Innere Sicherheit

Betrügern auf der Spur

[14.02.2014] Intelligente Analyse-Software kann die Polizei bei Ermittlungen effektiv unterstützen. Das zeigt ein Modellversuch von IBM, BITKOM und dem Landeskriminalamt NRW.

Die Bedrohung durch Cyber-Kriminalität in Deutschland hat im vergangenen Jahr mit rund 64.000 Fällen einen Höchststand erreicht. Laut Polizeilicher Kriminalstatistik (PKS 2012) sind die Betrugsfälle im Vergleich zum Jahr 2011 um 7,5 Prozent gestiegen. Die Schäden belaufen sich auf mehrere Milliarden Euro. Phishing heißt der neue Trend, bei dem persönliche Passwörter, TAN-Nummern und Kreditkartendaten über das Internet erschlichen und für Finanztransaktionen missbraucht werden. Die Notwendigkeit, sich technisch gegen diese neue Form der Kriminalität zu rüsten und möglichst präventiv tätig zu werden, wird immer größer.
Wie mithilfe von Big-Data- und Analysetechnologien Kreditkartenbetrüger schneller identifiziert werden können, zeigt ein Modellversuch, der im Jahr 2012 mit IBM, dem Branchenverband BITKOM und dem Landeskriminalamt (LKA) Nordrhein-Westfalen durchgespielt wurde. Hierfür hat IBM gemeinsam mit Beamten des LKA und mit Zustimmung der Staatsanwaltschaft ein bereits abgeschlossenes Ermittlungsverfahren gegen eine internationale Phishing-Bande zu einem Kreditkartenbetrug rekonstruiert. Eingesetzt wurde dafür IBM Content Analytics (ICA), eine intelligente Analyse-Software zur Auswertung strukturierter und unstrukturierter Daten.

Straftaten im Internet schneller aufklären

Im Modellversuch wurden rund eine Million Dokumente mit einem Speichervolumen von 20 Gigabyte, die sich auf von der Polizei beschlagnahmten Festplatten befanden, in die ICA-Software eingespeist. Die Anwendung überprüfte Personen- und Städtenamen, Transaktionsnummern, Bankleitzahlen und Kreditkartennummern auf Wechselbeziehungen. Auch semantische Bausteine wie der Jargon der Hacker-Szene flossen in die Analysen ein. Auf Basis der individuell implementierten Analysebausteine half die IBM-Software, Sachzusammenhänge herauszustellen und diese mittels Korrelationskoeffizienten auszuwerten. Die Inhalte wurden dann nach Relevanz und Häufigkeit aufbereitet und verknüpft.
Im vorliegenden Fall konnte auf diese Weise beispielsweise anhand der ICQ-Chat-Nummer eines Verdächtigen nachgewiesen werden, mit wem er kommunizierte und in Chat-Protokollen TAN-Nummern, die für den Online-Betrug eingesetzt worden waren, identifiziert werden. So gelang es, aus umfangreichen Verbindungsgeflechten sehr viel schneller tatrelevante Informationen herauszufiltern und zahlreiche Beweise für illegale Transaktionen zu sammeln. Im Modellversuch hat es nur eine Stunde gedauert, die riesige Datenmenge nach Relevanz und Häufigkeit auf- und vorzubereiten, die semantische Analyse war innerhalb weniger Stunden abgeschlossen. Was folgte, war die menschliche Interpretation der Ergebnisse, die auf dieser Datengrundlage wesentlich schneller möglich war.
Analyse-Software wie IBM Content Analytics gehören zwar noch längst nicht zum Standardrepertoire bei den Ermittlungen der Polizei und der Sicherheitsbehörden. Das LKA-Beispiel zeigt jedoch, wie effektiv solche Lösungen die Arbeit der Polizei unterstützen können. Entsprechende Software kann bei der Aufklärung von Straftaten im Cyberspace tatsächlich einen entscheidenden Vorteil bringen – sowohl hinsichtlich der Schnelligkeit als auch beim Auffinden bestimmter Korrelationen. Insbesondere bei semantischen Analysen und der Mustererkennung bieten diese Instrumente entscheidende Zeitvorteile.

()

Dieser Beitrag ist in der Februar-Ausgabe von Kommune21 im Schwerpunkt Big Data erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Panorama, Big Data, Polizei