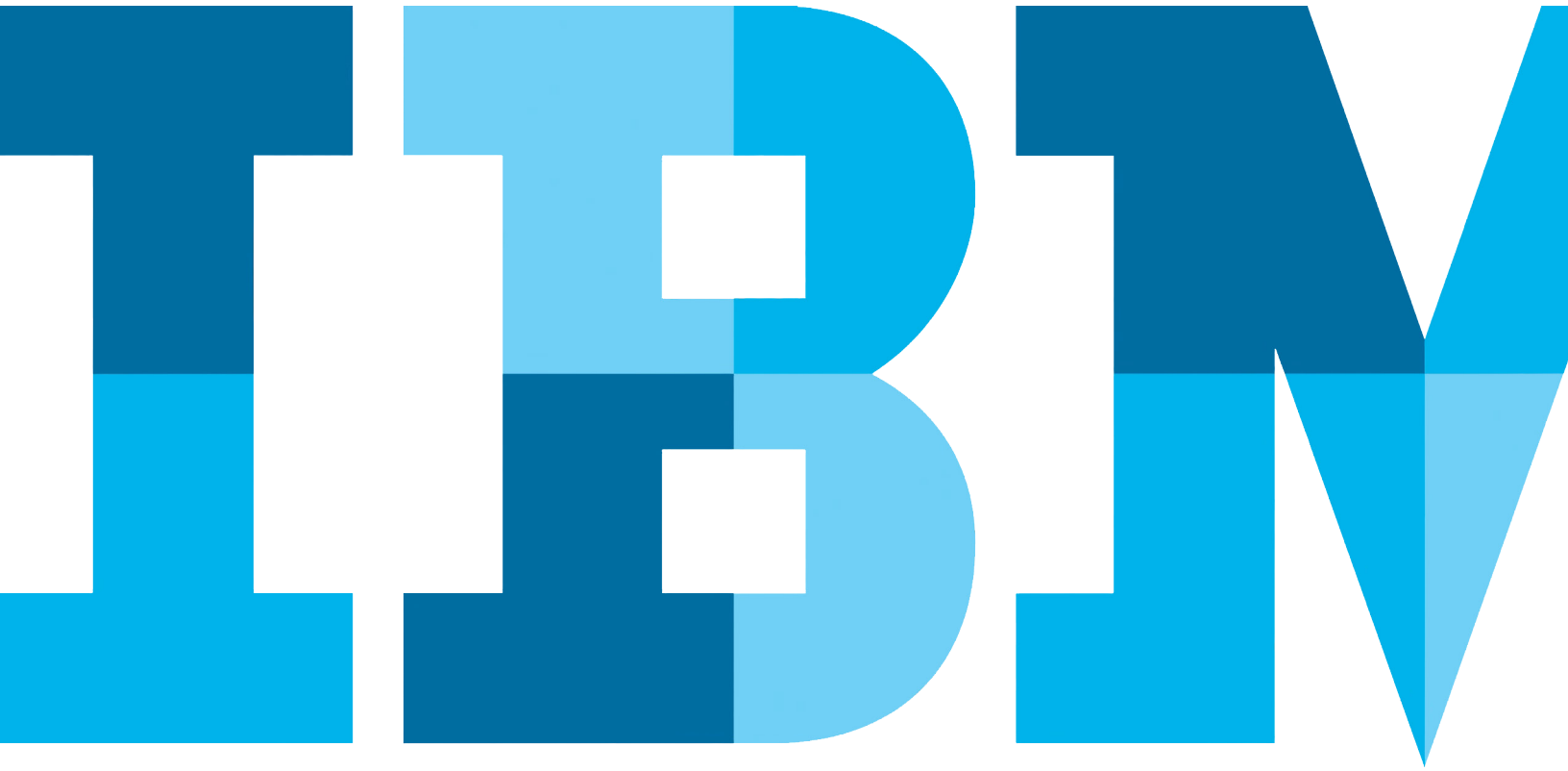
TechTarget Custom Media

July 2015

Thought-Leadership-Artikel

Umfassende Datensicherheit gegen interne und externe Angriffe

Autor: Oliver Schonschek



IBM

51 Prozent aller Unternehmen in Deutschland ist in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden, so eine Studie des Digitalverbands BITKOM. Der entstandene Schaden für die gesamte deutsche Wirtschaft wird auf rund 51 Milliarden Euro pro Jahr geschätzt. Die Angriffe gehen dabei nicht nur von Hackern aus dem Internet aus, im Gegenteil.

Laut der BITKOM-Umfrage sind es vor allem aktuelle oder ehemalige Mitarbeiter, die als Täter in Erscheinung treten: 52 Prozent der betroffenen Unternehmen hat diesen Personenkreis als Täter genannt. Der IBM 2015 Cyber Security Intelligence Index belegt die Risiken durch die sogenannten Innentäter ebenfalls: 55 Prozent aller Cyberattacken auf Unternehmen kommt aus den eigenen Reihen. Unter den Angreifern finden sich oft ehemalige Angestellte, Dienstleister mit Systemzugriff oder arglose Mitarbeiter, die Opfer von Kriminellen werden.

Viele Unternehmen haben Probleme damit, interne und externe Angreifer frühzeitig zu erkennen, geeignete Gegenmaßnahmen zu ergreifen und die richtigen Präventivmaßnahmen zu finden. Das liegt unter anderem daran, dass die zu schützenden Informationen in zahlreichen Datenbanken verteilt sind. Ein durchgehender und umfassender Schutz über Plattform- und Systemgrenzen hinweg ist hier notwendig. Eine Lösung wie IBM InfoSphere Guardium ermöglicht genau diesen plattformübergreifenden Schutz der Daten und verhindert so Datenpannen und unberechtigte Zugriffe auf vertrauliche Informationen.

Interne Schwachstellen erkennen und beheben

Innentäter müssen sich in den meisten Fällen keine raffinierten Angriffstechniken einfallen lassen, wie es die externen Hacker tun. In der Regel reicht es aus, dass sie die Schwachstellen ausnutzen, die die Datenbanken in den Unternehmen aufweisen. Schwachstellen sind in diesem Fall zum Beispiel zu umfangreiche Zugriffsberechtigungen, Systemprivilegien, die nur für eine kurze Zeit benötigt, aber nicht wieder zurückgenommen wurden. Wenn ein Mitarbeiter eine Abteilung wechselt oder ein Projekt verlässt, wird oftmals vergessen, die entsprechenden Berechtigungen für die jeweiligen Datenbanken zu entfernen. So sammeln Mitarbeiter vielfach Berechtigungen an, die sie nicht benötigen, aber missbrauchen könnten.

Hier steuert das IBM InfoSphere Guardium Vulnerability Assessment gezielt dagegen. Vorkonfigurierte und regelmäßig aktualisierte Risikotests überprüfen die Datenbanken, ob unsichere Konfigurationen, fehlende Aktualisierungen, zu einfache Passwörter oder andere Schwachstellen zu finden sind. Mit diesen Sicherheits- und Risikotests werden auch mögliche Angriffspunkte für externe Datendiebe aufgespürt und behoben.

Berechtigungssysteme überprüfen und absichern

Die Schwachstellensuche von IBM InfoSphere Guardium spürt auch verdächtige Aktivitäten auf, die von internen Datenbank-Nutzern ausgehen. Dazu gehören die gemeinsame Nutzung eines Datenbankzugangs durch verschiedene Anwender und damit die Weitergabe von Passwörtern genauso, wie die auffällig häufige Anmeldung von Administratoren oder Datenbankzugriffe

zu ungewöhnlichen Zeiten, wie zum Beispiel am Wochenende oder nach Dienstschluss.

Die aufgedeckten Berechtigungsprobleme und verdächtigen Zugriffe meldet IBM InfoSphere Guardium entsprechend einer definierten Eskalationskette. Neben der Alarmierung im konkreten Verdachtsfall bietet die Lösung auch regelmäßige Sicherheitsbewertungen. Diese Berichte enthalten die festgestellten Schwachstellen mit einer risikoabhängigen Priorisierung und bieten zudem Hinweise zu den notwendigen Maßnahmen zur Behebung der Schwachstellen. Der Zeitpunkt der Berichtserstellung lässt sich ebenso individuell festlegen wie die Verteilung der Berichte, so dass interne Workflows und Zuständigkeiten abgebildet werden können.

Mit Verschlüsselung gegen unerlaubte Zugriffe

Unberechtigte Zugriffe verhindert eine Lösung wie IBM InfoSphere Guardium zusätzlich dadurch, dass die Daten entsprechend ihrer Vertraulichkeit und ihres Schutzbedarfs verschlüsselt werden. IBM InfoSphere Guardium Data Encryption verschlüsselt die zu schützenden Daten, ohne die legitimen Nutzer in ihrer Tätigkeit zu behindern.

Die Verschlüsselung arbeitet automatisch und läuft im Hintergrund ab. Das Management der digitalen Schlüssel und die Definition der Verschlüsselungsrichtlinien erfolgt zentral, ohne weiteren Aufwand für die Benutzer. Mit dieser plattformübergreifenden Verschlüsselung sorgt IBM InfoSphere Guardium nicht nur für die Erfüllung von Compliance-Vorgaben, sondern es verhindert auch den Missbrauch vertraulicher Daten durch Innentäter oder externe Angreifer.

Aktuelle Bedrohungen und Risiken in Echtzeit berücksichtigen

Die Erkennung und Abwehr interner und externer Attacken erfolgt bei IBM InfoSphere Guardium auf Basis von Risikobewertungen in Echtzeit. Dadurch kann die Priorisierung und Umsetzung der Schutzmaßnahmen, wie zum Beispiel die Verschlüsselung gefährdeter Daten, auf die aktuelle Bedrohungslage abgestellt werden. Ein Austausch sicherheitsrelevanter Informationen mit der Security Intelligence Plattform IBM QRadar erweitert den Echtzeitschutz von IBM InfoSphere Guardium zusätzlich.

Mit der Suche nach Schwachstellen, der Prüfung der Nutzerberechtigungen, der Verschlüsselung vertraulicher Informationen und der Sicherheitsintelligenz in Echtzeit bietet IBM InfoSphere Guardium eine umfassende Datensicherheit gegen Attacken, ganz gleich, ob diese von außen oder aus den eigenen Reihen kommen, und unabhängig davon, in welcher Datenbank sich die zu schützenden Daten befinden.