

Date : 19/05/11

L'exploitation des logs est en train de vivre une évolution importante...



Il n'y a jamais eu autant d'incidents informatiques visant les données sensibles des individus, le vol d'informations critiques dans les entreprises ou les administrations. Comment donc croire que les gouvernances des états et des entreprises s'en remettent aux seules lignes de logs que nous connaissons et dont l'évolution est faible depuis 30 ans? Qu'est-ce qu'un log ? En informatique, les logs sont les témoins d'une suite d'événements qui concernent l'activité du réseau, des serveurs et des applications. Ils constituent une trace informatique légale avec des informations sur l'origine, le séquençage et les interactions d'un utilisateur avec l'environnement source. Quelles limites ? La plupart des applications sont très verbeuses à savoir qu'elles produisent un très grand nombre de logs.

Dans des SI à fort trafic, ces quantités deviennent astronomiques et par conséquent, difficiles à capter autant qu'à stocker. Dans cette masse d'informations, trouver un log revient à chercher une aiguille dans une botte de foin, ce qui lorsque c'est nécessaire ou obligatoire devient une pénible gageure. D'autre part, les logs sont difficilement lisibles pour le commun des mortels, ils sont écrits dans des formats disparates et leur interprétation requiert une machinerie et des personnels hautement qualifiés.

Quelles obligations ? Ainsi que l'expliquait Maître Walter, avocat spécialisé au barreau de Paris, les fournisseurs d'accès Internet ou FAI sont dans l'obligation de collecter et pouvoir fournir des preuves de connexion sous forme de logs pendant 1 an. La notion de FAI englobe les entreprises qui utilisent l'Internet de manière marchande. En réalité, nous sommes tous plus ou

Évaluation du site

Ce site s'adresse aux professionnels des technologies numériques. Il leur propose des articles concernant l'actualité de leurs métiers ainsi que des services : produits, promotions, espace emploi, etc.

Cible
Professionnelle

Dynamisme* : 22

* pages nouvelles en moyenne sur une semaine

moins contraints d'archiver nos logs afin de pouvoir les restituer sur requête judiciaire. Que faire? Bien sûr certains proposent des systèmes sophistiqués et soit disant pro-actifs, qui s'avèrent très complexes à mettre en œuvre, gourmands en ressources et économiquement prohibitifs. A l'usage, les technologies dites de SIEM s'avèrent pour le moment insuffisamment matures. Et si la solution était ailleurs ? Certes les logs sont et resteront longtemps les preuves nécessaires en cas de litige, cependant, ils nécessitent de nombreux traitements avant d'être exploitables.

Or, ce que veut un responsable informatique, ou un responsable d'entreprise, c'est voir et avoir une meilleure lecture de l'incident, en clair et tout de suite. L'idée de transposer ainsi le paradigme de la vidéo surveillance existante dans nos villes au Système d'Information, lui même en pleine urbanisation, nous conduit à proposer une autre approche : la vidéo surveillance du SI. C'est probablement une combinaison de la trace vidéo donnant une image immédiate et "humaine" d'un incident de sécurité, et les logs correspondants qui permettront d'arbitrer une situation à l'amiable, ou au tribunal dans l'avenir... Est-on en train d'assister à l'apparition des logs vidéo? ... Wallix est éditeur de logiciels de sécurité informatique, spécialisé dans la gestion des risques liés à l'accès aux infrastructures informatiques critiques des entreprises.

L'éditeur propose des solutions innovantes pour la gestion des identités et des accès, la traçabilité avec une approche simple et économique, sans contraintes de déploiement dans le système d'information du client, et en conformité avec les nouvelles normes de sécurité informatique. Les solutions Wallix sont commercialisées à travers un réseau de partenaires revendeurs et intégrateurs informatiques. La société est installée en France, au Royaume Uni et aux Etats Unis. Wallix est lauréat de l'Oseo Innovation, du programme PM'UP, et partenaire du Pôle de compétitivité System@tic Paris Région. La société est soutenue par des investisseurs privés tels que les fonds Access2Net, **Sopromec**, Hedera et Venturis Capital.