

Big Data birgt Risiken

Firmendaten Je mehr Informationen bei einem Unternehmen zusammenlaufen, desto schwieriger ist es, sie zu schützen. Klassische Mittel stossen an ihre Grenzen.

VOLKER RICHERT

Die Explosion des Datenaufkommens geht Hand in Hand mit der dezentralen Datenhaltung und Vernetzung. Immer neue Quellen werden erschlossen und verstärken die Datenmassen, womit bisher unbekannte Sicherheitsrisiken einhergehen. Denn die meisten bestehenden Datenschutzmassnahmen und Sicherheitswerkzeuge sind nicht für riesige Datenvolumina ausgelegt, wie man kürzlich beim ICT-Forschungs- und Beratungshaus Experton Group konstatiert hat. Kommt hinzu, dass BI-Tools (Business Intelligence) primär keine eigentlichen Sicherheitsaufgaben wahrnehmen. Sollen sie doch vielmehr den Anwendern Fragen beantworten, um bessere Erkenntnisse für die Unternehmensführung zu gewinnen.

Zwar nehmen diese Tools das Thema Security ernst. Doch mit den vielen Technologien, die als Datenquellen genutzt werden, existieren ebenso viele Wege, den Zugriff auf die Daten löchrig zu machen.

Ganzheitlicher Ansatz

Martin Rast, Regionaldirektor Schweiz und Österreich beim BI-Spezialisten Qlik, umschreibt das Problem so: «Der Fokus einiger Big-Data-Anbieter lag stark auf

dem Sammeln, Speichern und Auswerten von Informationen; die vielfachen Security-Herausforderungen rund um Big Data sind dabei in den Hintergrund getreten.» Aber diese Entwicklung sei nun stark im Wandel und dies werde auch in Zukunft kontinuierlich weitergehen. Mit dem stärkeren Engagement für die Security im Big-Data-Umfeld würde auch das Vertrauen in

solche BI-Systeme gesteigert, ist Rast überzeugt. Er betont denn auch, dass «ein ganzheitlicher Security-Ansatz gewählt werden muss, der vom Eingangspunkt der Daten bis hin zum Nutzen der Informationen durch den Anwender den gesamten Prozess umfasst».

Sicherheitsmassnahmen in Netzwerken und Firewalls, Verschlüsselung und Verschleierung, Zugriffsberechtigungen und Monitoring sowie Audits werden künftig zusammenarbeiten, um gemeinsam sichere Umgebungen zu schaffen.

Doch offensichtlich sind derartige Systeme noch Mangelware. Denn gerade die im Datenschutz so zentrale Anonymisierung personenbezogener Daten stellt nach wie vor eine «grosse Herausforderung» dar, wenn umfangreiche Datenmengen einer sogenannten Maskierung unterzogen werden sollen, hielten die BI-Spezialisten der Experton Group soeben fest. Und zwar insbesondere darum, weil hierzu die personenbezogenen Daten erst

einmal aufgespürt werden müssen, um sie dann der bei Big Data üblichen automatischen Bearbeitung unterziehen zu können. Wobei unstrittig sei, dass dieses Vorgehen bisher schon bei überschaubaren Datenmengen nicht immer zuverlässig klappe. Komme noch die geforderte Kontrolle, ob die Datenmaskierung erfolgreich war, hinzu, würde das Werkzeuge erfordern, die zuverlässiger und schneller arbeiten als das Anonymisierungsprogramm selbst. Wobei allen Beteiligten bei diesen Anforderungen klar ist, dass – wie generell bei Big Data – auch bei einer solchen Kontrolle ein manuelles Vorgehen genauso ausgeschlossen ist, wie man sich in diesem Bereich sicher nicht auf Stichproben beschränken kann.

Der fehlende Überblick

Beim global tätigen IT-Dienstleister CSC stimmt man der Analyse grundsätzlich zu: «Big-Data-Technologien von heute sind sich der Inhalte in den Datenbanken nicht bewusst.» Die heutigen BI-Tools seien als «Report-Generatoren» auch nicht in der Lage, Security-Verstösse bei speziellen Auswertungen zu erkennen, sagt Peter Ronchetti, Vorsitzender der Geschäftsleitung von CSC Schweiz. Vielmehr werde bisher noch der Schutz personenbezogener Daten an die Datenerzeuger delegiert, während die BI-Prozesse von den Datenauswertern abgesichert würden. So sind bei Big Data grundlegende Fragen noch ungeklärt. Nicht nur muss,

wer Daten schützen will, sie erst einmal identifizieren. Schon ganz am Anfang ist zu klären, welche Kategorien personenbezogener Daten überhaupt vorliegen, zumal davon der Schutzbedarf abhängt. Rast konstatiert denn auch, dass mit den wachsenden Datenmengen die Gefahren für Datenmissbrauch und Kontrollverlust steigen: «IT-Abteilungen haben oft nicht den nötigen Überblick darüber, welche Daten überhaupt im Unternehmen vorhanden sind und wer Zugriff darauf hat – oder besser nicht haben sollte.» Für Rast ist deshalb das als Data Governance umschriebene Organisationskonzept ein zentrales Stichwort. Denn abgesehen von

der rein technischen Seite erfordere der Umgang mit Big Data zusätzlich eine Kultur der Verantwortung im Unternehmen, wobei beispielsweise genau geklärt werden müsse, wer für welche Daten verantwortlich ist.

Tom Sprenger, Technologiechef des Informatikunternehmens Adnovum, ergänzt zu den technischen Aspekten: «Das Paradigma der Perimeter-Sicherheit sowie etablierte Access-Mechanismen stossen zunehmend an Grenzen.» Über kurz oder lang können in Big-Data-Projekten die Daten und Berechtigungen nur noch automatisiert verwaltet und über adaptive Methoden geschützt werden. Dabei gehe

KEINE STRATEGIE Die Leiden der IT-Chefs

Studie In der Studie «Big Data Analytics in Cyber Defense» der Analysten des Ponemon Institute wurden 2013 mehr als 700 IT-Sicherheits-Experten befragt:

- ▶ 56 Prozent kennen zwar Sicherheits-technologien für Big Data Analytics,
- ▶ 61 Prozent meinen, dass damit dringliche Sicherheitsprobleme von unstrukturierten Daten aus dem Cyberspace zu lösen sind, doch nur
- ▶ 35 Prozent haben derartige Technologien tatsächlich im Einsatz.

Zudem hat das Beratungshaus Steria Mummert in seinem «Business Intelligence Maturity Audit» 2013 festgestellt, dass von den rund 650 befragten IT-Spezialisten.

- ▶ 38 Prozent in Big-Data-Projekten mit schlechter Datenqualität kämpfen,
- ▶ 72 Prozent über keine BI-Strategie verfügen und
- ▶ 70 Prozent keine Data Governance vorweisen können.

es darum, so Sprenger weiter, auf der Basis von Metadaten und dem Verhalten des Benutzers dynamisch den Zugriff auf Daten gewähren oder verweigern zu können (siehe Interview rechts).

Zwar eignen sich BI-Tools hervorragend für sogenannte Offline- oder Post-Access-Analysen. Dabei könnten auch sicherheitsrelevante Metadaten wie etwa Zugriffslogs via BI ausgewertet und hinsichtlich Anomalien durchsucht werden, um Auffälligkeiten im Datenzugriff oder Benutzerverhalten zu erkennen. Bei Banken oder Kreditkartenfirmen würden auf diese Weise bereits heute auffällige Zugriffe herausgefiltert und betrügerische Transaktionen ausfindig gemacht. Und derartige Werkzeuge würden auch immer ausgereifter und mächtiger. Damit der Schutz aber wirklich greife, gibt Sprenger zu bedenken, müsste die Erkennung von Anomalien allerdings in Echtzeit erfolgen können.

Unstrukturierte Datenmengen

Daniel Tydecks, Spezialist für Complex Event Processing bei der Software AG, weist darauf, dass es bei klar strukturierten Massendaten noch vergleichsweise einfach ist, sie zu analysieren und abzusichern. Überall dort aber, wo unstrukturierte Daten die automatisierte Bearbeitung von Informationen erschweren und zusätzliche Interpretationen erfordern,

würde es auch in Sachen Datenschutz schnell sehr komplex. So ist es beispielsweise möglich, Social-Media-Streams zu Unternehmen in Real-Time-Analysen zu verwenden. Sicherzustellen, dass dabei keine personenbezogenen Daten ungewollt verarbeitet werden, ist aufgrund der Natur der Datenquelle schwierig. CSC bestätigt, dass bei strukturierten Daten die bekannten und bewährten Sicherheitsmechanismen greifen, im Bereich der unstrukturierten Daten aber bessere Funktionalitäten für den Datenschutz erforderlich sind: «Die heutigen Tools sind nicht in der Lage, den Inhalt zu erkennen. Inhaltsbezogene Zugriffsregeln können daher nicht umgesetzt werden.».

So reicht es heute auch nicht mehr aus, einen Schutzwall um das Unternehmen zu bauen und die Tore zu bewachen. Vielmehr sind, um im Bilde zu bleiben, zusätzliche Patrouillengänge im Innern zu machen. Konkret müssten Massnahmen für die innere Sicherheit wie Angriffserkennungssysteme und Anomalie-Erkennung an Bedeutung gewinnen, heisst es bei Adnovum.

CSC betont, dass die Abbildung von komplexen Berechtigungsstrukturen in den BI-Tools durch Identity-Management-Werkzeuge wegen sich schnell ändernder Anforderungen weiterhin die wichtigste Sicherheitsfunktion ist.

Es reicht nicht mehr, einen Schutzwall um die Firma zu ziehen.

«Es wird schwieriger, Daten zu schützen»

Das digitale Universum wächst schnell. Die Auswertung und Verknüpfung der Daten via Business Intelligence (BI) bietet Unternehmen und Institutionen laufend neue Möglichkeiten. Tom Sprenger, Technologiechef von Adnovum in Zürich, erklärt, wie man diese Potenziale nutzen kann, ohne die Kontrolle über die Daten zu verlieren.



Tom Sprenger
Technologiechef,
Adnovum,
Zürich

Warum ist die Sicherheit im Zeitalter von Big Data ein Problem?
Tom Sprenger: Durch die vermehrte Dezentralisierung der Datenhaltung, die Vernetzung von Daten und die Explosion der Datenmenge wird es schwieriger, Daten mit klassischen Mitteln zuverlässig zu schützen. Das Paradigma der Perimetersicherheit sowie etablierte Access-Management-Mechanismen wie Role-Based Access Control (RBAC) stossen zunehmend an Grenzen. Über kurz oder lang können die Daten und Berechtigungen nur noch automatisiert verwaltet und über adaptive Methoden geschützt werden, welche auf der Basis von Metadaten und dem Verhalten des Benutzers beruhen.

Sie sprechen in Sachen Big Data von einem Paradigmenwechsel, warum?
Daten werden heute zunehmend applikations- und systemübergreifend ausgewertet. In der Konsequenz ist ein Schutz von Daten aus reiner Applikations- oder Systemsicht nicht mehr ausreichend. Mit der Verschiebung vom Paradigma der Applikations- und Systemverantwortlichen hin zur Data Ownership, also zur Verantwortung für Daten über System- und Applikationsgrenzen hinweg, können Daten übergreifend geschützt und so zum Beispiel die rechtlichen Vorgaben eingehalten werden.

Warum reichen für Big Data Security die inzwischen doch ausgereiften BI-Tools nicht aus?
Heutige BI-Tools verfolgen grundsätzlich einen anderen Zweck und dienen eben der Unterstützung von Business

Intelligence (BI). Aus Sicht ihrer analytischen Fähigkeiten wären diese Werkzeuge genügend potent, um in der Big Data Security ihren Dienst zu tun. Die Herausforderung liegt aber in einer anderen Dimension, und zwar in der Echtzeitfähigkeit. Neben der Anforderung, Security-Informationen zum Beispiel aus Logfiles offline zu analysieren, müssen die Werkzeuge fähig sein, in Echtzeit die notwendigen Security-Regelwerke auszuführen und gegebenenfalls entsprechende Aktionen auszulösen. Ein Beispiel wäre der forcierte Logout des Benutzers.

Welche Bedeutung kommt den Metadaten beim Aufgleisen von Big Data Security zu?
Die Metadaten bilden die Grundlage, auf der die adaptiven und damit dynamisch agierenden Mechanismen für die Big Data Security aufsetzen. Von daher sind die Metadaten und insbesondere deren Verfügbarkeit und Qualität von zentraler Bedeutung.

Welche drei Schritte sind wesentlich zur Umsetzung einer Data-Ownership-Strategie?
Die Identifikation der Datenpools, die Zuordnung der Daten zu Schutzklassen und die Definition von Zugriffsprozessen basierend auf der Risikoeinschätzung. Dabei gilt es, auf Datenflüsse, Datenmenge, Zugriffsmustern oder Verknüpfung mit anderen Daten zu achten. Ist eine solche Strategie einmal etabliert, sind regelmässige Reviews und Audits einzuplanen, um Veränderungen frühzeitig zu erkennen.

INTERVIEW: VOLKER RICHERT

38

Prozent der Big-Data-Projekte kämpfen mit schlechter Datenqualität

72

Prozent der IT-Chefs verfügen über keine BI-Strategie

70

Prozent der IT-Chefs können keine Data Governance vorweisen

FOTOLIA