

Täter im digitalen Dschungel – Betrugsbekämpfung bei Amazon.com

Unbestritten ist Amazon heute der grösste Online-Händler weltweit. Bekannt geworden als digitaler Buchhandel bietet Amazon.com heute „die weltgrösste Auswahl“ an Produkten aus nahezu allen Bereichen. Amazon führt Millionen Artikel in Kategorien wie Elektronik, Küchen- und Haushaltsgeräte, Bücher, Musik, DVD, Video, u. v. m. und hat über 35 Millionen Kunden. Einige davon aber lieber nicht...

von Gabriele Dobenecker

Ist im traditionellen Handel der Ladendiebstahl ein Problem, machen Online-Händler andere Formen der Kriminalität zu schaffen. Die vorherrschende Betrugsform, mit der Amazon.com zu tun hat, ist der Kreditkartenmissbrauch – wie bei allen Händlern, die Waren über Internet, Telefon oder Versand verkaufen. Das Aufdecken und Vermeiden solcher Aktivitäten ist eine Priorität, da nämlich die Händler, und nicht etwa die Bank des Kartenbesitzers, die finanzielle Verantwortung für diese Form des Betrugs tragen. Die Täter wenden bei Online-Händlern die gleichen Techniken an, wie sie auch im herkömmlichen Einzelhandel beobachtet werden. Da sie jedoch mit jedem Klick einen rückverfolgbaren Datenpfad hinterlassen, sind sie leichter zu fassen. Zu den typischen Tricks, um an Kreditkarteninformationen zu kommen, gehören:

- ▶ **Dumpster-Diving:** Die Täter durchsuchen Mülltonnen nach Kreditkartenzuweisungen und verwenden die darin enthaltenen Angaben.
- ▶ **Double-Swipes:** Die Karte wird in einem Geschäft zweimal durchgezogen. Daten aus dem zweiten Kartendurchzug werden für betrügerische Zwecke genutzt.
- ▶ **Erfundene Kreditkartennummern:** Die Täter finden heraus, welche Banken die

Kreditkartennummern (meist kleinere Banken) nicht sofort abgleichen.

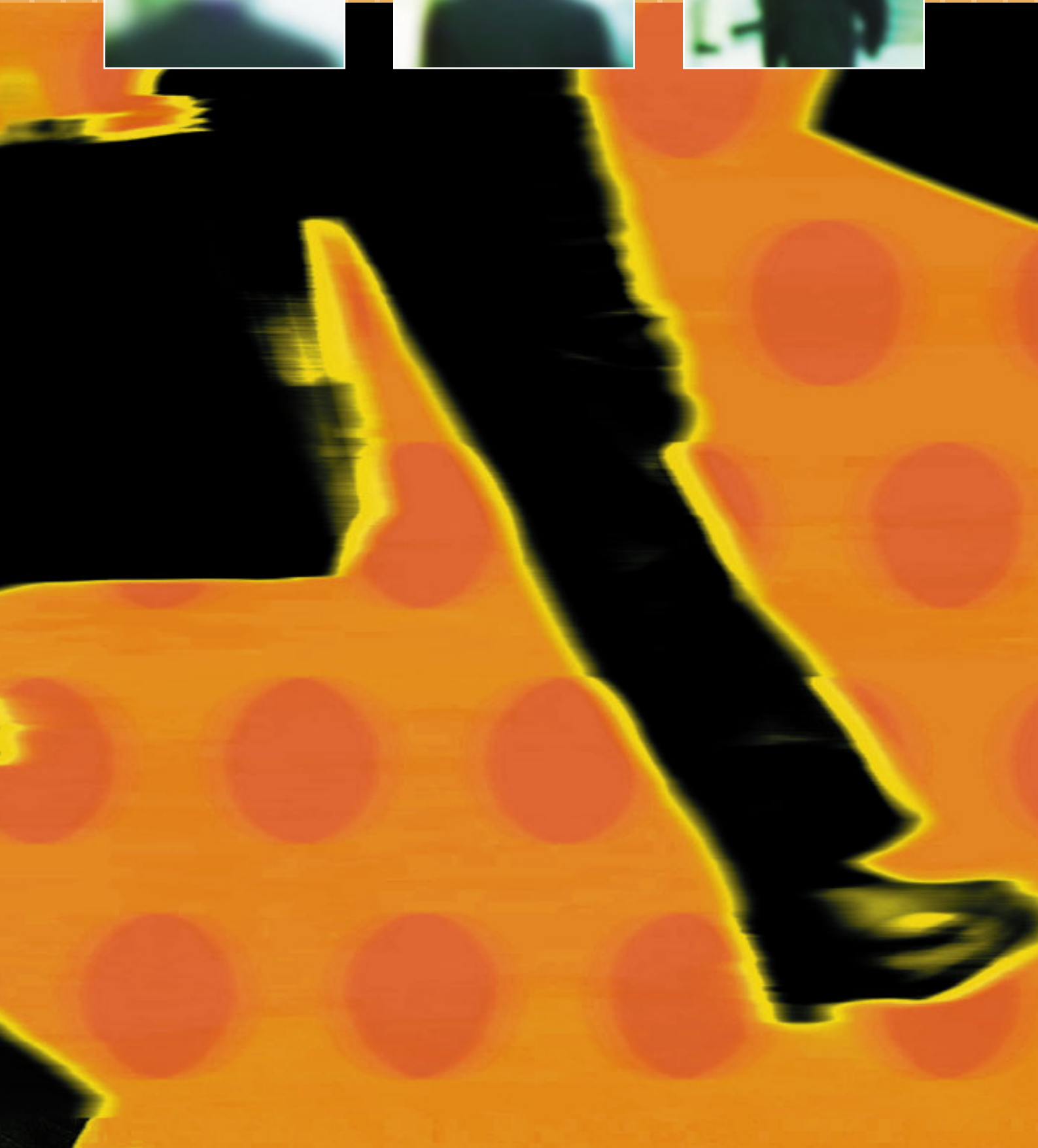
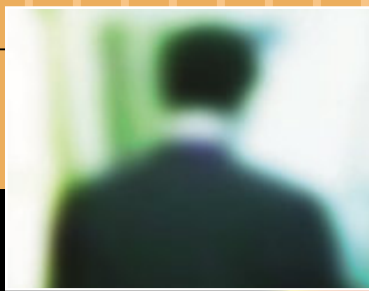
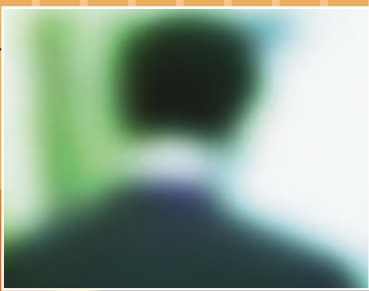
Dadurch erhält der Händler die Bankautorisation nicht vor Versand der Ware. Der Betrüger erfindet dann Kreditkartennummern, die denen der Bank ähnlich sind, im Wissen, dass der betrügerische Warenkauf von der Bank wahrscheinlich nicht sofort autorisiert wird.

„Betrüger zeigen im Allgemeinen ähnliche Verhaltensmuster“, sagt Jaya Kolhatkar, Direktor für Betrugserkennung bei Amazon.com. „Dadurch kann Missbrauch leichter aufgedeckt werden, da man in den Transaktions- und Kundendaten nach entsprechenden Mustern Ausschau halten kann. So kaufen Betrüger gerne Waren, die sie auf dem grauen Markt leicht absetzen können, wie z. B. Elektronikprodukte. Natürlich lassen sie die Waren nicht an die Anschrift schicken, die zu Rechnungszwecken verwendet wird, weshalb eine nicht an die Rechnungsadresse gelieferte Bestellung ein erster Hinweis sein kann. Ausserdem verwenden sie üblicherweise die schnellste Zustellmethode. Allerdings bedeutet einer oder mehrere dieser Umstände natürlich noch lange nicht, dass tatsächlich ein Betrug vorliegt, doch in Verbindung mit anderen Faktoren sind dies typische Verdachtsmomente, denen wir nachgehen.“

Betrug unterbinden

Betrug war immer schon ein Risiko im Geschäftsleben. Aber die digitale Welt bietet erhöhte Betrugsmöglichkeiten. Die zunehmende Automatisierung von Transaktionen schafft ein Umfeld, das Betrug erleichtert, und die oft fragwürdige Sicherheit von Netzwerken und Servern trägt das ihrige dazu bei. Viele Unternehmen, die eShops im Internet aufgesetzt haben, haben Sicherheitsaspekte ignoriert und sind für Hacker mit kriminellen Absichten oft leichte Beute beim Zugriff auf sensitive Daten, die später zum Betrug verwendet werden.

Sind hohe Sicherheitsstandards eine Möglichkeit, Betrug zu verhindern, bietet Data Mining eine wirksame Technologie, Betrug zu erkennen und zu unterbinden. Alle Daten, die im eBusiness anfallen – Kundenkontaktpunkte, Transaktionen, Kaufmuster – können benutzt werden, um typische Verhaltensbilder zu kreieren und dagegen untypisches, potentiell betrügerisches Verhalten zu erkennen. „Betrugserkennung ist eine der Schlüsselanwendungen von Data Mining“ sagt Ralph Kimball, Mitautor des Buches „The Data Warehouse Toolkit: Building the Web-Enabled Data Warehouse“ (John Wiley & Sons, 2000). Data Mining kombiniert ausgefeilte Datenanalysetechniken mit hochperfor-



Über Amazon.com

1995 von Jeff Bezos als virtuelle Buchhandlung im Internet gegründet, ist Amazon heute einer der grössten eCommerce-Anbieter.

Vom Visionär des eCommerce avancierte Amazon innerhalb von nur sechs Jahren zur Weltmarke und zum Muster für eCommerce-Anbieter. Vom Online-Buchhändler entwickelte sich Amazon zur Online-Handels-Plattform. Heute ist Amazon.com, Inc., die Nummer eins des Buch-, Musik- und Videohandels im Internet und zählt zu den 100 wertvollsten Marken der Welt, noch vor Shell, Burger King, Barbie, Nivea und Siemens. (Quelle: World's Most Valuable Brands Ranked by Interbrand 2001). Amazon bietet gemeinsam mit seinen Handelspartnern das weltgrösste Angebot an Büchern, CDs, DVDs, Videos, Spielwaren, Software, Unterhaltungselektronik, Heimwerkerartikel, Drogerie und Kosmetik, Haus- und Gartengeräte sowie Küchenartikel.

Über die Amazon-Handelsplattform, zShops und Online-Auktionen kann jedes Unternehmen und jeder einzelne User seine Produkte an über 35 Millionen Amazon.com-Kunden in 160 Ländern verkaufen. Das Amazon-Zahlungssystem stellt eine einfache und sichere Bezahlung in den Vordergrund. Amazon.com betreibt vier internationale Websites:

www.amazon.co.uk, www.amazon.de, www.amazon.fr und www.amazon.co.jp. Weitere Tochtergesellschaften von Amazon.com sind unter anderen die Internet Movie Database (<http://imdb.com>), die die Recherche von 275.000 Film- und Unterhaltungsprogrammen und 1.000.000 Schauspielern und Filmcrewmitgliedern ermöglicht, und PlanetAll (www.planetall.com), ein webbasierter Adressbuch-, Kalender- und Erinnerungsservice.

manter Technologie, um Unternehmen das Wissen zu geben, das sie benötigen, um Betrug aufzudecken oder sogar zu verhindern.

Unbekannte Muster erkennen

Betrugserkennung ist eine ermüdende und arbeitsintensive Aufgabe, die traditionell nur unzulänglich durch Informationstechnologie unterstützt wurde. Data Mining hat sich hier als effektive Waffe erwiesen: Der Prozess der Selektion, Exploration und Modellierung grosser Datenmengen hilft, bisher unbekannte Muster, Zusammenhänge oder Trends zu erkennen. Solche Muster beinhalten normalerweise unübliche Daten, beispielsweise die hohe Zahl von Versicherungsfällen einer einzigen Person oder ungeklärte Beziehungen wie z. B. verschiedene Firmen unter der selben Adresse.

Die Herausforderung bei Betrug ist dessen seltenes Auftreten: Sind von 80 Millionen Transaktionen weniger als 1 Prozent betrügerisch, gleicht die Suche leicht der einer Nadel im Heuhaufen. Ein Ansatz ist hier das sogenannte „predictive Modeling“ – eine Technik, die sich auf die wahrscheinlichsten Betrugsfälle fokussiert, oft durch die Verwendung von Entscheidungsbäumen. Im Bereich des Kreditkartenbetruges beispielsweise haben Erfahrungen gezeigt, dass diese Betrugsart häufiger von Männern begangen wird, also nimmt man das Geschlecht als erstes Entscheidungskriterium im Entscheidungsbaum. Ist die Häufigkeit in der Altersgruppe der 20-30-jährigen am grössten, hat man das zweite Kriterium. Weitere Kriterien können Ausbildung, Einkommen oder Wohnort sein. Je mehr Informationen man über die Kunden besitzt, desto näher kommt man der Aufdeckung potentieller Betrugsfälle.

Andere Formen des predictive Modeling betreffen das übliche Verhalten. Wenn ein Kunde seine Kreditkarte noch nie in einem Casino verwendet hat, wird die Karte mit ähnlichen Accounts gruppiert. Werden nun mit dieser Karte plötzlich hohe Beträge in verschiedenen Casinos bezogen, wird ein Alarm ausgelöst. „Durch die Information über vergangene Transaktionen „kennt“ das System das typische Verhalten, wie die

üblichen Einkäufe und Umsätze.“ sagt Autor Ralph Kimball.

Betrug bekämpfen

Eine weitere Herausforderung ist die Kreativität der Betrüger, die ständig neue Tricks entwickeln. „Es gibt viel mehr Betrug als heute festgestellt wird.“ sagt Frank Prince, eBusiness-Analyst bei Forrester Research. „Wenn jemand Ihre Web-Site lahm legt, merken Sie es sofort. Wenn Sie jemand betrügt, kann es sein, dass Sie es nie merken, ausser Sie wissen, wonach Sie suchen müssen.“

Dazu ist eine Masse von Daten nötig, die idealerweise in einem Data Warehouse gesammelt werden. Schlechtes Data Mining ist oftmals die Folge von schlechter Datenhaltung und schlechter Datenqualität. Dazu kommt die Notwendigkeit, Daten aus möglichst vielen Datenquellen zu kombinieren – all das setzt einen integrierten „end-to-end“-Data-Warehouse-Ansatz voraus.

Amazon.com war bereits früh darum bemüht, das Betrugsrisiko zu verringern und entschied sich für SAS als Grundlage seines Betrugserkennungssystems. Amazon.com analysiert damit die Verhaltensmuster von Betrügern und entwickelt Auswertungsmodelle (Scores), die auf die Wahrscheinlichkeit eines betrügerischen Verhaltens schliessen lassen. „Diese Scores lassen wir gegen die Kundendatenbank laufen“, erklärt Kolhatkar. „Anschliessend ordnen wir die Ergebnisse mithilfe von SAS nach Prioritäten. Natürlich müssen wir einen potenziellen Betrug eingehend prüfen, bevor wir rechtliche Schritte ergreifen; Daher weisen wir den Ergebnissen aus dem Scoring-Verfahren Prioritäten zu und beginnen mit den Fällen, die die höchste Priorität aufweisen. Unser gesamtes diesbezügliches Reporting, d. h. die Aufzeichnung der verfolgten Fälle mit ihrem Status, erfolgt ebenfalls mit SAS.“ Laut Jaya Kolhatkar sorgte „die Implementierung des SAS-Projektes zu einer erheblichen Senkung der Betrugsversuche auf unserer Site. In den ersten sechs Monaten nach Einsatz ging die Zahl der Fälle um 50 % zurück.“

www.sas.com/switzerland