

Investissez dans la sécurité



Avec la crise financière et la récession économique qui se profile, chacun se demande quelle stratégie adopter en termes d'investissements. Notre recommandation est simple : ne remettez pas en cause vos investissements en matière de sécurité. Les dangers et les risques sont plus importants que jamais, et les conséquences d'une faille de sécurité seront toujours infiniment supérieures au coût de la mise en place des mesures de protection correspondantes.

L'explosion des réseaux unifiés autour d'Internet et la prolifération des points d'accès au Web constituent de vrais défis. Ces informations qui s'échangent sont souvent personnelles, elles véhiculent propriété intellectuelle stratégique et informations sensibles pour l'entreprise : elles doivent être sécurisées. J'insiste : il s'agit là d'un enjeu majeur, pour les Entreprises comme pour les États. Nous avons tous en tête les récentes failles – énormes – rapportées par la presse concernant aussi bien de très grandes entreprises que des administrations de pays très développés. Personne n'est à l'abri d'un accident ou d'une malveillance. Ne coupons pas les investissements en sécurité !

Bull, a toujours beaucoup investi dans la sécurité et beaucoup innové. Quelques exemples :

Notre filiale Evidian, leader européen de la gestion des identités, sécurise l'accès aux données et aux applications et libère l'entreprise de l'extrême complexité du système d'information. Banques, États, opérateurs de télécommunications, organismes de santé, industriels nous font confiance pour sécuriser l'accès à leur système d'information et protéger les travaux confidentiels de leurs équipes de R&D ou les données confidentielles de leurs clients, patients ou citoyens.

Grâce à nos technologies de chiffrement, Bull peut interconnecter des équipes pluridisciplinaires dans le monde entier, faisant de l'entreprise collaborative une réalité. L'exemple le plus éloquent est le plateau virtuel de Dassault Aviation sécurisé par Bull. Utilisé pour le développement de son avion d'affaires Falcon 7X, il a permis de réduire ses coûts et cycle de développement.

Dernière innovation majeure de Bull, terriblement pertinente pour notre monde ouvert : *globull* qui réconcilie sécurité et mobilité. Avec l'accès sans limites à Internet, la mobilité est moteur de compétitivité, mais elle engendre des risques croissants, tant en diversité qu'en intensité. C'est pourquoi Bull a inventé *globull* : un disque dur sécurisé par microprocesseur, totalement inviolable, testé par la défense française. Il permet de se connecter partout dans le monde, sur n'importe quel PC et d'avoir instantanément tout son environnement de travail et toutes ses données... et il tient dans la poche ! Déjà, les personnels diplomatiques de l'Union européenne l'utilisent et l'administration française l'a retenu.

Je profite de cet éditorial pour vous faire part du classement d'*HPCwire*, la plus célèbre revue au monde pour le calcul scientifique intensif, qui nous place dans le Top 5 des entreprises à suivre en 2009. Bull, aux côtés de poids lourds de l'industrie tels qu'Intel et Microsoft est la seule entreprise non américaine de ce classement : un bel hommage aux hommes et aux femmes de Bull pour leur talent inventif et leur esprit d'innovation.

Didier Lamouche,
Président-Directeur Général

SOMMAIRE

- **p.2/Tribune** : Hassan Maad – Vers une sécurité qui libère votre entreprise.
- **p.4/Invité du mois** : Professeur Thomas Lippert, Directeur du Centre de calcul de Jülich, Allemagne.
- **p.5/Temps forts** : HPC, Bull classé parmi les cinq sociétés mondiales à suivre en 2009. Étude Bull-Forrester sur l'Open Source.
- **p.8/Succès** : Caisse des Congés Payés du Bâtiment. Dassault Aviation. Union européenne. Deutsche Bahn. Mulzer.
- **p.12/Parole d'experts** : Le futur de la sécurité. L'utilisateur au cœur de la sécurité.
- **p.15/Solutions** : Bull System Manager. Gouvernance de portefeuille de projets informatiques.
- **p.17/En bref** : Vers une sécurité agile. Evidian dans le cadran Gartner du SSO d'entreprise.
- **p.20/Agenda**

TRIBUNE

Vers une sécurité qui libère votre organisation

Par Hassan Maad, Directeur Général, Bull Evidian.

L'approche sécurité de Bull repose sur une conviction : la sécurité est porteuse de valeur à condition d'être pleinement agile, orientée métier et alignée sur la stratégie de l'entreprise. Loin d'être seulement le prix d'une assurance tous risques, elle peut générer trois types de bénéfices : amélioration de la productivité, gains en flexibilité et différenciation concurrentielle. Le retour sur investissement pour la sécurité est alors possible.

(page 2)

INVITÉ DU MOIS

Calcul intensif : l'Europe au premier plan

Professeur Thomas Lippert, Directeur du centre de calcul de Jülich.

Pourriez-vous nous présenter les principales missions du centre de calcul de Jülich ?

Le centre de calcul de Jülich est l'un des plus grands centres de calcul

dans le monde. Il est dédié aux travaux de recherche conduits par les universités et l'industrie en Allemagne...

(page 4)

SÉCURITÉ

Vers une sécurité qui libère votre organisation

Passez à l'offensive et garantisiez la confiance



Par Hassan Maad, Directeur Général, Bull Evidian.

L'approche sécurité de Bull repose sur une conviction : la sécurité est porteuse de valeur à condition d'être pleinement agile, orientée métier et alignée sur la stratégie de l'entreprise. Loin d'être seulement le prix d'une assurance tous risques, elle peut générer trois types de bénéfices : amélioration de la productivité, gains en flexibilité et différenciation concurrentielle. Le retour sur investissement pour la sécurité est alors possible.

d'une organisation même ou avec son environnement. Les risques sont multiples : vol, perte de données confidentielles, fraude, vandalisme, chantage au déni de service, intelligence économique, etc. Un défi de plus en plus complexe avec l'ouverture vers les partenaires, les clients et les citoyens.

L'actualité nous le rappelle sans cesse. Personne n'est à l'abri d'un accident ou d'une malveillance. Les conséquences peuvent être désastreuses pour les organisations qui en sont victimes, avec des pertes financières qui ne sont pas des moindres. Dès lors, l'organisation se développant dans un écosystème élargi fera face à un impératif paradoxal : conjuguer ouverture et contrôle.

Sécurité : protection ou prison ?

Face à cet enjeu paradoxal, l'effort des entreprises est significatif. Pour les plus préoccupées d'entre elles, de 6 à 9 % des budgets informatiques sont consacrés à la sécurité, avec des équipes et des directions dédiées. Compte tenu des sommes en jeu, la question n'est plus seulement une question d'investissement, mais de mesure de rentabilité.

Aujourd'hui pourtant, force est de reconnaître que le système actuel arrive à ses limites. Car, les protections nécessaires pour un système ouvert et distribué posent un vrai défi aux directions informatiques. À chaque nouvelle menace, une nouvelle solution. À chaque faille un nouveau patch. Le résultat : un mille feuilles coûteux de solutions de sécurité souvent hétéroclites

et mal intégrées, empilées au fil des années, conduisant à de multiples barrières et protections, portant souvent de nouvelles contraintes pour les utilisateurs et faisant obstacle à l'agilité de l'organisation.

Ce défi est accru par l'ubiquité du système d'information et la « consommation » de l'informatique : l'utilisateur utilise de plus en plus ses outils personnels (smartphones, netbooks, Facebook, etc.) dans des contextes variés et pas uniquement au sein de l'entreprise et de sa bulle sécurisée. Submergé de contraintes imposées par une sécurité non adaptée, l'utilisateur n'hésitera plus à contourner les solutions en ouvrant de nouvelles failles, à l'image de l'usage de mini SI se développant sur la toile.

L'urgence dans ce cas est de recentrer la sécurité sur l'utilisateur et de mesurer l'efficacité des solutions par leur capacité à libérer l'utilisateur dans son travail. La protection ne doit pas se transformer en prison.

L'émergence d'un nouveau paradigme

Il est facile d'assimiler la sécurité à l'image de la citadelle ou de la défense permanente contre les attaques et les menaces. Cette vision étroite de la sécurité a conduit pendant longtemps à privilégier les solutions uniquement orientées sur la technologie.

Une approche totalement nouvelle est aujourd'hui nécessaire. Une approche adaptée à la création de valeur, centrée sur les hommes et les processus métiers. Une sécurité non plus seulement défensive, mais agile et proactive dans un monde ouvert.

Dans les années 2000, l'affaire Enron et de multiples appels à la transparence financière et à la protection des données ont conduit à un renforcement majeur des contraintes réglementaires. Ces contraintes, traduites par différents textes (SOX, Bâle 2, Solvency 2, HIPAA, LCEN, etc.), ont toutes intégré des règles strictes en matière de sécurité informatique. Ceci a marqué l'entrée de la sécurité dans le domaine du contrôle interne et des exigences d'audit. La crise financière actuelle et les divers scandales symptômes d'un pilotage déficient du risque, devraient voir s'accroître encore fortement ces réglementations dans les années à venir.

Un défi paradoxal : conjuguer ouverture et sécurité

L'alignement des systèmes d'information sur la stratégie de l'organisation fait aujourd'hui ressortir la sécurité comme un enjeu majeur. Les contraintes imposées par les différents textes relatifs aux métiers reflètent son importance vitale pour les années à venir. Car, avec la dématérialisation croissante, jamais les échanges n'ont été aussi critiques au sein

(SUITE)**Vers la sécurité d'un monde ouvert**

Sécurité défensive	Sécurité agile et proactive
Citadelle	Immunité intégrée
Orientée technologie	Alignée sur les processus métiers
Centrée sur l'informatique	Plaçant l'utilisateur au centre de la sécurité
Locale	Ubiquiste et mobile
En silos	Intégrée

Cette sécurité de nouvelle génération comporte trois caractéristiques majeures :

- **Agilité.** Plus que jamais, l'agilité de l'entreprise est un facteur essentiel de la réussite de ses missions. Poussée par des changements économiques à grande vitesse, toute organisation agit dans un espace de confiance dépassant ses frontières. L'utilisateur est dans ce contexte partout, dans l'enceinte de son organisation, chez le client, chez le partenaire, sur la route, accédant à son bureau à distance pendant ses vacances, etc. L'utilisateur est aussi le partenaire, le client, le citoyen. Son accès à l'information se fait à tout moment, de n'importe quel point et depuis différents moyens de communication. La sécurité doit savoir le suivre partout et suivre avec agilité la reconfiguration permanente de ses relations dans les écosystèmes métiers.
- **Orientation métier,** car basée sur l'analyse des risques et des opportunités métiers. Les contraintes et les priorités d'un industriel diffèrent fondamentalement de ceux d'un opérateur télécom, d'une banque ou d'un service public. Dans ce domaine, il n'y a pas de solution universelle : chaque stratégie de sécurité doit s'adapter aux enjeux et processus métiers spécifiques. Mieux, elle doit les soutenir et les améliorer. En ce sens, au-delà de la technologie, il est essentiel de se rappeler que la sécurité est avant tout un projet organisationnel.

- **Centrage sur l'utilisateur.** La sécurité n'est pas un produit, mais un processus. Trop compliquée à utiliser, administrer ou auditer, elle sera contournée. Nous le constatons, l'utilisateur est au cœur de la stratégie de sécurité, il contribue d'une manière active au renforcement de la sécurité du système. Un utilisateur qui adhère à un processus de sécurisation est un véritable gage de réussite. Il est donc important que l'ergonomie des outils soit prise en compte dès le début. Les exigences de sécurité induisant des tâches répétitives et reposant uniquement sur le facteur humain sont un danger. Les outils de gestion des accès et de SSO et l'essor qu'ils rencontrent, en sont la meilleure illustration.

Vers une sécurité créatrice de valeur

La sécurité se retrouve ainsi à la croisée de trois chemins, celui des technologies de l'information, de la politique métier de l'entreprise et des exigences utilisateurs. Elle ne pourra offrir le service attendu par tous que si elle réussit le pari de la réconciliation de la technologie avec le métier et l'usage qui en est fait.

Pionnier de la sécurité, Bull a engagé une telle approche depuis plusieurs années. En tant que concepteur de solutions de sécurité à haute valeur ajoutée dans des technologies clés, avec une approche conçue pour aligner la sécurité avec les enjeux métiers et humains. Citons notamment la gestion des identités et des

accès (avec Bull Evidian), la mobilité (avec globull™), le chiffrement (avec Bull TrustWay), la gestion des transactions (avec Bull Crypt2Pay et Bull MetaPKI) et la sécurité des données (avec Bull StoreWay). Une expertise soulignée par les analystes qui ont régulièrement distingué l'offre du Groupe Bull par de nombreux Trophées et notamment celle d'Evidian, reconnu comme le leader européen en gestion des identités et des accès.

En tant que conseil, intégrateur et infogérant, accompagnant les grandes organisations dans la mise en place de solutions de sécurité « sur mesure », adaptées à des enjeux et processus métiers vitaux. Des grandes réalisations comme la sécurité de TéléTVA ou TéléIR, celle de Chorus, celle du plateau virtuel de conception du Falcon 7X de Dassault Aviation ou l'équipement monétique de 95 % des banques françaises en témoignent.

L'approche sécurité de Bull repose sur cette conviction : la sécurité est porteuse de valeur à condition d'être pleinement agile, orientée métier et intégrée dans la stratégie d'entreprise. Loin d'être seulement un centre de coûts, elle peut alors générer trois types de bénéfices : amélioration de la productivité, gains en flexibilité, différenciation concurrentielle. Loin d'être un frein, elle devient alors un levier de développement métier.

HPC

Calcul intensif : l'Europe au premier plan

Professeur Thomas Lippert, Directeur du centre de calcul de Jülich.



Pourriez-vous nous présenter les principales missions du centre de calcul de Jülich ?

Le centre de calcul de Jülich est l'un des plus grands centres de calcul dans le monde. Il est dédié aux travaux de recherche conduits par les universités et l'industrie en Allemagne. Il est totalement intégré dans une structure très importante, celle du Forschungszentrum Jülich (i.e le centre de recherche Jülich), ce qui signifie pour Jülich travailler sur des domaines dont les enjeux sont immenses : l'énergie, le vieillissement de la population – importante problématique de la recherche aujourd'hui – ou les sciences des matériaux. Tous ces domaines tirent partie de la simulation numérique ou en dépendent très largement. Sans la simulation numérique, les progrès seraient beaucoup moins importants. Pour la plus grande partie de domaines, nous fournissons des heures de calcul à l'Allemagne – et à l'Europe – avec des supercalculateurs parmi les plus puissants du monde.

Pouvez-vous nous dire quelques mots sur le projet JuRoPA ?

JuRoPA signifie « Jülich Research on Petaflops Architectures ». JuRoPA est un supercalculateur de plus de 200 Téraflopps qui est vu comme un seul système dédié au traitement d'un seul problème, tels que ceux dont nous avons parlé. Les systèmes ou les problèmes sont transcrits en codes applicatifs qui doivent tourner très longtemps sur de multiples combinaisons. C'est pourquoi il est impératif pour nous d'avoir des systèmes très performants qui soient capable de monter en puissance facilement ; ce sont des systèmes qui peuvent intégrer un très grand nombre de processeurs – dans notre cas jusqu'à 16 000 cœurs de calcul, soit 2 000 nœuds de biprocesseurs ayant chacun 4 cœurs – qui travaillent de façon cohérente, avec un réseau d'interconnexion très puissant, pour résoudre un seul et même problème. C'est le défi auquel nous devons faire face, parce que ce système sera, si cela réussit et je suis sûr que allons réussir, le plus grand système véritablement évolutif de cette nature. À noter qu'il est basé sur des composants « disponibles sur étagères », que Bull et nous-mêmes avons choisi ensemble : les meilleurs composants du marché que nous devons intégrer pour réaliser un système qui travaille en cohérence sur les problèmes évoqués.

Pour moi, en tant que physicien, la complexité est la caractéristique la plus frappante des applications et elle est commune aux grands défis dont nous parlions, comme la recherche pour l'énergie, la construction de nouvelles centrales électriques ou la construction d'ITER*. Et la plupart de ces grands défis dépendent de la recherche des sciences de la matière. Tout ceci est d'une extrême complexité. Nous devons composer avec un nombre immense de combinaisons, de

nombreuses interactions très compliquées, de nombreuses relations très compliquées et nous devons procéder à très nombreuses étapes d'optimisation. Tout ceci contribue à la complexité ; or nous devons maîtriser cette complexité. C'est pourquoi, nous avons besoin de systèmes très complexes pour faire face à la complexité. Aussi avons-nous des supercalculateurs très complexes, des supercalculateurs qui intègrent de nombreux composants devant interagir, être pilotés et administrés, etc. Avec ces supercalculateurs hyper complexes, nous maîtrisons la complexité.

Cette complexité est-elle la raison de votre choix pour Bull ?

Oui, nous avons choisi Bull parce que nous pensons que Bull peut être un véritable partenaire. Nous ne sommes pas un simple client de Bull, nous sommes partenaires. Par ses succès, Bull a prouvé qu'il était capable de réaliser de telles machines. Bull sait maîtriser les grands systèmes ; il en a les compétences. Et puis il y a cette proximité entre la France et l'Allemagne et également une volonté politique d'y réaliser quelque chose de grand. J'ai le sentiment que Bull va dans la bonne direction pour développer des choses intéressantes. C'est ce que je veux, le développement de la technologie en Europe.

Je serais très heureux si ensemble, en Europe, sous le leadership de Bull, avec les contributions de nombreux autres, nous pouvions construire des systèmes multi-Pétafloppiques d'ici à 2012. C'est l'objectif que nous devrions suivre et être les premiers à le réaliser. Naturellement, c'est ultra complexe et difficile. C'est un vrai challenge ! Mais je suis sûr que nous avons de bonnes chances de réussir.

* ITER : International Thermonuclear Experimental Reactor.

DISTINCTION

Calcul haute performance : Bull est classé parmi les cinq sociétés mondiales à suivre en 2009

Lors du salon Supercomputing 2008 qui vient de se tenir à Austin, *HPCwire*, revue d'une très grande notoriété dans le monde du calcul haute performance (HPC), a retenu Bull parmi les cinq premières entreprises à suivre en 2009.

Par ce classement, Bull figure aux côtés des plus grands noms parmi lesquels Intel et Microsoft. Bull est par ailleurs la seule entreprise non américaine à être nommée.

Le classement exprime le vote d'un panel de personnalités du monde du HPC et le choix des rédacteurs de *HPCwire* issus du monde de l'industrie.

Reconnaissance prestigieuse au sein de la communauté HPC, ce prix est une grande fierté pour Bull ainsi que pour l'industrie française et européenne, quasi inexistante dans le domaine du calcul haute performance il y a quelques années, au premier rang mondial aujourd'hui, aux côtés des plus grands.

Ce prix témoigne de la place exceptionnelle que tient Bull dans le domaine du calcul haute performance, avec plus de cent clients, dans quinze pays et sur trois continents, et fournisseur de supercalculateurs parmi les plus puissants du monde, comme ceux du centre de recherche Jülich en Allemagne, de l'Université de Cardiff au Royaume-Uni ou du GENCI en France.

Repousser les limites de la recherche en Europe

Simulation numérique

Bull est devenu un acteur incontournable de la simulation numérique haute performance avec une croissance exceptionnelle, de nombreux records mondiaux et des contrats significatifs avec les plus grands centres de recherche européens.

Bull
Architect of an Open World

ENQUÊTE

Une étude montre que l'Open Source ouvre la voie à la nouvelle génération des systèmes d'information d'entreprise

- L'Open Source devient la dorsale cachée de l'industrie des logiciels ;
- L'Open Source permet de réduire les coûts et constitue un véritable levier d'innovation pour le long terme ;
- L'Open Source révolutionne les méthodes de travail des départements informatiques.

En ouverture de l'Open World Forum, événement international majeur de l'Open Source, Bull a publié les résultats d'une enquête innovante menée pour son compte par le cabinet Forrester Consulting en octobre 2008. Conduite auprès de 132 dirigeants et directeurs informatiques de grandes entreprises européennes déjà utilisatrices de l'Open Source, cette étude évalue les nouveaux modèles d'adoption de l'Open Source par les entreprises. Forrester a ainsi pu établir que ces entreprises abordent le logiciel sous un angle fondamentalement nouveau.

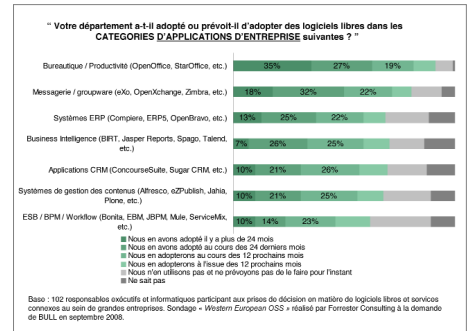
« L'étude publiée aujourd'hui confirme la pertinence de notre vision » a déclaré Jean-Pierre Barbéris, Directeur Général de Bull Services et Solutions. « En tant qu'Architecte d'un monde ouvert™, nous avons été parmi les premiers à contribuer aux communautés et à utiliser les Logiciels libres au cœur de nos solutions, des supercalculateurs à notre nouvelle plateforme de sécurité mobile, globull™. Aujourd'hui, avec Libre Energie™ et Virtual Shore™, nous sommes encore parmi les pionniers des services Open Source. Seul acteur informatique européen présent sur toute la chaîne de valeur des technologies de l'information, nous souhaitons être à l'avant-garde pour aider les entreprises à s'appuyer sur les Logiciels libres pour bâtir leurs systèmes d'information de demain ».

L'Open Source devient la dorsale cachée de l'industrie des logiciels

Bull souhaitait aller plus loin que les nombreux livres blancs et études déjà réalisés sur le sujet et déterminer l'impact global de l'Open Source sur les systèmes d'information des grandes entreprises. L'étude s'est donc intéressée exclusivement aux entreprises qui utilisent déjà l'Open Source, ce qui représente aujourd'hui entre 15 % et 24 % environ des entreprises nord-américaines et

européennes. L'étude démontre que les composants Open Source sont aujourd'hui présents partout. Les utilisateurs savent pertinemment que les éditeurs sont en train d'introduire massivement l'Open Source dans leurs solutions, et donc dans toutes les entreprises, transformant les systèmes d'information en un savant mélange de logiciels libres et de logiciels sous licence. 22 % des entreprises interrogées préfèrent même un environnement totalement Open Source.

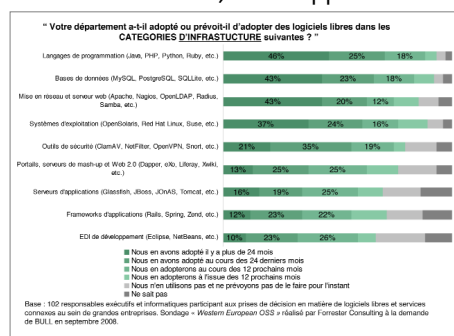
Si, il y a quelques années, l'Open Source était essentiellement utilisé dans le cadre de projets expérimentaux ou de prototypes, ses composants sont maintenant au cœur des applications critiques, des services et des produits stratégiques de 45% des entreprises interrogées. Autre conclusion de l'étude, l'Open Source est désormais présent dans les couches applicatives métiers, et non plus seulement au niveau des infrastructures et des intergiciels. L'adoption des outils de productivité et des applicatifs métiers Open Source est en forte croissance. Les entreprises sont notamment de plus en plus nombreuses à avoir, au cours des 24 derniers mois, adopté l'Open Source pour les applications de CRM (31 %), de décisionnel (33 %), ainsi que pour les progiciels de gestion (38 %). Étant donnée la multiplication des offres d'applications d'entreprise Open Source, on peut dire que cette adoption, certes forte, reste encore en deçà des opportunités*.



Les entreprises utilisatrices de l'Open Source sont satisfaites de leur choix. En matière de qualité et de robustesse, l'Open Source répond aux attentes de 92 % d'entre elles, voire les dépasse. Une écrasante majorité d'utilisateurs, 70 %, aura de plus en plus recours à l'Open Source.

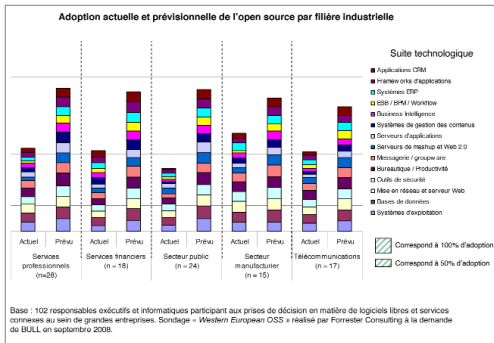
L'Open Source permet non seulement de réduire les coûts, il offre aussi et surtout un levier d'innovation pour le long terme. L'étude démontre l'importance de l'Open Source en matière de compétitivité et d'innovation. En période de crise économique, la motivation première pour l'adoption de l'Open Source est la réduction des coûts (56 %). Mais ce n'est pas la seule, et de loin. L'indépendance vis-à-vis des éditeurs rentre en ligne de compte après de 45 % des personnes interrogées. Viennent ensuite d'autres motivations telles que la flexibilité et l'innovation.

Quelle que soit l'approche qu'ils adopteront, les dirigeants d'entreprise et les décideurs informatiques découvriront avec l'expérience que les économies de coûts de licence, les faibles barrières à l'entrée et l'évolution rapide des projets ne sont pas les seuls avantages apportés par l'adoption de logiciels libres. Les apports du modèle Open Source vont bien au-delà en apportant plus d'innovation, plus d'adaptation aux évolutions technologiques. Parce qu'il est de plus en plus au cœur de grands projets



(SUITE)

d'infrastructure, l'Open Source permet de saisir toutes les opportunités. C'est en conjuguant économies et rapidité de mise sur le marché que l'Open Source devient un atout redoutable aux mains des entreprises qui sauront s'en servir de manière stratégique pour maximiser l'efficacité de leurs investissements logiciels.



L'adoption par filière n'est pas uniforme. Il est intéressant de noter que le secteur qui communique le plus sur l'Open Source, à savoir le secteur public, n'est pas le plus avancé, même si un pays comme la France est très en avance sur le sujet. Le secteur public est néanmoins celui qui formule les plans les plus ambitieux pour l'avenir. L'industrie a actuellement le plus d'expérience de l'Open Source à tous les niveaux de la suite technologique. Embarqué dans des produits tels que les appareils électroniques, les voitures, les trains ou les avions, l'Open Source a déjà fait ses preuves. Le taux d'adoption est également élevé dans les services (médias, transports, négoce, etc.) en raison des investissements massifs dans les infrastructures Web pour les services et le e-commerce, qui dépendent fortement de composants Open Source. Sans surprise, le secteur des télécommunications est à la pointe de l'usage des systèmes Open Source, confronté à la nécessité de fournir à des millions d'utilisateurs des services à bas coût. Réputée comme plus conservatrice, la finance n'est cependant pas en reste pour l'utilisation de l'Open Source, plus particulièrement dans les environnements de développement, mais également les applications d'entreprise.

L'émergence d'un état d'esprit Open Source au sein des grandes entreprises révolutionne les départements informatiques
L'étude montre que les principes de l'Open Source sont de plus en plus

transposés aux meilleures pratiques d'entreprise. Le libre partage du code source (46 %) ou bien la manière de former des communautés de contributeurs et de consommateurs (42 %), qui sont caractéristiques des projets d'Open Source, sont désormais transposés au microcosme de l'entreprise. La création de suites logicielles ouvertes dans l'entreprise et des services réutilisables va vers une sorte de communauté Open Source d'entreprise.

Pour les décideurs, négliger l'Open Source est à terme impossible. Utilisé par les développeurs, intégré aux piles logicielles, l'Open Source leur laisse le choix entre observer une intrusion irréversible ou opter pour une stratégie proactive d'adoption.

Une inévitable utilisation tactique de l'Open Source

Les entreprises dépourvues d'une politique Open Source ne pourront être que surprises de constater sa pénétration croissante dans leurs propres applications. Cette approche passive face à l'adoption de l'Open Source aboutit généralement à un ensemble de réactions prévisibles : refus de croire que l'Open Source est déjà dans la place, colère face à une perte de contrôle inattendue, marchandage pour tenter de restaurer les processus existants, passage du point de non-retour, et enfin acceptation des logiciels libres.

L'alternative : les dix meilleurs pratiques pour une adoption réussie

L'étude fait ressortir la nécessité pour les entreprises de mettre en œuvre une approche volontairement stratégique de l'Open Source, s'appuyant sur les préconisations suivantes établies par des professionnels du logiciel auprès des entreprises déjà utilisatrices :

- 1 Choisir le bon composant au bon niveau de l'infrastructure IT.
- 2 Bien calculer le coût total de possession.
- 3 Définir une stratégie de support pour les systèmes Open Source.
- 4 Améliorer les capacités de gestion du cycle de vie des applications.
- 5 Scanner les projets pour identifier les risques liés aux licences.
- 6 Évaluer les options Open Source avant d'envisager une solution commerciale.

- 7 Intégrer et industrialiser la gestion des déploiements Open Source.
- 8 Adopter des pratiques de développement agiles en tandem avec l'Open Source.
- 9 Définir une politique Open Source cohérente au sein de l'entreprise.
- 10 Participer à des communautés Open Source phares.

Une gouvernance informatique stricte est nécessaire à cet égard. À titre d'exemple, 60 % des entreprises interrogées l'ont pleinement compris et ont déjà déployé des bases de code et de piles logicielles centralisées pour distribuer les versions Open Source approuvées dans l'entreprise.

La sécurité est le défi N°1 identifié par Forrester sur le logiciel libre, dans cette étude comme dans d'autres. Vient ensuite la disponibilité de services, de prestations de support et de compétences autour des différentes offres. Les intégrateurs de systèmes et les centres de compétence dont ils disposent, apportent les réponses à ces problématiques.

Ces conditions réunies vont générer une adoption professionnelle de l'Open Source aussi simple que celle des logiciels propriétaires. Ce qui importe est le coût de possession (TCO). 48% des entreprises interrogées soulignent aussi l'importance des références clients. Ceci est un signe indiscutable que l'adoption de l'Open Source se généralise.

L'étude est téléchargeable gratuitement sur: <http://www.bull.fr>

* L'étude s'est focalisée exclusivement sur les entreprises qui utilisent déjà sensiblement l'Open Source. Fin 2007, l'étude intitulée « Forrester's Enterprise And SMB Software Survey, North America And Europe, Q3 2007 » a révélé que la proportion des entreprises qui s'appuient ainsi sensiblement sur l'Open Source est de 24 % en France, 21 % en Allemagne, 17 % aux USA, 17 % au Canada et 15 % en UK. Ceci signifie que lorsque cette étude évoque un taux d'adoption de 38 % pour les systèmes ERP libres par exemple, cela signifie que 38 % * 24 % = 9,1 % des entreprises en France sont concernées, ce qui est déjà un chiffre important.

ASSURANCE

La CCPB RP choisit Bull pour le pilotage de la refonte de son système d'information

Pour le Projet d'Entreprise CAP 2011 de la CCPB RP, Bull fournit des prestations de conseil et d'assistance à maîtrise d'ouvrage sur trois ans

La CCPB RP a choisi Bull comme partenaire pour l'accompagner tout au long de son projet de refonte de son système d'information basé sur SAP. Ce projet stratégique doit permettre à la Caisse d'atteindre d'ici 2011 trois objectifs principaux : l'amélioration de la qualité des prestations et du service rendu à ses clients, l'optimisation des frais de gestion, ainsi que la valorisation des ressources internes en enrichissant les tâches.

La mission d'Assistance à Maîtrise d'Ouvrage (AMOA) confiée à Bull prend en compte l'ensemble des composantes métier, fonctionnelles, techniques et humaines du projet, depuis la définition des enjeux jusqu'au projet de transformation :

- préconisation et identification des besoins d'évolution ;
- recherche et qualification de la solution ;
- définition des postes et profils métier ;
- accompagnement au changement ;
- conseil sur l'architecture et la politique de sécurité du SI ;
- assistance au pilotage des chantiers.

La CCPB RP s'appuie en particulier sur le savoir-faire de Bull en méthodologie de conseil et de pilotage de projet, ainsi que sur ses expertises SAP, architecture technique et applicative, sécurité et accompagnement du changement.

« Nous avons été particulièrement vigilants pour assurer un accompagnement sans faille à ce changement d'ampleur » souligne Pierre-Yves Tanguy, Directeur Général de la CCPB RP. « CAP 2011 étant un projet d'entreprise qui doit nous permettre d'atteindre nos objectifs stratégiques, nous avons décidé de nous associer les compétences qui en garantissent le succès. La prestation de conseil conduite par Bull nous permet de répondre à cette attente ».

À terme plus de 26 000 sociétés adhérentes et 165 000 prestataires salariés vont bénéficier des évolutions apportées par CAP 2011, notamment grâce à la mise en place d'une Gestion de la Relation Client, d'une « vue à 360° des

clients », d'un portail Internet temps réel pour une interaction constante avec le système d'information.

Un projet novateur qui s'inscrit dans une forte démarche participative

Le nouveau système d'information reposera sur une suite complète SAP incluant ECC, HCM, CRM, BW et un nouveau module en France, TRM (Tax and Revenue Management). Le progiciel intégré deviendra ainsi le référentiel unique pour l'ensemble des fonctions de l'entreprise.

Pour maîtriser les nouveaux modes de fonctionnement qui découleront du nouveau système, la CCPB RP adopte une démarche participative à tous les niveaux de l'entreprise. Bull a ainsi contribué à la mise en place d'un cadre méthodologique comprenant des ateliers d'expression du besoin qui ont impliqué la moitié des collaborateurs de l'entreprise. Bull a également défini un accompagnement au changement complet incluant la communication et l'évolution des compétences et des nouvelles fonctions.

Le projet sera pleinement opérationnel en octobre 2010.

▼ Accompagnement au changement

Zoom sur le Plan de communication du Projet CAP 2011 réalisé par Bull Formation



Le plan de communication déployé au sein de la Caisse a pour objectif de faire connaître le projet et d'informer sur son déroulement afin de rassurer et de lever toute appréhension éventuelle.

Une réelle identité a été donnée à ce projet pour qu'il soit reconnu et repéré sur tout document le concernant. Un logo associé à un nom a été créé. Ainsi parle-t-on à présent du projet CAP 2011.

La régularité de l'information est assurée par un support écrit ; le journal du projet, baptisé « ENSEMBLE ».

De périodicité trimestrielle, « ENSEMBLE » informe sur tout événement concernant CAP 2011. Il est le journal de tous les collaborateurs de la Caisse.

Le plan de communication prend également appui sur une communication de proximité relayée par l'encadrement intermédiaire afin de développer l'interactivité permettant de chasser toute rumeur éventuelle et d'être le plus concret possible. Le rôle de l'encadrement intermédiaire est de renforcer le dialogue et de réguler les échanges en se positionnant au carrefour de l'information, l'information descendante et l'information ascendante, et en devenant Ambassadeur du Projet CAP 2011.

Chaque Ambassadeur CAP 2011 anime régulièrement des ateliers d'information / mobilisation auprès de son unité. Pour cela il reçoit un kit de communication incluant des outils de présentation prêts à l'emploi qu'il s'approprie au cours d'un atelier dédié à cet effet.

L'enjeu principal est d'obtenir l'adhésion de tout le personnel nécessaire à la réussite globale du Projet CAP 2011 sachant que chacun ne pourra accepter ce changement que s'il est convaincu de la nécessité de le mettre en œuvre et du bénéfice apporté.

PROJETS DE SÉCURITÉ

Dassault Aviation : une première mondiale dans la conception industrielle sécurisée

L'avion d'affaires de Dassault Aviation – le Falcon 7X – a été conçu autour d'un plateau virtuel sécurisé. Une vingtaine d'entreprises partenaires réparties dans six pays d'Europe de l'Ouest et d'Amérique du Nord, 1 000 ingénieurs, ont travaillé ensemble et à distance à la conception détaillée de l'avion.



L'architecte industriel Dassault Aviation bénéficiait d'une visibilité totale et permanente sur les données : une disponibilité et un partage des données

qui ont permis de développer le Falcon 7X dans des délais et avec un niveau de qualité et des gains de productivité records.

« Ce plateau ne pouvait exister qu'en s'appuyant sur une infrastructure IT de confiance, déclare Jean-Paul Weber, Chef du département SSI de Dassault Aviation. L'offre de Bull a prouvé son efficacité notamment lors des tests d'intrusion intensifs ».

Le système repose sur un double niveau de sécurité : authentification forte des utilisateurs et sécurisation du réseau VPN, une solution qui garantit une sécurité optimale de l'architecture.

L'Union européenne adopte globull™

Le Secrétariat général du Conseil de l'Union européenne (SGC UE) a fait l'acquisition de globull™, le bureau mobile crypté conçu par Bull en vue d'équiper ses personnels diplomatiques.

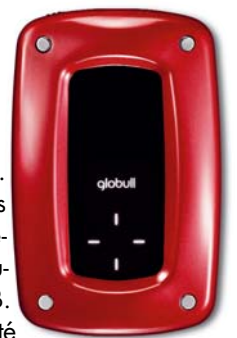
Les quelques 3 500 fonctionnaires du SGC UE sont en effet amenés à énormément se déplacer et à emporter avec eux des documents très confidentiels. Depuis plusieurs années, dans le cadre de son projet NOMAD, le SGC UE cherchait une solution fiable et pratique conjuguant mobilité et haute sécurité. Avec ses technologies issues du monde de la défense, son ergonomie soignée et sa discrétion, globull™ a

aussitôt séduit les experts INFOSEC du Secrétariat Général. Après une rigoureuse phase de test, de configuration spécifique et d'expérimentation, globull™ a été officiellement présenté en avril 2008 aux 27 États membres.

globull™, une révolution dans la mobilité
Ce mini coffre-fort chiffré de 120 grammes protège des intrusions, des virus et logiciels espions par ses technologies

de niveau « défense ». Il lève ainsi toutes les vulnérabilités inhérentes aux PC sécurisés et aux clés USB. L'utilisateur en mobilité peut conserver avec lui le cœur de son ordinateur en toute confiance.

Plus d'informations : <http://www.myglobull.fr>



Deutsche Bahn contrôle 1 million d'accès utilisateurs pour aligner sécurité et processus métiers



Deutsche Bahn, l'un des principaux opérateurs de transport en Europe, a

décidé de mettre en place un système de gestion des identités pour maîtriser l'accès de ses 60 000 utilisateurs à ses 800 applications métiers. Après une étude exhaustive des solutions du marché, l'opérateur a choisi de s'appuyer sur l'offre de Bull Evidian, leader européen de la gestion des identités et des accès. Son atout : une approche centrée sur les

utilisateurs, analysant et contrôlant les accès au million de comptes utilisateurs de Deutsche Bahn selon ses processus métiers. L'opérateur pourra ainsi renforcer ses procédures de contrôle interne et auditer en permanence que seuls les utilisateurs autorisés accèdent à ses applications stratégiques. Un nouveau gage d'excellence pour Deutsche Bahn.

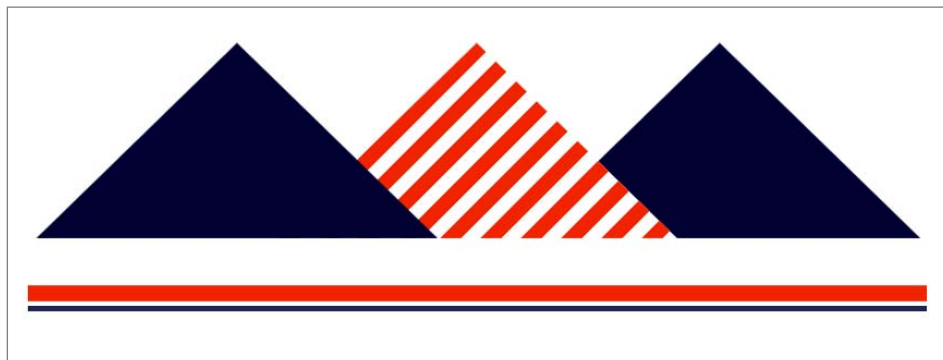
BTP

Mulzer préfère Bull Escala pour supporter ses applications d'entreprise

Mulzer Crushed Stone vient de commander un nouveau système Escala équipé de disques EMC en réseau SAN, de sous-systèmes de sauvegarde, de logiciels accompagné des services d'installation et de support. Grâce à cette nouvelle infrastructure, Mulzer bénéficiera d'une sensible augmentation de puissance permise par les nouveaux processeurs POWER6™ disponibles sur les serveurs Escala de Bull. Mulzer est client de Bull depuis 1976, date d'achat de leur premier système.

De par son activité, Mulzer Crushed Stone situé à Tell City dans Indiana, concerne des millions de personnes tous les jours. Entreprise familiale depuis 60 ans, Mulzer fournit en effet du calcaire, du sable et des graviers pour les pistes de l'aéroport international, les routes, les autoroutes inter États et les barrages des fournisseurs d'énergie. Tous les jours, Mulzer livre des milliers de tonnes de pierres concassées pour tous les projets de construction de son territoire de prédilection, qui vont de simples allées jusqu'aux plus larges autoroutes. Mulzer est par ailleurs le grand fournisseur de matériaux de construction de toute la vallée de l'Ohio.

Mulzer compte sur les solutions d'infrastructure de Bull pour supporter son application ERP MINCOM, qui gère tous ses actifs et tous les équipements utilisés dans ses activités quotidiennes. Cette importante application permet aussi à Mulzer de planifier les activités de maintenance sur tous ses équipements



qu'elles soient ou non prévues ; elle est accessible via le Web. Basés sur la technologie POWER6™, les nouveaux systèmes Escala équipés des dispositifs de virtualisation apportent plus de performance, augmentent le taux d'utilisation des systèmes et leur efficacité, tout en réduisant le coût total de possession et en étant plus faciles à administrer.

Mulzer Crushed Stone a été fondée sur une vraie philosophie qui guide encore la compagnie aujourd'hui : Donner à chaque client l'attention qu'il est en droit

d'attendre d'une entreprise familiale, le supporter avec les moyens d'une grande entreprise et de telle façon que chaque emploi gagne en qualité.

Mulzer est également convaincu que la protection des ressources naturelles est de la plus haute importance. C'est pourquoi l'entreprise travaille activement avec l'Association des conglomérats de minéraux d'Indiana pour développer des standards stricts de recyclage à l'échelle de l'État, tout en poursuivant un programme de protection environnementale.

SÉCURITÉ

Le futur de la sécurité

Par **Lionel Mourer**, Directeur du Pôle Conseil en Sécurité, Bull.

Mobilité, « cloud computing », m-paiement, réseaux sociaux et mondes virtuels, etc. : quelles nouvelles menaces se profilent ?
Bref tour d'horizon de problématiques qui prendront demain une importance croissante.



Cinq défis pour la sécurité de demain
Les menaces qui pèsent sur le système d'information évoluent sans cesse... Nul ne sait vraiment où les pirates porteront leurs attaques, mais les dernières études nous éclairent sur certaines des prochaines menaces. Faisons un rapide état des lieux sur quelques unes d'entre elles :

- D'ici fin 2008, l'humanité devrait compter 4 milliards de téléphones mobiles ! Cela laisse rêveur et forcément cela finira bien par intéresser quelques « méchants ». Toutefois, même si les attaques permettant des dénis de service existent déjà « en laboratoire », il est peu probable qu'elles se répandent largement. Le hacker « moderne » cherche plus l'appât du gain que la célébrité ! Or les banques commencent à proposer des services – tels que des paiements, des validations de transactions, etc. – via les réseaux mobiles, et le téléphone sert alors de terminal avec son O/S, ses applications et ses propres failles... Reste que le marché du paiement par mobile (appelé « m-paiement »), en est encore aux balbutiements, mais devrait être promis à un grand avenir...
- La mobilité n'a pas fini de s'étendre ! Les parts de marché des ordinateurs portables ne cessent de progresser, sans compter les smartphones et autres mobiles intelligents. De fait, le nomade est de plus en plus connecté et il devient une cible privilégiée : prendre la main sur un poste « nomade », c'est accéder à l'ensemble du système d'information que lui confère ses privilèges... Or, généralement, les utilisateurs nomades sont ceux qui bénéficient des accès les plus élargis au sein de l'entreprise. Alors, ici aussi, les pirates – des mafias, mais aussi quelquefois des concurrents, voire des gouvernements... – cherchent à obtenir les « ouvertures » vers les informations vitales (critiques et/ou confidentielles) de l'entreprise.
- « Cloud Computing, SAAS, Software+ Services », etc. après la révolution de l'informatique distribuée, le rêve d'une informatique re-centralisée revient en force, délivrée à la demande, aussi simplement que l'eau ou l'électricité. C'est une avancée majeure. Mais les centrales informatiques de demain ne seront-elles pas une cible idéale pour les hackers ou les terroristes ? En 2008, un simple accident électrique a coupé pendant des heures l'accès de milliers d'entreprises à leurs données métiers stockées sur Amazon EC2. On imagine l'impact économique potentiel d'une attaque concertée et de grande ampleur...
- Pour finir, parlons des menaces « exotiques », qui pourraient toutefois, à terme, poser de réels problèmes d'organisation, voire de société comme par exemple, le truquage des résultats des machines à voter ou la modification du trafic info pour les GPS... Concernant ce dernier point, imaginez une flotte de véhicule, gérée par GPS, avec des chauffeurs persuadés d'être « sur le bon chemin » mais en fait « dérouter » pour un véritable vol, non virtuel celui-là... ; ou encore un pirate qui enverrait un faux signal GPS vers un avion en plein vol, afin qu'une position et une indication de temps erronées s'affichent. Cela pourrait permettre de jeter des avions en vol les uns contre les autres ! Les techniques existent déjà, même si elles restent encore peu accessibles à tout un chacun.

L'imagination humaine est sans limite – pour le meilleur et pour le pire – et celle des pirates aussi... C'est pourquoi il faut continuer, plus que jamais à identifier ses risques, mettre en œuvre un niveau de protection adéquat selon ses processus métiers et veiller, encore veiller, toujours veiller...

Aujourd'hui, Bull, au travers de son offre globale de services en sécurité, peut vous accompagner dans vos projets d'évolution de votre système d'information, et décliner les meilleures pratiques pour gagner en efficacité et aligner votre SI sur vos processus métiers.

SÉCURITÉ

L'utilisateur : au cœur de la sécurité du futur

Avec la révolution de la mobilité, le monde change de paradigme, passant d'une sécurité centrée sur l'informatique à une sécurité centrée sur l'information.

Par Emmanuel Forgues, Chef de produit globull™, Bull.



Alors qu'il y a seulement quelques années nous acceptions des délais de réponses de quelques jours par courriers ou de plusieurs heures avec le fax) il est désormais devenu insupportable d'attendre une heure pour obtenir une réponse. La technologie actuelle est maintenant suffisante pour une prise de décision plus rapide et plus efficace. Nous passons d'un mode de travail collaboratif de proximité à un mode d'échange de données dans un système qui se déplace avec son utilisateur. Plutôt que de se retrouver dans un seul et même endroit pour travailler, les utilisateurs se trouvent maintenant au centre même d'une bulle d'information qui se déplace avec les moyens nécessaires pour s'interconnecter. Les DSI (Directeurs des Systèmes d'Information) doivent désormais être en mesure de sécuriser les environnements de travail des utilisateurs nomades où qu'ils travaillent.

L'accès aux technologies de communication (voix et données) et la banalisation de l'utilisation de l'ordinateur

Depuis ces dernières années, nous constatons un changement radical dans la manière de communiquer. Les nouvelles technologies transforment le comportement des utilisateurs, qui se retrouvent dans un tourbillon mêlant leur vie professionnelle à leur vie privée. Ainsi, une compagnie aérienne qui demande à ses clients d'imprimer chez eux leurs propres billets résout ingénieusement la gestion de ses enregistrements. Avec 16.7 millions d'abonnés à Internet haut débit en France fin juin 2008 (Source ARCEP), les français peuvent aujourd'hui aisément franchir le pas vers le télétravail. Comment la transition se passe-t-elle pour les utilisateurs ? Quid de la prise en charge de ces nouveaux travailleurs par les directions informatiques ? N'est-ce pas une chance formidable de repenser l'environnement de travail pour se concentrer sur l'essentiel : la donnée et son environnement ?

à la maison pousse l'utilisateur à travailler occasionnellement de chez lui en se connectant au système d'information de son entreprise. Les DSI sont déjà tellement impliqués dans une logique de services et de sécurité, qu'ils sont contraints d'inclure, dans la stratégie de protection des SI, tous les nouveaux équipements (smartphones, clients légers, ordinateurs ultraportables, netbooks, etc.) utilisés par cette nouvelle génération de travailleurs.

Dans cette recherche de la mobilité, l'utilisateur est souvent tenté d'utiliser différents moyens (ou supports ?) allant de la clé USB au netbook. Cette multiplication des données rime dangereusement avec une augmentation des risques.

- Vol physique ou logique (virus, worms, etc.) d'un exemplaire de ces données sensibles.
- Mauvaise synchronisation des données après une modification.
- Mixité des données sensibles et des données personnelles / source des confusions.
- Perte.

L'actualité montre que l'accès au savoir de ses concurrents est une source de pouvoir et que les méthodes pour y parvenir sont de plus en plus nombreuses. Nous pouvons en citer aisément deux types :

- **En s'appuyant sur les faiblesses technologiques ou humaines**

La propagation virale par « storm »,

profite par exemple de la connexion d'un disque / clé USB pour se copier dessus. Le déplacement de ce support vers un autre ordinateur offre une chance à ce virus d'être exécuté et donc d'infecter une nouvelle machine. La prolifération des virus tient aussi de la prolifération des supports de stockage... la donnée se promène maintenant hors de l'entreprise. Cette information est hors contrôle. L'utilisation d'espions industriels pour se procurer des informations permet ainsi à un pays de rattraper son retard technologique.

- **Une méthode qui s'adosse à la loi**

Les mesures permettant de « combattre le terrorisme » mises en place aux États-Unis après le 11 septembre 2001, autorisent le transfert des données personnelles des passagers (PNR : Passenger Names Records) des compagnies aérienne aux autorités américaines avec l'accord des autorités européennes (28 mai 2003) : nom, mode de paiement, numéro de carte de crédit, numéro de téléphone, adresse de facturation, préférences alimentaires. De même, la loi du 29 août 2008 (Court of Appeals for the Ninth Circuit) élargit le droit des agents des douanes américaines à fouiller les appareils électroniques (ordinateurs portatifs, baladeurs numériques, assistants numériques...) des personnes entrant sur le territoire des États-Unis. Pourtant ces appareils électroniques peuvent contenir des données importantes ou confidentielles

(SUITE)

pour le voyageur ou son entreprise. Ces dernières peuvent donc devenir publiques. Sans soupçon précis, les supports peuvent ainsi être divulgués à des tiers dans le but d'être traduits ou décryptés.

Pour contrer (ou tout du moins essayer) toutes ces atteintes à des informations sensibles ou personnelles, il existe un arsenal d'outils et de services impressionnant pour les entreprises. Il serait fastidieux de tous les énumérer mais dressons en ci-dessous une liste non-exhaustive à titre d'illustration :

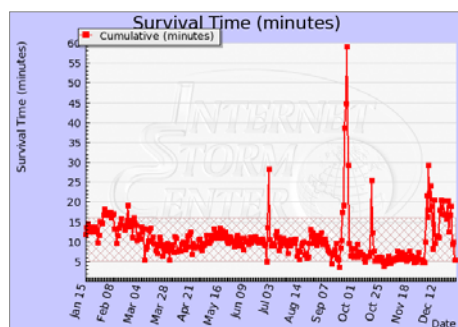
- **Protection logicielle**

Dans sa société ou à l'extérieur, l'utilisateur doit se protéger contre les attaques malicieuses. Que ce soient des malwares, des spywares, des rootkits, des storms, des e-gènes, des scareware, des ranswares ou des exploits, tous ces codes malicieux œuvrent pour un seul but : accéder aux données et pouvoir en tirer un avantage financier. Malheureusement, aujourd'hui même, les meilleures solutions (anti-virus ou firewall) ne peuvent proposer une protection instantanée totale. Il existe toujours un delta temps plus ou moins important entre l'apparition d'une attaque et le moment où l'utilisateur dispose d'une protection de l'éditeur. L'utilisateur doit garder en mémoire qu'un anti-virus n'est pas une protection qui rend son ordinateur imprenable. Or aujourd'hui l'exploitation d'une faille de sécurité par les codes malveillants est toujours plus rapide.

En 1999, une faille était exploitée en moins de 10 à 15 jours après sa découverte.

En 2003, ce délai est passé à moins de 15 minutes.

En 2008, il faut compter moins de 4 minutes...



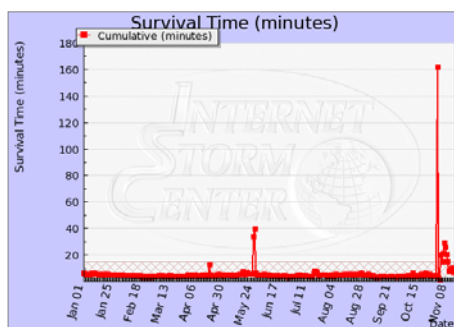
- **Protection des connexions**

Pour faire le lien entre le poste de travail et l'accès au réseau de l'entreprise, il existe des méthodes variées d'authentification et d'autorisation : code secret conservé par l'utilisateur, « dongle » générant un code, biométrie, etc. De par la multitude des niveaux de sécurité recherchés, toutes ces méthodes offrent des degrés de sécurité différents. Le code secret est, par exemple, largement plus confidentiel que la biométrie qui accompagne généralement l'empreinte de l'utilisateur autour de l'équipement.

- **Protection des données**

Chiffrement logiciel : Avec le nombre croissant d'accès aux informations, la nécessité de chiffrer les données d'un utilisateur est primordiale. La base d'un bon chiffrement est avant tout la génération d'un nombre aléatoire non prévisible. Il s'agit là de l'un des premiers défis dans la sécurité car la génération d'un tel code est d'une complexité insoupçonnée pour la plupart des utilisateurs. Une fois ce code généré, le chiffrement des données peut commencer, souvent au détriment des ressources de l'ordinateur et rendant, dans certain cas, son utilisation contraignante. Toutes les solutions logicielles demandant à l'utilisateur de saisir son code sur le clavier sont vulnérables aux 'keyloggers'. Une fois cette information récupérée, le code secret est envoyé pour analyse (cassage) à l'auteur du code malveillant.

Chiffrement matériel : Ces solutions peuvent générer des codes aléatoires très peu prédictibles, contrairement à la solution logicielle. Une telle solution est de fait plus onéreuse, mais elle apporte les garanties d'une sûreté de chiffrement nettement plus forte. Pour pouvoir assurer une protection maximale, le code généré ne doit à aucun moment sortir de l'équipement, le rendant ainsi vulnérable.



Un tel équipement devient alors pratiquement inviolable même pour des professionnels de la sécurité.

Aujourd'hui, les solutions de protection des données sont très souvent associées au matériel de l'utilisateur mais pas suffisamment à ses données. En cas de mobilité, l'utilisateur va utiliser des équipements qui ne sont pas les siens. L'utilisateur peut se « recréer » un environnement de travail avec les solutions nouvelles que sont les « bureaux virtuels » ou « desktop online » : il lui est alors possible de travailler partout à condition d'avoir accès à ses propres données et d'avoir un accès Internet. Malgré cela, les protections ne sont pas encore suffisantes pour garantir une sécurité maximale lors du transfert des données ou de leur stockage.

La nouveauté résulte dans le fait que la donnée – qu'elle soit d'ordre privé ou professionnel – doit être capable de suivre l'utilisateur sans prendre le risque d'être dégradée ou accessible par un tiers. En faisant abstraction du matériel (smartphone, ultraPC, laptops, etc), la solution globull™, lancée par Bull en 2008, permet à l'utilisateur de se déplacer avec toutes ses données et son environnement, de la façon la plus sécurisée qu'il soit. La machine d'accueil devient donc du consommable, ce qui pour l'entreprise permet d'accroître ses économies de gestion de parc mais aussi d'augmenter la rentabilité d'un collaborateur. Bull est prêt aujourd'hui à introduire le concept de la machine hôte devenant un simple socle grâce auquel l'utilisateur peut connecter son environnement ultra-protégé; le rendant lui-même ultra-mobile.

Avec cette approche, la sécurité change enfin de paradigme, passant d'une sécurité centrée sur l'informatique à une sécurité centrée sur l'information et l'utilisateur.

Plus d'information :

Livre blanc « Mobilité et sécurité : la fin du péril ? » <http://www.bull.com/p/register.php?id=127&lng=fr>

globull™, la plate-forme de sécurité mobile la plus sûre au monde :

<http://www.myglobull.com>

Vidéo de l'annonce globull :

http://www.bull.com/websem/140_fr/

SERVEURS

Bull renforce son initiative pour le Bio Data Center et lance Bull System Manager

Une solution simple d'administration des infrastructures informatiques depuis un point de contrôle unique

Bull vient d'annoncer Bull System Manager (BSM), une suite logicielle qui facilite l'administration de systèmes en tous types d'environnements, hétérogène ou non, tout en les amenant à leur plus haut niveau d'efficacité.

Une contribution clé à l'initiative Bio Data Center™ de Bull

Bull System Manager enrichit l'initiative Bio Data Center de Bull en proposant un point d'entrée unique pour l'administration de ces environnements. La garantie de niveaux de services qu'il apporte et l'utilisation de processus particulièrement automatisés font de BSM un atout dans le renforcement des infrastructures des centres informatiques. Le Bio Data Center porte sur des éléments suivants :

- Déploiement de processus opérationnels de très grande qualité.
- Adoption d'une topologie efficace proposant une répartition équilibrée entre virtualisation et consolidation.
- Intégration de technologies puissantes à l'état de l'art pour les serveurs et le stockage.

Une intégration transparente de composants Open Source

Par l'intégration transparente de nombreux composants Open Source dont Nagios, enrichi, testé par Bull, BSM a pour principales spécificités de permettre une administration automatisée des tâches, un contrôle depuis un point central, d'offrir une solution d'administration « virtualisable », puissante et modulaire.

Bull System Manager simplifie l'administration des serveurs Bull Escala, NovaScale et Blade Series et des systèmes de stockage Bull StoreWay, et renforce également leur disponibilité. BSM s'appuie sur une architecture 3-tier et s'intègre facilement au sein des plates-formes d'administration telles que Bull Open Master, HP OpenView, CA Unicenter et IBM Tivoli par le biais d'un CIM (Common Information Model) et du protocole SNMP (Simple Network Management Protocol).

Des tâches administratives automatisées Bull System Manager intègre la notion de rôles. Il permet aux administrateurs de spécifier les tâches de paramétrage, organise et administre les systèmes en groupes arbitraires, crée des « vues » selon les paramètres requis, techniques ou organisationnels. Le système de notification rapide lors d'alertes permet une analyse en profondeur qui conduit au déploiement simultané d'une solution correctrice.

Un seul point de contrôle

Bull System Manager c'est aussi un accès sécurisé aux systèmes distants. Il contrôle l'utilisation et la performance des éléments critiques tels que les processeurs, les disques, la mémoire quelque soit le système d'exploitation. Il diminue les coûts liés à l'exploitation grâce à une console unique et indépendamment du nombre de plates-formes sur lequel les applications sont déployées.

Une solution « virtualisation ready »

Un seul outil suffit pour avoir une vue hiérarchisée et synthétisée du statut des machines virtuelles, et ce indépendamment de la technologie utilisée pour leur élaboration. BSM identifie automatiquement les machines virtuelles et les rattache au serveur physique dont elles dépendent.

Une solution d'administration associant puissance et modularité

Les fonctionnalités d'administration de BSM apportent une vue synthétique sur l'état du parc. Elles détectent notamment les anomalies, les notifient aux entités concernées. BSM recueille automatiquement tous les événements en provenance des systèmes d'exploitation comme des systèmes d'administration. Il offre une visualisation et un suivi de la configuration matérielle, jusqu'au niveau des partitions.

Des centres d'expertise et de support

Les clients bénéficieront pleinement des centres d'expertise de Bull, que ce soit pour définir, déployer ou administrer leurs infrastructures complexes. Les prestations des centres couvrent un vaste spectre qui comprend la définition d'architectures, l'évaluation des environnements applicatifs par POC (Proof of Concept) et les audits énergétiques. Bull Télé-Services apporte à l'environnement de Bull System Manager des services de pointe en 24x24, 7jx7.

Un coût de possession optimisé

Parce qu'il est ouvert et facilement intégrable, Bull System Manager administre tout type de serveurs sous AIX®, Linux® ou Windows® et réduit le coût par système administré par une maîtrise accrue de leurs coûts d'administration. De plus, son architecture permet une administration à distance, facteur de flexibilité accrue.



SERVICES

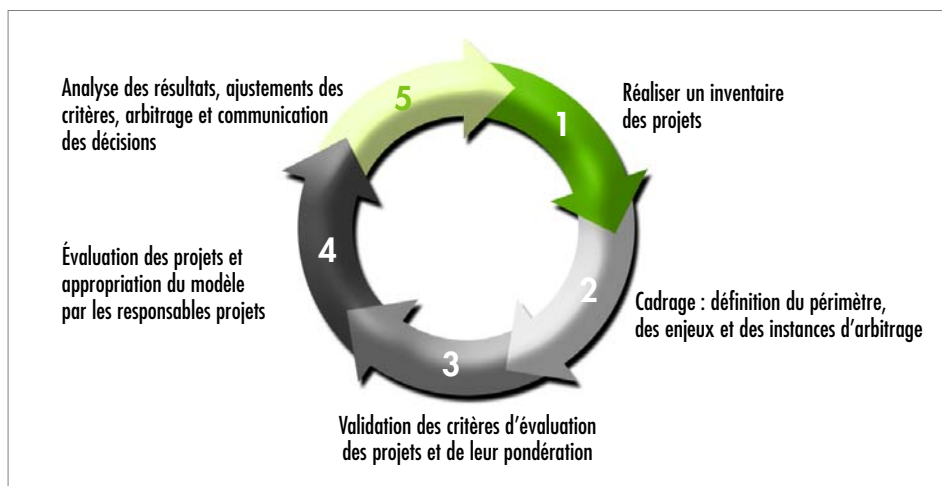
La gouvernance de portefeuille de projets informatiques : plus stratégique que jamais

Besoins étendus, délais raccourcis, complexité technologique accrue... la maîtrise des projets est au premier plan des préoccupations des DSI. D'ailleurs, les cabinets d'étude du marché pointent largement du doigt des taux d'échec impressionnants : 30% des projets informatiques dépasseraient de 10 à 20 % le budget ; un projet sur quatre coûterait finalement le double de ce qui avait été prévu initialement ; 29 % seulement des projets s'achèveraient en temps et en heure, au budget imparti et avec la qualité de service attendue.

Les raisons invoquées : une mauvaise estimation initiale, l'élargissement du champ fonctionnel du projet, des problèmes d'interdépendances ou de conflits entre plusieurs projets conduits en parallèle, etc. Au final, 39 % des directions informatiques n'auraient pas une vision fine de leur portefeuille de projets, ce qui ne permettrait pas d'anticiper ces dysfonctionnements.

Constituer un portefeuille de projets informatiques vise à objectiver l'attribution des investissements informatiques et à concilier les attentes des différents clients de la DSI. A l'heure où les ressources financières et humaines sont souvent limitées, il est en effet impératif de mettre en place un processus rigoureux de sélection des investissements informatiques qui permette de maximiser le retour sur investissement pour l'entreprise. Il s'agit de piloter l'ensemble des projets de façon à être en mesure de décider en permanence de ce qui doit être fait, sur la base de la valeur des projets, des risques, des priorités et des moyens du moment. Schématiquement, le portefeuille projets n'est qu'un simple instrument de comparaison. Celui-ci n'a d'intérêt et de devenir qu'à condition d'être accompagné par des processus dédiés (arbitrage) et des acteurs aux responsabilités clairement définies (pouvoir de décision). Enfin, il doit répondre aux différents objectifs stratégiques, économiques et opérationnels de l'entreprise.

Bull Management, l'entité conseil et intégration de Bull, a développé cette expertise et propose une démarche structurée, adaptable à chaque entreprise. Cette démarche s'appuie sur la brique logicielle PPMTM de la société IT4 Control, solution de gestion de portefeuille de projets (Project Portfolio Management).



La démarche proposée par Bull permet de déterminer des critères d'évaluation d'un projet :

- Contribution à la valeur stratégique métier.
- Contribution à la valeur stratégique informatique.
- Mesure de la valeur économique du projet.
- Mesure des risques du projet.
- Mesure des risques liés à la non réalisation du projet.

En parallèle, trois éléments essentiels concourent à l'atteinte des objectifs fixés :

- L'identification des actions transversales dans les projets. Chaque application dispose de son propre cycle de vie. Une fois les projets recensés, catégorisés et valorisés, il convient de définir les actions transversales à ces projets.
- La cohérence fonctionnelle du système d'information, souvent occultée dans la conduite de projets informatiques mais une des bases de sa pérennité.
- L'adaptation à la culture et à l'organisation de l'entreprise, pour garantir l'efficacité et la pérennité de gouvernance du portefeuille de projets.

▼ Quelques bonnes pratiques de la Gestion de Portefeuille Projet (PPM)

- Définir des critères d'évaluation homogènes, objectifs et mesurables.
- Impliquer la Direction Générale en amont lors de la définition des objectifs stratégiques et du processus d'arbitrage.
- Favoriser une démarche itérative pour ajuster les mécanismes d'évaluation et de pondération en impliquant les responsables métier.
- Adapter le processus d'arbitrage et de gouvernance au contexte de l'entreprise.
- Mettre en place un outil pour pérenniser la démarche de la gestion de portefeuille, en s'appuyant sur des processus éprouvés.

INITIATIVE 7

Vers une sécurité agile

Bull lance une approche faisant de la sécurité un levier de développement métier

Bull lance la septième initiative de son programme 7i, « Garantir la confiance », pour aider les entreprises à se développer en toute sécurité dans un monde ouvert.

Avec plus de 100 milliards de dollars de pertes par an¹, la sécurité est aujourd'hui un enjeu vital pour les entreprises. Pour lutter contre les malveillances et les attaques nouvelles, les systèmes de sécurité ont pourtant dû agréger au fil des années de multiples solutions hétérogènes, finissant par altérer la vitesse de développement des entreprises et l'agilité de leurs lignes d'activité.

Pour aider les entreprises à passer d'une démarche purement défensive et réactive à la mise en place d'une politique de sécurité proactive et agile, Bull annonce un ensemble de services et de solutions permettant de réconcilier sécurité et agilité, en faisant de la sécurité un véritable levier de développement métier et un puissant moteur de changement.

« Vivre dans un monde ouvert et mobile ouvre des perspectives sans limite... à condition de savoir conjuguer mobilité et sécurité » a souligné Jean-Pierre Barbéris, Directeur Général de Bull France et de Bull Services et Solutions. « Dans ce monde ouvert, il faut pouvoir interagir en toute confiance avec les écosystèmes de ses clients et de ses partenaires. Notre ambition : apporter toutes les dimensions d'une sécurité intégrée, agile et orientée métier pour créer les écosystèmes de confiance de demain. »

Faire de la sécurité un levier de développement métier

Si la sécurité est aujourd'hui reconnue comme un impératif majeur, 40 % des DSI² estiment que leur sécurité est peu, voire mal alignée avec leurs impératifs métiers.

Conseil, intégrateur, infogérant et fournisseur de solutions de sécurité, Bull renforce aujourd'hui ses équipes de conseil pour aider les entreprises à faire de la sécurité un levier de développement

Initiative 7 : Garantir la confiance

Face aux attaques qui vous menacent, jour après jour, les protections s'empilent et vous emmurent. En vous accompagnant dans la mise en oeuvre d'une sécurité intégrée, agile et adaptée à votre métier, Bull vous permet de ne plus devoir choisir entre sécurité et productivité. Avec Bull, la sécurité ne sera plus une contrainte, mais un levier de développement pour votre entreprise.

Pour en savoir plus sur nos 7 initiatives, visitez notre site web www.bull.fr/7i

BULL
Architect of an Open World™

*Architecte d'un monde ouvert

métier et d'agilité, en permettant de mieux :

- Aligner sécurité et processus métiers, conformément aux meilleures pratiques et normes (ISO 2700x, PCI-DSS, etc.).
- Bâtir des systèmes de sécurité puissants mais aussi flexibles au service du développement de l'entreprise.
- Accompagner et faire évoluer les systèmes dans le temps, depuis l'élaboration de plans de secours (PRA/PCA) jusqu'à l'infogérance totale du système d'information sécurisé.

Ces services s'appuient sur la capacité de Bull à intégrer les meilleures technologies du marché et sur les solutions développées par le Groupe dans trois domaines d'investissement à forte valeur ajoutée :

- La continuité d'activité au travers les offres Bull Bio Data Center™ et StoreWay™ sur la protection des données.
- La gestion des transactions et des flux VPN avec MetaPKI, MetaSign, Crypt2Pay, utilisés par 95 % des banques françaises pour leurs transactions, et chiffreurs TrustWay certifiés EAL2+.

(SUITE)

- La gestion des identités et des accès grâce aux solutions logicielles de sa filiale Evidian, premier éditeur européen d'IAM (Identity and Access Management). Evidian permet d'accélérer le développement de ses clients dans un monde ouvert en proposant une gestion des identités alignée sur les processus métier et de manière transparente pour les utilisateurs. L'offre Evidian rend possible l'harmonisation de la sécurité des applications, au cœur de l'entreprise mais aussi vers tous ses interlocuteurs, partenaires ou clients, en introduisant une administration des politiques de sécurité basées sur des rôles et rendant possible de « *Vivre dans un monde ouvert et mobile qui ouvre des perspectives sans limite* ».

Démocratiser la mobilité sécurisée pour les entreprises et les PME

En lançant son offre de mobilité haute sécurité globull™, une solution révolutionnaire pour réconcilier sécurité et mobilité, Bull démocratise et rend accessible à tous les technologies de mobilité issues de la défense. 77 % des utilisateurs doivent aujourd'hui transporter des données sensibles sur leurs laptops et des clés USB non sécurisées. Un risque majeur qui peut *in fine* freiner la mobilité.

L'offre Bull permet ainsi aux utilisateurs des entreprises et des PME de :

- Retrouver partout 100 % de leurs données et 100 % de leur environnement de travail, en toute confiance. Véritable coffre-fort chiffré de 120 grammes, en cours de certification EAL3+, globull™ permet à tout utilisateur de retrouver partout son environnement sur n'importe quel poste, PC, portable, ou ultra portable. Il lui suffit de s'authentifier sur le clavier tactile de globull™ pour retrouver d'un seul clic son environnement personnel. Solution la plus sécurisée au monde, globull™ lève les vulnérabilités existantes des PC sécurisés.
- Déployer et administrer les environnements, les applications, les données et les profils utilisateurs sur tout globull™, mais aussi PC, Nettop, Netbook, etc. Avec ses partenaires, globull™ offre ainsi une réponse au besoin de gestion de multiples terminaux par utilisateur.
- Garantir la sauvegarde et la restauration des données individuelles. L'environnement mobile protégé par globull™ peut ainsi être en permanence sauvegardé et restauré à distance.
- Utiliser la signature électronique en contexte de mobilité, grâce au stockage sécurisé par globull™ de tous les certificats du marché pour authentification et

signature électronique. De plus, un partenariat avec Chambersign (issue du réseau français des Chambres de commerce et d'industrie) permet d'utiliser des solutions sectorielles dans les domaines de l'audit et de la santé.

Intégrer une gestion sécurisée des accès aux applications avec les solutions de gestion des accès de Bull Evidian, disponibles dans les environnements Windows® mais aussi Linux®, globull™ permet de renforcer sécurité et productivité, en combinant authentification forte et SSO (Single Sign-On) pour l'accès à toutes les applications de l'entreprise et ce quel que soit le lieu où se trouve l'utilisateur.

L'offre sécurité de Bull s'appuie sur une expérience acquise chez certains des principaux opérateurs de télécommunications européens, des piliers du secteur bancaire (SWIFT, Caisse des Dépôts, etc.), de grands institutionnels, des leaders de l'industrie (EADS, Renault Nissan, Sanofi, Total, etc.) et des acteurs de la Défense.

Plus d'information sur l'initiative 7 et l'offre sécurité de Bull : www.bull.fr/7i

(1) Source : Mi2G

(2) Source Etude Bull

DISTINCTION

Evidian dans le Cadran des Leaders du Single Sign-On d'Entreprise

Evidian, filiale de Bull, a été classé dans le cadran des leaders, édition 2008, du « Magic Quadrant for Enterprise Single Sign-On » de Gartner. Evidian est le premier fournisseur européen, et l'un des leaders mondiaux, de logiciels de gestion des identités et des accès. Depuis plus de dix ans, Evidian édite des logiciels d'authentification unique d'entreprise (ESSO) pour des centaines de moyennes et grandes organisations.

« Le single sign-on est de plus en plus au cœur du dispositif de gestion des identités et des accès. Ainsi, pour les entreprises, choisir une offre ESSO de grande qualité est des plus critiques » a déclaré Hassan Maad, Directeur Général d'Evidian. « Nos clients exigent que nous leur apportions des solutions d'entreprise à l'état de l'art. Notre positionnement dans le cadran des leaders de Gartner est pour moi la démonstration de notre capacité à déployer des solutions de ESSO robustes et sécurisées pour les grandes entreprises et administrations. »

Publié le 18 septembre 2008, le rapport de Gartner analyse le marché du ESSO et évalue douze solutions. Les positionnements sur le cadran prennent en compte la dimension visionnaire de l'éditeur ainsi que sa capacité à la mettre en œuvre.

Selon Gartner, « Les leaders du marché du ESSO font la preuve de leur faculté

constante à conquérir de nouveaux clients dans tous les secteurs d'activité et sur tous continents. À l'extrémité supérieure du cadran, ils ont de très bonnes, voire d'excellentes références clients et une offre qui s'intègre facilement aux systèmes cibles. Les leaders démontrent également un engagement à apporter rapidement les évolutions de leur produit attendues par leurs clients. »

Résultant de plusieurs années d'expérience et d'innovation, Evidian Enterprise SSO est une solution logicielle qui offre des fonctionnalités uniques pour ce qui est de la mobilité et de la confidentialité des données. La solution d'Evidian va au-delà des outils de SSO traditionnels en s'intégrant aux procédures métier de l'entreprise. Elle apporte des fonctions de gestion s'appuyant sur les rôles qui accélèrent le retour sur investissement et garantissent sécurité et productivité aux utilisateurs.



Evidian Enterprise SSO peut être déployé seul ou avec d'autres modules de Evidian IAM Suite – comme la gestion de politiques, le provisionnement et l'authentification forte. Il est de même compatible avec d'autres solutions de gestion des identités du marché. Le SSO permet ainsi de tirer le meilleur parti des investissements en gestion des identités des entreprises.

Paris, le 17 décembre 2008

Mornings du libre

Le BPM, pivot de la mise en œuvre d'une démarche SOA.

Chaque mois Bull vous propose un rendez-vous autour d'une thématique liée à la mise en œuvre de l'Open Source dans les systèmes d'information.

Animées par des experts, ces matinées se veulent avant tout pragmatiques. Leur objectif : apporter un véritable contenu technique aux Directions Informatiques amenées à s'appuyer de plus en plus fréquemment sur les logiciels libres et désireuses d'en tirer pleinement profit. L'expérience des grands projets Open Source, ses liens avec les communautés, sa capacité à supporter de nombreux composants associés à une longue prati-

que du logiciel libre acquise dans ses centres de R&D font de Bull un acteur majeur du monde de l'Open Source.

Venez nombreux partager cette expérience mercredi 17 décembre, sur le thème : Le BPM, pivot de la mise en œuvre d'une démarche SOA. L'importance du cadre méthodologique et les points clés de la démarche. L'approche Open Source de Bull.



De 9 h à 11 h au Centre Régus, Paris La Défense, Tour Ariane (accueil à 8 h 30).

Inscrivez-vous dès maintenant :
<http://www.bull.com/fr/mornings>

Londres, les 23 et 24 mars 2009

Gartner Identity & Access Management Summit 2009

Aujourd'hui, toute entreprise dispose d'une solution pour gérer les accès et les identités (IAM, Identity and Access Management). Quels que soient les utilisateurs : employés, partenaires, clients en ligne, gérer leurs identités numériques et leurs accès au système d'information et aux données de l'entreprise est critique.

IAM est désormais la clé de voûte de la sécurité du SI – un programme efficace d'IAM peut conduire à de réels bénéfices en termes de réduction de coûts, de conformité aux règlements et de gouvernance informatique. Cependant, relativement peu d'entreprises en Europe ont un programme IAM formel – près de la moitié développent des procédures et des outils d'investigation et plus d'un quart d'entre elles sont en train de définir des procédures et utilisent des outils relativement basiques.

La maturité en termes d'IAM est atteinte lorsque l'entreprise a optimisé ses processus IAM et a intégré les outils afférents dans une architecture IAM en osmose avec l'organisation de l'entreprise et les a alignés sur ses besoins métier. Tout l'enjeu est là.

Evidian est sponsor Platinum du Gartner IAM Summit 2009 et sera heureux de vous accueillir sur son stand.

Pour plus d'information : <http://www.gartner.com/it/page.jsp?id=749726>



Londres, du 28 au 30 avril

Infosecurity Europe

Infosecurity Europe est le plus important salon pour les professionnels de la sécurité informatique ; il attire plus de 10 000 visiteurs qui viennent :

- découvrir les meilleures pratiques, et les plus récentes solutions et les technologies en la matière ;

- s'informer et partager les sujets les plus brûlants au cours d'un programme de conférence étoffé.

Evidian démontrera ses solutions E-SSO et de mobilité sur son stand D45.



Pour plus d'information :
www.infosec.co.uk

Marrakech au Maroc, du 22 au 24 avril 2009

Conférence WCO* sur les technologies de l'information

Gestion intégrée des frontières : les technologies de l'information sont-elles essentielles ?

Le salon mondial des douanes organisé par l'OMD, l'Organisation Mondiale des Douanes qui compte 169 pays membres, aura lieu à Marrakech, au Palmeraie Golf Palace.

Cet événement mondial est particulièrement apprécié des Douanes qui toutes doivent appréhender la chaîne du commerce international dans son intégralité et assurer la transition d'un contexte relativement fermé vers un environnement mondialisé avec des volumes d'échange considérablement accrus et des exigences nouvelles en termes de sécurité, d'efficacité et de contrôle des frontières. Les technologies de l'information jouent un rôle crucial dans ce nouvel environnement douanier qui met en exergue l'importance de la sécurité tout en facilitant les échanges dans le monde.

Nous sommes heureux de vous convier à la conférence Bull qui aura lieu le 23 avril de 14 h à 14 h 30 en session plénière.

Jean-François Betbeder, Vice-Président de la division mondiale dédiée aux solutions Impôts et Douanes démontrera comment e-biscus™ permet aux Douanes d'interagir dans un environnement mondialisé. Ouverte et flexible, la suite logicielle e-biscus de Bull facilite le commerce légal en détectant les fraudes et en accélérant les processus de dédouanement, tout en faisant respecter les règlements internationaux dans toute leur complexité. Nos experts vous accueilleront sur le stand Bull pour vous présenter la solution e-biscus ainsi que les services associés. Bull a acquis une reconnaissance internationale dans le Secteur Public pour son expertise, en particulier dans le domaine de l'alignement des systèmes douaniers sur les nouvelles exigences internationales. Dans le cadre de leur

préparation à l'accession à l'Union européenne, de nombreux pays ont choisi Bull pour développer des solutions conformes aux exigences européennes. Il s'agit de la Bulgarie, de Chypre, de la Hongrie, de la Lituanie, de Malte, de la Pologne, de la République Tchèque et de la Roumanie ; l'Irlande et le Maroc ont également choisi les solutions de Bull pour moderniser leurs systèmes douaniers.

Pour plus d'information :

http://www.wcoomd.org/event_factsheet_conference.htm

* WCO : World Customs Organization (OMD en français, Organisation Mondiale des Douanes).

Créée en 1952 sous le nom de Conseil de coopération douanière, l'OMD est un organisme intergouvernemental indépendant dont la mission est d'améliorer l'efficacité des administrations des douanes. Regroupant 169 gouvernements membres, elle est la seule organisation intergouvernementale mondiale qui soit compétente en matière douanière.

Londres, les 9 et 10 Juin 2009

Smart Healthcare Expo

Smart Healthcare live
9-10 June 2009 | Earls Court, London
Procuring Healthcare ICT

Smart Healthcare 2009 est l'événement majeur pour le monde de la santé qui vient y découvrir les nouvelles solutions et technologies pour moderniser les services de santé, réduire les coûts et offrir aux patients des choix plus larges. **Evidian démontrera ses solutions sur le stand SH18.** **Plus d'information :** www.smarthealthcareexpo.com/smc09/show_link1.asp#



Hambourg en Allemagne, du 23 au 26 juin 2009

ISC'09 - Solving identity, access and mobility

Le plus grand événement européen consacré au calcul haute performance (HPC) se déplace à Hambourg en 2009.

En quatre jours, cette conférence et exposition offre sous un seul toit une plateforme unique pour se former, rencontrer d'autres experts ayant les mêmes centres d'intérêt, et mettre en relation clients et fournisseurs. Avec plus de 1 500 participants prévus – grands noms de l'industrie du HPC, spécialistes en informatique et scientifiques – et plus de 120 exposants venus de 45 pays, l'édition

2009 d'ISC sera la plus importante et la plus intéressante jamais organisée.

Le programme de conférences comprendra comme toujours des intervenants prestigieux, ainsi que deux après-midi consacrées aux secteurs de la météo et de l'aéronautique, et des sessions spéciales dédiées au « cloud computing », aux architectures cluster/multi-cœur, au calcul intensif sismique, aux applications du

secteur pétrolier, aux GPU et à la gestion et l'exploration de volumes extrêmes de données.

La 33^e édition du célèbre classement mondial des supercalculateurs TOP500 sera annoncée à ISC'09.

Bull, sponsor Gold d'ISC'09, accueillera sur son stand sa filiale science + computing, spécialiste de l'intégration de solutions HPC et démontrera ses plus récentes offres en la matière.

Plus d'information :

www.supercomp.de/isc09