JETZT MAL EHRLICH

Wenn Mitarbeiter den eigenen Arbeitgeber bestehlen, zerbricht nicht nur Vertrauen – auch die Existenz des Unternehmens kann auf dem Spiel stehen. Einen Ausweg bieten nur wirksame Kontrollen.

Für die Eigentümer des Schlossherstellers bricht eine Welt zusammen, als ihnen der langjährige Prokurist eröffnet, dass er Firmengeld veruntreut hat. Insgesamt 26 Millionen Euro. Dabei haben sie dem erfahrenen und seriösen Mann vertraut, ihm die Kontrolle über alle Unternehmenskonten gegeben. Noch dazu war er der strenggläubigen Familie über die Kirchengemeinde empfohlen worden. Und jetzt rutscht das Unternehmen seinetwegen nur knapp am Zusammenbruch vorbei.

Das Schicksal des traditionsbewussten Familienunternehmens zeigt deutlich, wie zerbrechlich selbst über Jahre gewachsenes Vertrauen in der Geschäftswelt sein kann. Und es wirft die Frage auf, warum es bei dem Hersteller von Sicherheitstechnik mit mehr als 3.000 Mitarbeitern keine internen Kontrollen gab, um den Betrug zu verhindern.

Der Prokurist hatte leichtes Spiel. Er nutzte ein zuvor inaktives Bankkonto, um immer wieder Kredite aufzunehmen, mit denen er kurzfristigen Kapitalbedarf der Firma decken wollte – so erklärte er es zumindest der Bank. In Wirklichkeit flossen die Millionen an ihn. Das ging jahrelang gut und wäre womöglich weiter geglückt, wenn die Bank nicht 2015 den Geldhahn zugedreht und eine Rückzahlung gefordert hätte. In diesem Moment brach das System zusammen – und auch das Vertrauen der Firma in den Prokuristen, der seit 27 Jahren dort beschäftigt war.

VORSICHT IST PROGRAMM
Strikte Regeln für Mitarbeiter schützen Unternehmen gegen Angriffe aus dem Cyberspace.

DER GANZ NORMALE LEICHTSINN

Das Beispiel des Schlossherstellers ist drastisch, aber keinesfalls die Ausnahme. Dass unendliches Vertrauen im Berufsleben leichtsinnig ist, lässt sich mit Zahlen belegen. Nach einer Studie der Unternehmensberatung EY (Ernst & Young) ist fast jeder vierte befragte Manager bereit, unethisch zu handeln, wenn es seiner Karriere dient. Dabei zeigen gerade Teilnehmer im Alter zwischen 25 und 34 Jahren besonders wenig Unrechtsbewusstsein.

Diese Haltung schlägt sich in der Geschäftswelt offenbar nieder. Das Beratungshaus PwC fand heraus, dass etwa die Hälfte aller befragten deutschen Unternehmen innerhalb von zwei Jahren mindestens einmal mit einem signifikanten Fall von Wirtschaftskriminalität konfrontiert wurde. Dabei ist die Dunkelziffer hoch. „Wirtschaftskriminalität gehört zu den Deliktsbereichen, bei denen Taten nur entdeckt werden, wenn auch kontrolliert wird", sagt Steffen Salvenmoser, Partner bei PwC und Experte für Wirtschaftskriminalität. Viele Fälle bleiben auch deshalb verborgen, weil Unternehmen nicht wollen, dass die Öffentlichkeit davon erfährt. Sie schlagen dennoch zu Buche. Allein da, wo die Polizei aktiv wurde, richteten Wirtschaftskriminelle laut BKA 2017 einen Schaden von 3,7 Milliarden Euro an.

MORALISCHER KOMPASS AUSSER BETRIEB

Unternehmen, die sich vor kriminellen Mitarbeitern schützen wollen, stehen vor einer schwierigen Situation. Denn meistens handele es sich nicht um gewöhnliche Kriminelle, sagt Bernd Noll. Der Pforzheimer Wirtschaftsprofessor erforscht die Profile von Wirtschaftskriminellen. Viele von ihnen bleiben lange unverdächtig. „Sie hatten weder eine schwere Kindheit, noch sind sie auf die schiefe Bahn geraten oder durch Straftaten in Erscheinung getreten."

Doch was treibt diese Täter an? Warum schädigen sie ihre Firma und bringen ihre eigene Existenz in Gefahr? Auslöser sei oft ein Defekt des moralischen Kompasses, sagt Noll, verursacht durch einen Wertebruch wie Scheidung, schwere Krankheit oder ein anderes einschneidendes Erlebnis, das auch im Verborgenen liegen kann.

Verschwendungssucht ist die mögliche Folge. Der Prokurist kaufte laut Berichten eine Yacht für 3 Millionen Euro, richtete sich eine Villa mit heizbaren

Außenwegen für 7 Millionen Euro ein. Er gönnte sich erlesene Weine und in den Zimmern standen handgeschreinerte Möbel aus Tropenholz. Kurioserweise fiel niemandem auf, dass sich der Mann diese Besitztümer von seinem Gehalt gar nicht leisten konnte.

In seinen Untersuchungen über Tätertypen fand Noll heraus, dass neben chronischem Geldmangel auch Habgier ein häufiges Motiv darstellt. Dass sich Mitarbeiter in der Firma bedienen, kann aber auch an der Angst vor dem sozialen Abstieg liegen, etwa wenn sie sich durch ihren Lebensstandard fehlende Anerkennung von Eltern oder Ehepartnern verdienen wollen. Ein weiteres verbreitetes Motiv ist Rache – zum Beispiel wenn sich ein Angestellter bei einer Beförderung übergangen fühlt.

Der angeklagte Prokurist jedenfalls erweckte vor Gericht den Eindruck, seine Motive für die Tat verdrängt zu haben. Er wisse nicht mehr, wann und warum er begonnen habe, Geld für private Zwecke abzuzweigen. Seine Absicht sei es gewesen, die Beträge irgendwann zurückzuzahlen. „Tatsächlich habe ich aber ab einem gewissen Zeitpunkt Maß und Überblick verloren", sagte er in der Verhandlung laut Süddeutscher Zeitung. Das Gericht ließ diese Entschuldigung nicht gelten und verurteilte den Mann in diesem Frühjahr zu sechs Jahren Haft.

„ES HAT BLÖDERWEISE GEKLAPPT."

Maßlosigkeit – diese Begründung passt auch auf andere Fälle, in denen Angestellte das Vertrauen ihrer Arbeitgeber missbraucht haben. Eine 35-jährige Veranstaltungsmanagerin aus Frankfurt sollte regelmäßig Rechnungen an Kunden verschicken. Sie versah die PDF-Dokumente einfach mit ihrer eigenen Bankverbindung. Das Geld der Kunden landete auf dem Privatkonto der Frau. Ihre Erklärung vor Gericht wirkte entwaffnend. „Ich habe da so rumprobiert und es hat blöderweise geklappt", sagte sie laut Frankfurter Rundschau. Dann machte sie es immer wieder. In 21 Fällen flossen insgesamt 34.000 Euro in ihre Tasche.

Der leitende Angestellte, der gegen Schmiergeld von Lieferanten überhöhte Rechnungen bezahlt, der Arbeiter vom Recyclinghof, der wertvolles Metall mitgehen lässt oder der Kellner, der ein paar Bierfässer mehr bestellt und auf eigene Rechnung verkauft – diese Fälle der letzten Jahre haben eines gemeinsam: Die Täter wurden unzureichend kontrolliert. „Vertrauen muss Grenzen haben", sagt der Jurist Rüdiger Kirsch, bei Euler Hermes für Vertrauensschäden zuständig. Für ihn ist mangelnde Kontrolle oft sogar der Auslöser dafür, dass Mitarbeiter in die Illegalität rutschen. „Wer alle Freiheiten genießt, entwickelt über die Jahre sein eigenes Verständnis von Gerech-

ABSOLUT VERTRAULICH!

Unter falscher Identität bringen Cyber-Gangster Angestellte in Firmen dazu, ihnen ein Vermögen zu überweisen.

Diese E-Mail fällt dem Buchhalter des Unternehmens sofort ins Auge. „Absolut vertraulich" liest er in der Betreffzeile. Absender ist sein Geschäftsführer. Eine vertrauliche Übernahme stehe an, für die ein hoher Geldbetrag sehr schnell auf ein ausländisches Konto überwiesen werden müsse. Mit niemandem, auch nicht mit ihm, dem Chef, dürfe er darüber reden. Wenn Kollegen von dem Deal erführen, sei das sensible Geschäft bedroht. Der Buchhalter fühlt sich unter Druck, ist aber auch geschmeichelt, da der Geschäftsführer ihm vertraut. Er überweist die Summe. Erst später wird ihm klar, dass er Betrügern aufgesessen ist.

Was sich unglaublich anhört, passiert regelmäßig in deutschen Unternehmen. Laut einer Umfrage des Beratungshauses PwC wurden 40 Prozent aller größeren deutschen Unternehmen innerhalb von 24 Monaten zumindest einmal Ziel einer Attacke, die als „Fake President" bezeichnet wird. In 5 Prozent der Fälle waren die Angreifer erfolgreich.

Der Schaden kann in die Millionen gehen. Und das Geld ist so gut wie immer verloren. Es wird im Zielland auf mehrere Konten in anderen Weltregionen weiter verteilt. Die Polizei kann die Zahlungsströme dadurch kaum mehr nachverfolgen. Das Unternehmen bleibt auf dem Schaden sitzen.

Erschwerend kommt hinzu, dass es organisierte, internationale Banden sind, die mit dem Trick Geld erschwindeln. Sie planen ihre Taten gründlich, Informationen beziehen sie aus Handelsregisterauszügen, Firmen-Websites und durch soziale Netzwerke, in denen die Betrogenen nicht nur ihren beruflichen Werdegang, sondern oft auch private Details preisgeben. Das macht es für die Täter einfach, sich Vertrauen zu erschleichen.

tigkeit." Und das müsse nicht immer mit dem des Unternehmens oder des Gesetzgebers übereinstimmen, sagt Kirsch und schildert den Fall eines internationalen Konzerns, der bei seiner mexikanischen Tochter acht Jahre lang keinen Prüfer aus der internen Revision vorbeischickte. Die laxe Kontrolle wirkte wie Gift. Der Landeschef zwackte Millionen für sich selbst ab. Über lange Zeit bemerkte den Schwindel niemand.

DER RAHMEN PRÄGT DEN MENSCHEN

Für Firmen ist es unmöglich, selbst mit teuren Auswahlverfahren zu erkennen, ob der leitende Mitarbeiter kriminelles Potenzial hat, sagt Experte Noll. Das habe auch mit den Stellenprofilen zu tun. „Es gibt Unternehmen, die suchen gezielt Manager, die nicht nur entscheidungsfreudig und hartnäckig sind, sondern auch bereit, bis an die Grenzen des Rechts zu gehen." Eigenschaften, die sich in anderer Ausprägung auch bei Wirtschaftskriminellen wiederfänden. Außerdem prägten auch die Rahmenbedingungen im Unternehmen die Menschen, die dort arbeiteten. Wenn die Verhältnisse kriminelle Energie begünstigten, nütze das beste Bewerbungsverfahren nichts.

Immer weniger Firmen sind bereit, Fehlverhalten ihrer Mitarbeiter als Kollateralschaden zu verbuchen. Gleich nach Auffliegen des Betrugs begann der geschädigte Schlosshersteller, ein Compliance-System aufzubauen – genauso wie viele andere deutsche Unternehmen in den vergangenen Jahren. Diese Kontrollmechanismen richten sich in erster Linie gegen Datenschutzverletzungen und Korruption, werden aber schrittweise auf weitere Deliktfelder ausgedehnt – wie Vermögensdelikte, Geldwäsche oder Insiderhandel. Die Programme haben vor allem in größeren Unternehmen dazu geführt, dass die Zahl der Verstöße auf einzelnen Feldern abnimmt. Kleinere Unternehmen zeigen sich hingegen noch reserviert, weil die Chefs der Ansicht sind, dass sie ihren Beschäftigten vorbehaltlos vertrauen können.

ABSOLUTEN SCHUTZ GIBT ES NICHT

Kontrolle ist auch wichtig, wenn die Gefahr nicht im Unternehmen, sondern von außen droht. Beispielsweise über das Internet. Nach Zahlen von PwC haben 46 Prozent der befragten deutschen Unternehmen in den vergangenen 24 Monaten eine Cyber-Attacke festgestellt. Die Täter spähen zum Beispiel Passwörter und andere sensible Daten aus, sie sabotieren Computer oder verletzen Patent- und Markenrechte. Eine besonders beliebte Masche nennt sich „Fake President". Internetbetrüger geben sich dabei als leitende Manager oder ihre Vertreter aus und veranlassen Mitarbeiter dazu, hohe Geldbeträge zu überweisen (siehe Kasten Seite 5).

Strikte Regeln für die Mitarbeiter stellen zwar auch gegen Cyber-Attacken einen guten Schutz dar. Aber es gibt Grenzen. Kontrollen im Unternehmen müssen wirksam sein, aber nicht so streng, dass eine Kultur des Misstrauens entsteht, warnt Noll. „Dadurch würde das Unternehmen auf andere Weise geschädigt – was ebenfalls nicht wünschenswert ist." EH