

Motiv Security Management voor Databases

Beveiliging binnen de kaders van wet- en regelgeving

De wet- en regelgeving op het gebied van informatiebeveiliging wordt steeds strenger. Zo vereisen Sarbanes-Oxley, Basel II, Voorschrift Informatiebeveiliging Rijksoverheid en ISO 17799 bijvoorbeeld dat uw informatiebeveiliging toetsbaar is. In bepaalde gevallen moeten u zelfs tekenen voor het geïmplementeerde beveiligingsbeleid bij uw organisatie. Voor veel bedrijven liggen hier flinke uitdagingen, omdat ze veel heterogene systemen en processen inzetten. Motiv helpt bedrijven bij deze uitdagingen met verschillende diensten rond beveiliging en beveiligingsbeleid. Met Motiv Security Management voor Databases richten we ons op de kern van uw activiteiten: uw bedrijfsgegevens.

Onze dienstverlening is gericht op het gebruik van Oracle en Microsoft SQL Server. Samen met de Security Officer stelt Motiv een database beveiligingsplan op wat voldoet aan de eisen die voor uw organisatie gelden op het gebied van ICT-beveiliging. De praktische uitvoering en controle daaropvolgend vinden plaats met behulp van het Information Risk Management-platform (IRM) dat Motiv bij uw organisatie implementeert.



Real-time bewaking

IRM is een softwareoplossing die niet alleen uw databases beschermt tegen aanvallen, maar ook inzetbaar is om beveiligingslekken op te sporen, het gebruik van de database te bewaken en het gebruik van de data vast te leggen. De bewaking van de database vindt bijna real-time plaats. Dat betekent dat uw beheerafdeling onmiddellijk gewaarschuwd wordt wanneer er sprake is van misbruik van data. Denk hierbij aan het overtreden van de beveiligingsregels, een aanval op uw data of informatiediefstal.

Met het oog op regelgeving is het in de regel ook nodig dat u het gebruik van data nauwkeurig vastlegt. Dan is het uitsluitend monitoren van gebruikersgedrag niet voldoende. Dankzij speciale audit-rapportagemogelijkheden binnen IRM is altijd inzichtelijk wie wanneer welke regelgeving heeft overtreden.

Motiv Security Management voor databases voorziet in de volgende onderdelen:

Controle op beveiligingsrisico's

De continue controle op beveiligingsrisico's is een belangrijke stap in het verstevigen van de beveiliging van uw database.

- Automatische controle van de database- en configuratiebeveiliging
- Identificeert en beheert databasebeveiligingslekken
- Geeft gedetailleerde rapportages
- Honderden voorgedefinieerde regels
- Ongelimiteerd toevoegen eigen regels

Bewaking van de database

Motiv biedt voortdurende bewaking van uw database en herkent beveiligingsrisico's, variërend van brute aanvallen tot het subtiel bekijken van vertrouwelijke informatie.

- Gedrag van gebruikers
- Veranderingen in privileges
- Veranderingen in de metadata
- Veranderingen in de content

Auditing en analyse:

De audit-informatie geeft de beveiligingsdeskundige genoeg informatie om wijzigingen in het beveiligingsbeleid door te voeren. Daarnaast vereisen tal van regelingen het vastleggen van gebruikersgedrag.

- Login-fouten
- Mislukte databasebewerkingen
- Verdacht gebruikersgedrag
- Excessief lezen van data
- Aantonen dat security-maatregelen effect hebben en eventuele incidenten toelichten;
- Bewaking dat automatische update-mechanismen van bijvoorbeeld virus-, spam- en spyware-filters goed functioneren.

Motiv Security Management voor Databases

Beveiliging binnen de kaders van wet- en regelgeving



Stappenplan

Motiv Managed Security voor Databases biedt een gestructureerde aanpak, waarbij we de volgende stappen doorlopen:

1. DBMS-beveiligingsplan.

Samen maken we aan de hand van uw beveiligingseisen een databasebeveiligingsplan. Hierin komen alle regels te staan waaraan uw beveiliging moet voldoen.

2. Controle DBMS-omgeving.

De databaseomgeving wordt met behulp van IRM gecontroleerd.

3. Implementatie van het beveiligingsplan.

In deze stap worden het DBMS-beveiligingsplan en de gevonden problemen omgezet in regels en geïmplementeerd in het IRM-platform. Dit gebeurt op basis van standaard vooraf gedefinieerde regels en eigen klantspecifieke regels.

4. Bewaking risico's en beveiligingsregels.

Het IRM-platform bewaakt de geïmplementeerde regels en geeft waarschuwingen bij het overtreden van de regels.

5. Vastleggen DBMS gebruik

In het beveiligingsplan is ook opgenomen welke acties binnen de monitor vastgelegd moeten worden. Denk hierbij aan voorschriften en regelgevingen. Daarnaast kan deze vastlegging later gebruikt worden voor onderzoek naar het gebruik van de databasegegevens.

6. Review database beveiliging

Regelmatige review van de waarschuwingen en de vastlegging van het database gebruik leidt tot het verder beveiligen van uw database omgeving. De gevonden items in de review fase worden opgenomen in het beveiligingsplan en geïmplementeerd in IRM



Partnership met IPLocks

Voor het IRM Platform maakt Motiv gebruik van de software van IPLocks, dat marktleider is op het gebied van databasebeveiliging en -bewaking, het opsporen van beveiligingslekken en de analyse van database-audits.

Motiv: professioneel en eigenzinnig

U heeft een netwerk- of databaseprobleem en zoekt een sparringpartner? Of u wilt nieuwe webtechnologie of een beveiligingsoplossing integreren in uw bestaande infrastructuur? Misschien heeft u gewoon een complex technisch probleem met uw IT-infrastructuur, dat opgelost moet worden.

In al deze gevallen is Motiv u graag van dienst. Want ons uitgangspunt is, dat elke klant anders is. En daarom zijn we voor de ene klant een sparringpartner en voor de andere een systems integrator. Bij weer een andere klant zorgen we er gewoon voor dat een probleem snel wordt opgelost. In welke rol u ons ook inschakelt, wij kijken altijd naar de veiligheid van uw infrastructuur en systemen. Want data- en systeembeveiliging loopt als een rode draad door onze activiteiten.

Contactinformatie

Motiv IT masters BV
Poortdijk 13
3402 BM IJsselstein

Tel: +31 30 687 7007
Fax: + 31 30 687 7006
info@motiv.nl