HORS SERIE

Global Security Mag

THE LOGICAL & PHYSICAL SECURITY MAGAZINE

Hors série N°002 - Prix : 5 € - octobre 2008

SPECIAL

BANQUE & ASSURANCE

EN PARTENARIAT AVEC

infosecurity FRANCE

STORAGE EXPO

19 ET 20 NOVEMBRE 2008 PARC DES EXPOSITIONS - PORTE DE VERSAILLES

SÉCURITÉ, STOCKAGE...

ANALYSES, DÉBATS, SOLUTIONS
2 SALONS, 130 EXPOSANTS

DÉCOUVREZ EN EXCLUSIVITÉ LE PROGRAMME DES CONFÉRENCES ET DU CONGRÈS !

19-20 NOVEMBRE 08

PARIS, PORTE DE VERSAILLES - PAVILLON 5

infosecurity
FRANCE

- Intrusion
- Phishing
- Chevaux de Troie
- Sécurité de la VoIP
- Mobilité
- Continuité d'activité...

www.infosecurity.com.fr

STORAGE
EXPO

- Archivage et conservation de l'information
- Virtualisation du stockage
- Gestion de cycle de vie des données (ILM)
- Protection des données...

www.storage-expo.fr

DEMANDEZ VOTRE BADGE GRATUIT !

www.infosecurity.com.fr ou www.storage-expo.fr

Reed Expositions

Code invitation : GLO

Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE

infosecurity FRANCE

STORAGE EXPO

Hors série octobre 2008
spécial **Banque & Assurance**

ÉDITO

L'arbre ne doit pas cacher la forêt

La crise qui secoue actuellement le secteur financier ne doit pas occulter la nécessité pour les entreprises de ce domaine de continuer à œuvrer pour améliorer leurs processus en matière de sécurité et de stockage. En effet, il est quasiment sûr, à ce jour, que les banques et les assurances arriveront à se tirer du mauvais pas dans lequel elles se sont mises par des stratégies de placements risqués. Par contre, la COB et l'opinion publique auront sans doute moins de mansuétude si des manquements en matière de sécurité ou d'archivage apparaissent à nouveau. Une deuxième affaire Kerviel ne sera sans aucun doute plus tolérée. Ainsi, il est primordial que les dirigeants et les RSSI de ces entreprises continuent à travailler et à investir afin de protéger leurs établissements et leurs clients contre les attaques des pirates informatiques. En effet, ils doivent peut-être redouter qu'en plus des escroqueries habituelles, les « déçus » du système ne se déchainent pour se venger des pertes financières qu'ils auront essuyé… l'arbre de la crise financière ne doit donc pas cacher la forêt de la sécurité informatique…

Marc Jacob

© Slavoljub Pantelic

REVUE TRIMESTRIELLE
Hors Série n°002 – Octobre 2008
www.globalsecuritymag.fr et
www.globalsecuritymag.com
ISSN : 1961 – 795X
Dépôt légal : à parution
Editée par SIMP
RCS Nanterre 339 849 648
17 avenue Marcelin Berthelot
92320 Châtillon
Tél. : +33 1 40 92 05 55
Fax. : +33 1 46 56 20 91
e-mail : marc.jacob@globalsecuritymag.com

RÉDACTION
Directeur de la Publication :
Marc Brami
Rédacteur en chef :
Marc Jacob
Rédactrice :
Emmanuelle Lamandé
Assistante :
Sylvie Levy
Responsable technique :
Raquel Ouakil
Photos :
Marc Jacob
Comité scientifique :
Pierre Bagot, Francis Bruckmann, Eric Doyen, François Guillot, Mauro Israël, Olivier Iteanu, Dominique Jouniot, Patrick Langrand, Yves Maquet, Michel Van Den Berghe, Thierry Ramard, Hervé Schauer, Wayne Sutton, Catherine Gabay, Zbigniew Kostur.

PUBLICITE
Reed Expositions
Alexandra Colbeau
Tél. : +33 1.47.56.65.44
Alexandra.colbeau@reedexpo.fr
Jamila El Aidi
Tél. : +33 1.47.56.65.50
Jamila.elaidi@reedexpo.fr

PAO
Imadjinn sarl
Tél. : 02 51 53 01 46
e-mail : info@imadjinn.fr

IMPRESSION
Imprimerie Hauguel
8-14 villa Léger
92240 Malakoff
Tél. 01 41 17 44 00
Fax 01 41 17 44 09
e-mail : info@imprimerie-hauguel.fr

ABONNEMENT
Prix du numéro Hors Série :
5 € TTC (TVA 19,60%)
Abonnement annuel au magazine :
50 € TTC (TVA 19,60%)

SOMMAIRE

UN PROJET D'IAM DOIT IMPLIQUER L'ENSEMBLE DES UTILISATEURS

Par Christophe Tallot, Senior Manager Management du Contrôle Interne, Mazars
David Luponis, Manager Management du Contrôle Interne, Mazars

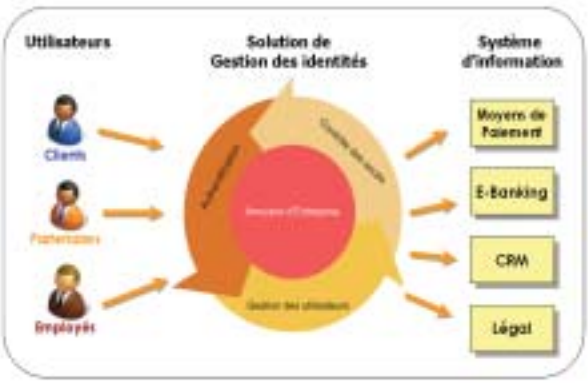

Christophe Tallot


David Luponis

Il n'y a pas si longtemps, le challenge consistait à maintenir les clients, les fournisseurs et le personnel hors du système d'information. Aujourd'hui, il s'agit de les y intégrer pleinement en administrant des profils et surtout en « donnant aux bonnes personnes les bons droits d'accès, au bon moment ».

La gestion des identités ou IAM (Identity and Access Management), et par extension des droits d'accès, a pour objectif de fédérer la gestion de l'ensemble des identités et droits d'accès d'un utilisateur du système d'information de son entreprise. Pour être complète, la solution de gestion des identités doit s'appréhender suivant 4 axes :

- L'authentification, dont les mécanismes permettent de s'assurer de la validité de l'identité déclarée par une personne. Il s'agit, par exemple, d'un numéro de code PIN, de certificats numériques (PKI), d'authentification dite forte (type SecurID), de biométrie, de cartes à puce virtuelles, de passeport électronique...
- Les contrôles d'accès pour lesquels il s'agit de s'assurer que les utilisateurs n'ont accès qu'aux applications, ou ressources, auxquelles ils ont droit. Aussi connus sous l'appellation « Infrastructure de gestion des privilèges », ils permettent, par exemple, de fournir un service de Single Sign-On (SSO) pour les applications Web et permettent également de réduire les coûts d'exploitation associés.
- La gestion des utilisateurs ou « provisioning » est le terme décrivant les technologies de gestion d'un grand nombre d'utilisateurs. Elle s'appuie le plus souvent sur des processus automatisés en temps réel ou « workflow » qui donnent les droits d'accès à toutes les applications nécessaires à un nouvel entrant dans la société pour exercer son activité.
Ce provisioning doit permettre de gérer le cycle de vie d'un utilisateur sur le système d'information, depuis son embauche, et donc de l'affectation de ses premiers droits sur les applications, jusqu'à son départ (De-provisioning) – et donc la suppression de ses habilitations, en passant par ses changements de postes (Re-provisioning) ayant un impact sur les droits aux applications et les données accessibles. Il en est de même pour tout nouveau partenaire ou client. Les fonctionnalités des outils utilisés pour cette gestion peuvent être centralisées ou déléguées aux utilisateurs.
- L'annuaire utilisateur d'entreprise qui permet de stocker, en toute sécurité, des informations relatives aux utilisateurs, et en particulier leurs profils. Les accès à l'annuaire sont réalisés au moyen du protocole standard LDAP (Lightweight Directory Access Protocol).



Le passage d'un système informatique centralisé (fin des années 70 jusqu'à la fin des années 80), qui, à l'époque, permettait la centralisation des identités et des droits d'accès (grâce aux applications RACF et TopSecret, par exemple) vers des systèmes d'informations dits ouverts, a engendré la multiplication des services et des serveurs afin de répondre au mieux aux attentes des utilisateurs.
Quand, par le passé, un collaborateur utilisait un identifiant unique afin d'accéder à des applications transactionnelles, ce même utilisateur se retrouve aujourd'hui avec quasiment autant d'identifiants que d'applications ou de données accessibles.
Evidemment, lors du départ ou lors d'un changement de poste au sein de l'entreprise, l'absence de gestion centralisée, du système d'information, ne permet pas d'optimiser l'identité et les accès du collaborateur, ce dernier pouvant être identifié sur certains systèmes par un code d'entreprise unique, par exemple son code employé, ou bien par des identifiants plus facilement reconnaissables, par exemple, « pierre.dupont » ou « pdupont », ou encore par des identifiants sans rapport avec son identité, par exemple, « user1 », « maîtrise_ouvrage_4 », « responsable_BO ».
Cette multiplication des identifiants,


© Slavoljub Pantelic

combinée aux droits d'accès afférents à chacun de ces comptes, ne permet donc pas une gestion efficace des utilisateurs et de leurs droits sur le système d'information de l'entreprise ce qui limite évidemment la traçabilité et les possibilités d'audit, les systèmes ne suivant pas les traces de la même façon, ou pire encore, ne permettant pas toujours d'identifier les actions des utilisateurs.

La gestion des identités doit s'inscrire dans un projet de sécurité et de gestion des risques

Depuis le début des années 2000, les solutions technologiques ont relativement peu évolué et sont maintenant très semblables. Par contre, ce secteur a connu une forte concentration des éditeurs. Mais si ces derniers mettent en avant « leurs suites technologiques », la gestion des identités est avant tout un projet organisationnel et fonctionnel qui implique souvent une gestion des changements importante au sein de l'entreprise.
La gestion des identités ne prend tout sens que si elle s'inscrit dans un projet plus large de sécurité et de gestion des risques de l'entreprise. Comme nous le montre la dernière enquête du Clusif **(1)**, la gestion de la sécurité des entreprises françaises est rentrée dans un cycle de maturité. La première étape consistait à se prémunir des attaques externes. La seconde est de se protéger contre les agressions internes, représentant aujourd'hui 80% des incidents de sécurité, comme nous l'ont prouvé les récents évènements dans le milieu bancaire.

Dans ce contexte, et à l'heure des réductions de coûts des fonctions support, ainsi que grâce à la prise en compte de la sécurité au sein des projets, notamment pour les entreprises se conformant à la norme de management de la sécurité des systèmes d'information « ISO 27000x », un nombre croissant de banques, instruit des projets ou des « proof of concept » sur l'intégration de la gestion des identités et des droits d'accès dans leur système d'information.

Ces projets, comme tant de projets d'entreprise, ont une incidence sur les Directions informatiques, en ce qui concerne les choix techniques, d'intégration et de support, mais également des Directions métiers sur des aspects fonctionnels et notamment l'expression des besoins en terme de matrice des droits d'accès aux applications et aux données.

Ainsi, un projet de cette nature pris uniquement sous l'angle technologique aurait peu de chances d'aboutir à un succès, tant le mécontentement des utilisateurs serait grand. Il mènerait immanquablement à la mise en place d'infrastructures ou de solutions de contournement des mesures édictées par la seule Direction informatique.

L'implication des utilisateurs et des experts techniques au sein d'un projet de mise en œuvre d'un IAM est la garantie que les différents besoins, tant fonctionnels que techniques, seront correctement pris en compte.

A ce jour, notre expérience, tant en audit des systèmes d'information qu'en conseil, nous amène à constater que l'intégration d'IAM, au sein de Groupes bancaires, est réalisé en premier lieu sur des entités nationales ou régionales – le même projet au niveau international semblant être une tâche souvent « pharaonique » pour couvrir l'ensemble des utilisateurs et des applications.

Néanmoins, la mise en œuvre de tel chantier peut s'effectuer au sein de structures bancaires internationales par l'intermédiaire d'applications Groupe qui regroupent une population fonctionnelle d'utilisateurs homogène et plus restreinte (par exemple trésorerie, contrôle de gestion, comptabilité centrale, etc.).

Les banques françaises sont loin d'avoir atteint la maturité de leurs homologues étrangères

Dans de nombreux groupes bancaire, cette intégration fait suite à la nécessité de prendre en compte la sécurité, et donc l'IAM comme premier accès vers le système d'information, dans le cycle de vie des projets et donc de l'entreprise. Nous avons pu constater lors de nos interventions que les phases les plus importantes de cette intégration ne sont pas des étapes techniques, mais bien les étapes de recensement des utilisateurs, de leurs identifiants, des applications et des droits qui y sont liés.
Par ailleurs, en France, les banques, en particulier, sont loin d'avoir atteint la maturité de leurs homologues à l'étranger. La maturité des sites de e-banking hexagonaux est à ce titre révélatrice : authentification par simple mot de passe en France, alors qu'en Suisse, par exemple, l'authentification doit se faire à partir d'une SecureID nettement plus efficace.

Les objectifs des entreprises ayant fait le choix de centraliser leur gestion des identifiants et des droits d'accès sont multiples et nous pouvons notamment citer :
un support plus efficace notamment dans la gestion la création d'identifiants et l'affectation de privilèges,
des coûts d'exploitation réduits notamment parce que la centralisation permet en quelques clics à un administrateur de suspendre les droits d'accès d'un utilisateur au système d'information une traçabilité des actions plus rigoureuse, et évidemment une évolution du niveau de sécurité du système d'information de l'entreprise en garantissant des contrôles de premier niveau.

Les contraintes réglementaires liées à SOX, ou à Bâle2, pour les groupes bancaires, et Solvency2 pour les compagnies d'assurances, ou plus simplement le respect des recommandations, faites au sujet de la gestion des accès par ITIL V3, poussent les entreprises à quantifier et à qualifier leurs risques opérationnels, en précisant, entre autres, la sécurité du système d'information et l'accès à cet environnement.

L'IAM peut jouer ce rôle, s'il est géré convenablement, et peut devenir un facteur clé dans les contrôles appliqués aux systèmes d'information, tout en permettant aux entreprises de minimiser les risques liés à la gestion des utilisateurs et de leurs accès. ■■■

(1) Enquête du Clusif édition 2008, intitulée « Menaces informatiques et pratiques de sécurité en France »

HASSAN MAAD, EVIDIAN :

UNE GESTION DES IDENTITÉS ALIGNÉE SUR LES PROCESSUS MÉTIER

Interview par Marc Jacob


Hassan Maad

Evidian, fort de 2 millions d'utilisateurs de ses produits et 600 clients, est le leader européen de la gestion des identités et des accès (IAM). Face aux nouveaux enjeux en termes de sécurité, toutes les entreprises et en particulier les institutions financières déploient des solutions d'IAM. Hassan Maad, Directeur Général d'Evidian, estime que la gestion des identités est avant tout un projet organisationnel qui doit répondre aux exigences du métier de l'entreprise. Elle doit permettre d'améliorer les processus métier tout en assurant un contrôle des accès.

Global Security Mag : Pouvez-vous nous présenter votre entreprise ?

Hassan Maad : Evidian est un éditeur de logiciels de sécurité, spécialisé dans les solutions de gestion des identités et des accès. Nous proposons aussi des logiciels pour garantir le niveau de service et la haute disponibilité des systèmes et applications.

Premier éditeur européen de logiciels d'IAM, Evidian commercialise ses produits dans le monde entier et compte parmi ses 600 clients, de nombreuses entreprises des Fortune 500 et des grandes administrations. Nous sommes présents à travers un réseau de partenaires et de distributeurs sur l'Europe, l'Asie et depuis le début de l'année aux Etats-Unis. Près de 2.000.000 d'utilisateurs dans le monde se connectent tous les jours à leurs applications avec des logiciels de sécurité Evidian. Nous sommes une filiale du Groupe Bull avec comme actionnaires Bull et NEC.

GS Mag : Quel est votre produit phare pour 2008-2009 ?

Hassan Maad : Notre produit phare pour 2008-2009 est IAM Suite 8. Nous avons réalisé un focus très important dans le domaine des solutions de gestion des identités et des accès. L'IAM est devenu une priorité pour nos clients, en particulier dans les banques et institutions financières. Nos solutions leur permettent de gérer les risques liés à des accès malveillants au système d'informations. Parmi les grands succès de cette année, nous avons noté une forte croissance de la demande pour des modules d'entrée permettant un retour rapide sur investissement tels que le SSO d'entreprise. La priorité est alors de s'assurer de l'identité des utilisateurs du SI, avec des moyens sûrs d'authentification. De nouveaux moyens qui peuvent aussi remplacer la multitude de mots de passe encore nécessaire dans beaucoup de systèmes. Nous offrons la possibilité à nos clients de déployer la biométrie, la carte à puce, ou encore des badges de proximité… Nous constatons qu'il est beaucoup plus simple de construire un nouveau système de gestion des identités par étapes. De même, en démarrant par une gestion efficace des accès, on obtient des résultats très rapides sur le plan de la connaissance de « qui accède à quoi ».

L'IAM n'est pas qu'un enjeu technique, mais une question organisationnelle

GS Mag : Quels sont les principaux conseils que vous donnez à vos clients qui souhaitent démarrer le déploiement d'une solution d'IAM ?

Hassan Maad : Il me semble que là, plus qu'ailleurs, il faut que les exigences des utilisateurs et du métier soient les points de départ de tout projet d'IAM. Il s'agit là de repères qui doivent guider toute approche de mise en œuvre. Nous voyons encore des projets d'IAM qui sont des prolongements de la construction d'annuaires centralisés. La gestion des identités et des accès est loin de n'être qu'un enjeu technique, bien au contraire, c'est avant tout un projet organisationnel qui répond à des exigences du métier de l'entreprise et se trouve rapidement au cœur de ses processus.

GS Mag : Quels sont les principales références dans le milieu des institutions financières ?

Hassan Maad : Nous avons des succès dans plusieurs institutions financières en France, en Europe, au Japon et plus récemment aux Etats-Unis. Parmi nos références, une grande banque centrale en Europe, une des premières banques du Japon, un organisme international de gestion des transferts. Par exemple, Barclays utilise nos solutions pour permettre une authentification unique par biométrie des utilisateurs.

GS Mag : Pour conclure quel est votre message à nos lecteurs ?

Hassan Maad : Les régulations et les contrôles vont de plus en plus se renforcer. La demande de transparence financière a déjà fait naître des textes comme Sarbanes Oxley, Bâle II... Et les crises répétitives que nous vivons actuellement soulèveront des appels à encore plus de clarté sur l'usage de nos systèmes d'informations. Il est alors important que la sécurité ne soit pas un frein à l'agilité des organisations. Ainsi, les solutions d'IAM, en particulier, sont de véritables outils de contrôle interne alignés sur les processus métier de l'entreprise. ■■■

EVIDIAN
A Groupe Bull Company

Sergio Ribeiro - Frédéric Pierresteguy

FRÉDÉRIC PIERRESTEGUY, AVOCENT-LANDESK :

VOTRE IT PEUT DEVENIR UN CENTRE DE SERVICES

Interview par Marc Jacob

Avocent est un des acteurs principaux de la gestion des infrastructures IT jusqu'au poste de travail. En intégrant LANDesk, devenue sa division logiciels et services, elle offre la possibilité aux entreprises de mieux connaître et maîtriser leur parc IT et non IT. Frédéric Pierresteguy, DG EMEA Sud Avocent-LANDesk, estime que ses solutions permettent aux entreprises de dynamiser leurs processus et ainsi de transformer leur IT en un centre de services.

Global Security Mag : Pouvez-vous nous présenter votre entreprise ?
Frédéric Pierresteguy : Avocent est le spécialiste de la gestion des infrastructures du Data Center au poste de travail. Nous offrons des solutions de connectivité et d'administration des périphériques du SI : poste de travail, serveurs, PDA, équipements réseaux… Notre société d'origine américaine compte environ 1900 personnes dans le monde pour un CA de 620 millions de $. LANDesk est la division logiciels et services. Elle fonde son offre sur les solutions d'administration de parc, de gestion de la sécurité sans oublier la gestion fonctionnelle au sens d'ITIL.

GS Mag : Quel est votre produit phare pour 2009 ?
Frédéric Pierresteguy : En fait, nous avons plusieurs produits phares pour lequesls nous continuons à développer de nouvelles fonctions répondant à l'attente du marché. D'ailleurs, LANDesk a toujours été à la pointe de l'innovation et est reconnu comme leader dans la gestion du cycle de vie du parc informatique par le Gartner dans son « Magic Quadrant ». Ces produits phares s'articulent autours de trois grandes gammes de produits :
- LANDesk Management suite (LDMS), offrant une administration centralisée des operations IT pour l'inventaire, la télédistribution, la gestion des licences, le déploiement d'OS et la prise de main à distance.
- LANDesk Security Suite, se reposant sur la console LDMS et offrant une centralisation et une politique globale de la securité des postes de travail (antivirus, antispyware, gestion et encryption des ports USB, blocage d'application, mise en quarantaine, analyse comportementale, etc.).
- LANDesk Services Desk, Business Process Manager et Asset Life Cycle Manager. Ces produits offrent un outillage pour automatiser et optimiser les services aux utilisateurs dans une démarche complètement ITIL.

Ces trois gammes de produits peuvent fonctionner séparément, pour répondre à des besoins précis, ou de concert à partir d'une console d'administration commune. A partir de ce moment là, nos clients ont un outillage complet pour optimiser l'exploitation de leur parc, sécuriser leur ressources IT et apporter un service à leurs utilisateurs respectueux d'ITIL avec des tableaux de bord, des rapports et une automatisation complète des processus (workflow) supprimant l'erreur humaine. Nos clients font ainsi évoluer leur IT vers un centre de service démontrable et pérenne, où les coûts sont définis et limités.

GS Mag : Quels sont les principaux conseils que vous donnez à vos clients en termes de mise en œuvre de stratégie de gestion de parc informatique ?

Frédéric Pierresteguy : Ils doivent, en premier lieu, identifier l'ensemble de leur assets à l'aide d'outils techniques et dynamiques de gestion de parc. Cette première démarche leur permettra de maîtriser leur parc et d'appliquer de façon automatisée les bonnes procédures sécurité, système et services aux utilisateurs. La gestion quotidienne et l'évolution du parc se feront ensuite par la mise en place de bonnes pratiques ITIL, à l'aide de solutions de Service Desk, d'Asset Management et de Businesss Process Manager. Elles assureront une meilleure qualité de services aux utilisateurs ainsi qu'une meilleure automatisation des process d'exploitation du système d'information.

Une bonne gestion de parc passe par la mise en œuvre d'outils techniques et de process pour suivre dynamiquement l'évolution du SI.

GS Mag : Quelles sont vos principales références dans le milieu des institutions financières?
Frédéric Pierresteguy : Nous en avons plusieurs tant dans les banques que dans les assurances. Je peux citer, par exemple, Cofidis, La Banque postale, iBP, la Matmut, la Cie Financière Rotschild, Gras Savoye, SCOR…

GS Mag : Pour conclure, quel est votre message à nos lecteurs ?
Frédéric Pierresteguy : Avocent-LANDesk, à l'écoute de ses clients et du marché, continue à innover pour apporter des solutions performantes autour de la gestion des infrastructures dans un objectif constant de réduire les coûts d'exploitation associés. La suite LANDesk vous permet de couvrir l'ensemble des problématiques des besoins en ressource IT et non IT dans le domaine de la gestion de parc. Nous accompagnons nos clients pour transformer leur IT en un centre de services. ■■■

FICHE ENTREPRISE

Avocent | LANDesk

Date de création : 2000

Collaborateurs : 1900

CA : 620 millions de $

Solutions : Management des opérations IT, Management des Processus, Management des Incidents et Problèmes, et Management des changements et des configurations

Principales références :
Cofidis, La Banque postale, iBP, la Matmut, la Cie Financière Rotschild, le Crédit Agricole Asset Management, la Société Générale Asset Management, Gras Savoye, SCOR...

LA SENSIBILISATION : LE VACCIN DE LA SÉCURITÉ

Interview de Christophe Chaumont, responsable de la sensibilisation à la sécurité des Systèmes d'information de la BFI chez Natixis, par Marc Jacob


Christophe Chaumot

Christophe Chaumont est responsable de la sensibilisation à la sécurité des Systèmes d'information de la BFI chez Natixis. Il vient de mener une campagne de sensibilisation sur le site parisien de son établissement. Grâce à un quiz ludique de 5 minutes, il a pu obtenir des résultats satisfaisants. Pour lui, la sensibilisation, c'est comme les vaccins, les rappels doivent être réguliers.

Global Security Mag : Pouvez-vous nous présenter votre entreprise ?

Christophe Chaumont : Natixis est le partenaire bancaire de ceux - entreprises et institutionnels - qui construisent le monde de demain. Pour eux, les experts de Natixis interviennent dans cinq domaines complémentaires : la banque de financement et d'investissement, la gestion d'actifs, le capital investissement et la gestion privée, les services et la gestion du poste clients.
Coté en Bourse, et filiale de deux grands groupes bancaires, Banque Populaire et Caisse d'Épargne, qui détiennent chacun plus de 34 % de son capital.

GS Mag : Quelle est la taille de votre système d'information ?

Christophe Chaumont : La banque de financement et d'investissement de Natixis utilise plusieurs centaines d'applications. La plupart d'entre elles sont constituées de progiciels, mais nous avons également des applications maison, des applications « gros systèmes » et des applications externes, comme les plates-formes de négociation électronique, accessibles via internet.

Les actions de sensibilisation permettent de rappeler les principales règles en matière d'utilisation de SI

GS Mag : Dans un établissement bancaire où le personnel est généralement sensibilisé aux problèmes de sécurité, à quoi sert de mener des campagnes de sensibilisation sur la sécurité ?

Christophe Chaumont : Dans un établissement bancaire, les systèmes d'information sont un des maillons les plus délicats pour la sécurité, même si les acteurs et les utilisateurs y sont très sensibilisés.
Il est donc aussi important de mener des campagnes de sensibilisation à la sécurité que d'avoir des éléments de parade technique car aucune porte, même blindée, ne permet une sécurité à 100 %. Ces campagnes permettent de rappeler les règles principales de la politique de sécurité de façon ludique et de réviser les bonnes pratiques ou règles d'usage en matière d'utilisation des systèmes informatiques mis à disposition des collaborateurs de la banque.

GS Mag : Utilisez-vous des outils de sensibilisation du marché ?

Christophe Chaumont : Notre périmètre international nous a amené à faire une étude sur les différents outils de sensibilisation du marché pouvant s'intégrer à notre Intranet sécurisé, et qui, grâce à leur grande flexibilité, nous permettait de faire personnaliser nos messages. Après plusieurs tests, notre choix s'est porté sur CCI (un outil qui propose des scénettes de sécurité) et Sensiquiz un questionnaire à choix multiple de l'éditeur Conscio Technologies.
L'éditeur nous a accompagné dans la mise en place de l'outil et nous a apporté toute son expertise pour réussir l'intégration du produit dans notre système d'information et tenir compte de notre charte graphique.

GS Mag : Comment se déroulent vos campagnes de sensibilisation ?

Christophe Chaumont : L'objectif de notre campagne de sensibilisation est, dans un premier temps, de connaître le niveau de connaissance de nos collaborateurs afin de mieux cibler nos plans d'action.
Pour toucher un maximum de personnes des « Matinées de la sécurité » en avril 2008, pendant lesquels des PC à disposition permettaient aux personnes de venir répondre à un questionnaire de 5 minutes, non nominatif. Ce format était parfaitement adapté à la population des salles de marchés, habituée à beaucoup de réactivité.
Nous n'avons pas oublié les informaticiens, pour qui nous avons réalisé un quiz un peu plus technique, et auquel plus de 20 % de nos informaticiens internationaux ont participé à l'événement.
Afin de récompenser chaque personne, un mug avec un message de sécurité « N'oubliez pas de verrouiller votre poste de travail lorsque vous allez prendre un café » était remis à chacun.

GS Mag : Quels sont les principaux thèmes que vous avez abordé lors de votre campagne de sensibilisation ?

Christophe Chaumont : Notre campagne de sensibilisa-


© Slavoljub Pantelic

tion s'est calquée sur les grands thèmes de notre politique de sécurité.
Voici quelques exemples de questions :

■ POUR LES UTILISATEURS :
Sur le poste de travail
« Vous souhaitez installer un logiciel supplémentaire sur votre poste de travail comment faites-vous ? »
Sur le thème de la responsabilité
« Vous transmettez à un ami qui en a besoin dans son travail la structure des bases de données de votre entreprise. Que risquez vous ? »

■ POUR LES INFORMATICIENS :
Architecture et mécanisme de sécurité
« Sous quelle forme doivent être échangées les données entre une plateforme électronique de marché et un réseau non securisé (Internet) ? »
Traces
« A quelle fréquence doivent être analysées les traces ? »

GS Mag : Avez-vous rencontré des réticences de la part de votre personnel ?

Christophe Chaumont : Cette campagne était faite sur la base du volontariat. Le côté ludique et peu consommateur de temps a été très bien perçu par l'ensemble de la population. Le cadeau était le petit plus qui nous a permis de sensibiliser un maximum de collaborateur.
Bien sûr la direction avait été informée de cette campagne ; certains directeurs ont même participé au test. Pour un tel événement sur plus de 5 sites parisiens, nous nous sommes appuyés fortement sur notre service de communication pour relayer l'événement via nos média internes (mes- sages électroniques, sites intranet, campagne d'affichage).
Ce travail commun avec les différents services a permis cette réussite et l'adhésion du personnel.

GS Mag : Avez-vous, à ce jour, mesuré l'impact de votre campagne de sensibilisation ?

Christophe Chaumont : Le bilan de cette campagne est plus que satisfaisant. Nous avons touché plus de 25 % de la population parisienne, et 10 % à l'international Elle nous a permis de faire un premier bilan du niveau de connaissance pour l'ensemble des collaborateurs : plus de 65 % des collaborateurs connaissent les règles sur l'utilisation d'internet et de la messagerie.
Mais des améliorations doivent être faites sur la responsabilité des personnes vis-à-vis des données et l'utilisation des moyens informatiques mis à leur disposition. Des formations au Plan de continuité des activités, devront être faite pour parfaire leurs connaissances.

Pour nous la sensibilisation à la sécurité est vitale. Comme les vaccins, des rappels périodiques sont nécessaires pour ne pas perdre notre sensibilité aux risques. ■■■

FICHE ENTREPRISE

Natixis BFI
Christophe Chaumont

Fonction : responsable de la sensibilisation à la sécurité des Systèmes d'information de la BFI chez Natixis

Taille du SI : 750 applications

A VOS AGENDAS !
19 NOVEMBRE 2008 - SALON INFOSECURITY

EVENEMENT DEDIE A LA SECURITE INFORMATIQUE DANS LE SECTEUR DES BANQUES ET ASSURANCES !

La sécurité informatique dans les banques et assurances est plus que jamais d'actualité, nous vous proposons une journée au cœur de ces problématiques stratégiques !

9H30 – 10H15 : CLUSIF
Enjeux de la sécurité dans le secteur de la banque et de l'assurance.
Présentation des résultats sur l'étude « Menaces Informatiques et Pratiques de Sécurité en France » dans le secteur bancaire et assurance !

10H15 – 11H45 : EVIDIAN
Maîtriser les risques opérationnels avec la gestion des identités et des accès.
Présentation des résultats sur l'étude « Menaces Informatiques et Pratiques de Sécurité en France » dans le secteur bancaire et assurance !
La gestion du cycle de vie des accès des employés est nécessaire pour maîtriser les risques opérationnels. En s'appuyant sur le retour d'expérience de banques européennes et sur une étude de Datamonitor sur la gestion des identités et des accès en secteur bancaire, Evidian présente une approche pragmatique pour réduire les risques opérationnels.

11H45 – 12h30 : XMCO Partners
Real life : Rapport d'autopsies de cas réels de hacking dans le monde bancaire et de l'assurance.
Trop souvent, la sécurité informatique et les attaques sont abordées de façon théorique. Nous présenterons ici 4 cas réels de hacking où une entreprise s'est faite piratée. Nous décortiquerons le mode opératoire du pirate et les actions qu'il a pu réaliser en s'intéressant aux failles exploitées.
Il s'agira d'un retour d'expériences sur des cas réels où le cabinet Xmco Partners a été amené à intervenir en tant qu'expert.

14H00 – 15H15 : Groupe E-BANQUE (FNTC)
Kirviel", 2 Kirviel, 3 Kirviel : l'identité au cœur de la chaîne de Sécurité de la Banque.
Les architectures sont de plus en plus hétérogènes, les utilisateurs des applications métiers peuvent être internes ou externes : dans ce contexte, une des problématiques majeures de sécurisation des systèmes d'informations est liée à la gestion des identités. Les différents cadres juridiques et réglementaires (SEPA, Anti-blanchiment, Bâle II...) mettent également l'identité au cœur de nombreux sujets.
En s'appuyant sur un cas concret (solutions mises en place pour la sécurisation des accès au SI par les différents acteurs: employés, partenaires, clients...) les différents intervenants feront un résumé des principales problématiques auxquelles les DSI et RSSI des banques ont à faire face.

15H30 – 16H30 : GEMALTO
Retour d'expérience sur un déploiement de badge d'entreprise supportant l'identification numérique.

JEAN-MICHEL CRAYE, ORANGE BUSINESS SERVICES :

LE CHALLENGE DE LA SÉCURITÉ EST LA FLEXIBILITÉ

Interview par Marc Jacob


Jean-Michel Craye

Orange Business Services est la branche entreprises du Groupe Orange qui propose des services d'opérateur et conçoit des solutions sur mesure d'infrastructures IT tant en France qu'à l'international. La sécurité et la continuité de service sont au cœur de ses offres. Selon Jean-Michel Craye, Directeur marketing Sécurité d'Orange Business Services, le challenge de la sécurité est la flexibilité afin d'intégrer rapidement de nouveaux utilisateurs, de nouveaux sites ou de nouvelles activités.

Global Sécurité Mag : Pouvez-vous nous présenter Orange Business Services ?

Jean-Michel Craye : Orange Business Services est la branche entreprises du Groupe Orange. Elle propose deux types d'activités qui couvrent le marché français et international :
- le métier d'opérateur pour les utilisateurs mobiles, les réseaux et les services de communication.
- la partie services qui conçoit des solutions sur mesure pour nos clients dans le domaine des grands projets d'infrastructure IT.

GS Mag : Quelle est votre offre en matière de sécurité ?

Jean-Michel Craye : Nous avons une offre globale qui part du poste utilisateur avec des solutions d'authentification, de chiffrement et sécurité du poste de travail, en passant par la sécurité des réseaux inter-sites et locaux (solution UTM et routeur sécurisé). Elle prend aussi en compte la sécurité des datacenters avec la sécurité des applications et la virtualisation. Notre réseau VPN vient d'être certifié a nouveau par la DCSSI, pour toute la partie hors France.
Pour être complet, Orange Business Services accompagne ses clients par une démarche de conseils (certification PCI-DSS et ISO 27000) qui est indispensable à la réussite de la mise en œuvre de la sécurité.

GS Mag : Quelles sont vos solutions phares pour 2008 ?

Jean-Michel Craye : L'année 2008 a été très riche, on peut citer : la première offre de Business Contuinuity de synchronisation de données : i-SAN entre deux datacenters, mais aussi le lancement de la première gamme de router embarquant la sécurité native (Network Protect) ainsi que la montée en puissance des solutions sécurité UTM « tout en un » Unified Defense.

GS Mag : Quelles sont les sujets clés que vous allez aborder en 2009 ?

Jean-Michel Craye : Nous allons nous focaliser tout d'abord sur la supervision de la sécurité. Nous aborderons aussi la virtualisation comme outils de renforcement de la sécurité. Bien sûr, la sécurité des postes nomades, PC Portables et PDA et autres outils de mobilité, ne sera pas oubliée. Enfin, nous prendrons en compte les problématiques de sécurité associées dans le contexte de connexion aux datacenters (WEB 2.0, applications en ligne, etc).

Il est important de mettre en œuvre une architecture souple et réactive

GS Mag : Quels sont les principaux conseils que vous donnez à vos clients ?

Jean-Michel Craye : En fait, le chalenge de la sécurité est aujourd'hui la flexibilité. Elle doit s'adapter rapidement aux évolutions du monde financier et non le freiner.
Une bonne sécurité intègre rapidement de nouveaux utilisateurs, de nouveaux sites ou de nouvelles activités. Il est donc plus important de mettre en place une architecture souple et réactive, plutôt qu'une solution « parfaite » mais complexe à déployer et surtout à faire évoluer.

GS Mag : Quelles sont vos principales références dans le milieu des institutions financières ?

Jean-Michel Craye : Je peux citer entre autre le Crédit Municipal de Paris pour lequel nous avons assuré la refonte et la virtualisation de son informatique (par Néocles, filiale d'Orange Business Services). Nous travaillons aussi avec la plupart des grands groupes du monde de la banque et de l'assurance.

GS Mag : Pour conclure, quel serait votre message à votre clientèle ?

Jean-Michel Craye : La sécurité doit être synchrone avec le business de l'entreprise, tant sur le plan de l'accompagnement organisationnel que technique. En un mot une sécurité embarquée dans le métier et le SI.


Hervé Troalic

Orange accompagne la mise en œuvre de PCI DSS

Par Hervé Troalic - Directeur Pôle conseil sécurité

Ce référentiel concerne toutes les organisations qui stockent, traitent ou transmettent des données des titulaires de cartes bancaires.
Pour faire simple, ces données contiennent au moins le numéro de carte bancaire. Ce référentiel se présente sous la forme d'un code de bonnes pratiques de sécurité en 12 chapitres.

Le bénéfice attendu de la mise en conformité vis-à-vis de ce référentiel est une réduction des risques de sécurité sur les plateformes et principalement les risques de vols de données.
Ce référentiel est aujourd'hui surtout déployé dans les pays anglo-saxos mais l'Europe est aussi concernée sous l'impulsion des établissements bancaires en charge de faire déployer ce référentiel chez leurs clients sous peine d'amendes.

Dans ce cadre, les établissements bancaires doivent s'appuyer sur des cabinets d'audits certifiés par PCI pour attester que les clients des banques sont conformes. Sans rentrer dans le détail, il existe deux programmes de certification, le programme QSA (audits sur sites) et l'ASV (scans de vulnérabilités). En ce qui nous concerne, en tant que spécialiste reconnu de la sécurité du système d'information, nous avons décidé de nous positionner sur ces deux programmes (échéance fin 2008).

Nous serons donc en mesure d'attester de la mise en conformité mais nous sommes déjà capables d'accompagner nos clients sur la mise en conformité.

PCI / DSS (Payement Card Industry Data Sécurity Standard) est un référentiel de sécurité mis au point et promu par PCI (VISA / Mastercard / AMEX).

THIERRY CHARVET, DIRECTEUR DU MARKETING DE ORANGE BUSINESS SERVICES - TRADING SOLUTIONS :

SOLUTION DE TRADING : CONCILIER CONTINUITÉ ET FLEXIBILITÉ


Thierry Charvet

GS Mag : Quelle est votre approche de la continuité d'activité chez vos clients ?

Thierry Charvet : Notre approche de la continuité d'activité est d'être totalement en adéquation avec les besoins de nos clients. Ainsi, nous proposons des solutions qui s'adaptent tant au problème de catastrophe naturelle, d'attaque terroriste ou encore de pandémie. Pour les salles de marché en particulier, les institutions financières doivent être en conformité avec les législations en vigueur qui se renforcent tous les jours depuis les attentats du 11 septembre et de Londres. En Europe, par exemple, ces organisations doivent être en conformité aux accords de Bâle II et aux Etats-Unis à SoX et au Patriot Act qui visent notamment à obtenir de leur part une continuité d'activité face à toutes les situations de crises. De plus, les impacts financiers en cas de rupture d'activité pouvant se chiffrer en plusieurs millions d'euros par jour, ces entreprises souhaitent bénéficier de solutions de pointe et adaptées à ces enjeux. Ainsi, la continuité d'activité doit répondre à ces deux objectifs.

GS Mag : Quelles solutions proposez-vous ?

Thierry Charvet : Nous proposons donc des solutions adaptées à chaque contexte. Par exemple, dans le cas d'une destruction de salle de marché ou d'impossibilité d'accéder à un local inclus dans le périmètre d'un sinistre, nous proposons la mise en place de site de Back Up avec une image complète du site principal et utilisable dans la demi journée. Cette solution permet aussi de faire du re-routage de ligne. Le trader retrouve ainsi tout son environnement sur le site de repli. Dans le cas de pandémie avec blocage des transports, nous avons la solution « Mobile Voice Record » pour qu'ils puissent avoir accès à leur environnement depuis n'importe où via un BlackBerry, tout en étant enregistré comme l'impose la législation. Nous proposons aussi l'offre « Mobile Trader » qui permet à partir d'un PC personnel d'avoir accès depuis chez soi de façon sécurisé aux données nécessaires pour une reprise d'activité tout au moins partielle : contacts, applications....
Pour conclure, je dirais que le maître mot de nos solutions est la flexibilité afin de répondre à tous les besoins de nos clients.

DÉMATÉRIALISATION ET ARCHIVAGE ÉLECTRONIQUE : POUR UNE PLUS GRANDE EFFICACITÉ DES ÉCHANGES

Par Jean-Marc Rietsch, Président de FedISA


Jean-Marc Rietsch

La dématérialisation se limite pour beaucoup à la numérisation de documents papiers, alors que ses principaux bénéfices reposent dans la mise en œuvre de processus totalement dématérialisés, sans aucun papier. Il en est ainsi de notre déclaration d'impôt, de la déclaration de TVA ou encore des factures qui peuvent être totalement dématérialisées. Les applications sont de plus en plus nombreuses avec la dématérialisation des contrats à la consommation ou encore l'ensemble des réservations et des paiements sur Internet. Si cela permet avant tout une plus grande efficacité des échanges, il en résulte, bien évidemment, quelques contraintes supplémentaires.

Si les problèmes de sécurité de la dématérialisation sont importants, ils n'en restent pas moins gérables et maîtrisables. En revanche, nous sommes encore loin d'être suffisamment sensibilisés à celui de la perte de données : Quel remède trouver face à « l'Alzheimer des entreprises » ? Comment faire pour que l'entreprise fonctionne si elle perd sa mémoire ?

De plus, l'archivage électronique ne doit surtout pas être vu comme une simple transformation de l'archivage traditionnel papier en électronique. Il correspond en réalité à une nouvelle organisation du système d'information de l'entreprise et nécessite de prendre en compte l'ensemble du cycle de vie de la donnée. Les entreprises ont beaucoup à y gagner, car au-delà de l'information, il y a la connaissance, clé du succès face à la compétitivité de demain, comme le rappelle si justement Alain Juillet, Haut Responsable à l'intelligence économique en France.
Un profond changement est à opérer afin qu'un document soit assorti, dès sa création, d'informations complémentaires (les métadonnées) destinées à permettre son évolution et son archivage en toute conformité. La législation impose, en effet, de pouvoir apporter la preuve de l'identification de l'auteur d'un document dès son origine. On distingue trois grandes étapes dans la vie d'un document :
- de sa création jusqu'à être figé, validé ;
- la période de conservation imposée par des obligations légales, réglementaires, voire internes ;
- l'archivage patrimonial et historique qui ne représente qu'un faible pourcentage.

La notion même de validation d'un document, moment à partir duquel il n'est plus modifié, revêt une importance capitale dans tous les processus de dématérialisation. Dès cet instant, le document devient, en effet, archivable au sens électronique du terme tout en restant parfaitement accessible.

Les contraintes de la dématérialisation et de l'archivage électronique existent mais…

Contraintes techniques

La première des contraintes concerne le format logique des documents. En effet, un document électronique nécessite systématiquement un traitement de transcription de la suite d'octets enregistrée sur le support électronique (disque, bande, …) afin de le présenter de façon intelligible à l'utilisateur. Un tel traitement dépend essentiellement du format logique dans lequel sont enregistrés les documents électroniques. Il est ainsi fondamental d'utiliser des formats pérennes. On privilégiera ainsi des formats standard (normalisés, d'utilisation libre) à des formats fermés aux spécifications secrètes.

Le choix du support pose le véritable paradoxe de l'archivage électronique qui consiste à devoir conserver pendant de longues périodes, voire ad vitam aeternam, des données en utilisant des supports à l'obsolescence extrêmement rapide. La seule solution est en réalité d'anticiper cette évolution et de prévoir systématiquement une migration des données d'un support à un autre de façon régulière. Néanmoins certains types de supports sont plus appropriés que d'autres lorsque l'on traite d'archivage électronique. A ce niveau une notion est impor-


© Slavoljub Pantelic

tante à retenir, celle du WORM (Write Once Read Many) consistant à protéger la donnée d'une modification ou d'une suppression intempestive afin de garantir son intégrité.

Enfin, si la signature électronique apporte beaucoup de sécurisation à tout ce qui est dématérialisation permettant à la fois une bonne identification de l'auteur d'un document mais aussi le contrôle de son intégrité, elle impose certaines précautions en matière de préservation. En effet, se pose à la fois la nécessité de pouvoir vérifier à tout moment la signature et le problème de l'obsolescence cryptographique du procédé de signature.

CONTRAINTES LÉGALES ET RÉGLEMENTAIRES

Le point de départ a été donné par la loi du 13 mars 2000 conférant une véritable reconnaissance de valeur probante à l'écrit sur support électronique au même titre que l'écrit sur support papier. Même si les exigences en matière de dématérialisation sont de plus en plus nombreuses, les principales à retenir sont les suivantes :
- Intelligibilité : peu importe la forme de l'information, l'essentiel est qu'elle soit restituée de façon compréhensible par l'homme ;
- Identification : l'écrit sous forme électronique doit permettre d'identifier la personne dont il émane ;
- Intégrité : cette garantie d'intégrité s'applique au contenu informationnel de l'écrit électronique et pas seulement à son intégrité technique ;
- Pérennité : permet de respecter les durées de conservation prescrites par les textes en fonction de la nature du document et des délais de prescription.

A ces quatre exigences s'ajoute également la notion importante de confidentialité et d'accès contrôlé à l'information, particulièrement sensible au niveau de la loi « Informatique et Libertés » dont la CNIL est chargée de veiller au respect.

Vers une nouvelle organisation

Face à toutes ces contraintes les solutions existent :
- Qualification de l'information à l'aide des méta-données ;
- Mise en œuvre d'une logique projet face aux problématiques de dématérialisation et d'archivage électronique ;
- Méthodologie autour de la politique d'archivage ;
- Evolution des normes et autres interfaces plus techniques comme l'interface XAM (eXtensible Access Method) destinée à fournir une indépendance entre les applications, les logiciels d'administration et les systèmes de stockage…

LES TIERS DE CONFIANCE

Cette notion de tiers de confiance, présentée souvent comme une notion nouvelle, existe en réalité depuis fort longtemps avec les notaires. Les tiers de confiance sont incontournables d'un point de vue « légal » puisqu'ils se portent garant d'une partie de la chaîne de confiance qui doit être maintenue tout au long des processus de dématérialisation. Nous citerons succinctement les quatre tiers que l'on retrouve le plus fréquemment :
- Certificateurs (autorité, opérateur), agissent dans le domaine de la signature électronique et s'engagent quant à la validité du certificat au moment où il est utilisé ;
- Horodateurs, garantissent une date et une heure mais n'interviennent en aucune façon sur le contenu au sens informationnel ou intégrité ;
- Archiveurs, s'engagent à conserver les données qui leur sont confiées pendant toute la durée requise de façon intègre ;
- Autorité de gestion de preuve, établit une attestation de preuve témoignant de la validité de la signature électronique d'un document, tant sous son aspect intègre que sur la validité du certificat.

La dématérialisation est donc loin d'un simple phénomène de mode. En fait, nous n'en sommes qu'à ses balbutiements dans la mesure où elle touche tant les entreprises que les particuliers. Nous vivons ainsi à l'aube d'une réorganisation profonde des flux d'informations dans l'ensemble des organisations avec pour principal objectif de gagner en efficacité, sans pour autant perdre en relationnel. Il faut donc y voir une formidable opportunité pour les professionnels comme pour les particuliers, afin de permettre, au-delà de l'information, d'accéder à plus de « connaissance ».

A NOTER DANS VOS AGENDAS !
20 NOVEMBRE 2008 - STORAGE EXPO 2008

LA FEDISA CREE L'EVENEMENT SUR LE SALON STORAGE EXPO 2008 !

Stockage, Sauvegarde, Conservation et Archivage, complémentaires ou opposables ?

«Comment passer de la sauvegarde à l'archivage»? «Doit-on parler de gestion, de conservation ou d'archivage des mails»?
« Certification » d'un système d'archivage électronique: quelle(s) norme(s), quel(s) standard(s), quel(s) référentiel(s) ?
Cette journée sera l'occasion d'aborder les thèmes du Stockage, de la Sauvegarde, de la Conservation et de l'Archivage des données à la fois sous leurs aspects fonctionnels, techniques mais aussi juridiques et réglementaires.

Programme

9h30-10h15 : FedISA Stockage, Sauvegarde, Conservation et Archivage, complémentaires ou opposables ? Jean-Marc RIETSCH Président
10h15-11h00 : Beemo Technologie Mise en place d'une sauvegarde simple et fiable - cas client PME et Grand Compte : Olivier MAURAS Directeur Général
11h15-12h00 : Document@work Les tendances de l'ECM au jour d'aujourd'hui : Phédra CLOUNER Présidente
12h00-12h45 : STS-group Dématérialisation, archivage électronique et valeur probatoire, exemples concrets. Thierry BLANC Directeur marketing
14h00-14h45 : FedISA Irlande Aspect sécuritaire, trait d'union entre sauvegarde et archivage : Mathieu GORGE, Président
14h45-15h30 : Iron Mountain Digital Je suis serein, mes données déstructurées sont protégées, localisées, exploitables avec exemple client : Jean-Philippe FABRE Directeur technique Europe du Sud
15h45-17h00 : Table ronde Synthèse de la journée, débat autour du thème principal : Stockage, Sauvegarde et Archivage, pour la protection des données face aux risques pas seulement techniques…
17h00 : Fin des conférences


Olivier Mauras

OLIVIER MAURAS, BEEMO TECHNOLOGIE :

EXTERNALISEZ LA SAUVEGARDE DE VOS DONNÉES EN TOUTE SÉCURITÉ

Interview par Emmanuelle Lamandé

Face à la pléthore de données à sauvegarder aujourd'hui, les entreprises ont besoin de rationaliser leur système de stockage de production, en évitant toute redondance et en isolant les données cruciales. Dans cette optique, la société Beemo Technologie propose une alternative à la sauvegarde classique, à travers sa solution Data Safe Restore. Olivier Mauras, Directeur R&D chez Beemo Technologie, présente son offre de service globale qui se décline sur le modèle du SaaS.

Global Security Mag : Pouvez-vous nous présenter votre entreprise ?

Olivier Mauras : La société Beemo Technologie a été fondée en Novembre 2002 par Gabriel Biberian et moi-même. Nous intervenons sur le marché de la sauvegarde de données, en proposant une solution intermédiaire entre la sauvegarde classique et la télésauvegarde. A travers notre offre globale de services et notre solution Data Safe Restore, nous nous positionnons sur le marché du SaaS (Software as a Service).

GS Mag : Quel est votre produit phare pour 2009 ?

Olivier Mauras : Nous n'avons pas de nouveaux produits, mais des évolutions régulières de notre solution phare, Data Safe Restore. Nous la rendons toujours plus performante, par l'ajout de nouvelles fonctionnalités. La prochaine évolution est prévue pour le premier trimestre 2009. Les mises à jour sont régulières et se font automatiquement. Le client n'a donc pas à s'en préoccuper et ne s'en rend souvent même pas compte.

L'objectif est de rationaliser votre système de stockage

GS Mag : Quels sont les principaux conseils que vous donnez à vos clients au niveau de la mise en œuvre de stratégie dans le domaine du stockage des données ?

Olivier Mauras : Les entreprises se retrouvent aujourd'hui avec d'importantes quantités de données à sauvegarder. L'objectif principal est d'arriver à rationaliser le stockage de leur système de production. Il faut, tout d'abord, distinguer les données créées par l'entreprise des données OEM (OS, application). De plus, les données de production doivent être classées par typologie, afin d'appliquer pour chaque cas une politique de sauvegarde adéquate et de gérer plus facilement leurs cycles de vie. Ce sont principalement nos revendeurs et distributeurs qui prodiguent ces conseils auprès de nos clients et essaient de trouver un système de sauvegarde sur mesure répondant au mieux aux besoins du client.

GS Mag : Quelles sont vos principales références ?

Olivier Mauras : Nous adressons tous les types et les tailles d'entreprises, quel que soit leur secteur d'activité. Notre offre s'adapte aussi bien aux PME/PMI – qui ont aujourd'hui compris l'aspect stratégique et vital de la sauvegarde des données - qu'aux grands comptes, qui trouvent dans notre solution une réponse parfaitement adaptée à leurs besoins et très facile à déployer, notamment dans le contexte d'organisations multisites. Nous comptons de nombreuses références en France, parmi lesquelles la Fondation Jacques Chirac, la Croix Rouge, Transcausse ou la Principauté de Monaco.

Nous souhaitons étendre notre marché au niveau européen

GS Mag : Quelles sont vos perspectives de développement ?

Olivier Mauras : Nous voulons nous positionner parmi les principaux acteurs de solutions de sauvegarde en France et attaquer des marchés comme l'Angleterre, la Belgique, l'Allemagne, ou encore l'Espagne. SARL à l'origine, Beemo Technologie est aujourd'hui une Société Anonyme au capitale de plus d' 1M€. Nous souhaitons débloquer de gros investissements afin de pouvoir agrémenter notre offre de services et de prestations supplémentaires.

GS Mag : Pour conclure, quel serait votre message à votre clientèle ?

Olivier Mauras : La sauvegarde n'est pas quelque chose de compliqué, dans la mesure où vous vous orientez vers du service et que vous acquérez un système global. Nous vous offrons ce service global (équipement, prestation,…).

FICHE ENTREPRISE

Beemo technologie

Date de création :
Novembre 2002

Solution :
Data Safe Restore

Principales références :
Fondation Jacques Chirac, la Croix Rouge, Transcausse ou la Principauté de Monaco

THIERRY BLANC, STS GROUP :

NOUS VOUS PROPOSONS UN PASSEPORT POUR L'ÉCONOMIE NUMÉRIQUE

Interview par Marc Jacob


Thierry Blanc

Le passage à l'économie numérique est l'enjeu du 21ème siècle, estime Thierry Blanc, Directeur marketing de STS Group. Pour s'imposer, ce nouveau concept a besoin de l'établissement d'un véritable environnement de confiance numérique. STS Group propose des solutions techniques pour permettre aux entreprises de franchir ce cap. Pour Thierry Blanc, les outils techniques sont aujourd'hui disponibles, mais les entreprises doivent avant tout réfléchir à leurs objectifs et leurs pratiques.

Global Security Mag : Pouvez-vous nous présenter votre entreprise ?
Thierry Blanc : La création de notre société, en 2000, a coïncidé avec l'évolution majeure de la législation sur l'économie numérique*. Cette législation a permis de poser les conditions d'une nouvelle manière d'établir les usages commerciaux. Pour que cette nouvelle économie s'impose, elle a besoin de se doter d'un environnement de confiance. Nous avons justement créé STS Group pour proposer tous les composants techniques afin d'établir les bases de cette nouvelle société.

> Nos solutions permettent de gérer l'établissement et la conservation de la preuve numérique

GS Mag : Quel sont ces outils ?
Thierry Blanc : Nous proposons des modules logiciels pour gérer, en particulier, l'établissement et la conservation de la preuve numérique, en administrant les interfaces avec des tiers de confiances tels que tiers certificateurs, horodateurs et des autorités de gestion de preuve. Dans notre suite, on trouve entre autres un module qui a pour vocation d'établir la preuve électronique : STS Proof Server, et un coffre fort numérique pour la conservation sécurisée : STS Digital Vault.
Ces produits ont vocation à être exploités dans un certain nombre de domaines de l'économie numérique : archivage probatoire, échanges électroniques à valeur probatoire… Nous avons aussi élargi notre champ de prédilection en proposant un service de votre électronique par correspondance. Ainsi, le Barreau de Bruxelles élit son Bâtonnier avec notre solution. Nous avons la conviction que ces technologies peuvent apporter des solutions à la plupart des problématiques de l'économie numérique.

> La détermination d'une politique d'archivage doit précéder le déploiement de solutions techniques

GS Mag : Quels sont les principaux conseils que vous donnez à vos clients au niveau de la mise en œuvre de stratégie dans le domaine de l'archivage électronique ?
Thierry Blanc : Mon principal conseil est plus d'ordre méthodologique que technique. En effet, les outils techniques sont aujourd'hui de qualité et ont fait leur preuve. Par contre, trop souvent encore, les entreprises éludent la phase d'audit pour déterminer précisément leur politique d'archivage. Il n'est pas question pour elles de tout archiver, mais de déterminer, en fonction de leurs besoins, et des contraintes, légales, règlementaires, ou organisationnelles, quels sont les données et documents à conserver. La DCSSI propose des exemples de politique d'archivage. Des consultants spécialisés, des Fédérations professionnelles… peuvent aussi les aider.

GS Mag : Quelles sont vos principales références dans le milieu des institutions financières ?
Thierry Blanc : La plupart des grandes banques françaises sont nos clientes, à commencer par la Banque de France qui depuis 2005 utilise notre suite pour son socle d'archivage globale appelé ARCHV. On peut aussi citer la Société Générale, les Banques Populaires, les Caisses d'Epargne, le Crédit Agricole… l'UBP, la BCL, le Groupe des Cartes Bancaires. Dans le domaine de l'assurance, nous travaillons avec Areas, AGF, Winthertur…

GS Mag : Pour conclure, quel serait votre message à nos lecteurs ?
Thierry Blanc : Nous sommes à l'aube d'une révolution qui sera sans doute plus importante encore que la révolution industrielle. La démocratisation de l'économie numérique va démultiplier totalement les moyens d'action des entreprises. Elle va leur permettre de s'affranchir du temps et de l'espace. Demain, il sera possible de travailler avec n'importe quelle entreprise, qu'elle se trouve au coin de la rue ou à l'autre bout du Monde, dans les mêmes conditions de coûts et de délais. L'économie numérique est donc le passeport pour un nouveau mode d'échange. Nous avons l'ambition d'être un des maillons techniques pour assurer ce passage. ■ ■ ■

*** Directive européenne du 13 décembre 1999 qui a institué l'usage de la signature électronique. Cette directive a été suivie en France par la loi du 13 mars 2000 qui a modifié les articles 1316-1 et 1316-4 du code civil en précisant la définition d'un écrit électronique et des 3 conditions de sa valeur de preuve : - reconnaissance de l'écrit électronique des personnes physiques ou morales, - intégrité de la conservation des documents et - intelligibilité de ces documents dans le temps qui induit l'utilisation de format public donc normalisé (XML, PDF/A…).**

FICHE ENTREPRISE

STS GROUP
The Record Retention Company™

Date de création : 2000

Chiffre d'affaire :
11.300 millions d'€ en 2007
20 millions € en 2008

Solution : STS Suite

Principales références :
Banque de France, Banque Postale, BNP Paribas, Cofinoga, Groupement des Cartes Bancaires, Sofinco, UBP, Gras Savoye


Frédéric Bouzy

FRÉDÉRIC BOUZY, IRON MOUNTAIN DIGITAL :

LA SAUVEGARDE EST L'ASSURANCE VIE DE VOTRE ENTREPRISE

Interview par Marc Jacob

Iron Mountain bénéficie d'une longue expérience de la protection des informations quel que soit leur support : numérique ou physique. Iron Mountain Digital fournit des logiciels et des services de sauvegarde, de restauration et d'archivage de données. Pour Frédéric Bouzy, son Directeur Europe du Sud, une bonne sauvegarde des données doit permettre de localiser et retrouver des données où que l'on se trouve dans le monde. Selon lui, la sauvegarde est l'assurance vie de l'entreprise.

Global Security Mag : Pouvez-vous nous présenter votre entreprise ?

Frédéric Bouzy : Iron Mountain propose une gamme complète de solutions de gestion d'archives (records management) et de protection des données. Elle apporte son expertise et son expérience pour relever des défis complexes tels que l'augmentation des coûts de stockage, les litiges, la conformité aux obligations légales et réglementaires ainsi que la reprise après sinistre. Pôle technologique d'Iron Mountain, Iron Mountain Digital fournit des solutions et des services permettant la sauvegarde et la restauration des PC, des serveurs distribués ainsi que la sécurité des données des PC. Nous proposons également un service de gestion des e-mails qui inclut l'archivage externalisé, la continuité de service, la reprise après sinistre et la sécurité. Notre offre est adaptée à tout type d'entreprise, du grand compte à la PME.

Nous bénéficions de plus de 1020 sites de conservation dans le monde. Notre site souterrain historique a été acquis il y a 50 ans à l'Etat de New York. C'est une ancienne mine de fer où sont conservés des documents du gouvernement américain, les archives nationales des Etats-Unis, les sauvegardes informatiques des plus grandes entreprises américaines : les pellicules originales des films d'Universal Studios et de Walt Disney depuis les débuts d'Hollywood, les brevets de la machine à coudre Singer et de la statue de la Liberté…

Connected Backup a été vendue à plus de 2,5 millions d'exemplaires

GS Mag : Quel est votre produit phare pour 2009 ?

Frédéric Bouzy : Connected Backup est une solution de sauvegarde et de restauration des données. Nous avons vendu plus de 2.5 millions de licences de ce produit dans le monde. DataDefense permet, en cas de perte ou de vol d'ordinateurs, d'empêcher à des personnes non autorisées d'accéder aux données qu'ils contiennent. Nous annoncerons en 2009 de nouvelles avancées pour nos solutions phares Connected Backup, DataDefense & E-Discovery.

Suite au rachat de Stratify en 2007, nous proposons aussi des technologies pour rechercher dans le SI de l'entreprise des preuves électroniques utilisables lors de litiges.

GS Mag : Quels sont les principaux conseils que vous donnez à vos clients en termes de mise en œuvre de stratégie de sauvegarde et de protection des données ?

Frédéric Bouzy : Les entreprises doivent considérer la sauvegarde comme le premier élément à prendre en compte dans le cadre de leur PRA. Elles ne doivent pas négliger la sauvegarde et l'archivage des e-mails, en particulier dans le cadre de la lutte contre la fraude et la corruption.

GS Mag : Quelles sont vos principales références dans le milieu des institutions financières ?

Frédéric Bouzy : Iron Mountain compte parmi sa clientèle internationale de nombreuses sociétés réputées comme, par exemple, Deutsche Verkehrsbank et Bank of Scottland, Swiss Life Allemagne. Des institutions telles que Le Ministère des Finances Belge nous font également confiance.

GS Mag : Pour conclure, quel serait votre message à nos lecteurs ?

Frédéric Bouzy : Une bonne politique de sauvegarde des données doit permettre de retrouver et localiser ses données où que l'on se trouve dans le monde. Dans une époque en mutation permanente, il est primordial de mettre en place une stratégie de centralisation des données sensibles.

FICHE ENTREPRISE

IRON MOUNTAIN DIGITAL

Date de création : 1951
Le pôle technologique d'Iron Mountain, Iron Mountain Digital, a été créé suite au rachat de Connected en novembre 2004.

Collaborateurs :
19 500 personnes

CA : 2.7 milliards $ en 2007 (160 millions $ pour Iron Mountain Digital)

Solutions : Connected Backup/PC, Connected Backup/SV, LiveVault, DataDefense, Total Email Management Suite

Principales références :
Europcar, Leo pharma, Swiss Life, Ministères des Finances

KROLL ONTRACK®

Ontrack® Eraser

Logiciel d'effacement sécurisé

Principes

Ontrack Eraser est un logiciel flexible et simple d'emploi qui permet l'**effacement définitif et sécurisé des données**. Cet outil protège les entreprises contre les vols de données et leur permet de se conformer aux lois et réglementations en vigueur concernant la conservation des données et la protection des informations privées.

Facilité d'utilisation

Une installation et une utilisation facilitées par une interface intuitive, **Ontrack Eraser** s'installe sur un serveur ou directement sur le support à effacer. Gestion maitrisée de l'effacement au travers du réseau ou hors réseau. Création du support bootable d'effacement.

Garantie d'effacement

Ontrack Eraser est certifié par de nombreuses autorités : **OTAN, Ministère de la Défense américaine, CESG...** Vous choisissez parmi un nombre de certifications prédéfinies ou vous intégrez votre propre algorithme d'effacement et définissez le nombre de passes.

Mode de fonctionnement

Ontrack Eraser s'installe sur un serveur central depuis une clé USB. Le serveur gère les licences et les outils de reporting. En général, l'utilisateur connecte le disque dur à effacer au serveur. Ceci déclenche le processus d'authentification et l'effacement proprement dit. A la fin de l'opération, un rapport est produit et envoyé à l'utilisateur. **Ontrack Eraser** peut s'utiliser directement sur le support à effacer.

Flexibilité

Ontrack Eraser est compatible avec Windows™ ou Linux. Vous choisissez de configurer **Ontrack Eraser** pour l'effacement automatique de multiples supports, ou d'assigner plusieurs niveaux de sécurité à chaque nouvel effacement. Grâce au Configurateur, vous gérez vos procédures d'effacement.

Outils de Reporting – Traçabilité

Chaque effacement génère un « Certificat d'effacement » stocké sur le serveur Ontrack Eraser. **Ontrack Eraser garantit une traçabilité optimale** et enregistre automatiquement l'identité de chaque support effacé : type de support, taille, référence, date d'effacement, etc.

KROLL ONTRACK®

Plus d'info ?

Numéro vert : **0800 10 12 13**

www.ontrack.fr

Votre système d'information,
est-il une forteresse sans faille ?

- Intrusion
- Phishing
- Chevaux de Troie
- Sécurité de la VoIP
- Mobilité
- Continuité d'activité...

Journée spéciale Banques et Assurances !

Journée consacrée à la Sécurité informatique dans le secteur des banques et assurances.

Études de cas, retours d'expériences, cas réels du CLUSIF, EVIDIAN, FNTC, GEMALTO, XMCO

19 novembre 2008

Programme détaillé sur **www.infosecurity.com.fr**

infosecurity FRANCE

Analyses, débats, solutions : exposition et conférences

19-20 novembre 2008

PARIS, PORTE DE VERSAILLES - PAVILLON 5

Demandez votre badge gratuit sur
www.infosecurity.com.fr
Code invitation : GLO

Reed Expositions

En parallèle du salon :

STORAGE EXPO

www.storage-expo.fr

Le web 2.0

A besoin d'une sécurité 3.0

La seconde génération du web est en pleine expansion, elle offre des opportunités exceptionnelles de business. Mais dans la mesure où votre trafic réseau explose, vous êtes plus vulnérable aux attaques des "hackers" professionnels.
Pénétrez dans le monde de la Sécurité Nokia. Notre nouvelle gamme de solutions de sécurité IP offre la puissance et les dernières technologies nécessaires pour sécuriser toutes vos transactions réseau, indépendamment de leur nature.
Etes-vous prêt pour parler sérieusement de sécurité ?

Travaillons ensemble. Travaillons Mieux.

nokiaforbusiness.com

NOKIA

Nokia IP690

Nokia IP1280

Nokia IP2450

Nokia for Business

LA SÉCURITÉ : MISSION CRITIQUE... PAS MISSION IMPOSSIBLE.

Des menaces à foison, des solutions logicielles en surnombre et des fournisseurs toujours plus nombreux.
Pourquoi un élément aussi vital que la sécurité est-il si difficile à gérer ? Ne vous compliquez plus la tâche et adoptez McAfee.
Nous offrons des solutions de sécurisation complètes pour aider les entreprises de toute taille
à contrer plus facilement toutes les menaces qui les guettent. Le tout géré à partir d'une seule console.
Pour découvrir comment nos produits surclassent ceux de nos concurrents, visitez le site **McAfee.com**.

McAfee®

Une sécurité plus complète · Des coûts d'exploitation réduits · Un meilleur respect des réglementations