Das Böse ist immer und überall – und hinterlässt Spuren

Immer öfter wird der Computer zur Tatwaffe für Betrüger, Geldwäscher, Spione und sogar Terroristen. Doch prädiktive Data- und Text-Mining-Verfahren helfen bei der Aufklärung und Prävention von Verbrechen aller Art. *Josef Schmid*

Josef Schmid
Director Consulting SPSS (Schweiz) AG
info@spss.ch

Laut einer aktuellen Erhebung wurde in den letzten beiden Jahren jedes dritte Schweizer Unternehmen Opfer eines Wirtschaftsdeliktes. Mindestens so alarmierend: Bemerkt wird dies oft nur zufällig. Zunehmend lauern Gefahren für Unternehmen, Behörden und Kunden im Internet. Doch auch wenn die Angreifer aus dem Cyberspace zuschlagen, ist der angerichtete Schaden ganz real. In der Computer Crime and Security Survey 2005 gaben 639 Unternehmen Gesamtschäden in Höhe von über 130 Millionen Dollar an. Laut Schätzungen des FBIs haben über 95 Prozent aller im Internet verübten Delikte vermögens- und wirtschaftsrechtliche Motive, darunter Betrugsvergehen, Marken- und Copyright-Verletzungen, unlauterer Wettbewerb oder vorsätzliche Rufschädigung. Noch bedrohlicher jedoch sind digitale Angriffe von Terroristen, die ihre Gegner nicht mit Bomben, sondern durch die Störung kritischer Systeme empfindlich treffen wollen.

Dabei bieten vernetzte Systeme nicht nur mehr Angriffsflächen. Da die Täter von jedem Ort der Welt und zu jeder Zeit zuschlagen können, ist sowohl die Prävention als auch die Aufklärung von Cybercrimes erschwert. Doch genau wie bei «konventionellen» Delikten hinterlassen die Täter – so raffiniert sie auch vorgehen mögen – Spuren. Mittels dieser Daten können moderne elektronische Verfahren kriminelle Verhaltensmuster erkennen und Verbrechen verhindern oder aufklären.

Computer gegen Computer

Dem Gegner einen Schritt voraus und auch auf das bisher Ungeahnte vorbereitet zu sein, ist Aufgabe der Sicherheitsverantwortlichen in Unternehmen und Verwaltungen. Immer weniger können sie sich dabei aber auf Sicherheits-Patches, Firewalls, Antiviren- oder andere Standardlösungen verlassen. So setzt die US-Army prädiktive Data-Mining-Technologien ein, um auch in Netzwerk-Log-Daten, die nicht durch Intrusion Detection Systeme ausgewertet werden, potenzielle Bedrohungen aufzuspüren. Mittels Cluster- und Assoziationstechniken werden auch in Daten unterschiedlicher Quellen und Formate, die bisher zwar erfasst, aber nicht verarbeitet wurden, heimtückische Aktivitäten erkannt.

Dies ist ein erheblicher Sicherheitsgewinn gegenüber Systemen, die lediglich historische Reports generieren. Denn während diese meist nur vordefinierte Regeln wie zum Beispiel bestimmte Signaturen anwenden und jeden Alarm als isoliertes Ereignis behandeln, setzen prädiktive Verfahren jedes Ereignis in Beziehung, erkennen mögliche Angriffsmuster und entwickeln Regeln, um auf künftige Gefahren vorbereitet zu sein. Auf diese Weise schützt auch das Critical Infrastructure Assurance Program for Cyber Threats (CIAP-CT) die Systeme der US-Armee, indem es Cyber-Attacken auf zivile Infrastrukturen, die das US-Militär bei der Truppenverschiebung und -versorgung unterstützen, laufend analysiert, sicherheitskritische Ereignisse mit «red flags» versieht und geeignete Vorkehrungen für die eigenen sensiblen Systeme ergreift.

Hände weg von schmutzigem Geld

Nach einem ähnlichen Prinzip werden prädiktive Data-Mining-Verfahren im Kampf gegen die zunehmenden Fälle von Geldwäsche eingesetzt. In der Schweiz dient jeder zehnte Betrugsfall dem Zweck, unrechtmässig erworbenes Geld in den legalen Geldkreislauf einzuschleusen. Dies zu verhindern ist nicht nur Aufgabe der Banken, sondern auch der Fondsverwaltungen, Broker, Versicherer und anderer Unternehmen. Doch genauso fatal, wie kriminelle Machenschaften nicht aufzudecken, ist es, rechtschaffene Kunden und Bürger zu Unrecht zu verdächtigen. Aus diesem Grund müssen die eingesetzten Technologien äusserst exakt sein, um einerseits

Am wirksamsten kann gegen Bedrohungen vorgegangen werden, wenn einzelne Security-Anwendungen kombiniert werden

nichts und niemanden durch die Maschen schlüpfen zu lassen, aber auch niemanden zu Unrecht in Verruf zu bringen.

Die Geldwäscher gehen in drei Schritten vor: Zunächst muss das Geld in Umlauf gebracht werden, ohne Alarm auszulösen. Danach wird es mehrfach verschoben, so dass die Spur nur schwer zurückverfolgt werden kann. Schliesslich wird das Geld legal angelegt. Bei jedem Schritt hinterlassen die Täter digitale Spuren, die die Fahnder auf ihre Fährte bringen können. Doch muss man diese Spuren erkennen und verfolgen können. Der erste Schritt ist für die Geldwäscher am riskantesten, weshalb die meisten Massnahmen zur Verhinderung von Geldwäsche dort ansetzen. Die heute gängigen Verfahren nutzen hierfür einfache Abfrage- und Analysetechniken anhand vordefinierter Regeln. So werden etwa sämtliche Konten, auf denen die geringste Transaktion mindestens 1000 Dollar ausmacht, markiert. Transaktionen über 10 000 Dollar oder aus einem verdächtigen Land werden an die zuständigen Meldestellen weitergeleitet. Jeder verdächtige Vorgang muss manuell untersucht werden.

Data-Mining-Technologien hingegen analysieren eine Vielzahl von Transaktionen nach ganz unterschiedlichen Kriterien, um Anomalien, also von den üblichen Regeln abweichende Ereignisse und Verhaltensweisen, aufzuspüren. Diese Methode wird umso treffsicherer, je mehr sie auf prädiktiven Verfahren beruht und verschiedenste Parameter einbezieht: Mittels neuronaler Netze und selbstlernender Verfahren werden auch neue kriminelle Vorgehensweisen, etwa unüblich hoch verzinste Wertpapiere, grosse Einzahlungen an Geldautomaten, «schlafende» Konten oder die Benutzung falscher Identitäten, entlarvt. So werden auch neue Tricks der Geldwäscher rasch erkannt und vereitelt.

Mehr Sicherheit, weniger Aufwand

Damit prädiktive Analyseverfahren greifen, ist es weder erforderlich, dass ein Delikt mit dem Computer verübt wird, noch dass die Täter selbst elektronische Daten hinterlassen. Es genügen Statistiken und Polizeireporte, um die öffentliche Sicherheit zu erhöhen. Was konventionelle Verfahren schnell überfordert, ist mit prädiktivem Data- und Text-Mining eine lösbare Aufgabe: So werden in Tausenden von Schadensberichten, Polizeiakten, Zeugenaussagen oder wissenschaftlichen Artikeln verborgene Hinweise automatisch aufgespürt, in Beziehung gesetzt, ausgewertet und aufbereitet. Mit diesen Mustern können Bedrohungen frühzeitig erkannt, Gefahren abgewendet, Verbrechen aufgeklärt, Verhaltensempfehlungen entwickelt oder Sicherheitskräfte gezielt auf ihre Aufgaben vorbereitet werden.

Mit einem solchen Web-gestützten Führungs- und Steuerungsinstrument identifiziert das Österreichische Bundeskriminalamt Veränderungen in der Verbrechensstatistik, entwickelt Präventionsmassnahmen und plant nationale Einsätze. Anhand einer umfassenden Datensammlung, Methoden zur Auswertung sämtlicher Daten, einer aussagekräftigen Visualisierung und interaktiven Präsentationen können neuralgische Gebiete mit einer hohen Zahl spezifischer Deliktarten erkannt, die Polizeipräsenz der Situation angemessen geplant und Polizeieinsätze ausgewertet und optimiert werden.

Gemeinsam stärker

Auch im Kampf gegen terroristische Bedrohungen kommen Data- und Text-Mining-Technologien zum Einsatz. So erhalten die Fahnder aus zunächst unstrukturierten Daten in diversen Sprachen, darunter auch Arabisch und Chinesisch, aus Webseiten, Chat Rooms, E-Mails, Faxen oder aufgezeichneten Telefongesprächen den möglicherweise entscheidenden Hinweis, um den Angreifern einen Schritt voraus zu sein und das Schlimmste zu verhindern.

Am zuverlässigsten und wirksamsten kann gegen verschiedene Bedrohungen vorgegangen werden, wenn die einzelnen Anwendungen wie Data Warehouses, Data- und Text-Mining-Verfahren, Web-Analyse-Tools und Callcenter-Technologien kombiniert werden. Die Technik darf jedoch die Anwender, die als Juristen, Polizeiermittler oder Sachbearbeiter für Schadensfälle Spezialisten auf ihren jeweiligen Gebieten sind, nicht überfordern. Denn je mehr sich diese auf ihre eigentlichen Aufgaben konzentrieren können und dabei Unterstützung durch moderne leistungsfähige Verfahren erhalten, umso erfolgreicher werden sie im Kampf gegen die Kriminalität sein. ■

Quellen

CSI/FBI Computer Crime and Security Survey 2005
PricewaterhouseCoopers Global Economic Crime Survey 2005