Die Nadel im Heuhaufen finden: IBM kombiniert Sicherheit mit Big Data-Analytik

Die Nadel im Heuhaufen finden: IBM kombiniert Sicherheit mit Big Data-Analytik

Analyse historischer Daten schützt besser vor zukünftigen Angriffen
Unternehmen sehen sich seit kurzer Zeit mit raffinierteren Internet-Angriffen und einer steigenden Anzahl von Betrugsfällen konfrontiert. Zudem verändern die Nutzung von Social Media, mobilen Geräten und Cloud Computing sowie das exponentielle Datenwachstum die Sicherheitslandschaft von Grund auf. Mit IBM Security Analytics for Big Data kündigt IBM (NYSE: IBM) jetzt eine Software an, die in Datenmassen versteckte Bedrohungen schneller aufdeckt.
IBM Security Analytics for Big Data kombiniert die IBM Security Intelligence-Lösungen mit Big Data-Analytics: Die Software liefert mittels Echtzeit-Korrelationen fortlaufend Erkenntnisse zur Bedrohungslage, analysiert große Mengen klassisch strukturierter Daten (z.B. Security-Protokolle) und polystrukturierter Daten (z.B. E-Mails oder Social Media Content) und sichert dank Forensik-Funktionen Beweise für Angriffe oder Betrugsfälle. Auch komplexe Herausforderungen wie Advanced Persistent Threats, Betrug und interne Bedrohungen lassen sich mit diesen Funktionen besser bewältigen. Zudem schützen sie sensible Informationen stärker und verringern das Risiko von finanziellen Verlusten, Compliance-Verletzungen und Image-Schäden.
Die Depository Trust
 Clearing Corporation (DTCC) beispielsweise, ein US-amerikanisches Clearinghouse, nutzt moderne Datenanalysen, um Finanzmärkte und -systeme zu schützen. "Da Raffinesse und technologische Möglichkeiten der Cyber-Kriminellen stetig wachsen, müssen Finanzbranche und Regierungen auf risikobasierte Systeme umsteigen, die die Dynamik dieser neuartigen Bedrohungen miteinbeziehen", erklärt Mark Clancy, CISO, Managing Director, Technology Risk Management bei DTCC. "Die IBM Lösung "Security Analytics for Big Data" ermöglicht uns permanente Wachsamkeit sowie wichtige Einblicke in die historischen Aktivitäten unterschiedlichster Daten über mehrere Jahre hinweg."
"IBM Security Analytics for Big Data findet die sprichwörtliche ?Nadel im Heuhaufen. Nur haben wir es inzwischen nicht mehr mit einem Heuhaufen zu tun, sondern mit einem expandierenden Datenuniversum - und wir müssen fast das ?Sandkorn in dieser Galaxie finden", sagt Gerd Rademann, Business Unit Executive, IBM Security Systems Deutschland . "IBM Security QRadar kombiniert mit der IBM Hadoop-fähigen Plattform BigInsights erstmals wichtige Einblicke in historische und gegenwärtige Daten und schafft damit ein umfassenderes Datenverständnis als bislang möglich."
Intelligenz und Analyse in der Praxis
Um Advanced Persistent Threats oder Betrugsfälle aufzudecken oder interne Bedrohungen zu analysieren, wird eine neue Art von Lösungen benötigt. Diese müssen größere Datenmengen flexibler analysieren können und genauere Ergebnisse liefern. Um dies zu erreichen, kombiniert IBM Security Analytics for Big Data die Plattform IBM QRadar Security Intelligence mit der IBM Big Data-Plattform. Erstere bietet Echtzeit-Korrelation, erkennt Anomalien und liefert sofortige Berichte. Zudem sendet QRadar angereicherte Sicherheitsdaten an die Big Data-Plattform. Diese beinhalten Kontextinformationen wie die geografische Lage, betroffene Anwendungen, die Reputation involvierter Websites und Daten zur Anwenderidentität. Die Big Data-Produkte analysieren diese Informationen gemeinsam mit riesigen Mengen polystrukturierter und klassisch strukturierter Daten aus unterschiedlichen Quellen. Danach werden die Informationen wieder in QRadar zurückgespeist, wodurch ein kontinuierlicher Lernkreislauf entsteht.
Die wichtigsten Funktionen:
Echtzeit-Korrelation und Anomalien-Erkennung bei unterschiedlichsten Sicherheitsdaten Hochgeschwindigkeitsabfrage von Sicherheitsintelligenzdaten Flexible Big Data-Analyse strukturierter und unstrukturierter Daten - einschließlich Sicherheits-, Geschäftsprozess- und anderer Daten Grafisches Frontend-Tool zur Visualisierung und Untersuchung von Big Data Forensik für eine profunde Transparenz der Netzwerkaktivitäten Zusätzliche Funktionen und Services
IBM Security Analytics for Big Data verfügt über umfangreichen voreingestellten Security Intelligence Content. Dieser reicht von umfassender Datensicherheits-Taxonomie und automatisierter Datennormalisierung bis zu vordefinierten Regeln und Dashboards, die die Best-Practices der Branche kodifizieren und den Time-to-Value-Zyklus verkürzen.
Unterstützt wird die Lösung außerdem durch Security Analytics for Big Professional Services von IBM. Diese Services helfen Anwendern bei der Einführung von IBM Security Analytics for Big Data. Unter anderem bieten sie Design-Best-Practices und bewährtes Implementierungs-Know-how. IBM bietet diese Services auch Business- und Solution-Partnern für die Lieferung an den Endkunden an.
Verfügbarkeit
Die Produkte der IBM QRadar Security Intelligence und IBM Big Data Plattformen, einschließlich IBM InfoSphere BigInsights, sind voraussichtlich ab sofort verfügbar.
Über IBM Security
Das IBM Sicherheitsportfolio bietet eine umfassende Security-Intelligence, die Unternehmen dabei unterstützt, ihre Mitarbeiter, Daten, Anwendungen sowie die gesamte Infrastruktur zu schützen. IBM liefert Lösungen für das Identity- und Access-Management, das Security-Information- und Event-Management, die Datenbanksicherheit, Anwendungsentwicklung, das Risikomanagement, Endpoint-Management, die Intrusion-Prevention der nächsten Generation sowie vieles mehr. IBM betreibt eine der weltweit umfangreichsten Organisationen für Forschung, Entwicklung und Delivery in der Informationssicherheit. Dieses umfasst neun Security Operations Center (SOC), neun IBM Forschungs- und Entwicklungszentren, elf Entwicklungslabors für Softwaresicherheit sowie ein Institute for Advanced Security mit Zweigstellen in den Vereinigten Staaten, Europa und dem Asien-Pazifik-Raum. IBM überwacht 15 Milliarden sicherheitsrelevante Ereignisse pro Tag in über 130 Ländern und hält mehr als 3.000 Patente im Bereich der Informationssicherheit.
Weitere Informationen über IBM Security finden Sie unter www.ibm.com/security .

IBM Deutschland GmbH (Hauptverwaltung)
IBM-Allee 1
71137 Ehningen
Deutschland
Telefon: +49 800 225 5426
Telefax: +49 7032 15 3777
Mail: halloibm@de.ibm.com
URL: http://www.ibm.de
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=521247" width="1" height="1">

Pressekontakt

IBM Deutschland

71137 Ehningen

ibm.de
halloibm@de.ibm.com

Firmenkontakt

IBM Deutschland

71137 Ehningen

ibm.de
halloibm@de.ibm.com

IBM gehört mit einem Umsatz von 95,8 Milliarden US-Dollar im Jahr 2009 zu den weltweit größten Anbietern im Bereich Informationstechnologie

(Hardware, Software und Services) und B2B-Lösungen. Das Unternehmen beschäftigt derzeit 399.400 Mitarbeiter und ist in über 170 Ländern aktiv.Die IBM in Deutschland mit Hauptsitz bei Stuttgart ist die größte Ländergesellschaft in Europa.Mehr Informationen über IBM unter: ibm.com/de/ibm/unternehmen/index.htmlIBM ist heute das einzige Unternehmen in der IT-Branche, das seinen Kunden die komplette Produktpalette an fortschrittlicher Informationstechnologie anbietet: Von der Hardware, Software über Dienstleistungen und komplexen Anwendungslösungen bis hin zu Outsourcingprojekten und Weiterbildungsangeboten.