

Studien und Analysen

Identitätsmanagement und Mitarbeiterführung gegen Wirtschaftskriminalität

Gegen Innentäter hilft Kontrolle nur in Grenzen

Elmar Török, Bits und Bites

Die Studie „Wirtschaftskriminalität 2007“ von Pricewaterhouse Coopers (PwC) und der Martin-Luther-Universität Halle-Wittenberg zeigt ein komplexes Bild von Fällen der Bespitzelung, des Datendiebstahls und des Informationsmissbrauchs in deutschen Unternehmen. Sie lässt deutlich erkennen, dass Wirtschaftskriminalität nicht mit einfachen Mitteln aus der Welt zu schaffen ist. Die Abwehr muss den Menschen in den Mittelpunkt stellen – technisch bedeutet dies den Einsatz professionellen Identitätsmanagements, auf der sozialen Seite geschickte Mitarbeiterführung.

Fast jedes zweite deutsche Unternehmen ist in den vergangenen zwei Jahren Opfer von Wirtschaftskriminalität geworden. Dabei sind nicht etwa Hacker, Phisher oder gedungene Schnüffler die Hauptverursacher der Straftaten in Sachen Wirtschaftsspionage. Jede zweite Straftat, so die Studie „Wirtschaftskriminalität 2007“, wird von den eigenen Mitarbeitern der Unternehmen begangen. Dies ist sicherlich ein erschreckendes Ergebnis.

Es lohnt sich aber, genau hinzusehen, wie der Studie zufolge das Täterprofil aussieht: „Die Täter sind überall auf der Welt zumeist männlich (87 Prozent), überdurchschnittlich gebildet, etwa 20 Prozent gehören zum Senior- bzw. Topmanagement, sie sind in der Regel zwischen 30 und 50 Jahre alt und seit mehreren Jahren im Unternehmen beschäftigt (Deutschland 10 Jahre) und seit längerem in ihrer betrieblichen Position tätig gewesen (Deutschland 8 Jahre), wenn es zu unternehmensschädigenden Verhaltensweisen kommt.“

Der gute Manager als Feind

Die Autoren der Untersuchung hätten auch schreiben können: „Bei Wirtschaftskriminellen handelt es sich meistens um erfolgreiche Manager, die sich in ihrer Organisation durchsetzen konnten.“ So mag es ein Wirtschaftsberatungsunternehmen aber verständlicherweise ungern formulieren, weshalb es das Ergebnis lieber so ausdrückt: „Langjährigen Mitarbeitern mit viel Erfahrung und hohem Ansehen kann kein besonderer Vertrauensbonus entgegengebracht werden. Vielmehr ist der typische Wirtschaftsstraftäter in Unternehmen empirisch gesehen der normale, sozial angepasste Mitarbeiter bzw. Manager und daher nur schwer mit Hilfe prognostischer Verfahren zu identifizieren.“

Und auch die externen Täter sind gewissermaßen „Insider“: „Innerhalb der Gruppe der externen Straftäter drohen die größten Risiken durch Kunden und Mandanten des Unternehmens sowie Geschäftspartner (63

Prozent). Insgesamt gesehen werden Wirtschaftsdelikte folglich nur selten durch Unbekannte begangen, zu denen keine Geschäftsbeziehungen bestehen, sondern durch Personen, denen die Unternehmen zumindest ein gewisses Vertrauen entgegenbringen.“

Alle sind verdächtig – oder eben nicht

Diese Erkenntnisse haben fundamentale Konsequenzen für mögliche Abwehrstrategien. Das verbreitete Lamento gerade von Firmenleitern über „die Mitarbeiter“, die viel zu viele Freiheiten hätten und die man besser überwachen müsse, entbehrt einer festen Grundlage, denn die Feinde einer Organisation können auf jedem Level angeordnet sein – gerade auch auf der Leitungsebene und im Kreis von Personen, die aus heutiger Sicht mit acht bis zehn Jahren extrem lange in einem Unternehmen verweilen. Durch Position, Erfahrung und das Anhäu-

fen von Insider-Kenntnissen haben alteingesessene Topmanager außerdem das größte Potenzial, Schaden anzurichten.

Mit den Resultaten steht auch fest, dass es im Unternehmen keinen Rang und keine Position gibt, der man pauschal eine Kontrollfunktion zuweisen könnte. Auf jeder Hierarchieebene sollte jeder als so verdächtig oder unverdächtig behandelt werden wie jeder andere. Wollte man auf diese Erkenntnis mit passenden Kontrollmechanismen reagieren, hätte man schnell ein ähnlich sozial und ökonomisch ineffektives Misstrauenssystem wie in den untergegangenen Oststaaten zusammen. Übrigens gibt es hier auch eine kuriose Passage in der Studie „Wirtschaftskriminalität 2007“: Die Autoren sehen sich in der Pflicht, ein zunächst paradoxes und entmutigendes Phänomen zu erklären, nämlich den statistisch auffälligen anfänglichen Anstieg von Wirtschaftsvergehen nach einer Einführung von Kontrollmechanismen, zu denen etwa die Installation von Verfahren für das „Whistleblowing“ gehört. PwC und die Universität Halle-Wittenberg meinen, die Verschlechterung nach Kontrollverstärkungen beruhe darauf, dass einfach mehr Fälle aufgedeckt würden. Psychologen würden hier zu Recht fragen, ob man nicht auch hätte prüfen müssen, ob die Kontrolle selbst nicht eine Abwendung der Mitarbeiter von eigenen Unternehmen zur Folge haben könne – innere Kündigung als Reaktion auf Misstrauen mit der Folge einer gestiegenen Bereitschaft, gegen das Unternehmen zu arbeiten. Dass psychologische Effekte auch einberechnet werden müssen, belegt die Studie ja selbst, indem sie nachweist, dass die pure Existenz ethischer Unternehmensrichtlinien zu einer tatsächlich messbaren Reduktion von Wirtschaftsspionagefällen bei Unternehmen führt, die solche „Guidelines“ besitzen. Auch die Firmenkultur spielt der Studie zufolge eine wichtige Rolle. Man darf folgern: Ein Unternehmen, dass mit

seinen Mitarbeitern fair umgeht, tut einen wichtigen Schritt hin zu mehr Informationssicherheit.

Was die adäquate IT-Sicherheitstechnik für die beschriebene Situation in den Unternehmen betrifft, so zieht wohl das Unternehmen Econet in einer vor kurzem verbreiteten Stellungnahme die richtigen Schlüsse aus der Studie: Wer sein Unternehmen umfassend gegen die Gefahren von Wirtschaftsspionage und anderer Delikte absichern wolle, so meinen die Spezialisten des Provisioning-Anbieters, darf den gesicherten Umgang mit Benutzerkonten und deren Zugriffsrechten nicht vergessen. Kern sinnvoller Maßnahmen gegen Industriespionage sei es, dafür zu sorgen, dass jeder Mitarbeiter nur auf die Daten zugreifen könne, die er für seine Arbeit benötige und für die er autorisiert sei. So sollten beispielsweise Forschungs- und Entwicklungsdaten nicht für Praktikanten oder unberechtigte Mitarbeiter zugänglich sein. Mit einem weiteren Blick auf die nun schon mehrfach zitierte Studie darf man ergänzen: Personaldaten sollten nur Personalmanagern zur Verfügung stehen, Lagerdaten nur den Beschaffern und so weiter. Die simple Beschränkung der Zugriffsrechte, die man auf der physischen Ebene durch Türen und Schlüssel herstellt, muss einfach auch bei den IT-Ressourcen durchgesetzt werden. Weil solche Mechanismen nicht primär, sondern nur sekundär und für den Fall eines notwendigen Nachweises auf Kontrolle ausgerichtet sind, erzeugen sie auch weniger Widerstände als direkte Mitarbeiter-Kontrollsysteme.

Econet führt weiter aus, dass die kontrollierte Vergabe und zentrale Verwaltung von Zugriffsrechten mithilfe einer Identity-Management-Lösung die notwendigen Prozesse der Service-Bereitstellung und der Rechtevergabe transparent, beherrsch- und steuerbar mache. Unkontrollierte Rechteanhäufungen ließen sich vermeiden, und der zielgerichtete Rechteentzug funktioniere besser. Als System richtlinien-

gesteuerter Rechtevergabe verankert Identity Management die Sicherheit in der Struktur eines Unternehmens und sorgt damit für eine gewisse Unabhängigkeit der Schutzfunktionen von Personen und Positionen. Econet weiter: „Bei unternehmensweit gültigen Berechtigungskonzepten mit zugehörigen. Genehmigungs- und Freigabeprozessen erteilt nicht länger und womöglich ‚auf Zuruf‘ die Administration Berechtigungen auf eine bestimmte Dateiablage. Stattdessen entscheiden die Verantwortlichen in den Fachabteilungen, wer worauf zugreifen darf. Regelbasierte Prozesse, die die Einhaltung der Sicherheitsrichtlinien garantieren, ermöglichen sichere Self-Services über standardisierte und automatisch ablaufende Genehmigungs-Workflows mit Mehr-Augen-Prinzip.“

Compliance ist möglich

Hier findet sich dann auch genau jene Überwachungsfunktionalität, die aus Compliance-Gründen heute fast immer implementiert werden muss: „Durch die fest definierten und automatisch ablaufenden Prozesse ist [...] eine lückenlose Revision aller Rechteinträge und Genehmigungsschritte möglich. [...] Berechtigungs-Audits geben jederzeit und auf Knopfdruck Aufschluss darüber, welcher User auf welche Daten Zugriffsrechte besitzt, oder welche Mitarbeiter für eine bestimmte Dateiablage berechtigt sind.“

Die Scheu davor, sich des teils vermeintlich und teils wirklich komplexen Themas Identity Management anzunehmen, sollten Unternehmen also tatsächlich möglichst bald ablegen. Identitätsmanagement entwickelt sich zur Basis der Informationssicherheit der Zukunft und löst viele Probleme des Datenschutzes und der Bedrohungen durch Wirtschaftskriminalität direkter, als es andere Konstrukte wie komplexe Filteransätze zur Data-Loss-Prevention tun könnten. ■