ManageEngine
Log360

Basisprincipes van audits van SQL Server-logboeken

Inleiding

Elke databasebeheerder heeft twee grote zorgen: ervoor zorgen dat gegevens veilig zijn en dat de databaseserver beschikbaar is. Zoals u zou verwachten, zijn databases het belangrijkste doelwit voor aanvallen. Database-aanvallen kunnen niet alleen de productiviteit van bedrijven verlammen, maar ze kunnen ook gevoelige gegevens blootleggen. Dit heeft vaak juridische gevolgen. Wat erger is, is dat organisaties vaak pas weken of maanden na een inbreuk beseffen dat ze zijn aangevallen.

Regelgeving zoals de Algemene Verordening Gegevensbescherming (AVG) in Europa en de Notifiable Data Breaches (NDB) in Australië verplichten organisaties om gegevenslekken binnen een bepaalde periode aan de autoriteiten te melden. Deze voorschriften houden organisaties verantwoordelijk voor de beveiliging van de gegevens die ze opslaan.

De meeste organisaties richten zich op preventieve beveiligingsmaatregelen, zoals verificatie, versleuteling en kwetsbaarheidsscans. Deze maatregelen garanderen echter geen gegevensbeveiliging. Er is altijd een kans op een kwaadwillende aanval, die heel goed van binnenuit afkomstig zou kunnen zijn, om een beveiligingslek te misbruiken en echte schade aan te richten. Dat gezegd hebbende, is het essentieel dat beveiligingsteams kunnen detecteren en reageren wanneer er iets misgaat.

Het belang van SQL-logboeken

Wat als op dit moment iets misgaat met een van uw SQL-servers? Stel dat een gewone eindgebruiker de rol van databasebeheerder krijgt toegewezen. Wordt u hierover dan onmiddellijk geïnformeerd?

Een dergelijke gebeurtenis zou reden tot grote bezorgdheid zijn, aangezien deze de beveiliging van gevoelige gegevens in gevaar kan brengen. Scenario's als deze kunnen worden gedetecteerd door logboeken te ontsleutelen die zijn gegenereerd door SQL Server. Met een beheersysteem voor logboeken richten beveiligingsteams zich vaak onevenredig op een paar bronnen van gebeurtenissen, zoals netwerkapparaten en domeincontrollers. Vaak hebben ze niet hetzelfde niveau van zichtbaarheid op de systemen die gevoelige gegevens opslaan, zoals SQL-servers. Hierdoor missen beveiligingsteams de informatie die ze in een vroeg stadium nodig hebben om pogingen te dwarsbomen om hun database te beschadigen.

SQL-auditlogboeken vertellen een cruciaal verhaal. In feite worden verschillende gebeurtenissen, waaronder gebeurtenissen bij aanmeldingen, alleen op SQL Server geregistreerd. Organisaties moeten een auditspoor genereren en onderhouden om te zorgen dat activiteiten zoals openen, wijzigingen en andere belangrijke gebeurtenissen met betrekking tot de database worden bijgehouden.

De behoefte aan een oplossing voor beveiligingsinformatie en gebeurtenissenbeheer (SIEM, Security Information and Event Management) met een functie voor SQL-audits

De systeemeigen auditfunctie van SQL Server heeft enkele cruciale tekortkomingen. De logboeken bevatten veel waardevolle informatie. Maar de informatie is niet bruikbaar. Om te beginnen zijn geen ingebouwde rapportages en waarschuwingen beschikbaar. Zonder speciale hulpmiddelen kan het ook tijdrovend voor beveiligingsteams zijn om alle controlegegevens te doorzoeken.

Een SIEM-oplossing centraliseert auditinformatie van alle SQL-servers in uw netwerk voor effectieve analyses. Hierdoor kunnen beveiligingsteams snel bedreigingen voor de veiligheid ontdekken en hierop reageren, en om naleving eenvoudig aan te tonen.

Overwegingen en vereisten

Voordat u begint, zijn er enkele cruciale aspecten van SQL-audits die u moet overwegen:

1. **Volume van gebeurtenissen en prestaties.** Beveiligingsteams moeten het aantal SQL-servers in hun omgeving identificeren, evenals het aantal databaseverbindingen dat gedurende een dag plaatsvindt. De capaciteit van de server moet worden geanalyseerd om te zorgen dat de belasting door gebeurtenissen kan worden afgehandeld zonder prestatieproblemen te veroorzaken.

2. **Auditbeleid.** Het SQL-auditbeleid is standaard niet ingeschakeld. Daarom moet het worden geconfigureerd. Door 'geavanceerde controle' in te schakelen, krijgt u meer diepgaande inzichten in database-activiteiten. Beveiligingsteams moeten hun doelstellingen inzake beveiliging en naleving identificeren en vervolgens een auditbeleid definiëren dat de logboekvermeldingen genereert die ze nodig hebben zonder de prestaties in gevaar te brengen. Het auditbeleid kan dan worden geleverd via een Group Policy Object (GPO).

3. **Mechanisme voor verzamelen van logboeken.** Bepaal hoe de logboeken van SQL Server worden verzameld. De meeste SIEM-oplossingen op de markt bieden beveiligingsteams de flexibiliteit om een op agenten gebaseerd mechanisme of een mechanisme zonder agenten te kiezen om de logboeken te verzamelen. N.B.: Een mechanisme voor het verzamelen van logboeken zonder agenten vereist dat bepaalde poorten open blijven voor communicatiedoeleinden.

4. **Bedreigingen voor databases.** Houd rekening met de meest voorkomende databasebedreigingen, zoals SQL-injectie en misbruik van bevoegdheden. Een goed startpunt om uw beveiliging te beoordelen, is het evalueren van uw typische reactie op de belangrijkste databasebedreigingen. Vervolgens kunnen lacunes worden opgevuld door meer beveiligingsrapporten en -waarschuwingen te definiëren.

Auditrapporten plannen

Het genereren van auditrapporten is belangrijk voor het visualiseren en beoordelen van beveiligingsgebeurtenissen. Het basisdoel is alle wijzigingen die in de database zijn uitgevoerd, rechtstreeks vanaf de database-aanmelding bij te houden. Gebeurtenissen elke 24 uur beoordelen is een algemeen aanvaarde beste werkwijze. Meer volwassen organisaties moeten deze gebeurtenissen echter vaker beoordelen.

In grote lijnen omvatten auditrapporten inzake databases vier categorieën:

1. **Activiteiten inzake Data Manipulation Language (DML)**
2. **Activiteiten inzake Data Definition Language (DDL)**
3. **Activiteiten van gebruikers**
4. **Activiteiten van servers**

Beveiligingswaarschuwingen configureren

Het instellen van waarschuwingen voor compromisindicatoren (IoC's, Indicators of Compromise) is van vitaal belang om snel mogelijke gegevenslekken te ontdekken en hierop te reageren. Hoewel rapporten effectief zijn voor het periodiek beoordelen van gebeurtenissen, moeten er waarschuwingen worden ingesteld voor gebeurtenissen die onmiddellijk onderzoek vereisen. Het idee is om te letten op gebeurtenissen die onder normale omstandigheden niet mogen gebeuren. Enkele voorbeelden:

1. **Escalaties inzake privileges**
2. **Afsluiten/opnieuw opstarten van servers**
3. **Herhaalde mislukte aanmeldingspogingen en accountvergrendelingen**
4. **Wijzigingen aangebracht aan machtigingen (rollen)**
5. **Wijzigingen aangebracht aan gevoelige kolommen**
6. **Verdachte back-ups van gegevens**
7. **Bekende aanvalspatronen, zoals SQL-injectie**
8. **Wijzigingen aan het auditbeleid**

Verbeterde beveiliging met correlatie tussen gebeurtenissen

Organisaties die op zoek zijn naar een meer volwassen beveiliging, moeten gebruikmaken van geavanceerde technieken, waaronder correlatie en analyse van gebeurtenissen. Gebeurteniscorrelatie koppelt gebeurtenissen die plaatsvinden op SQL Server aan gebeurtenissen die plaatsvinden in andere delen van het netwerk. Dit geeft meer context over een ongebruikelijke gebeurtenis, zodat een compleet beeld wordt verkregen van de hele aanvalsketen.

Mogelijkheden voor SQL-audits van ManageEngine Log360

ManageEngine Log360 is een uitgebreide SIEM-oplossing die wordt geleverd met een vooraf gebouwde functie voor SQL-audits die alles aan kan wat in dit e-boek wordt besproken. En nog meer! Log360 ontdekt automatisch SQL-servers in uw netwerk. Het maakt audits mogelijk, verzamelt en archiveert logboeken, genereert uitgebreide auditrapporten en activeert waarschuwingen voor potentiële bedreigingen voor databases.

- **Diepgaande SQL-audits.** Het hulpmiddel wordt geleverd met vooraf gebouwde rapporten en waarschuwingen voor het volgen van elke belangrijke beveiligingsgebeurtenis op SQL Server. Neem voor meer informatie over alle beschikbare rapportage- en waarschuwingsprofielen contact op met ons ondersteuningsteam via log360-support@manageengine.com.

- **Correlatieregels om aanvallen te detecteren.** De krachtige engine voor correlatie van Log360 kan SQL-auditlogboeken correleren met informatie die is verzameld uit andere gebeurtenisbronnen. Op deze manier worden pogingen tot gegevenslekken in een vroeg stadium gedetecteerd. Voorbeelden zijn de detectie van verdachte SQL-back-ups en herhaalde pogingen tot SQL-injectie.

Over de auteur

Siddharth Sharath Kumar is een specialist in IT-beveiliging en -naleving in het productmarketingteam van ManageEngine. Hij schrijft artikelen en e-boeken, organiseert regelmatig webinars over belangrijke onderwerpen inzake IT-beveiliging en presenteert op congressen van ManageEngine en andere branche-evenementen over de hele wereld.