FAKTENBLATT

# Betrug ist nicht nur digital. Es ist auch eine physische Angelegenheit.

Betrug wird oft fälschlicherweise nur als digitales Problem, wie beispielsweise ein Hackerangriff, betrachtet. Es kann aber viele Formen annehmen, darunter auch die Offenlegung physischer Dokumente, die genauso gefährlich ist und oft übersehen wird.

## Hier sind einige Möglichkeiten, wie Sie Ihr Unternehmen möglicherweise gefährden:

### Umgang mit physischen Dokumenten

- **Ungeschredderte Papiere**: Dokumente mit sensiblen Informationen, z. B. Rechnungen, Verträge, Krankenakten, Personalakten, die in Mülleimern, auf Schreibtischen oder im Recyclingmüll landen, können gestohlen oder missbraucht werden.
- **Unsachgemäße Entsorgung**: Das Wegwerfen von Dokumenten ohne sichere Vernichtung wie beispielsweise Schreddern öffnet Tür und Tor für das Durchwühlen von Müllcontainern und Identitätsdiebstahl.

### Insiderbedrohungen

- Mitarbeiter oder Auftragnehmer könnten den Zugriff auf physische Akten missbrauchen, insbesondere wenn keine Kontroll- oder Nachverfolgungssysteme vorhanden sind.

### Social Engineering

- Betrüger können physische Dokumente verwenden, um sich als Einzelpersonen oder Unternehmen auszugeben und so Zugang zu Systemen oder finanziellen Ressourcen zu erlangen.

### Hybridangriffe

- Physische Dokumente können zur Unterstützung von digitalem Betrug verwendet werden, beispielsweise durch die Verwendung eines gedruckten Kontoauszugs, um die Identitätsprüfung bei Online-Betrügereien zu umgehen.

## Wie Sie Betrug jenseits digitaler Bedrohungen verhindern können:

### Führen Sie eine Datensicherheitsbewertung durch

- Prüfen Sie, wie vertrauliche Informationen digital und physisch gespeichert, abgerufen und entsorgt werden.
- Identifizieren Sie Schwachstellen bei der Dokumentenhandhabung, den Lagerbereichen und den Entsorgungsprozessen.
- Nutzen Sie diese Bewertung, um Richtlinien zu aktualisieren und Mitarbeiter entsprechend zu schulen.

### Setzen Sie eine Clean Desk Policy durch

- Verpflichten Sie die Mitarbeiter, am Ende des Arbeitstages alle vertraulichen Dokumente von ihren Schreibtischen zu entfernen.
- Bewahren Sie Unterlagen, USB-Sticks und sonstige Speichergeräte sicher auf, wenn Sie diese nicht verwenden.
- Dadurch wird das Risiko einer versehentlichen Offenlegung oder eines Diebstahls verringert, insbesondere in Gemeinschaftsbüros oder Großraumbüros.

### Schulen Sie die Mitarbeiter im Umgang mit vertraulichen Informationen

- Stellen Sie sicher, dass alle Mitarbeiter verstehen, was vertrauliche Daten ausmacht.
- Stellen Sie klare Richtlinien für die Aufbewahrung, Weitergabe und Entsorgung sensibler Dokumente bereit.
- Führen Sie Beispiele aus der realen Welt an, die zu physischem Betrug führen, um die Risiken zu verdeutlichen.

### Führen Sie eine „Alles-vernichten"-Richtlinie ein.

- Im Zweifelsfall vernichten Sie es. Dadurch entfällt das Rätselraten und es wird sichergestellt, dass keine vertraulichen Dokumente in die falschen Hände geraten.
- Bewerben Sie diese Richtlinie als einfache und effektive Methode zum Schutz von Kunden- und Geschäftsdaten.
- Ernennen Sie jemanden in Ihrem Unternehmen, der den Aktenvernichtungsprozess überwacht, z. B. indem er die Drucker auf herumliegende Dokumente überprüft.

**Weitere Informationen finden Sie unter shredit.de oder anrufen 0 8912 085 947**

**Wir schützen, was wichtig ist.**



Shred-it®
Ein Unternehmen von Stericycle®