CIO
MANAGEMENT DES SYSTÈMES D'INFORMATION

N°9 - SEPTEMBRE 2009 - 15 €

www.cio-online.com

La première plateforme communautaire d'échanges, d'information et de services à destination des CIO, DSI et Managers IT

ÉDITO

Repartira ou repartira pas ? L'économie française émet des signaux flous en cette rentrée 2009. Un an après la faillite de la banque Lehman Brothers, symbole de la crise des subprimes, l'incertitude règne. Elle touche à tous les domaines puisque même la grippe H1N1 reste difficile à cerner : grippe classique ou tueuse ? D'où viendra l'éclaircie ? Quoiqu'il en soit, il faut plus que jamais s'adapter au monde numérique, sans oublier de placer l'homme au coeur de l'entreprise à la lumière des drames vécus chez France Télécom.

SOMMAIRE

RETOUR D'EXPÉRIENCES

La sécurité est une course de fond

Face à l'évolution des usages, la sécurité des systèmes d'information doit s'adapter. Il s'agit surtout d'être persévérant et de savoir assembler la multitude de composants disponibles sur le marché. Impliquer les utilisateurs demeure indispensable. La sécurité est une tâche de longue haleine.

Il faut de la persévérance pour réussir un projet de sécurité informatique. Les obstacles sont multiples. Les directions générales sont souvent peu sensibilisées. Les budgets sont revus à la baisse face à la situation économique actuelle. Pour autant, les problèmes demeurent complexes, et impactent de nombreux services. Les technologies ne sont pas forcément matures. Le travail d'intégration des composants du marché est important. Sans compter l'impérative conduite du changement et la nécessité de délivrer une sécurité qui accèlère le business au lieu de mettre des bâtons dans les roues. Dès lors, nombre de chantiers dans les entreprises sont des tâches de longue haleine. *"Il faut donner de la visibilité à un projet de sécurité, sinon il est mort"* conseille d'ailleurs **Eric Doyen, RSSI (Responsable Sécurité du Système d'information) du Crédit Immobilier de France** qui a porté un projet de gestion des identités durant deux ans et demi. Sans oublier que *"La priorité est à l'économie"* rappelle **Serge Saghroune, RSSI du groupe Accor**.

Authentifier les utilisateurs

Dans les organisations, les besoins sont pourtant nombreux. En tête de liste, on trouve l'indispensable authentification des utilisateurs. Beaucoup de responsables sécurité ont engagé de telles démarches, par des voies diverses. La PKI demeure le nec plus ultra, mais les OTP (One Time Password) répondent à des besoins précis, et l'on trouve également quelques cas de déploiement du NAC (Network Access Control).
Le NAC est l'objet d'un destin paradoxal. Cette technologie est plébiscitée lorsqu'on interroge les responsables sécurité, mais elle est très peu répandue dans les entreprises car elle ▶

10 RESPONSABLES SÉCURITÉ TÉMOIGNENT

Eric Doyen
Crédit Immobilier
Ludovic Tardy
TBWA
Antoine Bajolet
TDF
Cédric Foll
Education Nationale
Jean-Patrick Lengrais
Société Générale
Lazaro Pejsachowicz
CNAM TS
Gilles Berthelot
Pompiers de Paris
François Gratiolet
Groupe La Poste
Serge Saghroune
Accor
Fabrice Pizzi
Eiffage

nécessite une infrastructure de réseau homogène. Le NAC identifie les utilisateurs et sert à mettre à jour leur poste de travail en conformité avec la politique de sécurité. Exemple : l'agence de communication TBWA a opté en juillet 2009 pour une solution NAC, afin de sécuriser ses 2000 postes, dont 80% fonctionnent sous McIntosh. La société a profité d'un renouvellement de ses équipements réseau pour mettre en place un NAC à base de matériel, des commutateurs d'Enterasys. Cette solution de NAC aura nécessité deux ans pour être élaborée en étudiant les offres de Cisco, Symantec et Enterasys.

Le NAC pour vérifier la conformité

> **Le NAC répond à la question de l'intégrité du poste de travail**
>
> ***Ludovic Tardy***
> *Agence TBWA*

« L'intégrité du poste de travail est ce qui nous a semblé le plus intéressant, que ce soit pour les postes internes ou pour les postes nomades », présente **Ludovic Tardy, responsable sécurité et réseau chez TBWA**. *« Beaucoup de gens viennent de l'extérieur sur nos sites et ont besoin d'accéder à l'impression, ou aux fichiers SharePoint, à des serveurs de fichiers et à des bases de données. Il n'y a pas toujours un administrateur pour valider la conformité des postes »* ajoute-t-il. La technologie employée fonctionne sous forme d'ActiveX ou de Java. Elle vérifie l'adresse physique (MAC) du poste, si un anti virus est présent, s'il est à jour, et si il y a des programmes interdits par rapport à la politique de TBWA. *« On notifie à l'utilisateur via une page Web, ce qu'il doit désactiver voire désinstaller avant d'accéder au réseau de TBWA, ou on notifie un sponsor chez TBWA concernant un problème sur un poste de travail »* précise Ludovic Tardy.

Au-delà du NAC, le plus puissant en matière d'authentification demeure la PKI. Elle est lourde à déployer mais élargit les usages afin d'établir la confiance sur l'ensemble d'internet. TDF, leader de la diffusion hertzienne en France, a recours à cette technologie. En 2008, la société a opté pour un service de PKI en mode hébergé chez Keynectis, ce qui en simplifie la mise en oeuvre. La PKI sert alors à dématérialiser les processus d'achats, et la signature des bons de commande. Une quarantaine d'acheteurs sont identifiés par des cartes à puce lors des transactions. Cette même technologie est employée afin d'authentifier les accès locaux des utilisateurs via Wifi, à la fois en 802.1x et via des certificats, et des nomades lors de connexions via le VPN. Dans ce dernier cas, c'est alors la passerelle VPN de technologie SSL, d'origine Juniper Networks, qui valide la configuration du poste de travail, via là aussi un Active X ou un applet Java. *« Il y a vérification que le firewall est activé, que l'antivirus est présent, et que le PC correspond globalement à un certain nombre de critères pour faire partie de notre réseau »* décrit **Antoine Bajolet, délégué à la sécurité des systèmes d'information chez TDF**. Il existe concrètement deux autorités de certification chez TDF selon qu'il s'agisse de distribuer des certificats "métiers" de signature de bons d'achats, ou de s'authentifier.

Sécuriser les accès depuis des PC inconnus

Si la PKI est saluée par tous comme assurant une authentification maximale des personnes et de leurs actions – sans possibilité de répudiation -, des solutions moins complètes mais durcies ont des avantages. C'est le cas à l'Education Nationale qui se félicite de son récent choix de la technologie OTP (One Time Password) de SecurID de RSA bien qu'elle possède sa propre PKI. Mais cette dernière est loin d'être la réponse à toutes les questions. En 2006, une nouvelle application a nécessité que les personnels des écoles primaires et des mairies puissent accéder à une base de données sensibles concernant les élèves. *« Il s'agit d'une population d'utilisateurs pour laquelle nous n'avons pas la maîtrise du poste de travail. Il nous fallait un mécanisme d'authentification forte sans aucune adhérence sur le PC. Nous avons retenu le dispositif OTP sous forme de calculette. Environ 70 000 ont été déployées auprès des utilisateurs. Nous réfléchissons à étendre cette solution aux enseignants du second degré.* ▶

LE ROI DE LA SÉCURITÉ EST TROP FACILEMENT MANIPULABLE

La question du retour sur investissement de la sécurité est récurrent. *« La sécurité n'a pas de prix mais a un coût »* a-t-on coutume de dire. Pour Serge Saghroune, RSSI du groupe Accor : *« On peut fabriquer de beaux ROI – on trouve cela chez les américains - en créant des tableaux de bord où on fait apparaître le nombre d'attaques bloquées, le nombre de virus détectés, le temps pour redémarrer les machines, etc. »*. On peut alors calculer un ROI selon le temps de blocage des utilisateurs. Mais *« Cela ne sert à rien, il faut présenter la situation avec des sommes plus crédibles »* estime-t-il. On peut aussi essayer d'estimer ce que coûte une panne de parefeu ou quel est le coût du blocage durant une heure des réservations ? Au final, *« Je suis très circonspect vis à vis du ROI de la sécurité. Il apparaît impossible à calculer. De plus, il est douteux car trop facilement manipulable. En cas d'attaque qui déclenche un problème d'image pour la société, par exemple, comment en évaluer le coût ? »* conclut-il. ■

L'OTP est un bon compromis en termes de simplicité d'usage et de sécurité tout en étant nettement moins coûteux que le token cryptographique de la PKI et sans les difficultés liées à l'environnement du PC » décrit **Cédric Foll, RSSI de l'Education Nationale**.

On remarque cependant d'une manière générale que la PKI connaît un second souffle. C'est le cas en particulier à la Société Générale. La banque possède une PKI depuis longtemps, mais elle ne concernait principalement que deux usages : l'authentification des échanges entre applications (plusieurs centaines), et dans une moindre mesure les postes nomades, afin d'établir une liaison VPN.

Le mode d'authentification doit être en adéquation avec les enjeux et les coûts

Jean-Patrick Lengrais
Société Générale

Classifier l'information avec les managers

Aujourd'hui, devant s'adresser à 160 000 personnes réparties dans le monde ayant des besoins différents et changeants, la PKI est envisagée sous un nouvel angle. Une autorité racine (AC ou Autorité de Certification) a été créée en décembre 2008. Tout le monde n'aura cependant pas besoin d'une PKI. *« Il faut identifier tous les métiers et toutes les informations pour voir qui a besoin d'une PKI »*, décrit Jean Patrick Lengrais, RSSI à la Société générale. La banque est donc d'abord partie sur l'élaboration d'une politique de classification et de protection de l'information qui s'impose à tous. Des groupes de travail sont mobilisés, en impliquant les managers, pour identifier toutes les informations et tous les systèmes qui nécessitent une sécurité renforcée. *« A partir de là, tout ne relèvera pas de la PKI. Selon la problèmatique, on aura une authentification simple, par identifiant et mot de passe. On peut aller un peu plus loin, avec des cartes matricielles de type bataille navale, et enfin l'offre PKI »* résume Jean Patrick Lengrais. *« L'objectif est d'être en adéquation avec les enjeux, et les coûts associés. Car une infrastructure a un coût, les certificats ont un coût, idem pour le logiciel de chiffrement de nos répertoires. »* Cela devrait représenter toutefois des dizaines de milliers de certificats. *« Les certificats d'authentification seront généralisés, mais le chiffrement ou la signature électronique, tout le monde n'en a pas besoin. »* Chaque utilisateur devrait alors disposer d'un badge unique sans contact pour les accès physiques et une panoplie de certificats logiques selon ses droits, afin de réaliser de l'authentification, de la signature ou du chiffrement.

A la Caisse Nationale d'Assurance Maladie, le problème est en fait inverse, remarque **Lazaro Pejsachowicz, RSSI du CNAM TS**. *« Là où une majorité d'entreprise voit les V.I.P manipuler des données sensibles, ce n'est pas le cas à la Caisse Nationale d'Assurance Maladie, où ce sont les employés de base qui y accèdent. »* La CNAM a donc installé depuis très longtemps une authentification forte sur la quasi totalité de ses postes. Le système a 15 ans, basé sur une PKI, et il est remis au goût du jour, selon les préconisations de l'Etat.Un appel d'offres va être dépouillé d'ici quelques semaines pour l'usage d'une nouvelle génération de cartes à puce. *« Il faut différencier la signature de chacun des employés, et la délégation de signature, sans oublier le certificat qualifié qui va avoir son importance sur le terrain économique »* rappelle Lazaro Pejsachowicz.

La traçabilité ou la démarche Forensic

Autre demande clé auprès des équipes sécurité : la traçabilité des actions des utilisateurs sur le système d'information. *« Ce sujet nous avait amené à réaliser un pilote avec un éditeur. Sans l'avertir, nous avions généré un certain nombre d'événements afin de tester sa capacité à identifier ces alertes. Lors du débriefing, nous avons convenu que la difficulté n'est pas tant de générer des traces, nos systèmes en génèrent déjà beaucoup, mais d'exploiter ces lignes. Retrouver une information pertinente dans des millions de lignes, ce n'est pas évident lors d'une réquisition judiciaire qui demande à retrouver une information donnée à une heure et un jour donné »* résume Jean Patrick Lengrais. Conclusion du RSSI : *« Il faut des outils qui à partir de régles pertinentes sachent faire un premier filtrage et effectuer de bonnes corrélations. Avec cet éditeur nous avons constaté que selon le niveau où l'on mettait la barre, soit l'outil ne voyait rien soit il voyait beaucoup trop d'informations, et donc il était inexploitable. »*

Pire, une estimation montrait qu'il fallait deux à trois personnes à temps plein dans la banque pour exploiter ces informations qui pourtant avaient déjà été filtrées et limitées au nécesaire, sans parler de deux autres personnes du côté de l'éditeur. Résultat, le ROI n'était pas intéressant et la décision fut alors prise de ne pas donner suite car en travaillant de façon manuelle, lors de demandes ponctuelles, il était possible de retrouver l'information recherchée. *« Mais en montant en puissance en nombre d'utilisateurs et en complexité du système d'information comme c'est le cas avec l'internationalisation du groupe, se repose la question de la corrélation de logs, et nous relançons ce projet »* indique Jean Patrick Lengrais. Il s'agit alors de traiter les logs informatiques et non les logs comptables. *« Quoiqu'avec la* ▶

> **Il faut un lien entre les logs applicatifs afin de corréler les événements**
>
> ***Cédric Foll***
> *Education Nationale*

généralisation des accès Web, contrairement aux traitements batch, on est amené à se poser la question de la corrélation des pistes d'audits et des connexions » annonce-t-il.

Ce que confirme **Fabrice Pizzi, RSSI du groupe Eiffage, leader du BTP** : *« Nous avons restreint la supervision de logs à deux applications spécifiques critiques, et nous réalisons une corrélation entre les logs applicatifs, de type piste d'audit, et les logs système grâce à une console de type SIEM (Security Information and Event Management) »* La console retenue est Exaprotect, complétée par du contrôle d'intégrité de Tripwire.

La quantité d'information pose problème

Cette question d'exploitation des logs s'est posée à l'Education nationale en cas d'incidents de sécurité. *« Nous nous sommes aperçus que nos dispositifs techniques pour exploiter les logs et la quantité d'information produite par nos différentes briques applicatives ou techniques posaient des difficultés »* se souvient Cédric Foll. Il entendait répondre à des questions telles que : comment valider le fait que depuis un poste de travail, il y a eu connexion sur différents comptes dans une application multi-tiers ? Est-ce que deux personnes naviguent en même temps sur une application donnée avec le même compte ? Le constat a alors été clair. Le réseau réunit de nombreuses briques applicatives qui produisent des logs : serveurs d'habilitations, serveurs d'authentification, reverse proxys, accélérateurs SSL, répartiteurs de charge, serveurs de bases de données et serveurs d'applications. *« Or, chaque brique produit des logs comme si elle était seule, et il est difficile de disposer d'un lien qui permette de corréler deux à deux les événements »* déplore Cédric Foll. Il était alors impossible de produire des informations du genre : l'utilisateur s'est connecté avec telle adresse IP, a accédé à telles pages et à telles données.
Le premier réflexe là aussi a été de prendre un produit d'éditeur et à le brancher sur le systèmes d'information. Mais l'absence de « lien » entre les logs des différentes briques empêchait là encore des corrélations. *« On avait des faisceaux d'indices comme l'horodatage, mais c'est limité »* relève Cédric Foll. Résultat, une étude est en cours afin de refondre une partie des applications en ce qui concerne la création de logs. Il s'agit de créer sur chaque équipement des éléments qui permettent de réaliser des jointures avec une console de type SIEM de centralisation et de corrélation d'événements. Dans un deuxième temps, il devrait y avoir l'acquisition d'un boîtier apte à réaliser cette corrélation afin de le proposer comme un service aux différents centres informatiques. Avant de se lancer dans une telle tâche, une étude de risques ainsi qu'une cartographie du système d'information ont été réalisées il y a dix huit mois afin de se pencher sur les applications les plus importantes en termes de sécurité, selon la classification DICP (Disponibilité Intégrité Confidentialité Preuve/trace). Celles-ci verront une partie de leur code être réécrit, notamment en ce qui concerne les accès aux bases de données. Car depuis le serveur d'applications, des « *pools* » de connexion sont utilisés pour accéder à la base de données, - une manière de programmer que l'on rencontre fréquemment - ce qui empêche de savoir quel utilisateur a déclenché quelle action en lecture ou écriture sur la base de données.

Parmi les priorités en matière de sécurité, on trouve naturellement la protection contre les fuites d'information. Un risque qui se multiplie dans ces périodes de forte concurrence, avec l'apparition de dispositifs tels que les clés USB de très grande capacité ou les réseaux ►

LA FEUILLE DE ROUTE DE LA SÉCURITÉ EN ENTREPRISE

Les tâches ne manquent pas pour le responsable sécurité en matière de protection de l'information. On peut lister les pré-requis pour tout système d'information :

- **Authentification des utilisateurs :** Identifiant/mot de passe, carte « bataille navale », OTP (One Time Password), PKI, NAC (Network Access Control), 802.1x
- **Chiffrement :** chiffrement de surface des disques durs, chiffrement au niveau fichier, chiffrement matériel ou logiciel, certificat de chiffrement par PKI
- **Prévention de la fuite d'information :** DLP (Data Loss Prevention) au niveau des postes de travail et des périphériques, sur les passerelles du réseau et sur les serveurs
- **Gestion des identités et des rôles :** plateforme d'IAM (Identity and Access Management), workflow d'attribution des droits, interconnexion des applications et provisionnement des droits
- **Confiance sur internet :** signature électronique via PKI
- **Supervision :** centralisation des logs, et corrélation, constitution de preuve juridique

> **Les réseaux sociaux sont autorisés à la demande des commerciaux et du marketing**
> ***Serge Saghroune***
> *Groupe Accor*

sociaux. *« Les réseaux sociaux étaient interdits. Depuis, à la demande des commerciaux et du marketing cela a été autorisé »* relève Serge Saghroune, qui ajoute *« l'usage de Facebook ou de Linkedin ne dépend pas complétement des équipes sécurité »*. De fait tout dépend de la politique de l'entreprise. *« Notre direction générale est ouverte à ce type d'usage, mais nous pouvions filtrer les URL correspondantes si nécessaire »* note Fabrice Pizzi**.** Au bout du compte, il relève que les filtres sont contournables, mais que les employés doivent plus globalement respecter une charte interne qui fixe les limites de ce qui est diffusable à l'extérieur.

Chiffrer d'abord les postes sensibles

Zbigniew Kostur, expert en sécurité et protection de l'information et ancien RSSI de Nexans, estime pour sa part que face au risque de fuite d'information : *« Le rêve de chaque RSSI, c'est de mettre du chiffrement presque partout après avoir mené une véritable analyse de risques »*. Mais *« le management demande combien ça coûte, à quoi ça sert, et considère trop souvent que les problèmes n'arrivent qu'aux autres. »* A partir de là, il faut recentrer le propos et passer par une importante phase d'organisation et définir plus précisément ce qu'il faut protéger, qui on doit protéger, et contre quoi.

« On peut dans un premier temps protéger en priorité les PC portables réellement mobiles, une fois que l'on est sûr que ces machines traitent des informations confidentielles » décrit-il. Il faut ensuite classifier les informations. « Une approche est de définir ce qui est critique pour la société, ce qui est interne et ce qui peut être partagé ». A partir de là, il s'agit de mettre en place une solution contre la perte, le vol, et la fuite d'information. *« Une occasion idéale de sensibiliser le management est de profiter d'un vol ou d'une perte de machine transportant des informations confidentielles. »* Zbygniew Kostur propose dans ce cadre un chiffrement de surface de tout le disque dur. Lorsque le PC portable est éteint, l'ensemble du disque est chiffré. *« Cela ne traite toutefois qu'un seul problème : celui du vol ou de la perte »* rappelle-t-il.

Unifier la protection du PC et des clés USB

> **Le support et l'administration de la solution sont des critères importants**
> ***Fabrice Pizzi***
> *Eiffage*

Cette mesure ne suffit pas, car *« 90 % des gens n'ont pas confiance dans leur ordinateur, et ils copient en clair les mêmes informations sur des CDs, des disques durs externes ou des clés USBs. Il faut donc déployer une solution qui effectue un chiffrement complet et, en particulier, au niveau fichier sur ces types de périphériques. Il en existe désormais dans le commerce »*. Enfin, ces informations circulent aussi par mail et messagerie instantanée, d'où la nécessité de chiffrer les mails. Dans ce cadre, Zbygniew Kostur défend des approches de chiffrement en mode Saas, pour les emails, assurant de facto, l'intéropérabilité entre des systèmes de messagerie hétérogènes.

Fabrice Pizzi aura quant à lui évalué pas moins de quatre solutions de chiffrement pour la centaine de nomades dont les portables contiennent des données confidentielles. Il a déployé finalement les disques USB externes et les clés USB de MXI Security, protégés en outre par biométrie, et le chiffrement logiciel Truecrypt pour les disques internes. Il relève que *« Les critères qui comptent lors de ces choix sont multiples : le support du fournisseur, la puissance de l'administration, les performances et même le poids du dispositif.»*
Reste le danger permanent : le stagiaire. « Stagiaire = cancer » annoncent certains experts en sécurité. Afin de prévenir la fuite d'information, *« Il convient de mettre en place de mini-DLP* ►

LE CHIFFREMENT ET LA SIGNATURE ELECTRONIQUE BOUDES A L'EDUCATION NATIONALE

Dès 2002, l'Education Nationale avait lancé sa PKI interne à base de boîtiers nCypher installés dans un bunker situé à Toulouse. *« Le but était d'interconnecter les réseaux de l'Education Nationale, en particulier les rectorats en les authentifiant via les certificats générés par la PKI »*, explique Cédric Foll, RSSI de l'Education Nationale.
Devant le succès, cette PKI a été étendue à d'autres sites, puis à l'ensemble des collèges et des lycées.
Aujourd'hui, dix mille sites sont interconnectés en VPN IPSec. Puis, la PKI a servi à authentifier les nomades via des tokens cryptographiques, qui protègent le certificat d'un usage frauduleux. Dix mille utilisateurs nomades ont reçu ces tokens jusqu'en 2006. Seule l'authentification a séduit dans ce cadre, tandis que la signature électronique et le chiffrement n'ont jamais réussi à s'imposer, notamment pour la messagerie, car l'usage en était trop complexe.
En novembre 2008, cette PKI a été élargie aux certificats serveurs, pour s'affranchir de la dîme de certains fournisseurs de certificats. *"Nos certificats sont reconnus dans les navigateurs Web"* souligne Cédric Foll.
Accessoirement, ces certificats sont reconnus par un prestataire d'envoi de SMS qui authentifie l'Education Nationale lors de l'envoi de messages aux parents en cas d'absence d'un élève. ■

> **Il faut travailler en accord avec le juridique et l'audit interne**
> ***Zbigniew Kostur***
> *Expert sécurité*

(Data Loss Prevention) *en termes d'applications, en cartographiant les risques. Si on ne demande pas un DLP général, cela sera accepté au niveau du management »* décrit Zbigniew Kostur. Cet expert en sécurité considère de plus qu'en matière de chiffrement, seuls les métiers savent quelles informations sont sensibles par rapport à un projet ou à un développement. *« Il faut travailler de concert avec le juridique et l'audit interne, à partir de là, le management accepte »*.

Agir au cas par cas

« L'approche tout ou rien ne fonctionne pas » confirme le Lieutenant-Colonel **Gilles Berthelot, Chef du système d'information des Pompiers de Paris**. Il a aussi opté pour du chiffrement de surface pour les PC portables. Quant aux équipements des forces projetées à l'étranger, le chiffrement n'étant pas toujours légal, il emploie un système de remasterisation complet du PC au départ et à l'arrivée. *« Les données ne sont extraites que par l'équipe informatique. Ce qui est une manière de se protéger des pays un peu sensibles »*. Pour ce qui concerne les clés USB, il estime qu'il est impossible de s'en protéger d'une manière globale exception faite des PC critiques qui n'acceptent que des clés USB chiffrantes et biométriques.

Face à cette montée en puissance des risques, on vit un vrai retour du coffre-fort électronique. Les entreprises déploient des solutions ciblées pour certains documents et de petits groupes de cadres y accédant. il existe plusieurs étapes de mise en oeuvre indique **François Gratiolet, RSSI adjoint du Groupe La Poste**. *« Il faut d'abord définir une politique de protection de l'information. Cela comprend aussi bien l'information orale que l'information numérique* » Cette politique peut prendre la forme d'un document qui décrit les enjeux et les objectifs de protection de l'infomation pour l'entreprise. *« La deuxième étape consiste à formaliser de manière simple une grille qui selon le média électronique et le niveau de confidentialité de l'information va proposer des solutions pour l'utilisateur »* poursuit-il. Certaines solutions seront transparentes pour l'utilisateur, car embarquées nativement sur son poste de travail, à l'instar de l'antivirus, du logiciel de chiffrement du disque dur, ou du logiciel de DLP (Data Loss Prevention). Et il existe des solutions de type service, dont le coffre-fort électronique. Ce service tiers sera activé par l'employé lorsqu'il voudra travailler sur des documents de façon confidentielle.

> **Les maîtrises d'ouvrage ont des cultures différentes de la classification de l'information**
> ***François Gratiolet***
> *Groupe La Poste*

Sensibiliser les métiers à la valeur de l'information

L'étape suivante sera-t-elle le DLP (Data Loss Prevention) ? *« Ces technologies sont intéressantes mais elles demandent des pré-requis. En premier lieu, il faut une validation de cette démarche par la direction générale, et une culture de la classification et de la protection de l'information. Cette culture est assez hétérogène selon les maîtrises d'ouvrage »* pose François Gratiolet. Dès lors, le premier pas consiste à faire en sorte que les métiers se posent la question : est-ce que mon information a de la valeur, et quel serait l'impact si elle était divulguée ? *« Il y a beaucoup d'éducation et de sensibilisation à faire sur ce point. Il faut amener les maîtrises d'ouvrage à se poser les bonnes questions »* reprend-il. François Gratiolet voit les solutions de DLP comme un outil de sensibilisation et d'aide à la classification des informations auprès des maîtrises d'ouvrage. *« Dans un monde utopique, ce sont les maîtrises d'ouvrage métiers qui doivent faire cette classification. En fait, le responsable sécurité doit proposer une assistance forte pour les accompagner dans cette démarche. »* De plus, cela éduque également l'utilisateur. Lorsqu'il manipule une information, il doit se demander si elle ▶

UN JUGE SE BASE SUR UN FAISCEAU DE PRÉSOMPTIONS

Lazaro Pejsachowicz RSSI de la CNAM TS partage l'opinion de Cédric Foll, RSSI de l'Education Nationale en matière d'analyse des logs issus des systèmes informatiques : *« On ne peut pas tout traiter de façon automatique. Le problème central est bien celui du « lien » entre les logs. Des traces par ci par là, on en a tous. Je ne crois pas à la corrélation de façon automatique. En revanche, je crois à une politique de « lien » pragmatique. Et au fait de se fixer un certain nombre d'objectifs limités et modestes. Et à partir de là, petit à petit, on commence à automatiser »*.
Des questions supplémentaires se posent si l'on entend générer des traces qui puissent servir de preuve vis à vis d'un juge : *« On essaie alors de créer une trace forte afin de montrer qu'une personne a agi d'une certaine façon. Or, des preuves irréfutables je n'en connais pas. Prouver l'identité, une action et le lieu est très difficile. On pourrait se décourager. Mais un juge travaille avec un faisceau de présomptions. On doit donc mettre en place des traces dans ce but. L'authentification forte en est une. Mais il faut y ajouter d'autres traces ou d'autres éléments qui ne sont pas des traces, mais que l'on présentera au juge »*. Ceci sans oublier *« Qu'il faut agir et réunir des traces selon les procèdures et le cadre réglementaire en vigueur, sinon la preuve tombe à l'eau. Le travail avec les juristes de l'entreprise est donc indispensable »* termine **Jean-Patrick Lengrais, RSSI à la Société Générale**. ■

est confidentielle ou au niveau secret, et selon la sensibilité de cette information, utiliser tel ou tel mécanisme. *« Avec les solutions de DLP Endpoint* (NDLR : DLP pour les points terminaux, et les périphériques*), il y a la possibité d'informer l'utilisateur sur le fait qu'il va envoyer un email ou un message électronique qui est confidentiel. »*

> **Faire attention aux outils dits "intelligents" qui deviennent vite chronophages**
> ***Gilles Berthelot***
> *Pompiers de Parisr*

Des sondes et des moteurs d'analyse

« Il ya deux types d'outils sur le marché » constate quant à lui, le Lieutenant-Colonel Gilles Berthelot. D'une part, on trouve les solutions qui dépendent de la classification faite par l'utilisateur sur le degré de confidentialité. Il faut alors faire confiance au responsable fonctionnel pour classifier son document. Il faudra alors se méfier autant « du paranoïaque que du naïf ». Et d'autre part, il y a les outils qui travaillent à partir d'une politique de sensibilité de l'information de l'entreprise. Ces outils sont capables de détecter la circulation de l'information qui pourrait être critique. *« Il s'agit de faire confiance à des sondes et à des moteurs d'analyse d'emails et de syntaxe, mais avec toute la prudence nécessaire autour de ces outils qui sont censés être très intelligents, mais qui deviennent vite chronophages si ils ne sont pas pertinents »*. Ce type de projet est long pense également Zbigniew Kostur et il convient de faire vivre la politique de sécurité associée, en particulier sur les filtrages mis en place et qui doivent évoluer.

Si le DLP paraît neuf sur le marché, en fait dès 2003, des solutions de protection de mails disposaient de fonctions similaires. Elles proposaient alors de ne montrer que les parties de documents chiffrés autorisées au lecteur, selon ses rôles dans l'entreprise et selon la politique de sécurité. *« Nous avions testé ce type de solution en mode externalisé, mais c'était peut être trop en avance sur son temps »,* se souvient Gilles Berthelot. Aujourd'hui, la gestion de l'identité a fait son chemin et la notion de rôle existe dans l'entreprise. *« C'est la brique de base, car avant de gérer des rôles, il faut avoir identifier tous ces rôles et identifier les personnes qui remplissent ces rôles. Maintenant que cette démarche a été faite, les entreprises sont peut-être plus réceptives au DLP et à la classification de documents. »*

> **L'absence d'une gestion fine des droits empêche la traçabilité**
> ***Eric Doyen***
> *Crédit Immobilier de France*

La définition des rôles prend du temps

Les projets de gestion des identités dans l'entreprise demeurent malgré tout longs à déployer. Outre la question du ROI, on bute sur la définition des rôles; l'automatisation du provisionning des comptes des utilisateurs au sein des applications et de leurs droits. Eric Doyen témoigne. Pour le Crédit Immobilier de France qui emploie 2800 personnes, il a abouti à la définition de 200 rôles, ce qui doit pouvoir être encore optimisé, car une des difficultés des projets d'IAM (Identity and Access Management) demeure la rationnalisation des rôles. Bénéfice : la gestion des droits s'en trouve renforcée. *« Auparavant, on fonctionnait par clônage des droits, ce qui empêchait toute traçabilité. Des personnes qui avaient dix ans d'ancienneté possédaient pléthore de droits, car au fil des postes, les autorisations n'étaient pas supprimées »*. Désormais un workflow est en place, géré par les ressources humaines. Ce qui est un atout car de nombreux projets d'IAM sont portés uniquement par l'IT et ne sont perçus que comme facteur de réduction des coûts lors de la création des comptes, ou via des dispositifs de type self service permettant de récupérer son mot de passe si on l'a oublié. Au Crédit Immobilier, les tickets de gestion des comptes des utilisateurs seront poussés de façon automatique lors d'une deuxième phase vers les applications internes. Le processus étant pour l'heure réalisé par les équipes IT.

Investir dans l'humain

Reste que si le choix et la mise en place des technologies sont importants, le facteur humain a aussi son rôle à jouer, notamment *« en des temps économiquement durs, où il vaut mieux penser à sensibiliser l'humain, plutôt que d'investir dans des solutions très complexes. »*, réfléchit François Gratiolet. Un avis qui est partagé par Gilles Berthelot, pour qui *« toutes les solutions techniques ne sont rien si les gens ne sont pas convaincus de l'utilité de protéger les données qu'ils manipulent »*. Il précise de plus que ce facteur humain dépend de l'entreprise, et cite l'exemple des pompiers où le système militaire permet d'être coercitif et d'imposer des politiques strictes, alors que d'autres entreprises ne sont pas adaptées à ce fonctionnement. *« Il faut que le management suive des séances de sensibilisation, ce qui entraîne le reste des équipes »* conclut Zbygniew Kostur. ■

Jean-Pierre Blettner

PETIT DÉJEUNER-CIO-METRIXWARE

CONFÉRENCE ORGANISÉE LE 30 JUIN 2009 PAR CIO

Piloter son patrimoine applicatif

Les applications informatiques d'une entreprise sont un patrimoine précieux qu'il s'agit de faire fructifier. Quatre grandes entreprises ont témoigné de leurs initiatives en la matière lors d'un événement organisé le 30 juin dernier par CIO et Metrixware, spécialiste de l'Application Portfolio Management et de la Gouvernance IT.

Les logiciels d'une entreprise représentent un coût mais aussi un patrimoine qu'il s'agit de faire fructifier. Or, trop souvent, l'état de ce patrimoine est méconnu et il n'existe pas de tableau de bord permettant de le faire évoluer en toute connaissance de cause. Il est pourtant vital pour les managers IT de mettre en place un pilotage de leur parc applicatif qui intègre toutes leurs contraintes : évolutions des métiers, budgets, ruptures technologiques, ressources humaines. Le tout en s'appuyant sur l'état réel de l'existant. Comment réussir une telle démarche ? C'est le thème stratégique qui a été traité le 30 juin dernier, lors d'un événement organisé par la rédaction de CIO et Metrixware, au centre Kléber à Paris.

Quatre témoignages

Une table ronde sur le thème de « *La gouvernance du patrimoine applicatif au bénéfice des performances de l'entreprise* » a été l'occasion de détailler concrètement les initiatives de quatre grandes entreprises. Pour les participants de la table ronde, c'est l'optimisation des coûts qui est à l'origine de leur démarche. Phat-Chua Lim, DSI de CNP Assurances, société d'assurance et de prévoyance et René Kraft, directeur général délégué du GIE Informatique de la Caisse des Dépôts et Consignation ont particulièrement détaillé les aspects qualimétriques. Cette approche mesure la qualité d'écriture technique des programmes. Elle facilite le pilotage de la sous-traitance, notamment en matière de TMA. Quant à Philippe Vibien, responsable de l'architecture des systèmes d'information de la banque d'investissement de la Société Générale (SGCIB) et Laure Tissinier, en charge du patrimoine applicatif au sein de la structure informatique du Groupement des Mousquetaires (Stime), ils ont montré comment quatre axes donnent la valeur de leur patrimoine applicatif : coûts financiers, ressources humaines, évolution des besoins métiers et des technologies.

Une mesure à l'occasion d'une migration

A la CNP Assurances, tout est parti de la migration vers un Mainframe d'IBM, il y a deux ans et demi. *« Nous avons alors constaté l'étendue de notre patrimoine applicatif »* se souvient Phat-Chua Lim. Afin de réduire les coûts, le nettoyage des programmes inutiles a été lancé, ainsi que l'analyse de la qualité - maintenabilité et évolutivité - des codes conservés. A la Caisse des dépôts, la démarche d'optimisation est venue des équipes internes et a comporté plusieurs benchmarking applicatifs afin de se comparer à des structures IT d'entreprises similaires. Puis le patrimoine a été évalué en termes de points-fonctions et des métriques associées. S'y ajoute comme à la CNP l'appréciation de la qualité des applications. *« Le tout est cadré dans une feuille de route d'évolution des technologies et des architectures »* indique René Kraft.

Anticiper à trois ans

A la Stime, la démarche a été initiée en 2004 par la modélisation des processus métiers, puis par le recensement des applications sous-jacentes. Et depuis deux ans, la DSI s'est penchée sur le portefeuille applicatif dans un esprit de gouvernance. *« L'objectif est de connaître le patrimoine applicatif afin de maîtriser sa transformation, d'anticiper l'évolution des métiers et l'obsolescence technique, de tenir à jour les compétences des équipes, le tout à un coût acceptable »* décrit Laure Tissinier. A la SGCIB, *« Le catalyseur est venu de la direction qui a demandé que la stratégie informatique soit clarifiée »*, explique Philippe Vibien. Trois axes ont été retenus afin d'évaluer le patrimoine : les coûts (quelles applications coûtent cher ?), la technique (conformité par rapport aux standards internes, et qualimétrie sur les applications critiques), et la capacité à porter l'évolution du métier (les investissements nécessaires). *« Nous voulons anticiper et disposer d'une vision à trois ans »* commente Philippe Vibien.

Pour en savoir plus

CIO

Retrouvez la vidéo **de la conférence** sur **CIO TV**

Côté tableaux de bord et indicateurs, point trop n'en faut. *« Des indicateurs, il y en a plein, il n'y a qu'à regarder la norme 9126. La difficulté c'est de choisir les plus pertinents par rapport à son parc et à son* ▶

activité. S'il y a trop d'indicateurs on ne sait plus piloter », souligne René Kraft. Philippe Vibien confirme qu'*« il ne faut pas sombrer sous les indicateurs, mais les restituer intelligemment, et pouvoir au besoin aller en profondeur. »*, et Laure Tessinier insiste sur leur pérennité, afin de disposer d'une vision dans le temps. *« Une information qui n'est pas représentative handicape au final le modèle, qui doit pouvoir vivre avec l'évolution du système d'information. »*, prévient, pour sa part, Vincent Ruelland, directeur des opérations de Metrixware.

20% des applications pour 80% des coûts

A la SGCIB, le focus est mis sur certaines applications. *« Il s'agit d'analyser les 20 % d'applications qui représentent 80 % des coûts. »* conseille Philippe Vibien. Il souligne que le critère coût doit guider les actions, en intégrant les coûts récurrents (infrastructure, maintenance évolutive et corrective) et ceux des projets. L'obsolescence des technologies doit également être regardée car elles constituent un avantage concurrentiel. Phat-Chua Lim s'attache à la qualité des codes informatiques et à la mesure d'impact, indispensable lors du nettoyage de code. René Kraft confirme l'importance de la robustesse et de l'évolutivité. Quant à Laure Tissinier, elle insiste sur l'évolution des compétences des équipes. Au global, Vincent Ruelland de Metrixware précise que si les concepts de qualimétrie sont bien compris et qu'il existe des outils sur le marché, il n'en est pas encore de même pour la gouvernance de plus haut niveau. *« C'est plus innnovant, chaque entreprise doit créer son propre modèle et arriver à le faire vivre »*.

La qualimétrie pour abattre les difficultés

Comme pour tout projet, il existe des difficultés. Phat Chua Lim souligne l'intérêt de la qualimétrie afin de dialoguer avec les sous traitants. Mais en interne, *« Il est difficile au début de faire adhérer les équipes car elles peuvent avoir un sentiment d'être espionnées, puis elles comprennent qu'il s'agit d'une aide. »* René Kraft revient sur la difficulté de définir les bons indicateurs. Ce à quoi adhère Laure Tissinnier qui y ajoute le défi de suivre les coûts dans une structure très globalisée. A la SGCIB, une étape qui a pris du temps est la normalisation du plan de classement des applications, par fonction. *« Afin que chacun parle le même langage pour des fonctions identiques »* indique Philippe Vibien. Le ROI n'aura pas été un frein. *« La gouvernance est un outil pour répondre à une demande des métiers »* justifie Philippe Vibien. De même à la Stime, le ROI n'a pas été évalué autrement que par la satisfaction de disposer d'une vision complète du patrimoine applicatif. Vincent Ruelland rappelle que *« quand on met en œuvre ce genre de solution, on s'adresse à une population très large au sein de l'entreprise »*. Le dialogue est donc important. « *Il s'agit d'un outil de progrès et non d'espionnage. »*

La confiance n'exclut pas le contrôle

En ce qui concerne les prochaines étapes, Phat-Chua Lim entend se diriger vers une phase de contrôle. Puis il mettra en place un outil de gouvernance. Quant à René Kraft, il veut : *« installer définitivement la cellule qualimétrie. Et la mettre au service de l'amélioration de la qualité de la production. »* Pour Laure Tissinier, c'est la mise en place de la qualimétrie qui constituera la prochaine étape. Enfin, Philippe Vibien estime que l'effort doit être porté sur le lien entre le patrimoine applicatif d'un côté et la gestion des portefeuilles de projets de l'autre. Il fait de plus remarquer que des initiatives viennent d'autres pôles de la Société Générale, et qu'il s'agit de les fédérer. Ce que confirme Isabelle Sipma, directrice de la stratégie du système d'Information du Groupe Société Générale, également présente lors de l'événement. Elle affirme la volonté d'une démarche transverse sur les six pôles métiers de la banque. Un plan d'actions ambitieux que l'on ne peut que recommander à l'ensemble des entreprises. ■

MARIER LES DÉMARCHES DE QUALIMÉTRIE ET DE GOUVERNANCE

Metrixware est un spécialiste de l'Application Portfolio Management et de la Gouvernance IT. Une discipline qui consiste à déliver aux DSI des informations ad hoc afin de piloter leur portefeuille applicatif.Les éléments de décision sont technologiques, économiques, métiers et humains, et cela pour chaque application. Fondée sur ces éléments, la gouvernance du patrimoine applicatif permet d'améliorer la qualité de service délivrée aux métiers tout en planifiant les évolutions du système d'information. On peut alors abouter deux démarches. La première consiste à évaluer la qualité des programmes avec des indicateurs de maintenabilité, d'évolutivité, et de fiabilité. La seconde prend en compte les angles financiers, techniques, de couverture métiers et les aspects humains. *« Souvent objectifs, ces critères peuvent aussi être subjectifs. C'est par exemple le cas de la satisfaction, qui peut être un indicateur valable pour une population assez importante »* indique Vincent Ruelland directeur des opérations de Metrixware. Ces différents facteurs sont ensuite pondérés afin d'être pertinents par rapport à l'entreprise, puis regroupés dans un tableau de bord simple et synthétique à destination des décideurs. ■

Pour en savoir plus

CIO

Retrouvez la vidéo sur **CIO TV**

Bien traiter les V.I.P sans mettre en péril la DSI

Dirigeants, commerciaux stars, avocats, traders, élus de collectivités locales : tous ces V.I.P ont leurs lubies et leurs caprices. Ce ne sont pas de simples utilisateurs que l'on peut traiter de façon standard. Pour autant, ils doivent respecter des règles de base.

Selon que vous serez puissant ou misérable, les jugements vous rendront blanc ou noir, disait déjà Jean de Lafontaine dans *Les animaux malades de la peste*. Il en est de même pour les V.I.P en entreprise vis-à-vis de l'informatique. Lorsqu'un utilisateur de base a un ennui avec l'informatique ou formule un souhait quelconque, il est renvoyé aux procédures standards et sa demande sera traitée selon les priorités, les budgets et les choix techniques préalables de l'organisation.

Mais le pouvoir hiérarchique du DSI cesse d'opérer quand il s'agit des V.I.P (Very Important Person) qu'il s'agisse de ses propres supérieurs (PDG, DG, DAF,...) mais aussi des autres cadres dirigeants ou, dans le secteur public ou associatif, des élus. Ces V.I.P ont parfois des exigences ou des attentes particulières que les DSI se doivent de satisfaire sans trop discuter. Et ce n'est pas toujours simple si l'on veut garder un minimum de cohésion au système d'information. Aborder cette question du traitement des VIP avec des DSI n'est pas évident. La plupart ont des anecdotes mais refusent d'en parler officiellement. Heureusement, les associations de DSI peuvent s'exprimer sur les généralités et les anciens de la fonction se souviennent de leurs propres expériences.

> **Les VIP veulent du simple et du fiable**
> ***Didier Lambert***
> *ancien président du Cigref et ancien DSI d'Essilor*

Un statut au contour à définir

Qui est VIP et aura droit à un statut privilégié ? *« La définition est très élastique car il n'y a aucun texte pour la réglementer, au contraire de la notion de cadre, par exemple »* soupire Jean-Pierre Corniou, ancien DSI de Renault et ancien président du Cigref, aujourd'hui directeur général adjoint du cabinet Sia Conseil. Il convient : *« Il y a toujours des tempêtes émanant de ceux qui n'obtiennent pas ce statut. Etre VIP est une question très sensible, très politique. Doit-on le réserver aux seuls membres du Comité Exécutif ? Mais on n'imagine pas qu'un directeur général rédige lui-même tous ses emails, il faut donc déclarer VIP les collaborateurs directs d'un membre du Comité Exécutif. Et il y a aussi les directeurs de filiales, surtout à l'étranger. Définir le périmètre des VIP est le premier écueil à franchir quand un DSI traite cette question. Chez Renault, nous avions une liste assez généreuse d'une centaine de personnes. »*

Egalement ancien président du Cigref et, par ailleurs, ancien DSI d'Essilor, Didier Lambert, confirme : *« être VIP est une question statutaire, les VIP étant ceux qui se croient plus importants que les autres. Classiquement, leur nombre dans une grande entreprise va d'une dizaine à une centaine et comprend le Comité Exécutif, les directeurs de filiales et les autres managers de rang 1. Leurs caractéristiques, c'est d'avoir un temps très précieux, qui coûte bien plus cher que celui d'un simple employé ou d'un cadre, et de se déplacer intensivement, y compris dans des contrées exotiques. »*

L'animal politique pas si dangereux

De son côté, le secteur public, en particulier les collectivités locales, a sa particularité : les élus. *« Beaucoup d'élus n'ont aucune sensibilité informatique et n'ont donc aucune exigence particulière »* tempère cependant Daniel Rigault, président du Coter-Club, le club des DSI de collectivités locales. Il ajoute cependant : *« lors d'élections, il peut y avoir des changements brutaux d'attitude de la part des élus, surtout s'il y a des changements de majorité. Dans une ville, récemment, le maire a pris la décision politique d'une bascule vers le logiciel libre. La DSI a dû procéder à des migrations non prévues et en dehors de tout plan initial d'évolution du système d'information. Ce type de décision brutale peut arriver mais c'est globalement rare. La plupart des difficultés n'ont pas lieu avec les élus mais, très classiquement, avec les cadres supérieurs. Mais si cela peut être une gêne* ▶

Pour en savoir plus
CIO
Retrouvez le témoignage de **la Ville de Metz,** cité par **Daniel Rigault** sur **CIO Online**

> **L'exemple vient d'en haut, les VIP doivent respecter les règles communes**
>
> ***Jean-Pierre Corniou***
> *ancien président du Cigref et ancien DSI de Renault*

occasionnelle pour tel ou tel technicien, le « traitement VIP » ne bouleversera jamais les priorités du service. La réparation d'un plantage de serveur, par exemple, restera prioritaire quoiqu'il arrive. »

Pour Didier Lambert, *« il y a trois races de VIP. La première est celle des techno-résistants pour qui un clavier n'est bon qu'à mettre entre les mains d'une secrétaire. Ceux là disparaissent par l'effet de renouvellement des générations. Puis il y a les VIP normaux qui attendent des TIC que cela serve leurs besoins et ceux de l'entreprise, d'une façon rationnelle. Enfin, les plus dangereux, ce sont les techno-fans qui craquent sur tous les gadgets à la mode et s'attendent à intégrer tous ces outils dans leur panoplie »*.

VIP service

On en vient ainsi au deuxième écueil du traitement des VIP : définir les services particuliers auxquels ils ont droit et leurs privilèges, en marge des normes générales. Daniel Rigault note : *« Quand un cadre supérieur reçoit en cadeau ou s'offre un objet communiquant comme un iPhone ou un Blackberry, il faut vite le lui mettre en route, lui paramétrer sa messagerie, etc. Parfois, cela peut impliquer que l'on doive acheter des connecteurs sur les logiciels du système d'information ce qui, bien sûr, n'était ni budgété ni prévu. Cependant, la standardisation en cours améliore nettement les choses sur ce point précis. »*

La gouvernance du système d'information, la gestion de la sécurité et toutes les bonnes pratiques peuvent être mises à mal par un VIP. Jean-Pierre Corniou estime : *« l'exemple ne peut venir que d'en haut et il est donc important que les V.I.P respectent les normes. J'ai toujours essayé de promouvoir les normalisations, même si certains éléments statutaires comme les Blackberrys sont parfois difficiles à éviter. Il est également dur de résister quand certains supérieurs craquent sur tous les derniers gadgets à la mode et en exigent l'intégration dans le système d'information. »* Didier Lambert se réjouit : *« J'avais réussi à interdire les Blackberrys »*.

Garantir un service sur un périmètre précis

Il est donc parfois compliqué de faire comprendre à ses supérieurs, sans culture technique, qu'il faut respecter certaines normes et mesures de sécurité. Mais au delà des *« arrangements »*, les VIP ont malgré tout de véritables besoins particuliers de niveau de service. *« Théoriquement, un VIP devrait disposer de tous les services du système d'information en permanence, 24 heures sur 24, 7 jours sur 7, où qu'il soit dans le monde »* décrit Jean-Pierre Corniou. Mais il admet aussitôt : *« en fait, aucun dirigeant ne lancera d'opération comptable. Par conséquent, ce qui est vraiment important pour un VIP, c'est le poste de travail au sens large (poste fixe, portable, PDA...) avec la messagerie et, pour certains, quelques services supplémentaires comme le fil Reuters pour les DAF. Le principal problème devient alors le détourage : parvenir à garantir un niveau de service particulier pour quelques personnes sur une partie précise du système d'information. »*

Pour Didier Lambert, *« en fait, les VIP ont des besoins spécifiques simples qui relèvent de la capacité à travailler en bureautique et messagerie y compris à l'autre bout du monde. Pour eux la fiabilité est plus importante que la rapidité. Les liaisons rapides sont plutôt à réserver à ceux qui en ont besoin, comme ceux qui surveillent en astreinte les processus applicatifs. »* ▶

Pour en savoir plus

CIO

Retrouvez l'interview de départ à la retraite de **Didier Lambert** sur **CIO Online**

6000 € POUR MODIFIER UNE PRÉSENTATION POWERPOINT

Le traitement particulier du VIP entraine des coûts spécifiques. Il y a bien sûr les outils particuliers en eux-mêmes (smarphones,...) mais surtout les services caractérisant les privilèges accordés ou leur assurant une certaine sécurité. Un niveau de service est choisi par arbitrage entre le coût et le besoin métier. Si le niveau de service augmente, son coût augmentera en général plus vite. Jean-Pierre Corniou professe : *« le soin accordé aux VIP est coûteux et il faut qu'ils en soient conscients. Chez Renault, j'avais mentionné une ligne spécifique dans le budget de la DSI intégrant autant les personnels dédiés que les services externalisés ou les petites attentions comme les kits internationaux de prises électriques. Une telle démarche fonctionne bien et sert l'image de la DSI auprès de la DG. Le service VIP est légitime car les dirigeants en ont un réel besoin pour se connecter à l'entreprise dans toutes les situations mais le coût doit être identifié. A l'époque où j'étais DSI de Renault, Carlos Ghosn était à cheval sur deux systèmes d'information indépendants (Renault et Nissan) et était une semaine au Japon, une en France et la troisième aux Etats-Unis. »*. Didier Lambert a une approche radicalement opposée. *« Pour moi, il n'est pas utile de faire apparaître le coût des VIP de manière spécifique car cela reste extrêmement marginal. En revanche, il faut faire attention et les sensibiliser régulièrement. J'ai vu une fois un VIP parti à l'étranger échanger pour des modifications et des relectures, un certain nombre de fois, une présentation Powerpoint avec sa secrétaire. Ce qui s'était traduit par une note de 6000 €. Les tarifs de roaming de données sont prohibitifs comme chacun sait. Nous avions, cette fois, là, négocié avec l'opérateur une remise après coup mais signalé l'incident au VIP. »* ■

Brancher un gadget mobile peut impliquer d'acheter des connecteurs logiciels qui n'étaient pas budgétés

Daniel Rigault
président du Coter-Club

La notion de qualité de service est essentielle. Les niveaux associés (SLA) sont définis selon les besoins de l'entreprise et ont un coût. Les VIP sont prompts à réclamer un SLA plus élevé sur certains aspects particuliers. Mais c'est au DSI de leur rappeler ce coût et qu'il ne s'agit pas de servir la vanité de telle ou telle personne. Malgré tout encore, des SLA plus élevés peuvent avoir un sens. *« Puisqu'ils doivent être joignables et travailler en permanence, les VIP peuvent bénéficier d'un sous-ensemble de règles particulières comme un changement ou une réparation du poste de travail à domicile, y compris dans une résidence secondaire à la campagne. Chez Renault, nous nous étions aussi posé la question de la ligne ADSL personnelle des membres du Comité Exécutif et à qui nous permettions un accès au système d'information en télétravail via un VPN »* stipule Jean-Pierre Corniou. Mais Didier Lambert réagit : *« normalement, un VIP n'a pas à traiter des questions dans l'urgence. S'il doit s'occuper d'urgences au lieu de stratégie, c'est qu'il y a quelque chose qui ne va pas dans l'organisation de l'entreprise »*.

Si le VIP utilise son propre matériel

Une telle maintenance proche de l'utilisateur VIP est plus simple qu'auparavant. Le navigateur devient le seul logiciel d'accès au système d'information, si celui-ci est « 100% web ». Cela devient plus compliqué s'il reste des logiciels en client lourd, et qu'il faut assurer leur bon fonctionnement n'importe où dans le monde puisqu'il faudra opérer sur le contenu même de la machine en cas de souci.

« Séparer les usages personnels de ceux professionnels est de plus en plus compliqué. La question devient explosive » concède Didier Lambert. Il ajoute : *« Reste que les VIP sont suffisamment peu nombreux pour que chacune de leurs demandes soit étudiée au cas par cas. Tout doit être vu au travers de deux questions : 'est-ce que la demande sert l'intérêt de l'entreprise ?' et 'Est-ce que c'est dangereux pour l'entreprise ?'. Il ne peut pas y avoir de réponse générale, d'autant que les technologies et les limites bougent sans arrêt. »*

Et si le VIP utilise son propre matériel, qu'il s'agisse d'un smartphone ou d'un PC, n'est-il pas tenté de solliciter la DSI pour l'aider en cas de panne ? Daniel Rigault rectifie : *« les prestations comme la réparation d'un ordinateur personnel restent discrètes, gérées « entre amis ». Pour éviter une extension de ce genre de choses, nous avons cependant décidé, dans ma communauté d'agglomérations, de ne pas revendre le matériel obsolète au personnel qui pourrait dès lors considérer que la DSI doit assurer l'après-vente. Cependant, la DSI doit bien traiter, parfois, l'apparition de virus ou d'autres problèmes sur des PC portables professionnels qui n'ont pas servi qu'à du travail. »*

Le traitement VIP peut frôler l'abus de bien social

Didier Lambert alerte sur l'aspect pénal du traitement des VIP : *« le DSI est là pour servir l'intérêt de l'entreprise, pas pour répondre aux demandes narcissiques et statutaires. Dans certains cas, on peut en arriver à commettre un abus de bien social ou à en être complice. Par exemple, les ressources de l'entreprise ne peuvent pas être utilisées pour délivrer un service personnel comme le dépannage d'ordinateur personnel, surtout à domicile, fournir du matériel à usage privé ou entretenir celui-ci. »* Il soupire : *« mais les plus problématiques sont les techno-fans qui viennent nous voir avec des problématiques d'informatique personnelle - comme des traitements sophistiqués dans Photoshop- totalement inconnues des informaticiens d'entreprise. »*

Pour en savoir plus

Legifrance

L'abus de bien social est défini dans l'article L242-6 du Code de commerce. L'alinéa 3 peut plus particulièrement s'appliquer au détournement des ressources informatiques pour un usage personnel.
sur
www.legifrance.gouv.fr

5 RAISONS POUR LESQUELLES LE DSI DOIT SE MÉFIER DES VIP

1. **L'informatique -comme l'intendance- doit toujours suivre les décisions** stratégiques, les évolutions d'organisation ou les déménagements. Dès lors, on ne demande pas son avis au DSI avant de prendre une telle décision et d'ailleurs pourquoi lui donner un budget ?
2. **L'informatique fait désormais partie des sujets traités dans la presse économique et généraliste**. Le PDG peut suivre les tendances et adopter lui-même la dernière mode, comme son épouse après la lecture des pages habillement. Quand ce n'est pas la faute de l'ordinateur, c'est donc celle de la presse.
3. **Les smartphones, iPod et autres objets communiquant sont des cadeaux plutôt courants.** Et il peut sembler normal que le directeur utilise le cadeau de sa femme ou de son fournisseur favori en le connectant au système d'information de l'entreprise. Enfin, s'il arrive à le faire marcher ou sinon, il faudra obligatoirement lui montrer comment faire !
4. **La vie d'un VIP c'est son entreprise.** Demander au help-desk comment on branche une console Wii ou comment on détoure une photographie de vacances sur Photoshop semble donc bien naturel.
5. **Au final, l'abus de bien social, c'est pour les autres.** Mobiliser les moyens de l'entreprise au service personnel d'un VIP, quoi de choquant ? Servir les demandes narcissiques et statutaires ne fait-il pas partie des tâches du DSI ?

> **Si un VIP doit traiter des questions dans l'urgence, c'est qu'il y a quelque chose qui ne va pas dans l'organisation**
>
> ***Didier Lambert***
> *ancien président du Cigref et ancien DSI d'Essilor*

Rappelons que l'article 314-1 du Code Pénal dispose que *« l'abus de confiance est puni de trois ans d'emprisonnement et de 375000 euros d'amende »* tandis que l'abus de bien social est lui puni par l'article L242-6 du Code du Commerce *« d'un emprisonnement de cinq ans et d'une amende de 375 000 euros »*. Voilà de quoi faire réfléchir un VIP trop exigeant. Certes, il n'y a pas encore de jurisprudence sur le détournement de help-desk ou de service de maintenance.

Savoir accueillir la demande du VIP

Certains VIP ont tendance à décrocher leur téléphone pour appeler directement le DSI au moindre souci. Il y a quelques années, un DSI d'un groupe du CAC 40 avait ainsi déclaré : *« je suis plus rapidement au courant quand l'email du PDG est en panne que quand notre ERP est planté ! »* Or passer par le DSI n'est pas vraiment ce qu'il y a de plus efficace, sauf peut-être pour marquer son statut, l'intervention devant de toute façon être réalisée par les techniciens appropriés. Le DSI ne pourra donc, au mieux, que lui-même décrocher son téléphone pour appeler l'équipe technique du help desk.

Jean-Pierre Corniou se souvient : *« chez Renault, l'identifiant de l'appelant au centre support permettait au répondant de savoir tout de suite qu'il avait affaire à un VIP. »* Au delà de l'affichage d'une gentillesse particulière, le répondant avait besoin de l'information, puisqu'elle lui permettait de savoir que la configuration utilisée différait légèrement de la norme générale. Un autre DSI confie anonymement : *« J'ai créé un help desk spécifique pour mon PDG car j'ai failli perdre mon poste parce qu'il n'avait pas été dépanné efficacement alors qu'il se trouvait à l'étranger. »*

LES BONNES PRATIQUES FACE AUX VIP

- **Rappeler que la DSI est là pour servir l'entreprise,** pas pour satisfaire des demandes personnelles.
- **Avoir une bonne vision du système d'information de l'entreprise,** de son architecture et de sa sécurité afin de répondre avec des arguments rationnels aux demandes particulières.
- **Toujours ramener les demandes particulières à une réponse aux deux questions fondamentales** : est-ce utile pour l'entreprise ? Est-ce dangereux pour l'entreprise ?
- **Sensibiliser régulièrement les VIP aux bonnes pratiques** en insistant sur leur rôle essentiel et leur responsabilité particulière.
- **Inciter les VIP à suivre des formations** adaptées à leurs besoins particuliers.
- **Veiller à la sécurité des objets mobiles,** de l'ordinateur portable au smartphone, notamment en chiffrant les disques durs et les e-mails.
- **Veiller à la sécurité des échanges de données** via des réseaux privés virtuels (VPN) mais aussi en cryptant les messages échangés.
- **Rappeler qu'un VIP, stratège de l'entreprise,** n'a pas (normalement) à prendre une décision dans l'urgence puisque le traitement des alertes relève des niveaux hiérarchiques inférieurs.
- **Savoir laisser des traces écrites** des consignes de sécurité afin de se dédouaner en cas d'incident.

« Le signalement en help-desk est plus pertinent qu'un help-desk dédié, qui resterait inutilisé la plupart du temps et coûterait très cher » juge pour sa part Didier Lambert. Il ajoute : *« sauf pour des raisons diplomatiques, le signalement est même inutile dans la plupart des cas si le traitement en niveau 1 est suffisant. Pour ma part, j'avais cependant mis en place un niveau 2 spécifique avec un spécialiste des communications par tous les moyens partout dans le monde et de tous les objets mobiles, ce qui est le vrai besoin particulier des VIP. »*

Eduquer ses VIP

Il n'en demeure pas moins que l'idéal est l'autonomie maximale des personnels dans leur usage des outils informatiques, VIP inclus. Or, d'un côté, les besoins de flexibilité des VIP sont particulièrement élevés : ils peuvent être à la campagne ou à l'autre bout du monde, avoir des besoins en dehors des horaires normaux des centres informatiques, etc. De plus, les VIP sont nettement moins arrangeants que la moyenne, affirmation du statut oblige. Ils peuvent disposer d'outils spécifiques, non choisis par la DSI voire non maîtrisés par elle (en particulier des objets mobiles et communiquant). Dès lors, les VIP doivent recevoir une formation afin de devenir autonomes face aux outils qu'ils utilisent mais aussi pour adopter de bonnes pratiques nécessaires à la sécurité de l'entreprise, dont ils ont d'ailleurs la charge en tant que dirigeants.

« Celui qui posera une question paraîtra stupide une fois ; celui qui ne pose pas de question restera stupide toute sa vie, dit le proverbe chinois. Il faut donc savoir inciter les VIP à poser des questions. Et même affronter l'écueil de faire admettre à un VIP qu'il a besoin d'une ▶

> **Il faut savoir faire preuve de pédagogie**
>
> ***Jean-Pierre Corniou***
> *ancien président du Cigref, ancien DSI de Renault*

formation » souligne Didier Lambert. Mais faire suivre des formations bureautiques en groupe à des VIP relève de l'impossible. Tant pour des questions d'emploi du temps que de besoins particuliers ou de défense du statut, il faut des cours particuliers aux contenus personnalisés. *« Il est important d'éduquer les VIP et cela fait partie du rôle du DSI de faire de l'andragogie, comme disent nos amis québécois, c'est à dire de la pédagogie pour adultes responsables »* professe Jean-Pierre Corniou. Il donne ainsi des exemples : *« mettre un mot de passe sur son PDA est le minimum minimorum. Il faut également ne jamais laisser un ordinateur portable dans une voiture si celui-ci contient des documents non-chiffrés. »*

Les prémunir contre le vol d'information

Pour Didier Lambert, *« la question n'est pas propre qu'aux seuls VIP mais à tous les personnels nomades et susceptibles de disposer d'informations importantes, ce qui inclut notamment les commerciaux et les juristes de base. Et là, la règle était simple chez Essilor : le disque dur de chaque ordinateur portable était chiffré en totalité avant qu'il ne quitte les locaux de l'entreprise. Pour les échanges par courriels, un outil supplémentaire de chiffrement était mis en place. »* En effet, un peu comme beaucoup de ménages veulent ignorer que la majorité des cambrioleurs passent par la porte, beaucoup de VIP imaginent que seuls des hackers cassant les sécurités logiques du système d'information voire se branchant sur les câbles réseaux du bâtiment peuvent pirater leurs précieuses données.

En réalité, crocheter la portière d'une automobile ou passer dans le couloir central du TGV pendant que le propriétaire d'un ordinateur est parti aux toilettes restent des méthodes courantes pour voler des machines avec tous leurs documents confidentiels. Plus discrètement, il suffit simplement parfois de copier quelques fichiers du répertoire « Mes Documents » d'un ordinateur allumé (mais au propriétaire absent) sur une clé USB.

Responsabiliser les VIP

> **Les délits d'initié et l'espionnage industriel existent !**
>
> ***Didier Lambert***
> *ancien président du Cigref et ancien DSI d'Essilor*

Didier Lambert rappelle que *« il n'y a pas que le secteur nucléaire ou la Défense Nationale à devoir faire très attention : les délits d'initiés et l'espionnage industriel, cela existe ! »* Quant à Jean-Pierre Corniou, il avertit : *« si un patron s'en moque ou n'est pas exemplaire, la réalité peut le rattraper plus vite qu'il ne le croit et le mettre davantage en péril lui que l'entreprise »* Une source de fuites est en effet assez aisément identifiable dans beaucoup de cas. Et la faute est bien caractérisée par une imprudence majeure qui sera peu appréciée par un Conseil d'Administration ou une Assemblée Générale d'actionnaires. Le tout est, comme à chaque fois qu'un supérieur hiérarchique commet une faute susceptible de retomber sur le DSI, de conserver les avertissements prodigués (e-mails, notes de service, rapports...). *« Ceci dit, aucune sécurité informatique n'est vraiment absolue et il est important de rappeler régulièrement aux VIP que si une information est vitale pour l'entreprise, il ne faut pas la mettre sur un support informatique »* affirme Didier Lambert.

Faire pour le mieux et positiver

« Face aux VIP, le DSI doit faire preuve de pédagogie et de souplesse tactique » conseille Jean-Pierre Corniou. Sa marotte lui aura d'ailleurs été d'un grand secours : *« la gouvernance, que je défends depuis toujours, permet d'objectiver la relation, de fixer les règles en expliquant pourquoi elles existent. Après, tout est plus simple, même avec les VIP. »* Quant à Didier Lambert, il se souvient : *« Chez Essilor, j'avais la chance d'avoir des VIP très raisonnables mais, de toute façon, le rôle du DSI est de servir l'entreprise, pas de récompenser un statut, même si ce statut existe et se justifie parce que le temps de travail des VIP est précieux. »*

Le traitement des VIP est enfin en lui-même un bon exercice pour les DSI. Selon Jean-Pierre Corniou, *« c'est la partie visible de l'iceberg. Si l'on est capable d'assurer un bon service aux VIP, c'est que, derrière, le système d'information est bien conçu. Et si l'on est capable d'isoler un budget spécifique pour le service aux VIP, c'est que le DSI a une bonne vision des coûts de chaque prestation et des niveaux de service demandés à chaque prestataire ou à chaque département. »* Pour Didier Lambert, *« vouloir être à tout prix populaire auprès des VIP est un piège et constitue un grand danger. Le travail d'un DSI est de faire tourner l'entreprise, pas de servir des égos. »* Jean-Pierre Corniou se réjouit : *« Discuter des SLA et des coûts associés avec les VIP a, en plus, une immense vertu pédagogique pour eux ! »*. Didier Lambert martèle quant à lui : *« j'ai passé mon temps à lutter contre l'idée que le statut donnait des droits particuliers, notamment en terme d'outils. Ce n'est pas le statut qui donne de tels droits mais le besoin professionnel dans l'intérêt de l'entreprise et uniquement lui. »* ■

Bertrand Lemaire

PUBLI-REDACTIONNEL

CONFÉRENCE STRATÉGIQUE

CONFÉRENCE ORGANISÉE LE 23 JUIN 2009 PAR CIO

Gérer les risques à l'heure du Cloud et de la mobilité

A l'ère du mobile roi, du Web 2.0 et du Cloud Computing, la sécurité de l'entreprise est à repenser. Cette question clé a réuni une centaine de responsables de systèmes d'information en juin dernier lors d'une conférence organisée par les rédactions de CIO et du Monde Informatique.

Sous la pression des nouvelles menaces venues d'internet, et devant la multiplication des outils de communication déployés hors du contrôle de la DSI, le Cloud Computing en tête, il devient urgent de repenser la sécurité informatique en entreprise. Le tout sans freiner pour autant l'activité des métiers. Tel est le thème de la journée organisée sous le titre « *La sécurité comme facilitateur du business* » par les rédactions de CIO et du Monde Informatique et qui a réuni une centaine de responsables IT à l'Automobile Club de France (Paris), le 23 juin dernier.

En ouverture, Hervé Schauer, expert en sécurité, est intervenu au nom du Clusif, le Club de la Sécurité Informatique Français. Il a martelé : *« On a perdu la maitrise des postes de travail »* placés en périphérie du système d'information *« ils sont très facilement compromis »*. De plus, les employés contournent de plus en plus la DSI en utilisant leurs propres outils de « *chat* » ou de partage de documents en ligne. Ils transfèrent des informations sur leur smartphone ou sur des clés USB. Mais leur capacité à faire plusieurs choses à la fois est un atout que l'entreprise ne doit pas négliger. C'est donc à la sécurité de s'adapter !

Encadrer le Cloud Computing

En préalable, l'analyse des risques s'impose. Cette tâche demeure un travail pointu qui devra s'inspirer des référentiels tels que l'ISO 27001, l'ISO 27005, le CRBF 97-02, Cobit ou Eebios. Telle est la recommandation de la table ronde qui a réuni Jean-Louis Bleicher, directeur du pôle Sécurité de la Banque Fédérale des Banques Populaires, Patrick Clément, RSSI d'Areva et Thierry Auger, RSSI du groupe Lagardère. Quant aux nouvelles technologies comme le Cloud ou le Saas, elles ne doivent pas être stoppées, mais encadrées.

Cette indépendance des collaborateurs exige une nouvelle génération de protections. *« Il faut protéger les accès Web, y compris le Web 2.0, se protéger contre les menaces mails, et empêcher les fuites d'information »* insiste Guillaume Girard, spécialiste sécurité chez Websense. Avec le DLP (Data Loss Prevention), il s'agit de *« différencier un vrai processus métier d'une fuite d'information »* souligne-t-il. Le bon type de donnée est-il envoyé par la bonne personne au bon endroit, et de quelle façon ?

Prévenir les risques de vol internes

Le risque de vol d'information est souligné également par Olivier Bodot, Technical Services Manager chez McAfee, pour qui les outils de prévention de la perte de données (DLP), de gestion des risques et de la conformité sont capitaux. *« Ces outils sont particulièrement nécessaires en temps de crise, quand les licenciements peuvent augmenter les risques de vol en interne »* constate-t-il. Websense comme Olivier Bodot pointent les risques liés au Web 2.0 et l'arrivée du Spear Phishing, un phishing très ciblé plus difficile à combattre. McAfee défend l'idée d'une protection basée sur la « *réputation* ». Il s'agit de 'noter' un site selon plusieurs vecteurs de réputation : l'adresse IP, le nom de domaine, l'URL, les contenus et les fichiers images.

Le poste de travail apparaît au centre de toutes les préoccupations. *« La stratégie des entreprises est souvent de rajouter des briques pour répondre à chacun des problèmes (codes malveillants, correctifs, contrôle* ▶

des applications), en faisant le choix du Best-of-breed. Cela revient de plus en plus cher » prévient Frédéric Guy, ingénieur avant-vente chez Trend Micro, partisan d'une protection via une console unique, grâce à laquelle on gère des modules supplémentaires, comme le DLP.

Face à l'augmentation des risques de fuites, le recours au chiffrement est plébiscité. Mais il doit être ciblé par population dans l'entreprise. Quant au DLP, il commence tout juste à être évalué et nécessite une classification des informations. Telle a été une des conclusions de la table ronde réunissant Zbiginew Kostur, expert sécurité, ancien RSSI de Nexans, Gilles Berthelot, Lieutenant-Colonel, Chef des S.T.I des Pompiers de Paris et François Gratiolet, RSSI adjoint du Groupe La Poste.

Chiffrer la voiture et non l'autoroute

Autre défi : les mobiles. Ils accèdent naturellement à internet, et hébergent un volume croissant de données sensibles. *« Pour autant, il faut garder le même niveau de sécurité et de confiance »* affirme Daniel Jouan, responsable commercial grands comptes chez RIM, qui commercialise la solution BlackBerry®. *« Nous avons choisi de chiffrer la voiture (les données) et non l'autoroute (le réseau). Cela allège la facture du client, notamment en situation de roaming. De plus, la seconde solution est souvent instable et trop gourmande pour la batterie du mobile »* relève-t-il. Une autre technologie mise en place par RIM consiste à définir des périmètres d'activité selon les applications. Par exemple, le GPS ne débordera pas inutilement sur l'infrastructure de l'entreprise tandis qu'une application de CRM sera cantonnée au seul réseau du client. Enfin, Daniel Jouan rappelle les atouts d'une administration à distance du parc mobile : effacement du terminal, verrouillage ou déverrouillage, déploiement de la politique de sécurité. Point important : *« La sécurité doit être sans compromis, et la plus transparente possible. Sinon, soit l'utilisateur essaiera de la contourner, soit il n'utilisera pas la solution »* termine-t-il.

Un réseau intelligent détecte les anomalies

Outre la mobilité, une autre tendance est le recours généralisé à l'externalisation et à l'éclatement des organisations entre de nombreux sites. Les équipements réseaux se multiplient. *« On fait face à une accumulation de systèmes d'exploitation hétérogènes, ce qui en complique la gestion »* décrit Laurent Paumelle, consultant avant-vente chez Juniper Networks, qui penche pour une convergence du réseau en termes de systèmes d'exploitation afin de gagner en stabilité et de réduire la complexité. Le réseau, une fois déployé, doit jouer lui-même le rôle de garde barrière. Il s'accompagnera d'un contrôle d'accès suffisamment fin pour suivre chaque utilisateur (groupe, machine utilisée, lieu d'accès, comportement). *« Une machine non conforme sera refusée, ou acceptée partiellement »* précise Laurent Paumelle. Les événements enregistrés par le réseau permettent ainsi de détecter tout comportement anormal. Par exemple, un utilisateur se connecte sur son PC de bureau, mais il n'a pas validé son entrée dans l'entreprise.

Cette question de l'authentification demeure récurrente. Elle a été examinée lors d'une table ronde réunissant Cédric Foll, RSSI de l'Education Nationale, Ludovic Tardy, responsable réseau de l'agence TBWA, Antoine Bajolet, délégué à la sécurité des systèmes d'information de TDF, Jean-Patrick Lengrais, RSSI à la Société Générale et Lazaro Pejsachowicz, RSSI de CNAM TS. La boîte à outils du RSSI déborde d'options parmi lesquelles il faut piocher à bon escient entre PKI, OTP (One Time Password) et NAC (Network Access Control). Autre constat : la supervision de la sécurité demeure un défi.

Automatiser les processus de sécurité

La sécurité périmétrique a explosé. *« On a évolué vers une sécurité périphérique liée au poste de travail »* résume Sergio Ribeiro, architecte technique Senior chez Avocent LANDesk. Il attire l'attention sur une priorité : automatiser les processus de déploiement et de maintenance d'une politique de sécurité. Un recueil de bonnes pratiques comme ITIL permet de structurer le déploiement de correctifs de sécurité : quel est l'impact ? Qui est responsable ? Idem pour la réinitialisation d'un mot de passe, la gestion des ports USB, etc. Mais si le workflow paraît simple, *« il est souvent bloqué par les objectifs divergents des différentes équipes (sécurité, déploiement, support) »* déplore Sergio Ribeiro. Il défend une approche dans laquelle l'utilisateur ne puisse pas contourner le workflow, et donc la sécurité. *« En améliorant la visibilité, on améliore la prise de décision. »*

Symantec, pour sa part, constate qu'il est temps de résoudre le hiatus entre les briques techniques déployées sur le terrain (NAC, DLP, chiffrement), et la gouvernance, la gestion des risques et les politiques de sécurité. D'énormes gains sont réalisables grâce à l'automatisation. *« La sécurité doit être transparente pour l'utilisateur, afin qu'il puisse travailler en toutes circonstances. On ne s'attache plus au support, mais à l'utilisateur et à l'information »* affirme Jérôme Asseray, ingénieur avant vente chez Symantec. Il conclut sur un élément clé : *« Il faut impliquer les métiers dans la sécurité. Ils sont les seuls à savoir quelles sont les informations qui ont de la valeur »*. Sans oublier l'indispensable sensibilisation de l'utilisateur final, sans l'adhésion de qui rien ne peut réussir. ■

Comment un DSI issu des métiers peut être crédible

Comment un DSI qui vient d'une fonction non-informatique peut-il être crédible et pertinent pour diriger un service hautement technique et spécialisé comme une DSI ? Caroline Apffel, associée au cabinet de conseil en ressources humaines Heidrick & Struggles, répond.

CIO : *Auparavant, tous les DSI étaient issus d'une filière technique informatique. Pourquoi y-a-t-il désormais des DSI issus du métier ?*

Caroline Apffel : parce que la technique pour la seule technique n'a pas de sens. Et les DSI issus de la technique informatique ont souvent été critiqués précisément pour leur manque de proximité avec les métiers. La question se posera cependant différemment selon la nature de la DSI dans l'organisation. Si la DSI est une fonction de support technique dans une industrie elle-même marquée par une culture d'ingénieur, cela n'aura rien à voir avec une entreprise où la DSI est « *au coeur du business* ».

> **Un DSI issu du métier s'impose par son approche managériale**
>
> ***Caroline Apffel***
> *Heidrick & Struggles*

CIO : *Est-ce que n'importe quel directeur métier peut « s'improviser » DSI ?*

Caroline Apffel : non, naturellement. D'abord, tout dépend de la place de la DSI dans l'organisation ainsi que du problème à résoudre par la nomination du nouveau DSI et de la place relative entre le métier et la technique. Si le problème à résoudre est managérial, l'entreprise ira chercher un manager et, dès lors, on peut pratiquement dire que cela importe peu qu'il vienne du métier ou de la technique informatique. C'est évidemment très différent si le problème est un marasme technique, qui est un cas où un vrai technicien sera sans doute nécessaire. Enfin, s'il faut réaligner la DSI sur le métier, un DSI issu du cœur de ce métier est une solution pertinente. Par exemple, dans la distribution, le DSI viendrait plutôt de la logistique, de la supply-chain ou des achats. Mais on a vu des DSI issus de la finance lorsque le problème à résoudre était la gestion des coûts, les budgets d'investissements et leur impact sur les marges opérationnelles. De fait, tout dépend de la raison pour laquelle on est allé chercher un DSI métier, ce qui impliquera la nature exacte du profil recherché. Mais, dans tous les cas, le DSI a comme mission d'assurer l'interface entre la direction générale, les directions métiers ou support et les équipes informatiques. Bien entendu, nous parlons ici d'organisations d'une certaine taille où il y a de vraies équipes techniques et un historique technologique.

CIO : *Alors, justement, face à ces équipes informatiques, comment un DSI issu du métier peut-il être crédible sur la technique qui reste tout de même centrale dans l'activité d'une DSI ?*

Caroline Apffel : la question n'est pas simple. Il faut tout d'abord que ce nouveau DSI soit présenté en complément de son équipe technique, et non pas en concurrence avec elle. Un DSI issu du métier n'a pas à expliquer à des techniciens compétents leurs disciplines ou à vouloir s'arroger des compétences dont il ne dispose pas. Il faut clairement expliquer la raison de son recrutement, de sa présence à la tête de la DSI, de ce qu'il va apporter pour valoriser l'expertise technique des équipes internes auprès des directions métiers et de la direction générale. Dans d'autres cas, le DSI sera amené à trancher des choix stratégiques mais sans, de lui-même, en général, faire des choix révolutionnaires sur le plan technique : il va regarder des critères managériaux ou financiers, de bon sens, non des critères techniques, même si la solution est innovante. Un DSI issu du métier s'impose par ce type d'approche, pas par une approche techno-technologique. Mais les équipes techniques ne sont pas plus bêtes que n'importe qui : si on leurs explique les raisons de la venue du DSI issu du métier, elles sont capables de l'entendre. Le travail du DSI est alors d'assurer l'interface avec la direction générale et les autres directions. Et un Directeur Général ou un directeur métier n'ont strictement rien à faire de la puissance d'un serveur ou de la bande passante du réseau pourvu que les applicatifs fonctionnent et répondent à leurs besoins. ■

Bertrand Lemaire

Pour en savoir plus

CIO

Retrouvez **Caroline Apffel,** associée chez Heidrick & Struggles sur **CIO Online**

« Flemmarder » au travail améliore la productivité

Flâner sur internet au boulot rend plus productif selon notre confrère CIO américain qui publie l'opinion de Mike Elgan blogueur spécialisé dans les nouvelles technologies. Il donne les huit raisons pour lesquelles cela améliore la qualité du travail.

Les 'flemmards' qui vont passer un peu de temps sur Facebook ou sur Twitter uniquement pour le plaisir sont plus productifs que ceux qui ne font que travailler, tout le temps. C'est ce qu'affirment des chercheurs de l'université de Melbourne avec une nouvelle étude (http://uninews.unimelb.edu.au/news/5750/). Les résultats indiquent qu'en moyenne, les employés qui utilisent internet dans un but personnel pendant leurs heures de travail sont plus productif de 9 % par rapport aux autres.

Mon expérience en tant que patron, qu'employé et que blogueur pour la revue Computer World, spécialisé dans les technologies et leur impact sur l'attention et la productivité me pousse à penser que les chercheurs n'ont regardé qu'une petite pièce du puzzle que constitue la gestion de l'attention. J'estime en effet que non seulement les 'flemmards' au bureau sont plus productifs que ceux qui ne pensent qu'à travailler, mais que de plus ceux qui travaillent depuis chez eux sont encore plus productifs. Et la plupart du temps pour les mêmes raisons.

L'hypothèse des chercheurs est que les employés qui font ce qu'ils appellent de la « *navigation internet pour le plaisir sur leur lieu de travail* » sont plus concentrés après cette pause. Mais cette explication n'est peut-être pas suffisante. Voici huit raisons pour lesquelles j'estime que le surf à but personnel sur internet améliore la productivité.

⊷ *Le subconscient continue de travailler :*

Contrairement au travail physique, qui s'arrête en même temps que le travailleur, l'esprit continue de travailler sur les choses auxquelles on ne pense plus consciemment. Cet efficace processus de résolution des problèmes intervient quand vous surfez sur internet pour la détente, quand vous regardez la TV, et notamment quand vous dormez. Flemmarder sur internet aide ce processus en mettant en retrait la réflexion consciente, qui est enclin à rester bloquée sans trouver de solution.

⊷ *Ça vous aide à vous débarrasser de vos problèmes personnels :*

Si vous êtes inquiet à propos de vos enfants, que votre épouse vous manque, ou qu'un problème personnel vous tracasse, vous ne serez pas pleinement concentré sur votre travail. Les réseaux sociaux, Twitter et les e-mails personnels vous permettent d'entrer rapidement en contact avec vos amis et votre famille, de savoir ce qui se passe, et de retourner au travail avec toute votre attention.

⊷ *L'amélioration des relations de travail :*

Les entreprises dépensent des fortunes en exercices et en sorties de « team-building », qui ne créent des liens que parce que tous subissent les mêmes interactions forcées. Les réseaux sociaux, en revanche, créent des relations de travail sans coût pour l'employeur. Oui, les gens parlent avec leurs amis et leur famille, mais aussi très couvents avec leurs collègues, ce qui favorise de plus le travail d'équipe.

⊷ *Les interactions en temps réel deviennent des interactions asynchrones :*

Une interaction sociale contrôlée par quelqu'un d'autre (c'est à dire une interruption) peut être dévastatrice pour l'attention. Une irruption inattendue de cinq minutes à peine de la part d'un collègue peut vous faire revenir en arrière d'une heure dans le travail. Ce genre d'interactions nuisibles pour la concentration est autorisé et même encouragé sur le lieu de travail, tandis que l'on se méfie des réseaux sociaux, ou qu'ils sont tout simplement interdits. Pourquoi ? Les interactions sociales sur Facebook ou Twitter sont, par définition, contrôlées par l'utilisateur. Elles interviennent donc entre, et non pas pendant des moments de grande concentration. Ces outils permettent une concentration productive sans l'interrompre.

⊷ *Les employés sont plus heureux :*

Les gens détesteront leur job s'ils ont vraiment envie de se connecter sur Twitter, Facebook ou Youtube pendant la journée, et qu'on les en empêche. Mais s'ils sont autorisés à vagabonder en ligne, ils seront en revanche plus heureux. Et des employés heureux sont des employés plus productifs. ▶

↔ *La « mauvaise flemmardise » est remplacée par de la « bonne flemmardise » :*

Si vous imaginez que personne n'a jamais perdu du temps au travail avant l'arrivée d'internet, vous vous trompez. Les gens perdent un temps énorme au travail à cause d'un bureau mal rangé, d'une mauvaise gestion des tâches qu'ils ont à mener, des bavardages de couloir, de longues conversations téléphoniques et... des réunions ! Toutes ces activités ressemblent et sont ressenties comme du travail car elles fatiguent l'esprit et consomment les heures. Et parce que les gens doivent toujours remplir leurs objectifs et respecter leurs dates butoirs, ce temps passé sur internet a souvent tendance à remplacer non pas le travail productif, mais plutôt les autres activités inefficaces.

↔ *Internet est éducatif :*

Surveiller les blogs, les flux RSS et Twitter introduira forcément les employés à de nouvelles techniques de gestion de leur temps, et stimulera leur esprit d'une autre manière. Par exemple, cet article que vous lisez pourrait vous être professionnellement utile d'une manière ou d'une autre. Mais ne devriez-vous pas plutôt travailler ?

↔ *L'esprit ne peut être enfermé :*

Vous pouvez forcer un employé à être présent dans un bureau, mais vous ne pouvez pas forcer son esprit à le suivre. L'esprit humain est une curieuse machine. Ne lui donnez rien d'autre à faire que travailler, aucun moyen pour satisfaire sa curiosité ou son désir d'interactions sociales, et il se rebellera. Plus précisément, il rêvassera, vagabondera. Il cherchera des moyens de saboter le travail des autres employés (car ça, au moins, c'est intéressant). En un mot, il emploiera son ingéniosité naturelle à trouver des moyens de ne pas travailler. Donnez lui la possibilité d'aller sur internet, et il ira chercher ce dont il a besoin quand il en a besoin, puis reviendra stimulé, inspiré et éduqué à un travail productif.

Et nous en venons aux télétravailleurs, aux « nomades numériques », et à la raison qui fait qu'ils sont les plus productifs des employés. J'estime que cela vient du simple fait qu'ils ne sont pas supervisés, et qu'ils peuvent surfer librement sur internet quand ils le désirent et pour n'importe quelle raison. Comme tous les télétravailleurs ou tous les travailleurs mobiles vous le diront, ils établissent un rythme pour conjuguer travail et détente sur internet, et maximiser leur efficacité dans l'un comme l'autre. Il est temps pour les décideurs d'abandonner leurs vieux préjugés, et de considérer les employés comme des télétravailleurs. ■

Mike Elgan, CIO.com US

PETIT DÉJEUNER-CIO-IBM-SOGETI

CONFÉRENCE ORGANISÉE LE 2 JUILLET 2009 PAR CIO

Testing as a Service

Le 2 juillet dernier, Le Monde Informatique et CIO ont organisé une réunion d'information sur le marché émergeant du « Testing as a Service », en partenariat avec SOGETI et avec la participation d'IBM Rational. Selon le cabinet PAC, cette formule représente en effet d'ores et déjà 15 % des activités de test logiciel et affiche cette année encore une croissance de près de 25 %.

Comment faciliter l'accès au testing logiciel dans un contexte de pression budgétaire ? En partenariat avec SOGETI et IBM Rational, Le Monde Informatique et CIO ont organisé cet été une conférence sur les solutions « Software Testing as a Service » (STaaS), dont la rapide montée en puissance est confirmée par les études. Selon Arnold Aumasson, consultant senior du cabinet PAC, ce marché émergeant a en effet progressé de plus de 30% en 2008 et va de nouveau croître de près de 25 % cette année, dans un contexte économique pourtant dégradé. Selon l'analyse du consultant, il n'y a là aucune contradiction, dans la mesure où le test "on demand" apporte justement de nouvelles réponses aux impératifs de contrainte budgétaire et de qualité des logiciels.

Tester pour garantir la qualité

En l'occurrence, les gains du STaaS lèvent effectivement 4 freins au développement du testing : des délais de mise en œuvre jugés trop longs, une gestion des ressources humaines complexe, des coûts qui restent élevés et la difficulté de suivre de façon constante l'évolution des normes et des meilleures pratiques. Sur ces différents points, l'externalisation du testing ouvre de nouvelles perspectives, qui pourraient notamment faciliter l'accès à cette activité pour les moyennes entreprises.
Sur cette base, François Darphin, Directeur de l'Offre Testing chez SOGETI, a rappelé la nécessité de définir une stratégie de test qui permet de suivre la qualité tout au long du cycle de vie des logiciels, sachant que le travail de test reste trop souvent considéré comme l'étape finale du développement. C'est notamment le rôle de l'approche TMap (Test Management Approach). Une observation complétée par Mathieu Pedelahore, responsable du centre de test de Bordeaux de SOGETI : *« La formule STaaS permet de réduire les délais de mise en œuvre à moins de 2 semaines et permet de réduire le coût du testing d'environ 25%. Au-delà, les bénéfices constatés portent sur un paiement à l'usage, les engagements de résultat et sur le fait qu'il n'est pas nécessaire de mettre en place une équipe socle avant de lancer un projet »*.

Industrialiser les tests pour en réduire le poids

L'accès à ces différents atouts demande toutefois un préalable : selon Philippe Gohin, Consultant Testing chez SOGETI, de tels résultats sont obtenus grâce à une industrialisation du travail de test, en se fondant sur des outils et des méthodes tels que RMC (Rational Method Composer), proposé par IBM Rational.
Pour Jean-Claude Vauthier, Consultant d'IBM Rational, l'un des premiers enjeux de cette industrialisation est ainsi de passer d'une approche « corrective » du testing à une approche « décisionnelle ». *« Lorsqu'ils sont gérés de manière traditionnelle, les tests peuvent représenter de 20 à 40% du cycle de développement des logiciels »*, a-t-il précisé.

Réduire les délais de retour sur investissement

En conclusion de cette matinée, Michel Speranski, Market Manager chez IBM Rational, a présenté la solution de Testing as a Service qu'IBM a mis en place en interne, notamment à destination de ses 35 000 développeurs. Associant la virtualisation, l'automatisation et la standardisation, la solution déployée par IBM amène à parler de « cloud testing ». Dans ce nouveau contexte, Michel Speranski a indiqué que les délais de provisionnement des tests étaient passés de plusieurs semaines à quelques minutes, tandis que les périodes de retour sur investissement des nouvelles applications ne se mesuraient plus en années, mais en mois. ■

Pour en savoir plus

CIO

Retrouvez la vidéo **de la conférence** sur **CIO TV**

Les directeurs marketing veulent de l'agile, du simple, du fonctionnel

Les directions marketing ont des attentes contradictoires vis-à-vis de l'informatique. Elles veulent une DSI agile tactiquement mais qui conserve une rigueur méthodologique structurante. Explications de Jean-Michel Raicovitch co-président de l'Association Nationale du Marketing.

CIO : En quoi les TIC impactent-elles les directions marketing ?

Jean-Michel Raicovitch : le métier et la pratique du marketing changent en profondeur à cause de l'évolution des TIC, notamment pour tout ce qui se rattache au web. Nous disposons désormais d'un lien direct avec le client dans la plupart des secteurs (services, distribution,...) et des types de clients (particuliers, entreprises). Le rôle même du marketing change car, d'un rôle de stratège, nous acquérons aussi un rôle dans la distribution. En particulier, nous devenons acteurs du marketing relationnel au travers du e-commerce, des programmes de fidélité (où l'informatique est indispensable) et de la prise en compte de la relation multi-canal (au delà du magasin, le téléphone, le web, la télévision interactive,...). Le secteur des études est également chamboulé avec l'apparition des panels en ligne. La direction marketing, de ce fait, travaille de plus en plus avec des prestataires informatiques comme les Web Agencies. Notre métier devient sans cesse plus complexe, plus riche, avec des dimensions technologique (informatique...) et financière (obligation de prouver un retour sur investissement de nos actions) croissantes. Pour accompagner ces changements, l'Adetem (Association Nationale du Marketing) a créé plusieurs groupes de travail, dont l'un sur le web 2.0.

CIO : Quels sont les besoins des directions marketing vis à vis des DSI ?

Jean-Michel Raicovitch : nos enjeux sont globalement dans le champ de la gestion de la relation clients (GRC) au sens large avec les segmentations et les typologies de clientèle, la mise en place du e-commerce, la mise en œuvre d'outils de marketing relationnel. Les besoins diffèrent selon le secteur d'activité. Dans la distribution en grandes surfaces, le marketing dispose d'énormément d'informations détaillées sur les clients. A l'opposé, dans l'automobile, le client vient au mieux une fois par an en concession en délivrant des données aux commerciaux. Dans les banques ou le transport aérien, ce sont des situations intermédiaires. Le marketing a alors certes besoin de s'appuyer sur un socle technique solide pour que les outils fonctionnent effectivement et avec des données fiables mais doit aussi disposer d'outils flexibles et agiles, capables d'évoluer de façon itérative et souple. Bref, tout ce que détestent les DSI.

CIO : Jusqu'où doit aller cette flexibilité ?

Jean-Michel Raicovitch : nous sommes conscients que le système d'information est un château de cartes fragilisé à force d'y coller des verrues. Mais notre besoin est qu'il prenne en compte nos besoins fluctuant, évoluant au fil d'itérations, et qu'il soit ouvert à de nombreux outils tiers, y compris à des ►

VERS UN CO-PILOTAGE DES WEB-AGENCIES

La direction marketing travaille de plus en plus avec des prestataires qu'il faut bien qualifier d'informatiques, notamment les web-agencies. Or le pilotage des prestataires informatiques dont les oeuvres vont devoir s'interfacer avec le système d'information est traditionnellement du ressort de la DSI. Comment éviter le divorce entre la DSI et la direction marketing au sujet de la garde des sites web ? *« Il ne faut pas un travail séquentiel avec la DSI, puis la direction marketing, puis le prestataire mais un travail en équipe, un co-pilotage de la web agency par la DSI et la direction marketing »* plaide Jean-Michel Raicovitch, co-président de l'Adetem. Il soupire : *« les agences ne sont pas toujours très industrielles dans leur approche et nous avons besoin de la validation technique par la DSI mais sans brider la créativité des agences. Le DSI doit donner une caution technique mais le donneur d'ordre doit rester la direction marketing. »* Les DSI veulent parfois maîtriser tous les budgets plus ou moins en rapport avec les TIC afin de rationaliser, transversaliser et mutualiser les dépenses. *« C'est évidemment louable mais il ne faut pas que cela devienne un prétexte pour défendre un territoire et bloquer l'agilité de l'entreprise »* termine Jean-Michel Raicovitch. ■

Pour en savoir plus

adetem
L'ASSOCIATION NATIONALE DU MARKETING

Retrouvez **l'Adetem,** sur son site web **www.adetem.org**

interactions avec des systèmes d'information d'autres sociétés quand ce n'est pas tout simplement d'interagir avec des utilisateurs finaux. Nous avons donc des conflits avec les *« vieux »* DSI accrochés à leurs normes techniques rigides comme si leur vie en dépendait. Mais, à l'inverse, nous pouvons aussi avoir des conflits avec de *« jeunes »* DSI qui ont au contraire tendance à s'affranchir du *« Legacy »*, du socle solide qui a tout de même l'avantage de mettre à disposition des données fiables et structurées. Il faut que le DSI accepte de nourrir les bouleversements du métier. Par exemple, jadis, dans la vente à distance, il y avait deux catalogues par an, un en été et l'autre en hiver. Aujourd'hui tout est en ligne et bouge sans cesse, avec des promotions personnalisées ou très ponctuelles. Nous avons donc besoin d'un nouveau calage. Certes, il faut tester les applications et les développer avec rigueur mais s'il faut trois mois pour commencer à disposer de quelque chose pour soutenir une opération, c'est trop tard : l'opération est finie. Il faut que le DSI soit capable d'agilité tactique tout en conservant la rigueur méthodologique structurante.

CIO : Pour atteindre cet objectif et ainsi servir vos besoins, qu'attendez-vous des DSI pour leurs propres pratiques professionnelles ?

Jean-Michel Raicovitch : Aujourd'hui, la vie de l'entreprise exige que tout le monde travaille en équipe, qu'il y ait une véritable collaboration horizontale. Il faut faciliter le travail en laissant à chacun une grande liberté d'action même si c'est aussi le rôle de certains -comme le DSI- de poser des règles pour que l'ensemble fonctionne harmonieusement. Cela suppose par exemple d'accepter de construire, sur de bonnes fondations, un échafaudage en bambous et de ne passer au béton que si c'est vraiment utile. Pour répondre aux besoins fluctuants du marketing, il faut certes s'appuyer sur un système d'information solide mais il n'est pas toujours nécessaire de développer une application qui ressemble à une cathédrale quand il s'agit de pique-niquer : une nappe à carreaux suffit. Le DSI doit être *« time to market »*, sans faire de l'art pour l'art. Nous voulons du souple, de l'agile, du simple, du fonctionnel. Il faut désacraliser la technique. Un excellent scientifique ou technicien ne se cache pas derrière des acronymes ou un jargon incompréhensible pour impressionner son auditoire mais au contraire est capable d'expliquer simplement ce que ses interlocuteurs doivent savoir pour comprendre. Ce qui pourrait parfois être intéressant, ce serait une DSI éclatée dans les services et qui co-rédigerait les cahiers des charges et co-piloterait les projets à partir des directions opérationnelles comme le marketing. Cela permettrait d'associer l'indispensable compétence technique à la compétence métier. Air France est un bon exemple de ce type de fonctionnement. D'un autre côté, que la DSI génère des boites noires n'est pas gênant pourvu que les entrées comme les sorties correspondent aux attentes.

CIO : De quels outils avez-vous besoin au quotidien ?

Jean-Michel Raicovitch : très peu de choses, finalement : tout ce qui tourne autour de la GRC, avec des outils de « requêtage » dynamique, des outils de décisionnel, des analyseurs de campagnes, une gestion dynamique des sites web qui permette de changer la « homepage » d'un site sans refondre le système d'information.

CIO : Et si vous ne deviez dire que quelques mots à un DSI ?

Jean-Michel Raicovitch : Soyez des co-acteurs dynamiques du changement de l'entreprise ! Sans vous, on ne peut plus rien faire mais il faut répondre aux défis des entreprises qui ont du mal à survivre dans le contexte actuel. ■

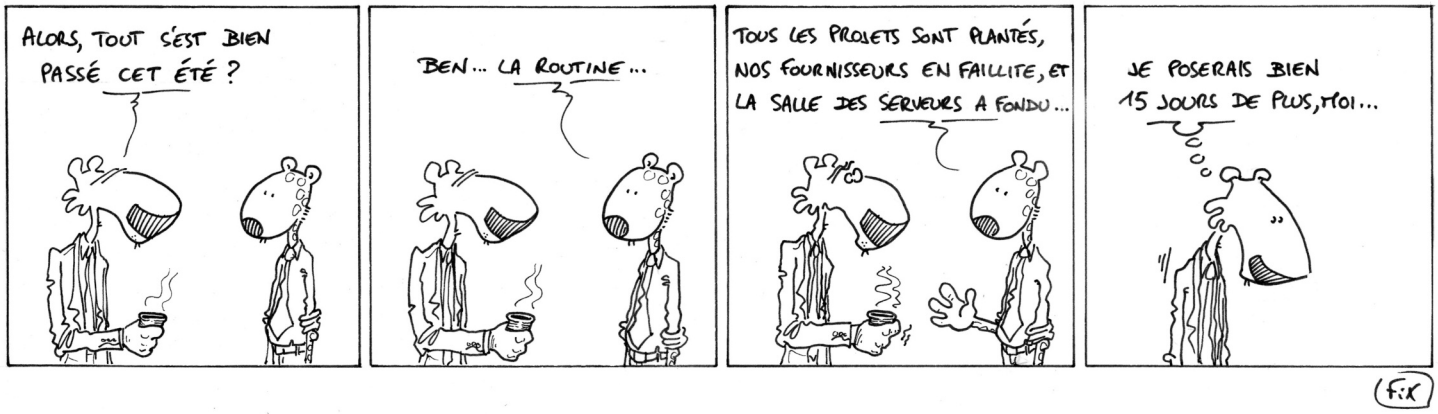
Bertrand Lemaire

COMMENT ÉNERVER SON DIRECTEUR MARKETING

- **Dire *« non, c'est impossible »*** avant même que le directeur marketing ait fini de parler.
- **Invoquer la sécurité** du système d'information toutes les trois phrases.
- **Ne pas comprendre qu'on puisse développer** une application périphérique à usage ponctuel sans un cahier des charges de mille pages, trois mois de réunions, six mois de développement, trois mois de tests, douze mois de mise au point, trois douzaines de certifications qualité et le respect d'une quinzaine de référentiels de bonnes pratiques.
- **Ne pas être en mesure de garantir la fiabilité** du socle technique du système d'information et des données générées.
- **Honorer une bible de normes techniques** rigides comme si c'était le troisième Testament de la Parole de Dieu.
- **Rester dans sa tour d'ivoire** (sa salle serveurs...) au lieu d'être co-acteur des projets métiers.
- **Quand, enfin, le DSI a obtenu son siège légitime** au Comité Exécutif, être tellement barbant et jargonneux qu'on le replace aussitôt sous l'autorité du DAF.

HUMEUR

RETOUR DE VACANCES



CIO EVENEMENTS 2009

Inscrivez-vous dès à présent aux conférences 2009 sur cio-online.com

DECISIONNEL 22 septembre 2009 - Paris

En période d'incertitude, le décisionnel apporte l'indispensable analyse des performances pour le pilotage de l'entreprise. A côté des plates-formes généralistes, des solutions métiers émergent. L'heure est à la démocratisation de la business intelligence.

JOURNÉE FORUM – SOA - Cloud Computing – Saas 6 octobre 2009

Maîtrise des coûts, recentrage sur le cœur de l'activité et exigence d'une meilleure réactivité poussent les entreprises à rechercher toujours plus d'agilité pour leur système d'information. Comment faire en sorte que la SOA tienne sa promesse d'enrichissement de l'informatique par les métiers ? Comment bénéficier de la souplesse apportée par le Cloud Computing et le Saas ?

MATINÉE DÉMATÉRIALISATION 15 octobre 2009

Sous la pression d'internet, la dématérialisation des processus et des documents s'impose au sein des entreprises et des organismes publics. L'heure est au basculement sur des solutions globales, efficaces de bout en bout, après le succès des projets départementaux afin de doper la compétitivité et les performances de l'entreprise.

BANQUE FINANCE 19 novembre 2009

En pleine crise économique et à l'heure des fusions/acquisitions, les banques doivent réussir rapidement leurs multiples chantiers de mise en conformité réglementaire et l'industrialisation de leurs plates-formes de services.

AMELIORER LA PERFORMANCE DE SON SI 26 novembre 2009

Le bon service au bon prix : dans ces périodes tendues d'un point de vue économique, une des missions clé de la DSI est d'arbitrer la qualité de service du système d'information selon les objectifs stratégiques de l'entreprise pour chacun des services délivrés.

SOMMAIRE N°10 - OCTOBRE 2009

Une publication de :
IT NEWS INFO - 6/8, rue Jean-Jaures 92800 Puteaux • Tél.: 01 41 97 61 45
Directeur de la rédaction : Jean-Pierre Blettner • jpblettner@it-news-info.com
Chef des informations : Bertrand Lemaire • blemaire@it-news-info.com
A collaboré à ce numéro : Vivien Derest
Principaux associés : Adthink Media et International Data Group Inc.
Président: Bertrand Gros
Directeur de publication : Marc Lavigne Delville

Directeur général : Jean Royné
Président du groupe Adthink Media : Sylvain Morel
Réalisation : Rémy Beaudégel
SEPIA Studio - 6 rue Jules Simon 92100 Boulogne
CIO est édité par IT NEWS INFO, SAS au capital de 3 000 000 €
Durée de la société :
jusqu'au 7/09/2106
Siret : 500 034 574 00029 RCS Nanterre