8 Tipps zur Vermeidung von Betrug in Ihrem Unternehmen

WHISTLEBLOWER PARTNERS

Betrug in Unternehmen ist ein großes und wachsendes Problem, da die Globalisierung, die Digitalisierung und die zunehmende Komplexität in vielen Bereichen, ebenso wie die Coronapandemie, das Risiko erhöht haben.

Betrug in Unternehmen ist ein größeres Problem, als viele Menschen denken. Ein Unternehmen kann durch internen Betrug bis zu fünf Prozent seines Jahresumsatzes verlieren. Dies zeigen internationale Studien. Auch dänische Unternehmen erleben einen starken Anstieg der finanziellen Cyberkriminalität, bei der Mitarbeiter dazu gebracht werden, Geld an externe Kriminelle zu zahlen.

Natürlich sind Kontrollen unerlässlich, aber auch wenn beispielsweise Audit-Tools einen großen Beitrag leisten können, ist die Lösung leider nicht so einfach. Genauso wichtig ist eine gute Arbeitskultur, in der die Mitarbeiter ermutigt und beeinflusst werden, die richtigen Entscheidungen zu treffen, damit sie keine bewussten oder unbewussten Fehler machen, die das Unternehmen teuer zu stehen kommen können.

Seit dem Ausbruch der Covid-19-Pandemie ist die Heimarbeit zur neuen Normalität geworden, und dieser Trend wird sich wahrscheinlich fortsetzen. Dadurch sind auch neue Risiken für die Unternehmen entstanden.

Im Folgenden sind einige Punkte aufgeführt, die im Zusammenhang mit Unternehmensbetrug zu beachten sind:

1. **Verstärkte Kontrolle und Sensibilisierung für die Verfahren im Unternehmen**

Weniger Mitarbeiter im Büro können dazu führen, dass die internen Abläufe gelockert werden, um einen reibungslosen Ablauf des Alltags zu gewährleisten. Passwörter können von Kollegen gemeinsam genutzt werden, und es besteht die Gefahr, dass ein und dieselbe Person Rechnungen genehmigen, Kreditorendaten ändern und Zahlungen genehmigen kann.
Dies schafft Möglichkeiten für Finanzbetrug, bei denen der Betrüger seine Spuren verwischen kann. Wenn dies in geringem Umfang über einen langen Zeitraum hinweg geschieht, kann der Betrug ein beträchtliches Ausmaß annehmen, bevor er – vielleicht – entdeckt wird.
Die Unternehmen sollten daher die internen Verfahren nicht lockern, auch wenn die Mitarbeiter zunehmend individuell von zu Hause aus arbeiten und die Kontrolltätigkeit ständig risikogerecht „regulieren“.

2. **Hohes Bewusstsein für Hackerangriffe, Phishing und andere Cyberkriminalität**

Kriminelle versuchen zunehmend, Unternehmen über Telefonanrufe (Vishing), Textnachrichten (Smishing) oder E-Mails (Phishing) persönliche Codes oder Informationen zu entlocken. Der

Betrüger gibt sich oft als Mitarbeiter einer Bank oder eines Geschäftspartners des Unternehmens, einer Behörde oder eines Zahlungsdienstleisters aus.
Bei einigen Unternehmen wird das E-Mail-System direkt gehackt, andere IT-Betrüger nutzen Phishing, bei dem ein Klick auf einen Link oder eine Datei in einer gefälschten E-Mail Zugang zu den IT-Systemen des Unternehmens verschaffen kann.
Es ist sehr wichtig, den Mitarbeitern zu vermitteln, dass sie unaufgeforderten Kontakten oder E-Mails, die ungewöhnlich oder seltsam aussehen, skeptisch gegenüberstehen sollten, und die Mitarbeiter sollten angewiesen werden, niemals persönliche Informationen oder Codes preiszugeben. Im Zweifelsfall sollten sich die einzelnen Mitarbeiter immer an die IT-Abteilung des Unternehmens wenden – besser einmal zu viel als zu wenig.

3. Vermeiden Sie CEO Fraud

CEO Fraud liegt vor, wenn ein Angestellter dazu verleitet wird, eine falsche Rechnung zu bezahlen oder eine nicht genehmigte Überweisung vom Firmenkonto auf ein Konto des Betrügers vorzunehmen. Der Betrüger gibt sich in diesem Fall als Führungsperson des Unternehmens aus.
Es ist wichtig, im Unternehmen Verfahren für die Bezahlung von Rechnungen und Überweisungen einzuführen und dafür zu sorgen, dass alle Anfragen, die nicht normal sind, überprüft werden, unabhängig davon, wie dringend die Überweisung laut E-Mail ist. Ein Anruf beim CEO kann oft den ganzen Betrug aufdecken und das Unternehmen vor großen Verlusten bewahren.

4. Vermeiden Sie Rechnungsbetrug

Beim Rechnungsbetrug gibt sich der Betrüger als Kunde oder Lieferant des Unternehmens aus und bittet darum, künftige Rechnungen über ein neues Bankkonto zu begleichen, das dem Betrüger gehört.
Es muss sichergestellt werden, dass die zuständigen Mitarbeiter über diese Art von Betrug informiert sind und wissen, wie sie ihn vermeiden können. Es ist daher unerlässlich, das für die Bezahlung der Rechnungen zuständige Personal anzuweisen, diese stets auf Unregelmäßigkeiten zu prüfen, feste Verfahren für die Abwicklung manueller Zahlungen festzulegen und die Rechtmäßigkeit der Zahlungsanträge zu überprüfen.
Es ist von Vorteil, ein automatisiertes Zahlungssystem zu verwenden, um die Anzahl der manuellen Zahlungen auf ein Minimum zu beschränken.

5. Vorsicht vor Betrug bei Änderung der Bankverbindung

Es ist wichtig, sich bewusst zu machen, dass es diese Art von Betrug bei der Änderung von Bankdaten gibt, und dass dieses Wissen an die Funktionen innerhalb des Unternehmens weitergegeben wird, die potenzielle Opfer solcher Änderungen von Bankdaten sein könnten.

Erhält das Unternehmen eine E-Mail, in der eine Änderung der Bankverbindung mitgeteilt wird, sollte der Lieferant stets angerufen und um eine Bestätigung der Richtigkeit der Kontoänderung durch den üblichen Ansprechpartner des Unternehmens gebeten werden.

6. Vermeiden Sie Mehrwertsteuerbetrug

Es besteht ein erhebliches Risiko, dass Unternehmen beim Handel mit Mehrwertsteuerkarussellen dem Mehrwertsteuerbetrug zum Opfer fallen. Mehrwertsteuerkarusselle sind gekennzeichnet durch den grenzüberschreitenden Handel mit Waren oder Dienstleistungen. In der Regel werden die Waren über einen Strohmann gehandelt, der beim Weiterverkauf der Waren keine Mehrwertsteuer ausweist oder abführt. Die Waren werden dann über einen oder mehrere Zwischenhändler gehandelt, bevor sie wieder aus Dänemark herausgeschickt werden und das Karussell weiterläuft.
Bei diesen Zwischenhändlern kann es sich um echte dänische Unternehmen handeln. Dies bedeutet, dass dänische Unternehmen leicht in eine Falle tappen können, die zu finanziellen Verlusten führen kann, z. B. in Form von entgangenen Mehrwertsteuerabzügen, unverkaufbaren Waren, einem schlechten Ruf oder unlauterem Wettbewerb in der Branche. In einigen Fällen kann ein ganzer Markt unterwandert werden, bevor der Betrug aufgedeckt wird.
Besteht auch nur der geringste Zweifel am Lieferanten oder an den Waren, die das Unternehmen zu kaufen beabsichtigt, sollte das Geschäft vermieden werden. Und es ist immer ratsam zu prüfen, ob die Unternehmen, mit denen das Unternehmen handelt, für die Mehrwertsteuer registriert sind. Dies kann durch die Abfrage der Mehrwertsteuernummern der Lieferanten geschehen.
Auf der Website des Dänischen Steueramts sind auch einige spezifische Punkte aufgeführt, die beim Kauf und Verkauf von Waren beachtet werden sollten.

7. Vorsicht vor Druckern

Drucker in Unternehmen können ein erhebliches Sicherheitsrisiko für ein Unternehmen darstellen, wenn nicht darauf geachtet wird.
Die Entwicklungen in der Druckertechnologie, einschließlich der Tatsache, dass Drucker die gleichen Hardwarekomponenten wie ein Computer enthalten, wie z. B. ein Laufwerk, ein Bedienfeld und eine Tastatur, bedeuten, dass Unternehmen Drucker genauso wie einen PC gegen Angriffe sichern sollten. Dies wird oft übersehen, obwohl sich dänische Unternehmen im Allgemeinen der Cyber-Bedrohung sehr bewusst sind.

8. Setzen Sie sich mit der Bank in Verbindung und erstatten Sie Anzeige bei der Polizei wegen Betrugs oder versuchten Betrugs

Wenn der Betrug über die Bank des Unternehmens begangen wurde, sollte die Bank immer kontaktiert werden, um den Betrag zurückzuerhalten. Wenden Sie sich im Falle eines Betrugs oder versuchten Betrugs immer an die Polizei, auch wenn Sie nicht Opfer des Betrugs geworden

sind. Denken Sie daran, die Unterlagen aufzubewahren und der Anzeige bei der Polizei beizufügen.