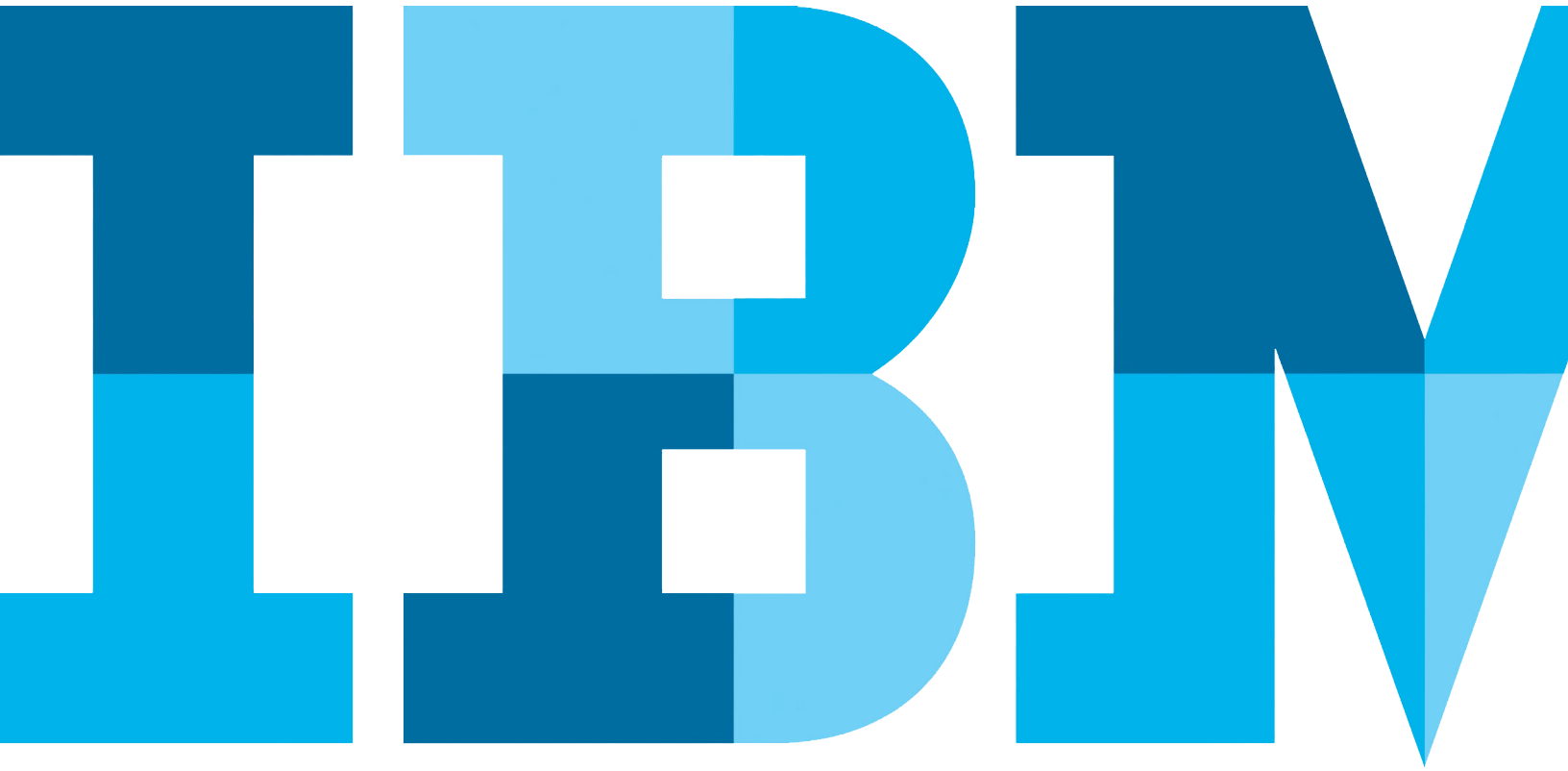
TechTarget Custom Media

July 2015

Thought-Leadership-Artikel

Datensicherheit in Echtzeit gegen dynamische Bedrohungen

Autor: Oliver Schonschek



IBM

81 Millionen bestätigte IT-Sicherheitsvorfälle, darunter rund 12.000 Cyberattacken und knapp über 100 Sicherheitsereignisse pro Unternehmen, das sind die besorgniserregenden Ergebnisse des aktuellen IBM Cyber Security Intelligence Index. Die Risikolage für Unternehmen ist ernst. Sie verschärft sich aber noch dadurch, dass viele Unternehmen die sie bedrohenden Ereignisse nicht rechtzeitig erkennen.

Wie die aktuelle Studie „2015 Cost of Data Breach Study" des Ponemon-Instituts zeigt, benötigten die Unternehmen rund ein dreiviertel Jahr, um Hackerangriffe zu entdecken. Selbst Datenverluste durch Anwenderfehler fielen erst nach rund fünf Monaten auf. Diese langen Zeitspannen bleiben nicht ohne Folgen: Gegenmaßnahmen können nicht zeitnah ergriffen werden, den Angreifern bleibt viel Zeit, die ausgespähten Daten zu missbrauchen. Dementsprechend hoch ist der Schaden für die Unternehmen. Im Durchschnitt beträgt der Schaden für ein Unternehmen in Deutschland ganze 3,5 Millionen US-Dollar pro Datenpanne.

Datensicherheitslösungen wie IBM InfoSphere Guardium bieten mit ihrem Echtzeitschutz die richtige Antwort auf die wachsenden, sich dynamisch ändernden IT-Bedrohungen. Interne Verstöße bei Zugriffen auf vertrauliche Daten werden ebenso erkannt und sofort gemeldet wie externe Angriffsversuche auf Datenbanken und Anwendungen. Abwehr- und Gegenmaßnahmen können umgehend ergriffen werden. Dies senkt nicht nur das Gefahrenpotenzial deutlich, sondern auch die Kosten, die sonst durch Datenpannen entstehen können.

Security Intelligence wird immer wichtiger

IT-Sicherheitsverantwortliche erkennen zunehmend die Bedeutung eines Echtzeitschutzes auf Basis von Security Intelligence, also der Nutzung moderner IT-Sicherheitsanalysen in Echtzeit. Die Chief-Information-Security-Officer-Studie 2014 besagt, dass für über 70 Prozent der Befragten die Nutzung von Security Intelligence in Echtzeit immer wichtiger wird. Allerdings zeigt die Studie auch, dass Security-Intelligence-Analysen noch relativ wenig ausgreift sind (54 Prozent) und verbessert beziehungsweise transformiert werden sollten.

In der Unternehmenspraxis vertrauen laut BITKOM viele Unternehmen immer noch auf einen reinen Basisschutz durch Anti-Viren-Schutz und Firewall. Solche Schutzlösungen jedoch bieten keine Möglichkeit, die internen und externen Zugriffe auf Datenbanken, Applikationen und auf vertrauliche Informationen zu überwachen, mögliche Zugriffsverletzungen zu erkennen und die notwendigen Maßnahmen einzuleiten.

Schwachstellen in Echtzeit erkennen, bewerten und melden

Das IBM InfoSphere Guardium Vulnerability Assessment sucht in Echtzeit und plattformübergreifend nach Schwachstellen in den zu schützenden Datenbanken, darunter auch Fehler in der Vergabe von Zugriffsberechtigungen. Aufgedeckte Anfälligkeiten werden sofort an die zuständige Stelle gemeldet, versehen mit einer Priorisierung der notwendigen Fehlerbehebungsmaßnahmen.

Die Risikotests, die IBM InfoSphere Guardium bei den zu schützenden Datenbanken und Applikationen ausführt,

muss das Anwenderunternehmen nicht selbst definieren oder konfigurieren. Hunderte von Sicherheitstests sind bereits im Standard in der Lösung hinterlegt. Als Echtzeitschutz bietet die Lösung von IBM zudem eine automatische und regelmäßige Aktualisierung der Testvorgaben, so dass auch neue und geänderte Risiken aufgedeckt werden können, wie zum Beispiel neu auftretende Sicherheitslücken in den überwachten Systemen.

Einbruchsversuche in Datenbanken und Anwendungen werden ebenso in Echtzeit erkannt, dafür sorgt das Data Activity Monitoring von IBM InfoSphere Guardium. Die sofortige Eskalation einer erkannten Bedrohung führt dazu, dass Systemeinbruchsversuche nicht erst nach Monaten erkannt werden, sondern in kürzester Zeit. Dadurch können Abwehrmaßnahmen eingeleitet und ein möglicher Schaden durch Angriffe minimiert werden. Zu den möglichen Reaktionen bei Verdacht auf Zugriffsmissbrauch gehören Sicherheitswarnmeldungen in Echtzeit oder zum Beispiel automatische Sperrungen von Zugängen.

Security Intelligence mit breitem Fundament

Die Überwachung der Zugriffe auf Datenbanken und Anwendungen berücksichtigt bei InfoSphere Guardium nicht nur die aufgestellten, aktuellen Regelwerke, sondern auch den Kontext der Zugriffe: Bei allen Aktivitäten in den überwachten Datenbanken und Anwendungen wird überprüft, „wer, was, wo, wann und wie“ durchführen will. So können Zugriffe, die prinzipiell erlaubt sind, trotzdem als Angriff enttarnt werden. Falsch positive und falsch negative Bewertungen von Zugriffen lassen sich deutlich mindern, die Qualität der Zugriffskontrolle steigt.

Bei der Erkennung von Verhaltensanomalien bei Datenzugriffen helfen Vergleichswerte, die die Lösung automatisch generiert und bei der Definition von Zugriffsregeln berücksichtigt. Abweichungen von der „Baseline“ können als Verdachtsmomente gewertet werden. Individuelle Anpassungen der Zugriffsregeln und Normalwerte lassen sich über eine speziell geschützte Benutzeroberfläche vornehmen. Durch die Integration mit der Security-Intelligence-Plattform IBM QRadar kann der Echtzeitschutz noch weiter angereichert werden.

Eine Lösung wie IBM InfoSphere Guardium verkürzt durch den Echtzeitschutz und die integrierte Security Intelligence deutlich die Zeitspanne bis zur Erkennung von Einbruchsversuchen und von Schwachstellen, alarmiert die zuständigen Stellen im Unternehmen und dokumentiert die ergriffenen Maßnahmen im Sinne der Compliance-Vorgaben. Dadurch wird die Lösung zu einem wichtigen Bestandteil des betrieblichen Risikomanagements.