

IT in Control

Motiv Security Information & Event Management

Security Information & Event Management cruciaal voor compliancy

Sarbanes Oxley, Basel II, code-Tabaksblat en ISO 17799. De lijst van wet- en regelgeving waar bedrijven vroeg of laat mee te maken krijgen, groeit. En daarvoor neemt de druk op IT-afdelingen om met technologie in te spelen op deze ontwikkelingen, verder toe. Daarbij gaat het om zaken als monitoring, rapportering en business continuity. Centraal staat de vraag in hoeverre een organisatie in staat is om op de juiste wijze verantwoording af te leggen over de bedrijfsactiviteiten. 'Wanneer is wat gebeurd en door wie' is een vraag die dan beantwoord moet worden. Juist met het oog hierop heeft Motiv een dienst ontwikkeld die hierin voorziet: Security Information & Event Monitoring (SIEM).

Security Information & Event Management is een relatief nieuw werkveld binnen de markt voor databeveiliging. Het richt zich op het controleren van de naleving van door een organisatie ingevoerd beveiligingsbeleid, zodat voldaan wordt aan wetgeving en compliancy-regelgeving. Met behulp van gespecialiseerde apparatuur worden alle activiteiten op een bedrijfsnetwerk gemonitord en geanalyseerd op basis van vooraf opgestelde beveiligingsregels. Op deze wijze kan een organisatie eventuele inbreuken op de beveiliging snel opsporen en herleiden tot de bron. Motiv werkt op het gebied van SIEM samen met Network Intelligence. Dit Amerikaanse bedrijf ontwikkelt de enVision-appliances waarmee hoogwaardige monitoring mogelijk is.

Met Security Information en Event Management krijgt u grip op de beveiliging van de informatiesystemen, netwerken en security oplossingen zoals firewalls en virus filters:

- Access Control – voor het monitoren van alle toegangspogingen tot bestanden, directories, database-records en applicaties.
- Configuration Control – voor het monitoren van de configuratie, de policies en de software die op systemen zijn geïnstalleerd.
- Malicious Software-detectie. Deze feature verzamelt en rapporteert over kwaadaardige code door virussen of malware.
- Policy Enforcement - verifieert dat alle gebruikers de regels volgen waardoor het risico van onbedoelde bekendmaking van vertrouwelijke informatie teruggedrongen wordt.
- User Monitoring and Management – deze mogelijkheid creëert een volledige audit van de activiteiten van alle niet-werknemers met toegang privé-gegevens en biedt stappen om het risico van gekraakte accounts te verminderen.

Wet- en Regelgeving

Security Information & Event Management speelt een steeds belangrijkere rol bij het voldoen aan regelgeving en wettelijke eisen.

- **Basel II** is specifieke wetgeving voor de bankwereld. Basel II richt zich op het vaststellen van kapitaal-eisen en risicobeheer, van toepassing. Basel II zal vanaf 2006 daadwerkelijk worden ingevoerd. In Nederland is DNB toezichthouder voor de invoering en naleving van Basel II. Financiële instellingen zullen om die reden aan DNB periodiek moeten aantonen dat zij voldoen aan de wetgeving zoals vastgelegd in het Basel II akkoord.
- Nederlandse **corporate governance code**, vaak aangeduid als de code-Tabaksblat, voor beursgenoteerde bedrijven heeft tot doel het verbeteren van de transparantie in de jaarrekening, betere verantwoording van de Raad van Commissarissen en een versterking van de zeggenschap en bescherming van aandeelhouders. De Monitoring Commissie Corporate Governance Code toetst jaarlijks op welke wijze en in welke mate de codevoorschriften door de Nederlandse beursgenoteerde vennootschappen worden nageleefd.
- De **norm NEN 7510** is een door het Nederlands Normalisatie-instituut ontwikkelde norm voor Informatiebeveiliging voor de zorgsector in Nederland. De norm is gebaseerd op de Code voor Informatiebeveiliging. Voor de zorgsector is een aangepaste versie van de Code opgesteld. De reden hiervoor is dat er met name specifieke extra aandachtspunten zijn, zoals privacybescherming, en het taalgebruik, dat voor de zorgsector niet volledig duidelijk is. De NEN 7510 wordt aangevuld met de NEN 7511 (Toetsbaar voorschrift voor solopraktijken, samenwerkingsverbanden en grote instellingen) en NEN 7512 (gegevensuitwisseling).
- Bedrijven met een beursnotering in de Verenigde Staten hebben te maken met de **Sarbanes Oxley-wet (Sox)**. De wet is ook van toepassing voor Nederlandse ondernemingen met een Amerikaanse beursnotering. Voldoen aan SOX komt er op neer dat in het financieel jaarverslag ook jaarlijks een hoofdstuk dient te staan dat de interne controle op de correctheid van de aangeboden cijfers evalueert. Deze wet is met name gericht op een goede financiële controle van bedrijven op twee niveaus: ontwerp / opzet van controles (design effectiveness) en werking (operating effectiveness).

IT in Control

Motiv Security Information & Event Management

Op weg naar compliance aan wet- en regelgeving

De verschillende regels hebben tot gevolg dat er meer grip moet zijn op de integriteit van (vergaande) geautomatiseerde informatiesystemen. De integriteit en de beveiliging van informatiesystemen moet aantoonbaar onder controle zijn. Om aantoonbaar onder controle te zijn, worden veelal de volgende maatregelen getroffen:

- Data zoals logging efficiënt te verzamelen, beschermen en opslaan.
- Basisregels te formuleren over het normale gebruik van systemen en netwerken, zodat afwijkende activiteit gemonitord kan worden.
- Rapportages te genereren over deze afwijkingen.
- Forensische analyses te maken van het gebruik van systemen en netwerken, met name voor wat betreft aangebrachte wijzigingen.
- Activiteiten nauwkeurig te monitoren en eventuele inbreuken op vastgestelde beleidsregels meteen te corrigeren.

Met Motiv Security Information en Event Management biedt Motiv een totaaloplossing voor aantoonbare integriteit en beveiliging passend binnen de wet- en regelgeving.

Motiv "IT in Control" programma

IT in Control betekent letterlijk Informatietechnologie is onder controle. Security Information en Event Management is de basis om de beveiliging beheersbaar te krijgen en te houden. Bij een afwijking ten opzichte van de norm wordt direct een alarm gegenereerd; en policy compliancy rapportages geven volledig inzicht in de kwaliteit van de beveiliging. Om beveiliging volledig onder controle te brengen zijn nog twee additionele maatregelen mogelijk:

- **Vulnerability Management** - beveiligingsexperts inclusief hackers vinden continu zwakheden in hard- en software. Deze worden onder andere gepubliceerd op site zoals Bugtraq en Securityfocus. Nadat een beveiligingslek is gevonden, levert de fabrikant een patch (pleister). Om vast te stellen of alle relevante beveiligingslekken met patches zijn dichtgezet, kunt u vulnerability management invoeren. Dagelijks wordt de beveiliging middels kwetsbaarhedenanalyse gecontroleerd op lekken. Zodra een beveiligingslek wordt gevonden, wordt dit gerapporteerd aan de ICT-afdeling.
- **Change Auditing** - directe rapportages van alle geautoriseerde en ongeautoriseerde wijzigingen op systemen en netwerk. Wijzigingen zijn immers een moment dat de mate van beveiliging eveneens kan wijzigingen. Door grip te krijgen op wijzigingen (change control) kan de ICT-afdeling ook meer grip krijgen op de continuïteit van de beveiliging

De rapportage in het kader van vulnerability management en change auditing kunnen naadloos worden geïntegreerd binnen Security Information en Event Management. Op die manier ontstaat een totale security cockpit. Vanuit deze cockpit heeft u "IT in Control".

Partner Network Intelligence

Network Intelligence – onderdeel van EMC – is marktleider in oplossingen voor Security Information en Event Management (SIEM). De EnVision appliances van Network Intelligence verzamelen bedrijfsbreed alle logging in het netwerk. Het LogSmart® Internet Protocol Database (IPDB) is een unieke oplossing voor het effectief verzamelen en opslaan van logging van elk willekeurig systeem met een IP-adres (zonder agents). EnVision appliances leveren hiermee zowel real-time als historische security en policy compliancy rapportages. Diepgaande forensische analyse is mogelijk via de ingebouwde Event Explorer.

Met Network Intelligence krijgt u policy compliancy en security monitoring volledig onder controle. Network Intelligence wordt veelal als security monitoring ingezet voor ondernemingen die te maken hebben met Basel II, SOX, Code-Tabaksblad of NEN7510.

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.

Motiv

Poortdijk 13

NL - 3402 BM IJsselstein

www.motiv.nl

info@motiv.nl

T +31 [0]30 - 68 77 007

F +31 [0]30 - 68 77 006