Diskrete Vorermittlung & Validierung des Verdachts
- **Interne Analysen:** Prüfung relevanter Daten wie E-Mail-Korrespondenzen, Zugriffsprotokolle, Datei-Downloads oder ungewöhnliche Aktivitäten auf Unternehmensservern – selbstverständlich unter Wahrung der Datenschutzvorgaben.
- **Informelle Gespräche & Beobachtung:** Ein diskretes Gespräch mit relevanten Personen kann erste Hinweise geben, ohne den Verdächtigen direkt zu konfrontieren. Gleichzeitig können ungewöhnliche Verhaltensmuster analysiert werden.
- **Einbindung interner und externer Experten:** Falls Indizien sich verdichten, sollte ein erfahrener Wirtschaftsdetektiv oder IT-Forensiker hinzugezogen werden, um Spuren professionell zu sichern.

Ein gut durchdachter Alarmplan in der Schublade gibt Unternehmen die Sicherheit, in solchen Fällen strukturiert und rechtskonform zu handeln. Er stellt sicher, dass Verdachtsfälle ernst genommen, aber auch professionell und mit maximaler Diskretion geprüft werden – zum Schutz des Unternehmens, der Mitarbeiter und der Integrität der Geschäftsprozesse.

ZAU: Sie haben die IT-Forensik angesprochen. Wie erfolgversprechend sind solche Untersuchungen und können sich Unternehmen auf eine solche Untersuchung vorbereiten?

Malberg: Die forensische Untersuchung von IT-Geräten hat in den letzten Jahren enorm an Bedeutung gewonnen, insb. zur Klärung von Compliance-Sachverhalten. Solche Analysen sind oft entscheidend, um Manipulationen, unbefugte Datenzugriffe, Lösch- und Kopiervorgänge oder andere Verstöße nachzuweisen und auf dieser Basis rechtssichere Maßnahmen zu ergreifen. Damit eine Untersuchung effizient und erfolgversprechend durchgeführt werden kann, sollten Unternehmen bereits im Vorfeld organisatorische und technische Vorkehrungen treffen. Ein zentraler Aspekt ist die akribische Dokumentation darüber, welche Mitarbeiter über welche Geräte verfügen. Dabei sollte auch festgehalten werden, ob die Privatnutzung der dienstlichen Geräte erlaubt, geduldet oder ausdrücklich untersagt ist. Solche Regelungen sind idealerweise im Arbeitsvertrag, einer Betriebsvereinbarung oder ähnlichen unternehmensinternen Richtlinien detailliert festgelegt.
Ein weiteres essenzielles Thema ist die Verwaltung von Zugangsdaten. Die Passwörter zu den dienstlichen Geräten sollten bei der IT-Abteilung hinterlegt werden, um im Bedarfsfall – z.B. bei einer forensischen Untersuchung oder in Abwesenheit des betreffenden Mitarbeiters – Zugriff auf die Systeme sicherzustellen. Zudem sind moderne Geräte in der Regel verschlüsselt, sodass für den Zugriff auf gespeicherte Daten oft ein BitLocker-Schlüssel bzw. ein Wiederherstellungsschlüssel erforderlich ist. Ohne diesen ist eine forensische Untersuchung meist nicht möglich. Daher sollten Unternehmen sicherstellen, dass diese Schlüssel zentral dokumentiert sind.
Besonders in Fällen eines schwerwiegenden Verdachts sollte verhindert werden, dass der Mitarbeiter noch in der Lage ist, sein Smartphone oder seinen Computer zurückzusetzen. Entscheidend ist hierbei oft der Überraschungseffekt – der Mitarbeiter sollte unvermittelt aufgefordert werden, die Geräte sofort herauszugeben. Dies verhindert, dass er Daten löschen oder Manipulationen vornehmen kann. Anschließend sollten die Geräte sofort ausgeschaltet werden, um eine mögliche Fernlöschung durch Cloud-Dienste oder MDM-Systeme (Mobile Device Management) zu verhindern.

Unsere Detektei unterstützt Unternehmen dabei, sich optimal auf eine Untersuchung vorzubereiten. Wir stellen eine umfassende Checkliste zur Verfügung, die vor der forensischen Analyse der Geräte ausgefüllt werden sollte. Diese hilft dabei, alle relevanten technischen und rechtlichen Rahmenbedingungen zu erfassen und eine reibungslose Untersuchung sicherzustellen. Sie glauben gar nicht, wie oft das nach unseren Erfahrungen selbst in sehr umsatzstarken Unternehmen versäumt wurde.
Ein weiterer kritischer Punkt ist die Beachtung der Mitbestimmungsrechte des Betriebsrats, sofern ein solcher im Unternehmen existiert. Das frühzeitige Einbinden der Arbeitnehmervertretung kann spätere rechtliche Auseinandersetzungen vermeiden und die Akzeptanz solcher Maßnahmen erhöhen.
Durch eine frühzeitige und sorgfältige Vorbereitung können Unternehmen sicherstellen, dass eine IT-forensische Untersuchung nicht nur technisch erfolgreich durchgeführt wird, sondern auch rechtssicher und mit minimalen Reibungsverlusten abläuft.

ZAU: Einen Alarmplan zu haben, insb. bei Datenmissbrauch, ist sicherlich wichtig. Aber können in der heutigen Zeit überhaupt noch heimliche Maßnahmen ergriffen werden? Man hört immer wieder, dass es kaum noch Möglichkeiten gibt, z.B. sog. „Blaumacher" zu überführen.

Malberg: Laut der aktuellen Entscheidung des BAG kann der Einsatz eines Detektivs zur Überprüfung einer Arbeitsunfähigkeitsbescheinigung in der Praxis durchaus zulässig sein, wenn er als mildestes Mittel betrachtet wird und die Maßnahme im Verhältnis zum bestehenden Verdacht steht. Voraussetzung dafür ist, dass zunächst geprüft wird, ob der Beweiswert der AU-Bescheinigung erschüttert ist und keine weniger eingreifenden Alternativen wie das Einschalten des Medizinischen Dienstes der Krankenkassen zur Verfügung stehen. Sind diese Kriterien erfüllt, spricht nichts gegen eine entsprechende Beobachtung. Ein professionell agierender Wirtschaftsdetektiv, der mit den rechtlichen Rahmenbedingungen vertraut ist, stellt sicher, dass der Einsatz rechtskonform erfolgt. Dadurch können Unternehmen ihre berechtigten Interessen wahren und gleichzeitig das Risiko eines DSGVO-Verstoßes vermeiden, der mit Bußgeldern von bis zu 4% des weltweiten Jahresumsatzes des Unternehmens verbunden sein kann.

ZAU: Wie sieht es mit anderen Delikten aus? Diebstahl, Arbeitszeit- und Spesenbetrug sowie Korruption sind häufige wirtschaftskriminelle Delikte. Welche Methoden setzen Sie in der Detektivarbeit ein, um auch solche Fälle aufzuklären, und worauf müssen Unternehmen achten?

Malberg: Diese Delikte verursachen nicht nur erhebliche finanzielle Schäden, sondern untergraben auch das Vertrauen in die Integrität eines Unternehmens. Eine lückenlose Aufklärung ist entscheidend, um belastbare Beweise zu sichern und rechtssichere Maßnahmen zu ermöglichen. Dabei setzen wir sowohl auf heimliche Ermittlungsmaßnahmen als auch auf offene Sachverhaltsklärungen, um die Wahrheit ans Licht zu bringen.
Beim Verdacht auf Diebstahl sind Observationen ein zentrales Mittel der Aufklärung. Unsere Detektive beobachten verdächtige Mitarbeiter oder externe Dienstleister diskret und doku-

Foto: istockphoto/BeeBright

mentieren, ob tatsächlich Waren, Betriebsmittel oder andere Unternehmenswerte entwendet werden. Besonders betroffen sind Lagerhäuser, Produktionsstätten oder der Einzelhandel, in denen unbemerkte Entnahmen oft erst nach längerer Zeit auffallen. In einigen Fällen kann eine verdeckte Videoüberwachung erforderlich sein, um Täter auf frischer Tat zu überführen. Diese Maßnahme ist jedoch nur restriktiv einzusetzen, da hier verschiedene rechtliche Aspekte unbedingt zu beachten sind. In anderen Fällen kann auch eine offene Befragung von Mitarbeitern oder eine gezielte Kontrolle von Lagerbeständen bereits wichtige Hinweise liefern. Unser oberstes Ziel ist es dabei, alle arbeits- und datenschutzrechtlichen Vorgaben einzuhalten, um sicherzustellen, dass die gewonnenen Beweise auch vor Gericht Bestand haben.

Arbeitszeit- und Spesenbetrug sind in vielen Unternehmen ein weit verbreitetes Problem und gehen oft Hand in Hand. Unsere Quote überführter Spesen- und Arbeitszeitbetrüger liegt bei nahezu 100%. Besonders häufig kommt es zu Manipulationen im Außendienst – hier machen wir nach unseren Erfahrungen die meisten Fälle von Arbeitszeitbetrug aus. Viele Außendienstmitarbeiter geben an, sich bei Kundenbesuchen oder auf Geschäftsreisen zu befinden, während sie tatsächlich privaten Tätigkeiten nachgehen oder gar nicht arbeiten. In solchen Fällen sind diskrete Observationen die effektivste Methode, um einen Betrug gerichtsfest nachzuweisen. Parallel dazu können offene Sachverhaltsklärungen, wie die Nachverfolgung von Terminen oder der Abgleich von Reisekosten mit tatsächlichen Kundenbesuchen, oft weitere Beweise liefern. Doch die wenigsten Unternehmen wollen aus verständlichen Gründen bei ihren Geschäftspartnern direkt nachfragen, ob der Mitarbeiter auch wirklich vor Ort war.

Die Korruption stellt eine besonders anspruchsvolle Form der Wirtschaftskriminalität dar, da Bestechung und unzulässige Absprachen meist im Verborgenen bzw. sehr engen Kreis der Mitwisser stattfinden. Aber auch hier können z.B. wirtschaftliche Verflechtungen zwischen Mitarbeitern und externen Geschäftspartnern erkannt werden. Ungewöhnliche Preisgestaltungen, auffällige Rabattierungen oder manipulierte Rechnungen sind oft erste Hinweise auf korrupte Strukturen. Um solche Vergehen aufzudecken, setzen wir auf gezielte verdeckte Ermittlungen und forensische Analysen von Geschäfts- und Finanzunterlagen. Je nach Situation kann es jedoch auch sinnvoll sein, offene Sachverhaltsklärungen durchzuführen, etwa durch gezielte Mitarbeiterinterviews oder den Abgleich von internen Vorgängen mit externen Vertragsabschlüssen.

Die erfolgreiche Aufklärung solcher wirtschaftskriminellen Delikte erfordert eine sorgfältige Kombination aus heimlichen Ermittlungsmethoden und offenen Befragungen sowie einer präzisen Analyse der relevanten Unterlagen. Unternehmen sollten Verdachtsfälle frühzeitig untersuchen lassen, um finanzielle Schäden zu minimieren und langfristige Reputationsverluste zu vermeiden. Unsere Erfahrung zeigt: Je professioneller eine Untersuchung geplant wird, desto höher sind die Chancen, den Sachverhalt vollständig und rechtssicher aufzuklären.

ZAU: Vielen herzlichen Dank für das Gespräch!

Das Interview führte Silvio Fricke (BVAU e.V.).