Date : 28/10/2014
Pays : FRANCE
Surface : 143 %

Decideo.fr

Mots : 966

> Lire cet article sur le site web

Big data et sécurité

Voici un sujet, vous allez dire, qui est à la mode. Certes, il n'y a pas une publication, un support de communication de technologie, d'IT, de mobilité ou d'Internet qui ne contienne au moins un article, un sujet sur ce thème. Sans être une fashion-victime, c'est un sujet d'actualité d'abord, et de loin par le potentiel suscité en business et en développement d'activités et affaires.

Comment ne pas enthousiasmer les « foules » quand, juste pour prendre un exemple, un opérateur télécom, possédant des quantités énormes d'informations de ses usagers, continuellement mises à jour et enrichies, peut proposer, tout en respectant l'anonymat de ses abonnés, une large et nouvelle gamme de services à des clients entreprises pour les aider dans la qualification étayée à travers des données fiables, d'une possible nouvelle zone de chalandise ? Et quelle avancée pour les équipes du développement commercial du même distributeur qui pourront interroger en ligne à travers des apps sur mesure, simuler graphiquement les flux des passants sur une heure, un jour, une semaine, un an, en connaissant parfaitement d'où ils viennent et où ils vont, leurs pouvoir d'achat, les moyens de transports utilisés, leurs dépenses moyennes, leurs lieux d'habitation, de travail, etc. etc. Les perspectives sont fantastiquement riches en déclinaisons d'utilisation, d'interrogation, de simulation et d'analyse de ces grandes quantités des données.
C'est grâce à ce potentiel de synthétisation, de manipulation sans fin, que le big-data nous pousse à rêver, comme une terre promise de nouveaux services, orientés métier, au cœur de l'objet d'existence de l'entreprise. Le big-data c'est l'exploitation de la quantité sans fin des données issues de l'usage de la mobilité, de l'Internet, des réseaux sociaux, des apps, de la dématérialisation de nos vies et de notre société.
Alors, au-delà des architectures de la collecte et du stockage de ces data-lakes, les technophiles retrouveront les notions du moment comme Hadoop, map reduce et autres NoSQL, apparues d'ailleurs avec les grands consommateurs de données tels que Facebook, Google ou Yahoo, les considérations de sécurité sont elles aussi très importantes.
D'abord la sécurité est indispensable pour sécuriser ces data-lake et les services business qui les utilisent. Intégrité des informations, chiffrement souverain des données dans le cloud, traçabilité des accès notamment des administrateurs et autres personnels à pouvoir, authentification et gestion dynamique des mots de passe, gestion des certificats de chiffrement et PKI (private-key infrastructure), protection des données personnelles, sécurité en mobilité, etc. etc. Ce sont juste quelques aspects de la couche de sécurité indispensable à mettre en œuvre. En septembre 2014 l'étude du cabinet de conseil Accenture positionne la sécurité comme étant le principal défi à la

Date : 28/10/2014
Pays : FRANCE
Surface : 143 %

Decideo.fr

mise en place d'une solution big-data (60% des dirigeants en France), devant les coûts et la pénurie des talents.
Mais ce n'est pas tout. Le big-data sécurité est en soit un formidable développement, une évolution vertueuse des outils et des processus propres à la sécurité Internet au sein des entreprises.
Relier intimement les logs et événements d'infrastructure (réseaux, systèmes, sécurité, mobilité, cloud,…) avec les événements des applications métier, tels que les logs de navigation, d'utilisation d'une application, la fameuse « application journey » ou voyage de l'utilisateur au sein d'une application, c'est alimenter un énorme espace de données de l'entreprise et donc pouvoir avoir potentiellement une vision complète des opérations et événements de sécurité ou de fraude.
En théorie c'est le rêve de tout RSSI, Fraude Manager ou Directeur Sécurité SI, voire des directions audit interne !
Gérer les incidents de sécurité en lien avec les plates-formes de SIEM (elles-mêmes interfacées avec les data-lakes d'information du SI et des applications), piloter les remédiations et mises en conformité des SI, obtenir une vision préventive de la sécurité, avoir un outil enfin complet, de bout en bout du SI, de lutte contre la fraude interne et clients, ce ne sont que quelques exemples des apports concrets.
En pratique les choses, organisationnellement d'abord, sont plus compliquées car les limites de responsabilités, les territoires hiérarchiques font que les accès des RSSI aux données des métiers ne sont pas permis.
Cela confirme dans la sécurité aussi, que le big-data est un nouveau rôle transverse au sein des entreprises. Un rôle transverse, un rôle agile, un rôle qui pour avancer doit s'affranchir des lourdeurs de mise en place et d'exploitation classiques des DSI des grands groupes.
Plus de 50% des organisations ont déjà mené des pilotes et mis en production des applications big-data, essentiellement au sein des métiers, du marketing, du développement business, des ventes, etc. Dans la plupart des grandes organisations et administrations, la fonction sécurité SI est pour l'instant concentrée sur les solutions de log management et SIEM (Security Incident and Event Monitoring). Ces outils de collecte et gestion des logs sécurité, composants fondamentaux des SOC, sont absolument nécessaires pour piloter et analyser la sécurité des infrastructures SI et Internet ; ils devront s'articuler et prendre en compte le lien, la cohérence architecturale au niveau du stockage, de l'indexation, du moteur de recherche, de la corrélation, etc. avec les solutions big-data. Certains éditeurs l'ont bien compris et en font bon usage.
Et à l'instar du big-data métier, le big-data sécurité favorise et permet le développement des nouveaux métiers au sein de l'entreprise. Par exemple les data-analystes en sécurité sont déjà une compétence recherchée et l'évolution vers le big-data sécurité des responsables de sécurité SI reste un enjeu important pour le métier.
Théodore-Michel VRANGOS, cofondateur et président d'I-TRACING, entreprise de conseil et ingénierie entièrement dédiée à la traçabilité de l'information et à la gestion de la preuve. Ancien Président de Cyber Networks, aujourd'hui BT France, qu'il avait fondée avec Laurent Charvériat, Théodore-Michel Vrangos a démarré sa carrière en tant que IT Business Manager au sein du Groupe Générale des Eaux (Vivendi) à Paris.
Master of Science en technologie de l'information de l'Université de Manchester (UK) et diplômé du Groupe **ESIEE.**