Kampf gegen Geldwäsche + Betrug

Kognitive Suche unterstützt Sicherheitsdienste im Kampf gegen Terrorismus, Betrug und Geldwäsche

Die steigende Cyberkriminalität stellt staatliche Sicherheitsdienste inzwischen vor ebenso große Herausforderungen wie „traditionelle" terroristische Bedrohungen. Mehr Personal zur Prävention abzustellen (wie es in Frankreich seit den Anschlägen von 2015 praktiziert wird), reicht nicht mehr aus als Antwort auf die Bedrohung. Autor: Hans-Josef Jeanrond, Chief Marketing Officer bei Sinequa (1)

(1) Sinequa bietet Global 2000 Unternehmen und öffentlichen Verwaltungen eine leistungsfähige Plattform für kognitive Suche und Analyse. Basierend auf den Ergebnissen jahrelanger sprachwissenschaftlicher Forschung und mit neuen Machine Learning-Algorithmen lassen sich mit der Sinequa-Plattform wertvolle Informationen aus sehr großen und komplexen Datenbeständen, aus strukturierten Daten von Unternehmensanwendungen und unstrukturierten Datenquellen gewinnen. Millionen von Nutzern in den weltweit größten und informationsintensivsten Unternehmen arbeiten mit der Sinequa-Plattform, darunter bei Airbus, AstraZeneca, Atos, Biogen, UCB, Credit Agricole, Mercer und Siemens. Bei der Weiterentwicklung seiner Expertise und der weltweiten Geschäftsaktivitäten arbeitet Sinequa mit einem breiten Netzwerk an Technologie- und Vertriebspartnern zusammen. [www.sinequa.com]

Die Menge an Datenquellen, aus denen sich Schlüsselinformationen über potenzielle Gefahren ziehen lassen, wird immer größer und unübersichtlicher. Mit reiner Manpower können Sicherheitsbehörden dies nicht mehr bewerkstelligen. Der Kampf gegen die Cyberkriminalität lässt sich nur gewinnen, wenn man mit großen Mengen von strukturierten und unstrukturierten Daten richtig umzugehen versteht und es gelingt, in kurzer Zeit Schlüsselinformationen aus diesen Daten zu extrahieren und zu analysieren. Dies wird die Arbeit von Sicherheitsbehörden revolutionieren.

Sie müssen dazu zunächst die untersuchten Datenquellen fortlaufend erweitern und die Interoperabilität zwischen ihren Systemen optimieren.

Anschließend können neueste Datenverarbeitungstechnologien wie Natural Language Processing (NLP), Machine Learning und Deep Learning zur Analyse der Quellen zum Einsatz kommen.

Sie machen die Arbeit von Sicherheitsbehörden effizienter und schneller, ermöglichen eine engmaschige Kontrolle der von Kriminellen genutzten Kommunikationsmittel und führen vor allem

dazu, dass die Behörden Anschläge antizipieren und somit rechtzeitig Gegenmaßnahmen einleiten können.
Moderne Softwareplattformen für Kognitive Suche wie Sinequa kombinieren solche Technologien, so dass sich die verschiedenen Analysemethoden gegenseitig verstärken. Die Ergebnisse aller Analysen werden in einem sogenannten „Logical Data Warehouse" gespeichert, das so bei allen eingehenden Daten und mit jeder Analyse permanent angereichert wird. Dadurch können Anwender mit der entsprechenden Zugriffsberechtigung sehr schnell auf die für sie relevanten und wichtigen Informationen zugreifen, ohne dass erst die Rohdaten durchforstet werden müssen.
Machine Learning Algorithmen verfeinern ihre Analysen in vielen Iterationen fortlaufend, so dass sie im Laufe der Zeit immer relevantere Ergebnisse liefern. Zusammen mit Sprachverarbeitung (Natural Language Processing, NLP) und einigen Deep Learning Algorithmen (Neuronale Netze) bieten sie Intelligenztechniken im Kampf gegen Terrorismus, Geldwäsche und Betrug. Die Effizienz von Nachrichtendiensten wird damit enorm gesteigert, die Kapazitäten für prädiktive Analysen erhöhen sich um ein Vielfaches.

Schutz vor Angriffen dank Insight Engine Technologie

Cognitive Search-Plattformen interpretieren Daten und erkennen Ähnlichkeiten in Themen und Inhalten, auch wenn Texte nicht das gleiche Vokabular verwenden. Sie können Netzwerke von Personen, Themen, Orten etc. abbilden. Sicherheitsdienste können damit kriminelle Aktivitäten und beteiligte Personen identifizieren.
Selbst bei den „Einzelgängern" ist es möglich, die Spuren, die sie zwangsläufig im Internet oder Darknet hinterlassen, zu entdecken - sofern die Polizei und Nachrichtendienste ihre Quellen mit kognitiver Suche auswerten und so Verhaltensmuster aufdecken und Gefährder daran hindern, aktiv zu werden.
Kognitive Suche spielt eine wesentliche Rolle bei der Bekämpfung der Geldwäsche, die eine der Hauptquellen für die Finanzierung des Terrorismus ist. Die Ermittler haben die Aufgabe, Cyberkriminelle zu identifizieren und müssen dabei in kürzester Zeit riesige Datenmengen nutzen. Über Cognitive Search erhalten sie bislang kaum mögliche Einsichten in diese Daten.

Sie können Finanzdaten wie Konto- und Kartennummern und Transaktionen und damit verknüpfte Personen miteinander vergleichen, um betrügerische Aktivitäten zu identifizieren. Sie können auch unvollständige oder „dünn gesäte" Daten aufspüren und kombinieren - und damit die Zusammenhänge zwischen Verdächtigen und Kapitalbewegungen nachvollziehen. Insight Engines nutzen diese Interaktionskartierung, um Spuren illegaler Aktivitäten aufzuspüren und zu den Tätern zurückzuverfolgen.
Die Überwachung sozialer Netze, von Diskussionsforen, Blogs und anderen digitalen Kommunikationsmitteln zur Verfolgung der organisierten Kriminalität ist für die Arbeit der Nachrichtendienste von grundlegender Bedeutung. Sie nutzen Open Source Intelligence (OSINT), die alle Informationen aus öffentlichen Informationsquellen umfasst.
Die jüngsten Terroranschläge haben gezeigt, dass Reaktionsfähigkeit der Schlüssel zu einer wirksamen Überwachung ist. Mit den Mitteln von kognitiver Suche lassen sich radikalisierende Profile schneller erkennen und in Echtzeit Einblicke in potenzielle Bedrohungen erhalten. Ohne Einsatz solcher Technologien stünden Polizei und Nachrichtendienste in aller Welt im Kampf gegen Cyberkriminalität längst im Abseits. ■