

Gaunereien verhindern

Betriebskriminalität: Nur zehn Prozent der Fälle werden erkannt und davon kann wiederum nur ein Zehntel wiedergutmacht werden.

Gastkommentar

••• Von Roland Beranek

STEYR. Viele Unternehmen befinden sich in der Blase, dass Betrug und Untreue sie nicht betreffen können. In der Realität kommt Betriebskriminalität aber sehr häufig vor. So gehen Studien davon aus, dass nur zehn Prozent der Fälle aufgedeckt werden und davon nur bei zehn Prozent der Schaden wieder gut zu machen ist.

Zudem folgen für die betroffenen Unternehmen häufig Imageprobleme, wie bekannte Fälle zeigen. Auch ist aufgrund der Haftung von Geschäftsführern (§ 22, GmbH-Gesetz) ein entsprechendes Rechnungswesen und internes Kontrollsystem für jedes Unternehmen ein Pflichtprogramm.

Vier-Augen-Prinzip – und mehr Basis jeder Rechnungskontrolle ist das Vier-Augen-Prinzip, das das Risiko von Fehlern und Missbrauch reduzieren soll.

Auch sollte nicht der Rechnungsfreigeber eine Rechnung überweisen dürfen. In der Praxis werden noch in vielen Unternehmen diese beiden einfachen Standards nicht eingehalten.



© BMD

Schon mit einer Eingangsrechnungskontrolle (ER-Kontrolle) könnten allerhand Betrügereien verhindert werden. Erster Schritt ist daher die Festlegung eines Workflows. Dieser definiert, welchen Weg bestimmte Rechnungen nehmen müssen, wer die Rechnungen zur Bearbeitung bekommt und wer sie schließlich zur Zahlung freigibt. Eingangsrechnungen in Papierform werden eingescannt, digitale Rechnungen ins System importiert und dann auf digita-

le Rundreise geschickt. Die zuständigen Mitarbeiter erhalten eine Aufgabe und per Mail eine Benachrichtigung. Auf diese Weise erfolgt die Erfassung der Eingangsrechnungen mit Eingabe der Daten, Kontierung und Freigabe. Schließlich steht einer Überleitung in die Buchhaltung nichts mehr im Wege.

Stammdaten-Check

Bei Eingangsrechnungen sollte immer ein Abgleich mit dem Echtzeit-Update Compass-

Realtime einhergehen, das die Stammdaten österreichischer Unternehmen direkt aus den Firmenbuchdaten des Compass-Verlags ausliest und in das BMD-Rechnungswesen übernimmt.

Damit entfällt die manuelle Eingabe von Stammdaten, wird das Risiko von Eingabefehlern vermindert und man erhält einen Hinweis, wenn Daten von rechtskräftig festgestellten Scheinunternehmen oder auch „erfundene Lieferanten“ in die Stammdaten geführt werden.

Mit dem Monitoring entgeht auch keine Änderung der Stammdaten mehr. Automatisch werden die Personendaten mit der Compass-Datenbank abgeglichen. Gefundene Änderungen werden in Form einer Aufgabe an den zuständigen Mitarbeiter gemeldet. Diese wertvollen Tipps können wohl nicht alle Gaunereien verhindern, aber zumindest die häufigsten.

Vertrauen ist gut, Kontrolle geht schneller!

Roland Beranek leitet die BMD Akademie. BMD ist der führende österreichische Hersteller hochwertiger Business-Software mit rund 28.000 Kunden.

www.bmd.com

Die Datenklauer gehen um

Nur ein Drittel der Firmen meldet Cyberangriffe.

WIEN. Zwei Drittel (66%) der heimischen Unternehmen erlitten in den vergangenen zwölf Monaten einen Cyberangriff – um fünf Prozent mehr als im Vorjahr. 2016 gab lediglich die Hälfte an, Opfer einer Cyberattacke gewesen zu sein (49%).

Phishing und Malware sind und bleiben die häufigsten Angriffsarten aus der virtuellen Welt. Knapp die Hälfte der be-

fragten Firmen (jeweils 47%) kam mit diesen Attacks in Berührung. Hier lässt sich ein eindeutiger Anstieg erkennen: 2018 waren 24% der Unternehmen von Phishing und 22% von Malware betroffen.

Zu diesen Ergebnissen kommt die Studie „Cyber Security in Österreich“ von KPMG, an der mehr als 340 Vertreter österreichischer Unternehmen teilnahmen. (pj)



© PantherMedia/Mohamad Razi Bin Husin

Cyberattacken sollten von den Firmen so rasch wie möglich gemeldet werden.