ZAHLUNGSBETRUG: WIE KÖNNEN SICH UNTERNEHMEN SCHÜTZEN?

accountant belastingconsulent
iab
BeExcellent.be!

ucm

BIBF IPCF

unizo
VERSTERKT ONDERNEMERS

Instituut van de Bedrijfsrevisoren
Koninklijk Instituut

febelfin

VBO Verbond van Belgische Ondernemingen
FEB Fédération des Entreprises de Belgique

isabel
beyond banking

Immer häufiger werden Unternehmen Opfer von Zahlungsbetrug.Die Strukturen von Zahlungsbetrug, der viele Gesichter besitzt, sind häufig so weit entwickelt, dass sie einem tatsächlichen Unternehmensmodell ähneln. In der Regel verfügen die Betrüger über weitreichende Informationen über die betroffenen Unternehmen, die sie über das Internet oder die sozialen Netzwerke sammeln.

Um diese - in zunehmendem Maße international auftretende – Form des Betrugs zu bekämpfen, schlossen sich die VBO, der Banksektor, die Wirtschaftsverbände und die Gerichtspolizei Brüssel (NIFO, *National and International Fraud Office*) zusammen.

Die Auswirkungen von Zahlungsbetrug sind erheblich. Es geht nicht nur um den eigentlichen finanziellen Schaden. Die Bemühungen, die Beträge, die in internationale und dunkle Kanäle geflossen sind, zurückzufordern, sind fast aussichtslos. Genauso sind die Folgen für die Arbeitnehmer zu nennen, die den Betrug nicht gleich als solchen erkennen.

DIE TÄUSCHUNG VON BUCHHALTERN UND FINANZMITARBEITERN IN BELGISCHEN UNTERNEHMEN

In erster Linie sollten die Mitarbeiter von Finanz-, IT- und juristischen Diensten sensibilisiert werden. Erhöhte Wachsamkeit und eine kritische Betrachtung der Situation helfen dabei, mögliche Betrugsszenarien zu durchschauen und aufzudecken.

Einige Zahlen

Seit September 2010 wurden bei der föderalen Gerichtspolizei Brüssel im Rahmen des Betrugs unter der Bezeichnung "im Namen der Geschäftsführung" (siehe *unten*) 32 Ermittlungen eingeleitet. Es geht um einen Betrag von über 37 Millionen Euro, wovon rund 13 Millionen tatsächlich auf ausländische Bankkonten der Betrüger überwiesen wurden. Bei den übrigen 24 Millionen handelte es sich um versuchte Überweisungen.

Im selben Zeitraum zeigen die aktuellen Zahlen in der Wallonie (Marche-en-Famenne, Neufchateau, Huy, Mons, Tournai, Nivelles, Lüttich und Charleroi), dass 31 Ermittlungen mit einer Gesamtsumme von 24 Millionen Euro eingeleitet wurden, wovon rund 4 Millionen Euro auf Bankkonten der Schwindler überwiesen wurden.

In Flandern sind die Zahlen unvollständig (Antwerpen, Turnhout, Löwen, Oudenaarde und Halle), zeigen jedoch 8 eingeleitete Ermittlungen, in deren Rahmen 3,5 Millionen Euro versucht wurden, zu unterschlagen. 2 Millionen Euro wurden auf die Bankkonten der Betrüger transferiert.

Diese Zahlen bilden nur die Spitze des Eisbergs. Zahlreiche Unternehmen vermuten einen Imageschaden und geben gar nicht erst an, Opfer einer Betrugsmasche geworden zu sein. Zudem betreffen die Zahlen nur einige wenige Arten von Betrug, die sich auf Identitätsmissbrauch und auf die Manipulation von Mitarbeitern beziehen (siehe unten). Weitere Betrugsformen, wie die Fälschung von Rechnungen, wurden gar nicht erst in diesen Zahlen aufgenommen (aufgrund mangelnder Statistiken zum Thema). Dennoch wurden den Polizeidiensten bereits tausende Fälle gemeldet.

Welche Betrugspraktiken sind hier konkret gemeint?

Der Betrug kann unzählige Formen annehmen. Wir unterscheiden hauptsächlich zwischen zwei Betrugspraktiken. Zum einen den Identitätsdiebstahl, zum anderen die Unterschlagung von Dokumenten.

Eine dritte Betrugsform greift auf *Malware* (Schadprogramme) zurück, die die Computersysteme angreift.

1. Betrug mittels Identitätsdieb stahl

Diese Betrugsform wird gelegentlich von einer Vorbereitungsphase begleitet.
Nachstehend finden Sie häufig beobachtete Szenarien, die Ihnen dabei helfen, den Betrug besser zu erkennen:

VORBEREITUNGSPHASE

Einsatz von Vorwänden:
Audit und Analyse von Zahlungsverfahren

- Der Betrüger kontaktiert ein Unternehmen oder eventuell das Tochterunternehmen eines internationalen Konzerns per Telefon oder E-Mail.
- Er gibt sich als Mitarbeiter eines öffentlichen Dienstes aus, als Auditor oder Unternehmensrevisor, der in diesem Rahmen die internen Zahlungsverfahren einleiten soll.
- Auf diese Weise versucht der Betrüger wertvolle Informationen zu erhalten, beispielsweise die Identität des Mitarbeiters, der befugt ist, die Zahlungen auszuführen.

Einsatz eines Vorwands: Computertest

- In diesem Fall nimmt der Betrüger ebenfalls per Telefon oder E-Mail Kontakt mit dem Unternehmen auf.
- Er gibt sich als Informatiker des Unternehmens aus, das für die Sicherung der Zahlungen verantwortlich ist.
- Unter dem Deckmantel, eine Anzahl von Tests' durchzuführen, versucht er dem Opfer sensible Informationen (Zahlungsverfahren, Kontosaldo, Kontonummer, usw.) zu entlocken.

DURCHFÜHRUNGSPHASE

- Der Betrüger nimmt telefonisch Kontakt mit einem Mitarbeiter des Finanzdienstes des betroffenen Unternehmens auf.
- Er gibt sich als CEO, CFO oder als Vertrauensperson des Unternehmens aus.
- Er fordert unbedingte Vertraulichkeit in Bezug auf seinen Anruf.
- Unter dem Deckmantel, dass beispielsweise eine Steuerkontrolle oder die Übernahme eines Unternehmens geplant sind, soll stets eine höchst dringende Zahlung vorgenommen werden.
- Er wird, unter Verwendung des Namens des CEO, CFO oder einer anderen Vertrauensperson des Unternehmens, mit Charme oder durch die Androhung möglicher Konsequenzen fordern, dass das Opfer die bestehenden Zahlungsverfahren umgeht.

Der Betrüger besitzt eine sehr überzeugende Art. Er wird beispielsweise einen „Pseudo-" Anwalt in das Gespräch einschalten, dem Opfer eine E-Mail senden, die der E-Mail-Adresse des Vorsitzenden, Finanzdirektors, eines Anwalts oder eines anderen Berufstätigen ähnelt, sowie unter einem falschen Vorwand ein größtmögliches Maß an Vertraulichkeit fordern.

Da er vor seinem Anruf bereits ausführliche Informationen über das Opfer besitzt (beispielsweise anhand der im Internet zu findenden Daten), kann er es sehr leicht beeinflussen.

Das Opfer steht aufgrund der Bitte um Verschwiegenheit unter starkem Druck.

2. Betrug auf der Grundlage der Unterschlagung von Dokumenten und insbesondere von Rechnungen

Auch diese Betrüger sind sehr gut organisiert:

- Nach der Unterschlagung von Rechnungen verändern sie die Kontonummer des Begünstigten;
- In einigen Fällen werden Kontaktanschriften des Ausstellers der Rechnung (Telefonnummern oder E-Mail-Adressen) ebenfalls verändert, so dass eventuelle Informationsanfragen (in Bezug auf die Gültigkeitserklärung der Rechnung) bei den Betrügern selbst eintreffen.
- In wiederum anderen Fällen beteuern die Betrüger, dass das vom Opfer angemietete Gebäude den Besitzer gewechselt hat und geben neue – und gefälschte – Angaben für die Mietzahlungen an.

Nimmt der Buchhalter Kontakt mit dem Rechnungsaussteller auf, um sich zu vergewissern, dass die neue Kontonummer tatsächlich die richtige ist, wird ihm gesagt, dass *"Ja, die Kontonummer von nun an eine andere ist"*...

3. Betrug auf der Grundlage von *"Malware"*

Malware ist der Sammelbegriff für schädliche Software. Sie wird unbemerkt und unbefugt auf Ihrem Computer installiert, meist beim Öffnen eines verdächtigen Anhangs, einer E-Mail oder eines Links.

Malware stört und manipuliert normale Computerprozesse, um unter anderem Informationen zu stehlen oder betrügerische Zahlungsaufträge zu erstellen, wenn Sie online mit Ihrer Bank verbunden sind.

Wie kann man sich gegen diese Betrugsmaschen schützen?

INFORMATION

Um diesen Formen von Betrug vorzugreifen ist es wichtig, dass entsprechende Informationen auf allen Ebenen des Unternehmens weitergeleitet werden.

VERWALTUNGSVERFAHREN

Die Verwaltungsverfahren des Unternehmens sollten auf die Senkung des Risikos zur Durchführung unbefugter Zahlungen ausgerichtet sein. Dies kann beispielsweise durch die Kontrolle und Genehmigung von Rechnungen und die strikte Befolgung der Verfahren zur Unterzeichnung der Rechnungen durch autorisierte Personen geschehen. Diese schriftlich festzulegenden Verfahren müssen dem Personal zur Kenntnis gebracht werden. Auch sollte die richtige Anwendung dieser Verfahren regelmäßig kontrolliert werden.

WICHTIGE WARNSIGNALE:

- **ungewöhnliche Transaktionen** auf der Grundlage der angeführten Gründe, des besonderen Betrags, der Umstände, usw.;
- **Geheimhaltungspflicht** (Einfordern von Vertraulichkeit, Gebrauch eines geheimen Codes, Bitte, den Gesprächspartner über sein Handy oder seine persönliche E-Mail-Adresse kontaktieren zu dürfen);
- **äußerste Dringlichkeit** (dringender Bedarf an Liquidität);
- **ungewöhnlicher Druck** zum Erhalt sensibler Informationen oder zwecks Durchführung einer Zahlung (ungewöhnliche Kontaktaufnahme durch den CEO oder CFO, Eingreifen eines Anwalts);
- Transaktionen auf **ausländische Konten** (außerhalb oder innerhalb Europas);
- Überweisung von liquiden Mitteln an einem **Freitag** oder am **Tag vor einem Feiertag** (wodurch das Geld nicht durch die Bank blockiert werden kann);
- **Änderung von Zahlungsdaten** eines Stammlieferanten;
- Eine E-Mail mit einem **Link zur Internetseite Ihrer Bank** und der Bitte, Ihren persönlichen Code einzugeben.

PRAKTISCHE PRÄVENTIONSTIPPS:

- Wenden Sie die **Sicherheitsvorschriften** und die **Zahlungsverfahren** strikt an. Achten Sie besonders auf die Regelungen in Bezug auf die **Aufgabenverteilung** und die **Unterzeichnungsbefugnisse** und das **unter allen Umständen.** Das System, wobei ab einem bestimmten Geldbetrag mehrere Personen unterzeichnen müssen, bietet einen sehr viel umfassenderen Schutz;
- Schützen Sie Ihren Computer ausreichend (u. a. durch die Aktualisierung Ihres Antivirenprogramms und die Sicherung Ihrer Wifi-Verbindung);
- Geben Sie keine Unternehmensinformationen weiter (Hierarchie, Befugnisse, Abwesenheiten, Liquiditäten, usw.), wenn diese per Telefon oder E-Mail angefragt werden;
- Kontrollieren Sie die **Identität Ihrer Gesprächspartner** bei geringsten Anzeichen eines Betrugsversuchs;
- Kontrollieren Sie die **Herkunft von Telefonanrufen;**
- Kontrollieren Sie die **Richtigkeit von E-Mail-Adressen und, bei Zweifel, die IP-Adressen,** von denen die E-Mails stammen (www.whois);
- Nehmen Sie Kontakt mit dem Auftraggeber über eine **andere Telefonnummer** oder E-Mail-Adresse auf, als die vom Gesprächspartner angegebene;
- Kontaktieren Sie systematisch die Lieferanten, wenn die **Zahlungsdaten** verändert wurden (Achtung: die Telefonnummer auf der Rechnung kann auch geändert worden sein und es ist gut möglich, dass eine Telefonnummer beispielsweise die Vorwahl "02" besitzt, in Wirklichkeit jedoch die Verbindung mit einem Anschluss herstellt, der dutzende Kilometer von Brüssel entfernt liegt);
- Seien Sie besonders vorsichtig, wenn eine Zahlung auf einem Konto erfolgen soll, dessen Nummer noch nicht im üblichen **Zahlungssystem** eingetragen ist;
- Zögern Sie nicht, die Konto- und Telefonnummern eines Unternehmens im **Internet** zu recherchieren;
- In Bezug auf die dem Staat zu überweisende **Steuer** (darunter auch die MwSt.), achten Sie darauf, dass die Kontonummern mit 679... oder BExx679x... beginnen;
- Lassen Sie sich nicht unter Druck setzen;
- **Besprechen Sie den Vorfall** mit Ihrem Vorgesetzten oder einem Kollegen, auch wenn ein hohes Maß an Vertraulichkeit gefordert wurde (sondern Sie sich nicht ab);
- Stellen Sie innerhalb des Unternehmens eine **Vertrauensperson** ein, an die die Mitarbeiter sich bei dem geringsten Verdacht von Betrug wenden können;
- Klicken Sie niemals auf einen **Anhang oder auf einen Link zu einer E-Mail**, deren Absender Sie nicht oder nicht gut kennen;
- Surfen Sie niemals über einen Link in einer E-Mail auf der Internetseite Ihrer Bank, um anschließend **persönliche PIN-Nummern** einzugeben;
- Falls beim Öffnen einer Anlage in einer E-Mail, deren Absender Sie nicht oder nicht gut kennen, ein Pop-up-Bild erscheint, in dem Sie aufgefordert werden, ein **„Makro"** auszuführen, lehnen Sie sofort ab!

BEI VERSUCHTEM BETRUG:

- Die **Polizei** einschalten;
- Die Unternehmen oder Beschäftigten warnen, wer seine Identität oder die Kontaktdaten auf den Rechnungen gefälscht hat.

FALLS DIE BEZAHLUNG AUSGEFÜHRT WURDE:

- Nehmen Sie unmittelbar Kontakt mit der **Bank** auf, um die Überweisung zu blockieren;
- **Anzeige** erstatten.

Zahlungsbetrug:
Wie können sich Unternehmen schützen?

KONTAKTPERSON :
Föderale Kriminalpolizei Eupen
Regional Computer Crime (RCCU)
pjf.eup.rccu@police.belgium.eu
Hauptinspektor Danny LOOS (087/596 222)

accountant belastingconsulent iab BeExcellent.be!

UCM

BIBF IPCF

unizo VERSTERKT ONDERNEMERS

Instituut van de Bedrijfsrevisoren Koninklijk Instituut

febelfin

VBO Verbond van Belgische Ondernemingen | FEB Fédération des Entreprises de Belgique

isabel beyond banking