

Innovative und *zielbewusste Betrüger*

*„Fraud and deceit abound in these days, more than in former times.“
(Betrug und Schwindel herrschen dieser Tage mehr als in früheren Zeiten.)*

Sir Edward Coke, Lord Chief Justice, 1602



Obwohl das Zitat mehr als 400 Jahre alt ist, treffen Sir Edward Cokes Worte heute noch genauso zu wie im Jahre 1602. Das Problem ist, dass, obwohl wir bessere Massnahmen gegen Betrug entwickelt haben, Betrüger ebenfalls dazugelernt haben. Sie sind die einfallsreichsten aller Kriminellen und nutzen die für uns alle verfügbaren neuen Technologien zu ihrem eigenen Vorteil aus. Mit dem globalen Vormarsch des Internets und zunehmender Vernetzung von Geschäftsdaten in digitaler Form bieten sich für Betrüger mehr Routen und Zugriffspunkte denn je zuvor. Und da diese Kriminellen so zielbewusst und entschlossen sind, wird es für Firmen schwieriger und schwieriger, sich gegen solche High-Tech-Verbrecher zu schützen.

Um Betrug zu bekämpfen, müssen Manager ein besseres Verständnis der allgemeinen Arten von Betrug erlangen, und sie müssen lernen, Strategien und praktische Gegenmassnahmen zu entwickeln, die unter Einsatz bereits vorhandener Ressourcen implementiert werden können.

Hacker, betrügerische Kunden und Feinde innerhalb der Tore

Elektronische Diebe können sehr kreativ sein, wenn es darum geht, Grossfirmen in die Tasche zu greifen. Einige Beispiele dafür sind:

- ▶ Gültige Kontoinformationen verwenden, um sich als Kunden auszugeben.
- ▶ Die Position eines „vertrauenswürdigen Lieferanten“ ausnutzen, um überhöhte Rechnungen auszustellen oder um Waren bzw. Dienste in Rechnung zu stellen, die nie geliefert wurden.
- ▶ Sicherheitsprotokolle innerhalb der Firma umgehen, um Veruntreuungen zu verdecken. Ja, leider sind gelegentlich auch Mitarbeiter der eigenen Firma an Betrugsvorgängen beteiligt, die für die Organisation zu schweren Schäden führen können. Dies ist oft sehr effektiv, da sol-

che Mitarbeiter wissen, welche Sicherheitsmassnahmen und Richtlinien implementiert werden. Sie haben darüber hinaus den Vorteil, dass sie genau über eventuelle Schwachstellen der Infrastruktur informiert sind.

Die Association of Certified Fraud Examiners (ACFE) in den Vereinigten Staaten schätzt Betrugsschäden im Jahr 2002 auf 6 Prozent des Gesamtumsatzes ein. Die Organisation führt weiter aus: „Angewendet auf das US-Bruttosozialprodukt entspricht dies Verlusten von ca. 600 Milliarden Dollar oder etwa 4 500 Dollar pro Angestellten.“ Ähnliche Zahlen werden aus Grossbritannien gemeldet.

Die ACFE hat noch mehr interessante Statistiken zu bieten: „Betrugsfälle durch Angestellte verursachen im Durchschnitt Schäden von 60 000 Dollar, während Betrugsfälle, die von Managern oder Führungskräften begangen werden, durchschnittlich zu Verlusten von 250 000 Dollar führen. Wenn Manager und Angestellte in einem Betrugsfall zusammenarbeiten, steigt der durchschnittliche Schaden auf 500 000 Dollar an.“ Die zunehmende Abhängigkeit von Technologie bei Geschäftstransaktionen und Identitätsprüfungen bietet zusätzliche Gelegenheiten für betrügerische Aktivitäten. Und wer schultert den Grossteil dieser Verluste? In erster

Linie muss die Firma sie von den Bruttogewinnen des Jahres abziehen, aber dies führt natürlich für Kunden zu höheren Preisen für Waren und Dienstleistungen. Letztlich müssen wir alle für Betrug bezahlen.

Warum ist es so schwierig, Betrugsfälle zu verhindern?

Keine Firma gibt gerne zu – nicht einmal intern – dass sie anfällig gegenüber Betrug ist. Dies schadet dem Image der Firma und bei Aktiengesellschaften kann es negative Auswirkungen auf den Aktienkurs haben. Nur wenige Führungskräfte und Manager wollen sich mit der Möglichkeit auseinandersetzen, dass ihre eigenen Mitarbeiter sie bestehlen könnten, weil sie diesen Mitarbeitern vertrauen müssen, damit die Firma funktionieren kann. Daher wird das Problem oft unter den Teppich gekehrt, mit dem Vorwand, dass das Problem nicht so ernst ist und dass ausserdem Schutzmassnahmen bereits in Kraft sind. Und ausserdem würden es die Rechnungsprüfer doch herausfinden, oder nicht?

Selbst wenn Betrugsfälle aufgedeckt werden, ist eine strafrechtliche Verfolgung nicht immer die finanziell attraktivste Lösung, da Strafen in der Regel mild sind und Kompensationszahlungen niedrig ausfallen, zumindest im Vergleich zu den entstandenen Verlusten.

Eine Reduktion der betrugsbezogenen Kosten von nur einem Prozent in einer Organisation kann typischerweise zu einem zehnprozentigen Gewinnzuwachs führen. Um einen vergleichbaren Zuwachs zu erzielen, müsste eine Organisation Verkäufe bedeutend steigern, Kosten senken oder die Belegschaft verkleinern.

Und obwohl der Kampf gegen Betrug nie endet wird, trägt jeder Franken, den Organisationen dadurch einsparen kann, zur Stärkung ihrer finanziellen und Marktposition bei.

Durch die Integration aller internen Daten-systeme in ein Data Warehouse zur Betrugsprüfung, können diese mit externen betrugsbezogenen Daten verglichen werden. Muster und Anomalien sind auf diese Weise besser erkennbar. Verdächtige Aktivitäten können isoliert, gemessen und verfolgt werden.

Schliesslich sollten Unternehmen ihre Strategie vervollständigen, indem sie bei erwie-senen Betrugsfällen Fachleute für die Untersuchung heranziehen. Gegen Betrüger, egal ob es sich um Kunden, Angestellte oder die lokale Zustellungsgesellschaft handelt sollten effektive Sanktionen, einschliesslich angemessene rechtliche Massnahmen zur Anwendung kommen. Machen Sie deutlich, dass Sie ein intelligentes Unternehmen führen, das sich gegen Betrüger zu wehren weiss!

Kreditrisikomanagement bei Lloyds TSB

Die Bank erwartet unternehmensweite Vorteile von Risikoverwaltungssystemen.

Lloyds TSB, ein führender Finanzdienstleister in Grossbritannien, hat SAS Risk Management for Banking als Grundlage seines Risikoverwaltungssystems ausgewählt. Die neue Anwendung ermöglicht Lloyds TSB, alle Anforderungen von Basel II zu erfüllen und darüber hinaus die Kapitalallokation zu verbessern, die finanzielle Transparenz zu erhöhen sowie die Profitabilität zu maximieren.

Das Basel II-Abkommen reguliert die Kapitalmenge, die Banken halten müssen, um

Kreditrisiken auszugleichen. Da die Lösung komplexe Analysen der Wahrscheinlichkeit von Zahlungsverzug seitens Kunden ermöglicht, erhält Lloyds TSB einen genaueren Einblick in die Kosten, die bestimmte Entscheidungen mit sich bringen können. Diese verbesserte Risikosegmentierung hat für Lloyds TSB bereits zu einer Reduktion der Kreditrisiko-Kapitalmenge von 20% für ungesicherte Darlehen und von bis zu 50% für Hypotheken geführt. Darüber hinaus kann Lloyds TSB viele ma-

nuelle Prozesse, wie z. B. das Erstellen von Risikoberichten, die Leistungsüberwachung und die Kreditbewertung automatisieren und auf diese Weise die Interaktion mit Kunden verbessern.

„Da Lloyds TSB die Geschäftsvorteile eines Risikoverwaltungssystems schon früh erkannt hat, können wir uns vor dem Inkrafttreten von Basel II Wettbewerbsvorteile erarbeiten“, führt Shahram Sharifi, Direktor für Kreditrisiko bei Lloyds TSB aus.