ÜBERBLICK ZUM THEMA „KONTODATENÄNDERUNGSBETRUG"

Raiffeisen Bank International
Member of RBI Group

Worum handelt es sich?

Im englischsprachigen Raum ist dieser Sachverhalt auch unter den Begriffen „Payments Re-direction Fraud", „Mandate Fraud" oder „Supplier Account Takeover Fraud" bekannt. Diese Betrugsart subsumiert die Änderung von Kontodaten von Lieferanten oder Kunden in Kombination mit Lastschrift- oder Daueraufträgen, Manipulationen von Kreditkartenaktivitäten oder Änderungen von Daten eines Mitarbeiterkontos.

Warnsignale

- Jede **unerwartete Anforderung**, die Zahlungsdetails oder Kontodaten eines Lieferanten zu ändern.
- Unabhängig ob via Telefon, E-mail, Brief oder Fax, jede Kontaktaufnahme mit Ihrem Unternehmen betreffend eine **Anpassung der Zahlungsdetails** sollte prinzipiell als **potentielles Warnsignal** behandelt werden.
- Die kontaktierende Person am Telefon reagiert oft **aggressiv** und versucht, **großen (zeitlichen) Druck aufzubauen**.

Kontakt

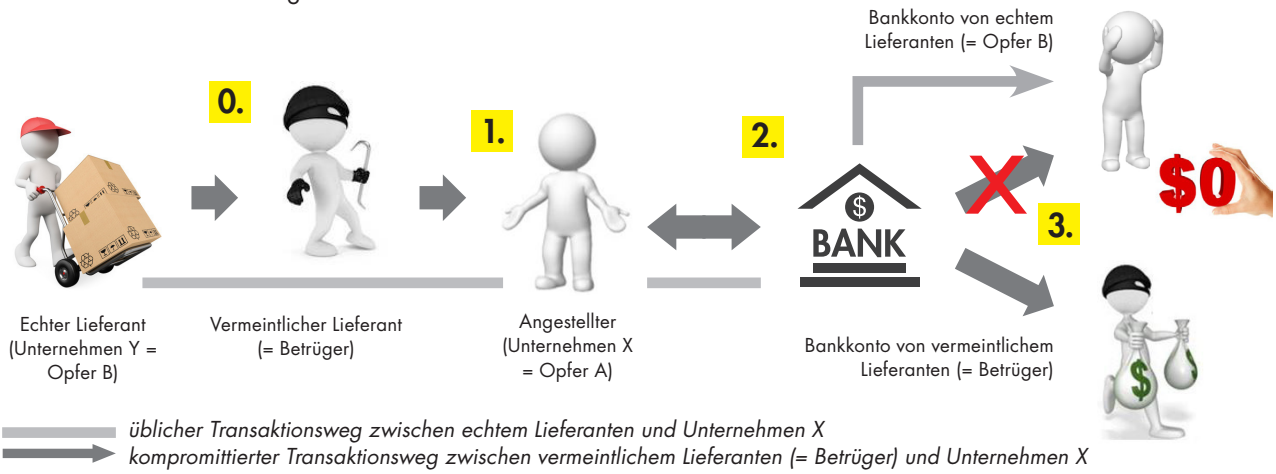
Bei **Fragen/Verdachtsmomenten** wenden Sie sich bitte an Ihren Kundenbetreuer oder direkt an **RBI Group Financial Crime Management** via **fraud@rbinternational.com**

Gerne validieren wir für Sie schnell und unproblematisch allfällige Verdachtsfälle.

Achtung: *die Änderung der Bankdaten ist ein* ***seltener*** *Vorgang und sollte daher bei jeder Anfrage mit* ***Misstrauen*** *behandelt werden. Solche Änderungen sollten nur auf Senior Managementstufe autorisiert werden.*

Wie ist der Ablauf?

0. Regelmäßige Zahlungen von Unternehmen X an seinen Geschäftspartner Unternehmen Y (z.B. Lieferant).
1. Der Betrüger kontaktiert das Zielunternehmen, Unternehmen X, via Telefon/E-mail/Brief und gibt sich als Repräsentant von Unternehmen Y aus (oftmals werden E-mails von gehackten Emailkonten des echten Lieferanten gesendet!). Der Betrüger informiert Unternehmen X über eine Änderung der Kontonummer von Unternehmen Y.
2. Angestellter von Unternehmen X ändert („aktualisiert") die Kontonummer in der Lieferantendatenbank.
3. Von diesem Zeitpunkt an endet jede einzelne Zahlung von Unternehmen X, gedacht für den echten Lieferanten, auf dem Konto des Betrügers.



üblicher Transaktionsweg zwischen echtem Lieferanten und Unternehmen X
kompromittierter Transaktionsweg zwischen vermeintlichem Lieferanten (= Betrüger) und Unternehmen X

Tipps um sich zu schützen

- Behandeln **Sie jede Benachrichtigung einer Kontoänderung** als Aktivität mit **hohem Risiko**.
- Verifizieren Sie eine Anfrage BEVOR Sie die Änderungen in der Datenbank implementieren oder die Zahlung ausführen. Achten Sie auch darauf, NICHT die Kontaktperson zur Verifizierung beizuziehen, welche auf der Benachrichtigung angeführt ist, sondern jene, die Ihnen bekannt ist.
- **Gleichen Sie täglich Ihre Konten ab**, um rasch potentielle betrügerische Zahlungen identifizieren zu können.
- Lassen Sie **niemals** Rechnungen **unbeaufsichtigt** im Büro oder auf Ihrem Schreibtisch liegen.
- Wo es möglich ist, sollten Sie mindestens zwei Kontakte bei den Lieferanten bestimmen, zu denen Sie regelmäßige Zahlungen tätigen. Damit können Sie Probleme bezüglich Rechnungen bestätigen lassen.