CIO
MANAGEMENT DES SYSTÈMES D'INFORMATION

N° 55 - SEPTEMBRE 2012 - 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

Le job de DSI se complique. Les défis traditionnels de la fonction sont déjà ardus. Il suffit de voir le faible pourcentage de projets informatiques qui sont livrés dans les délais et les budgets. L'émergence de la société numérique fragilise encore le temple dont le DSI doit rester le gardien. Les risques sont démultipliés à l'heure du Cloud et de l'utilisateur « Roi ».

SOMMAIRE

RETOUR D'EXPÉRIENCES

La gestion des risques informatiques en pleine tourmente

Du BYOD aux réseaux sociaux en passant par le Cloud Computing ou les menaces persistantes avancées, la gestion des risques IT doit prendre en compte de nouveaux phénomènes. Sans oublier une réglementation en pleine évolution ainsi qu'une population d'utilisateurs issue de la génération Y.

Les entreprises sont sous pression. Leur démarche de gestion des risques et la politique de sécurité associée doivent s'adapter rapidement face aux technologies émergentes, aux nouvelles menaces et à l'évolution des usages. Et il y a fort à faire depuis trois ans, avec l'arrivée des menaces persistantes avancées (MPA), le phénomène des réseaux sociaux, la demande pressante des utilisateurs d'utiliser leurs terminaux personnels pour accéder au système d'information dans le cadre des démarches de BYOD (*Bring Your Own Device*) ou la montée en puissance du Cloud Computing. S'imposent en outre de nouveaux textes réglementaires ainsi qu'une évolution radicale de l'attitude des utilisateurs vis-à-vis de la sécurité, avec la montée en puissance de la génération Y.

Pour répondre à cette gestion des risques IT, tous les services de l'entreprise doivent être mobilisés. Les responsables de la sécurité des systèmes d'information sont en première ligne. Les RSSI de l'Oréal, Pôle Emploi, Peugeot et SCOR ont ainsi pris à bras-le-corps la gestion des nouveaux risques IT.

9 DÉCIDEURS TÉMOIGNENT

Nicolas Peirani
Accor

Victor Vuillard
ANSSI

Christophe Jolivet
Eutelsat et Clusif

Étienne Papin
Cabinet
Feral-Schuhl / Sainte-Marie

Alain Bernard
L'Oréal

Philippe Ramon
Délégation interministérielle à l'intelligence économique

Michel Brouant
Pôle Emploi

Antoine Beligné
PSA Peugeot Citroën

Henri Guiheux
SCOR

EN RÉSUMÉ

L'ORÉAL

- Démarche BYOD et responsabilisation par rapport aux réseaux sociaux.
- Politique stricte vis-à-vis des services Cloud grand public.
- Adaptation des pratiques à l'arrivée de la génération Y.

PSA PEUGEOT CITROËN

- Gestion des risques adaptée à l'évolution vers un Cloud privé.
- Télétravailleurs assimilés à des utilisateurs nomades.
- Usage des réseaux sociaux encadré par une charte spécifique.

PÔLE EMPLOI

- Certification ISO 27001 pour répondre aux risques traditionnels et émergents.
- Prudence par rapport au BYOD, au télétravail et à la génération Y.
- Canal de communication avec l'ANSSI pour gérer les attaques.

SCOR

- Démarche BYOD temporairement limitée.
- Renforcement de l'organisation pour gérer les menaces persistantes avancées.
- Gestion des risques liés au Cloud externalisé, grâce à la contractualisation.

L'Oréal soigne sa génération Y

Chez L'Oréal, une stratégie BYOD a été définie afin de répondre à une forte demande des utilisateurs. Ceux-ci sont désireux d'utiliser leurs terminaux personnels dans l'entreprise pour accéder à la messagerie ou aux ressources du système d'information. Cette démarche se traduit par l'installation d'un applicatif de Good Technology, qui apporte une « *sandbox* », c'est-à-dire un conteneur sécurisé au sein d'un terminal grand public potentiellement non sécurisé. *« A l'extérieur de cette zone protégée, l'utilisateur fait ce qu'il veut. A l'intérieur, c'est la DSI qui a un contrôle complet »*, explique **Alain Bernard, RSSI de L'Oréal**. Cet applicatif donne l'accès à la messagerie Exchange - calendrier et contacts inclus - ainsi qu'à l'Intranet de L'Oréal. Les terminaux supportés fonctionnent sous Android ou iOS, sous réserve qu'ils ne soient pas « jailbreakés » ou « rootés ». Afin de couvrir des besoins supplémentaires, la DSI déploie un MDM (Mobile Device Manager) sur des terminaux qui appartiennent à L'Oréal et sur lesquels sont installées des applications sécurisées. *« Etant donné que nous finançons le smartphone ou la tablette, on peut le gérer comme un PC portable en imposant des mots de passe ou en bloquant iCloud, ce qui est impossible à réaliser en BYOD pur »*, explique Alain Bernard. Android est alors exclu car jugé trop ouvert.

La DSI contrôle une zone protégée dans le terminal personnel de l'employé

Alain Bernard
L'Oréal

Réseaux sociaux : ouverts pour des utilisateurs responsabilisés

Jusqu'à une période récente, L'Oréal filtrait les réseaux sociaux ainsi que les webmails. Mais leur usage est devenu un fait. De plus, le géant des produits cosmétiques embauche beaucoup de jeunes, friands de ces services. L'Oréal est en outre une marque orientée consommateurs, qui anime des pages Facebook ouvertes à tout le monde. L'usage de ce réseau social et plus récemment des webmails personnels a donc été autorisé. *« C'est davantage une problématique d'ingénierie sociale que de sécurité car Facebook ne pose pas de difficultés, dès lors que les systèmes et les antivirus sont à jour »*, précise Alain Bernard. En l'occurrence, il a fallu prendre en compte cet état de fait avec le service des Ressources Humaines et le service juridique. La charte d'usage des nouvelles technologies intègre ainsi de nouvelles règles qui responsabilisent les utilisateurs. Elles précisent par exemple les notions de devoir de réserve et de loyauté par rapport à l'employeur. *« On responsabilise les gens car on ne croit pas à des outils de filtrage efficaces, »* précise Alain Bernard. Il donne un exemple de règle mise en place : « *si on s'exprime à titre professionnel, il faut une validation par la hiérarchie ; si on s'exprime à titre personnel, il faut préciser qu'on ne parle pas au nom de l'entreprise.* »

D'un côté, l'application de cette charte, et plus généralement de règles de sécurité, est plutôt facilitée par la génération Y. *« Ces utilisateurs ne sont pas naïfs en matière de sécurité car ils ont déjà subi des vols de mots de passe ou ont été piratés »*, constate Alain Bernard. De plus, ils mesurent l'impact de ce qu'ils publient sur les réseaux sociaux. D'un autre côté, l'IT leur apparaît rétrograde. Leur niveau d'exigence en termes de connectivité et de réactivité tend à augmenter les risques. Ils demandent par exemple à utiliser des logiciels de voix sur IP tels que Skype ou de streaming qui posent de gros problèmes de sécurité ou de bande passante. ►

Les services Cloud grand public sont prohibés

> La génération Y n'est pas naïve en matière de sécurité
>
> ***Alain Bernard***
> *L'Oréal*

Vis-à-vis du Cloud Computing, une politique de sécurité a été définie. Elle formalise des exigences précises. L'accès à ces services est géré via la mise en place d'une fédération d'identité. *« En revanche, nous sommes totalement fermés à des services de Cloud personnels tels que Dropbox ou iCloud qui constituent un véritable cauchemar pour la sécurité »*, ajoute Alain Bernard. Et de citer un exemple de scénario catastrophe : un VIP configure chez lui le partage de fichiers sur iCloud, puis il va travailler. Il récupère alors des présentations PowerPoint sur son iPad qui sont immédiatement répliquées sur l'iPad de son fils qui est au lycée. Pour répondre malgré tout aux demandes des utilisateurs, la DSI évalue des solutions plus professionnelles qui permettront de maîtriser la synchronisation des terminaux ou de greffer une solution de protection contre les fuites de données de type DLP (*Data Loss Prevention*).

En matière de sécurité, on apprend de ses erreurs. L'Oréal a subi des attaques, par exemple en déni de service, notamment une en 2011 pour laquelle la DSI a tardé à réagir. Depuis, elle a mis en place des protections qui ont permis de mieux réagir lors d'une deuxième attaque. *« Nous réalisons maintenant un suivi des incidents à l'échelle du groupe, avec un partage des informations. Les protections sont basées sur l'expertise et la détection rapide »*, précise Alain Bernard. Pour raccourcir encore les délais de détection, la DSI met actuellement en place des salles de supervision de la sécurité de type SOC (Security Operations Center).

Enfin, à l'heure de la montée en puissance du Cloud, les questions que soulève le Patriot Act américain sont prises très au sérieux chez L'Oréal. *« Il n'est pas choquant que des services secrets américains ou français puissent accéder à nos informations dans certains contextes »* pense Alain Bernard. Pour autant, il estime que les risques se situent davantage dans le domaine de l'intelligence économique. *« Sous prétexte de sécurité de la Nation, les Etats ne pourraient-ils pas nous espionner ? Nous attendons des préconisations de la part des agences gouvernementales »*, demande Alain Bernard.

Pour en savoir plus

Retrouvez en vidéo
Alain Bernard
L'Oréal
sur **CIO Online**

Pôle Emploi articule sa stratégie sécurité autour d'ISO 27001

Face à L'Oréal qui joue l'ouverture progressive, Pôle Emploi déploie une politique de sécurité quasiment militaire. Celle-ci est tirée par la certification ISO 27001, le nec plus ultra de qui ce fait en la matière. Peu d'entreprises en France ont passé le cap de la certification. La norme sert le plus souvent de référentiel de bonnes pratiques dans lequel chacun pioche ce qui l'inspire. *« La certification ISO 27001 ne garantit pas une sécurité à 100 % mais elle permet une bonne appréciation des risques, notamment par rapport aux nouveaux phénomènes tels* ▶

BYOD, CLOUD, RÉSEAUX SOCIAUX : RÉPONDRE AUX NOUVEAUX RISQUES

Selon **Nicolas Peirani, IT Audit manager chez Accor**, les nouveaux risques liés au BYOD, au Cloud ou aux réseaux sociaux peuvent être pris en charge par une démarche de gestion des risques traditionnelle, dès lors que l'on fait preuve de souplesse. Pour rappel, la démarche consiste à identifier et quantifier les risques afin de les traiter de manière ordonnée en produisant des reportings sur la qualité de leur couverture, celle-ci prenant notamment la forme de contrôles. Nicolas Peirani souligne un point clé dans la démarche de gestion des risques informatiques : elle est de la responsabilité des métiers. Il conseille aussi de susciter une conscience des risques car il est par exemple inefficace d'imposer des mots de passe de 20 caractères si les utilisateurs les notent sur des post-it. De même, il faut se montrer pragmatique pour ne pas céder au découragement lié au caractère fastidieux de certaines méthodes. Enfin, il faut éviter la tentation de la généricité. *« La perte d'un mot de passe est un risque trop générique car très dépendant de l'application concernée, »* illustre Nicolas Peirani. Afin d'appliquer la gestion des risques aux évolutions des systèmes d'information, il donne quelques lignes directrices. Face aux réseaux sociaux, la gestion des risques doit prendre en compte la possibilité qu'un employé divulgue des informations stratégiques. Plutôt que d'en interdire l'usage, mieux vaut donc faire appel à la conscience et au professionnalisme des collaborateurs via des chartes et en réalisant des contrôles a posteriori. *« Encore rarement traité, l'autre risque des réseaux sociaux est celui que des clients s'expriment négativement »*, ajoute Nicolas Peirani. Concernant le Cloud Computing, il s'agit de garder la maîtrise de son usage, en contractualisant le contrôle des procédures d'administration et la possibilité d'une ré-internalisation. Il faut aussi obtenir une certaine souplesse en cas de besoins de développements spécifiques. Quant au BYOD, il est conseillé de définir les terminaux, les fonctions (intranet, applications métiers…) et le mode d'accès (direct, via un déport d'affichage…) que l'on autorisera. ■

Pour en savoir plus

Retrouvez en vidéo
l'intervention
de Nicolas Peirani
sur **CIO Online**

> L'étape de certification ISO 27001 est une concrétisation qui permet de renforcer la vigilance
>
> ***Michel Brouant***
> *Pôle Emploi*

que l'ouverture du système d'information, la génération Y, les nouvelles attaques ou le BYOD », estime **Michel Brouant, DGA technique de la DSI de Pôle Emploi**. La certification impose une cartographie des risques puis la mise en place d'opérations de contrôle correspondant aux zones à risques. Le fait d'être observé tous les ans par un organisme extérieur, l'Afnor, permet d'éviter tout écart par rapport à la norme. L'étape de certification proprement dite est une concrétisation dont l'existence permet de renforcer la vigilance et d'accompagner la conduite du changement des DSI des deux entités, Unedic et ANPE, qui ont donné naissance au Pôle Emploi.

BYOD et réseaux sociaux : une approche prudente

Le BYOD est un phénomène encore marginal au Pôle Emploi et ne concerne que des VIP, soit 150 à 200 personnes. Son usage est pour l'instant limité à un accès à la messagerie via une plate-forme sécurisée. D'autre part, une annexe au règlement intérieur décrit les consignes en cas de perte ou de vol d'un terminal. La principale disposition concerne une protection classique des terminaux par code secret PIN. Quant au télétravail, il est limité aux personnes souffrant d'un handicap physique. Elles ont accès au système d'information à partir de leur domicile via un réseau VPN, avec une authentification forte par jeton.

Les réseaux sociaux ne sont pas bloqués mais les sites prohibés le sont. De plus, l'usage de l'outil Internet en général est mesuré, analysé et publié auprès des managers en cas de comportement anormal. *« Une réflexion est en cours concernant l'utilisation des réseaux sociaux, plutôt professionnels, pour la recherche d'emploi »*, précise Michel Brouant.

Les comportements des utilisateurs, notamment ceux qui sont issus de la génération Y, sont très encadrés. Les droits et les habilitations des agents qui reçoivent des demandeurs d'emploi sont accordés selon des processus calibrés. Au siège, la direction générale et la DSI sont davantage demandeurs d'applications diverses. *« Nous avons réalisé un catalogue d'outils qui sont installés à la demande. Pour les demandes plus spécifiques, un canal est prévu. Mais les utilisateurs ne peuvent rien faire seuls car, comme les agents, ils ne sont pas administrateurs de leurs PC »*, tempère Michel Brouant. De plus, l'annexe au règlement interne précise les droits d'usage des outils informatiques dans un cadre professionnel défini.

Pour en savoir plus

Retrouvez en vidéo
Michel Brouant
Pôle Emploi
sur **CIO Online**

Pôle Emploi et l'ANSSI dialoguent afin de gérer les attaques

Le Pôle Emploi a subi quelques tentatives d'intrusion qui n'étaient toutefois pas très ciblées. *« Nous les avons vues arriver et le phénomène est resté raisonnable »*, précise Michel ►

SÉCURITÉ ÉCONOMIQUE : STOCKER DES DONNÉES SENSIBLES DANS UN CLOUD PEUT ÊTRE PASSIBLE DE SANCTIONS !

Placée sous l'autorité du Président de la République, la délégation interministérielle à l'intelligence économique a été créée en 2009, afin d'identifier les risques qui menacent les entreprises françaises et établissements publics : espionnage économique, débauchage de personnel, déstabilisation et de plus en plus, escroqueries.
« Représentant 23 % de ces attaques en 2011, les risques informatiques prennent la forme d'intrusions ou de vols d'ordinateurs, de logiciels et de clés USB », précise **Philippe Ramon, chef du pôle sécurité économique et affaires intérieures à la Délégation interministérielle à l'intelligence économique**. Cette délégation met en garde contre un recours croissant à l'ingénierie sociale pour identifier les personnes ayant accès à l'information, voire pour obtenir des codes d'accès. Elle conseille en outre, lors des déplacements à l'étranger, de prendre des précautions liées aux réglementations locales.
Ainsi, en arrivant en Chine ou en Russie, il est obligatoire de déclarer la détention d'informations cryptées.
Aux États-Unis, la douane peut copier les informations dont on dispose et saisir durant 22 jours le matériel contenant des données cryptées. *« Quant au Patriot Act, il s'applique quelle que soit la localisation de la donnée. Il suffit que la maison-mère du prestataire soit américaine »*, insiste Philippe Ramon.
Concernant le Cloud, il rappelle les risques qui découlent d'une perte de maîtrise du système d'information ou d'une absence de réversibilité. Mais le risque majeur, juridique, est lié à la localisation des serveurs.
Le code pénal français spécifie en effet, en substance, que le fait de rendre accessibles à une entité étrangère, des informations dont la divulgation est de nature à porter atteinte aux intérêts fondamentaux de la nation, est punie de 15 ans d'emprisonnement et de 225 000 € d'amende.
« La simple utilisation d'un service Cloud pour stocker des données sensibles peut donc être passible de sanctions », en conclut Philippe Ramon. ■

Pour en savoir plus

Retrouvez en vidéo
l'intervention
de Philippe Ramon
sur **CIO Online**

> **Il est difficile d'interdire Dropbox qui peut servir à des échanges avec des fournisseurs**
>
> ***Antoine Beligné***
> *PSA Peugeot Citroën*

Brouant. D'autre part, le service cyber-vigilance de l'ANSSI a récemment signalé que les PC de certains demandeurs d'emploi étaient infectés par des chevaux de Troie qui captaient les mots de passe et les identifiants. *« L'ANSSI nous a signalé les noms des demandeurs d'emploi en question, que nous avons alertés »*, explique Michel Brouant. La norme 27001 permet de vérifier que le canal d'informations entre le Pôle Emploi et l'ANSSI est bien actif.

Côté réglementation, un décret d'août 2011 oblige les fournisseurs de services de communication publics, tels que les Fournisseurs d'Accès à Internet, à conserver les traces des échanges pendant deux ans. *« On ne le fait pas car on ne fournit pas de tels services mais on y viendra sans doute en 2013 »*, conclut Michel Brouant.

Le « Bring Your Own Software » chez Peugeot

Face à l'évolution des usages, il faut savoir s'adapter parfois même quand le réflexe sécuritaire inciterait à tout bloquer. Ainsi, chez le groupe Peugeot Citroën, les évolutions sont multiples.

Premier exemple, à l'heure du BYOD, Peugeot Citroën constate l'émergence d'un autre phénomène tout aussi inquiétant d'un point de vue de la sécurité : le Bring Your Own Software. Certains utilisateurs souhaitent en effet stocker des données sur des services de stockage tiers afin de les partager. Ce changement dans les usages doit être intégré par les équipes de la sécurité informatique. *« Il est par exemple difficile d'interdire Dropbox car des intervenants externes peuvent mettre des fichiers en partage sur ce service, qui deviendra de fait un point de passage obligé. On est donc obligé de préparer cette ouverture, c'est une question de sensibilisation, de comportements »*, explique **Antoine Beligné, RSSI de PSA Peugeot Citroën**.

Autre évolution majeure, les réseaux sociaux sont autorisés chez PSA Peugeot Citroën, d'autant que le constructeur a créé des pages professionnelles pour rechercher des collaborateurs et des clients. Dès lors c'est une charte qui fixe les règles du jeu. Elle précise que ces réseaux permettent de promouvoir l'entreprise et ses produits et que chacun doit y faire preuve de courtoisie et s'en tenir à sa compétence. *« Ce document est différent d'une charte informatique classique car il s'applique en tout lieu et à toute heure »*, ajoute Antoine Beligné.

Dans un registre différent, lorsque le télétravail a été autorisé chez Peugeot, il a été traité comme le cas des utilisateurs nomades. *« Quand les RH ont lancé un pilote, la DSI a simplement appliqué un dispositif existant, basé sur des PC portables, un tunnel VPN et une authentification par certificats »*, relate Antoine Beligné. Il suffisait donc d'équiper d'un PC portable, les futurs télétravailleurs qui n'avaient jusqu'à présent qu'un PC fixe. Parallèlement, une analyse de la confidentialité de l'information a permis de vérifier si elle était compatible avec le télétravail. Et une annexe au contrat de travail a précisé la gestion de la confidentialité dans des lieux privés. ▶

LA LOI SUR LE SECRET DES AFFAIRES N'EST PAS INDISPENSABLE

La loi sur le secret des affaires, qui vise à sanctionner le vol d'informations sensibles, a été adoptée le 23 janvier 2012 en première lecture. Mais selon **Étienne Papin, avocat du cabinet Feral-Schuhl Sainte-Marie**, *« elle a peu de chances d'aboutir dans un avenir prévisible. »* De plus, elle est incomplète. Par exemple, elle spécifie qu'une information n'est protégée que si elle a fait l'objet de mesures de protections spécifiques, dont la nature devra être précisée par un décret. En somme, les entreprises ne peuvent guère compter sur ce futur texte mais selon Étienne Papin, il n'est pas certain qu'il soit indispensable. Pourtant, explique-t-il, il n'existe pas de droit général de propriété sur l'information. Le code de la propriété intellectuelle ne concerne que des objets précis : œuvres de l'esprit, dessins et modèles, brevets ou bases de données. Et les protections sont très circonscrites et ne protègent que l'objet lui-même, jamais l'information. Heureusement, différentes lois offrent des protections périphériques. Bien que le vol ne concerne que des objets matériels, les tribunaux commencent ainsi à reconnaître la possibilité de voler une information, du moins quand il y a support physique, comme une clé USB. Le délit d'abus de confiance permet aussi de protéger l'information. D'autre part, certains secteurs comme les télécoms sont légalement contraints de s'assurer que les informations personnelles qu'ils transportent ne sont pas divulguées à des tiers. La loi Godfrain de 1988 protège pour sa part les systèmes d'information contre les intrusions frauduleuses. Selon Étienne Papin, ces différents textes pourraient être suffisants moyennant une modification à la marge du code pénal. *« Il s'agirait par exemple de confirmer dans le code pénal que l'information peut faire l'objet d'un vol ou d'un abus de confiance, même en l'absence d'atteinte à un support matériel »*, estime Étienne Papin. ■

Pour en savoir plus

Retrouvez en vidéo **l'intervention d'Etienne Papin** sur **CIO Online**

Le Cloud privé redéfinit les standards

> **Le cloisonnement des informations est défini par les responsables métiers**
> ***Antoine Beligné***
> *PSA Peugeot Citroën*

Chez PSA Peugeot Citroën, le Cloud Computing prend la forme d'un vaste Cloud privé à l'échelle de l'entreprise, progressivement mis en place depuis plusieurs années. Avant son déploiement, les applications de Peugeot étaient classifiées selon quatre niveaux de risque. Avec l'arrivée du Cloud, les notions d'administration, de disponibilité, d'intégrité et de confidentialité ont été revues. Le concept de Cloud sous-tend en principe un mélange et une mutualisation de toutes les applications dans un seul nuage, quelle que soit leur classification.

Mais l'entreprise n'a pas voulu réaliser ce grand écart. *« Certaines applications de niveaux différents ont été regroupées mais le Cloud préserve une certaine segmentation »*, précise Antoine Beligné. Ce choix est dicté par des contraintes techniques, comme le fait que l'arrêt d'un serveur physique provoque celui de nombreuses machines virtuelles. De plus, la segmentation permet d'intégrer les risques liés aux personnels informatiques. *« La gestion des différents administrateurs techniques impose un cloisonnement des informations, défini par les responsables métiers »*, précise en effet Antoine Beligné.

PSA Peugeot Citroën externalise toutefois certains services dans le Cloud public. Afin d'en contrôler l'accès, un outil de fédération d'identités présente une application SaaS comme si elle était hébergée en interne. La sécurité s'en trouve améliorée car l'utilisateur n'a pas à gérer plusieurs identités et plusieurs mots de passe. Concernant la sécurité des données gérées par ces services, le volet contractuel fait l'objet d'un compromis, décidé avec la maîtrise d'ouvrage, entre les risques et le coût global de fonctionnement. *« Avec des services SaaS de premier prix, le contrat ne peut pas être négocié. Si l'on veut des spécificités, le coût augmente »*, précise Antoine Beligné.

Dans le cadre d'une externalisation plus traditionnelle, la DSI assure la sécurité en gérant la transition entre le réseau interne et l'extérieur. *« On doit alors distinguer les services métiers et ceux de la DSI, tels que le développement, la télé-exploitation ou la télémaintenance »*, explique Antoine Beligné. Pour ces derniers, il s'agit d'ajuster le niveau d'administrateur des personnels distants et d'assurer la traçabilité. Un dispositif contractuel permet en outre de sensibiliser les prestataires (qui peuvent eux-mêmes avoir les leurs) pour les inciter à ▶

POLITIQUE DE SÉCURITÉ : 13 BONNES PRATIQUES

Christophe Jolivet, RSSI d'Eutelsat et représentant du Clusif, cite treize bonnes pratiques afin de construire et de faire évoluer une politique de sécurité.

1. **Confier la définition de la politique de sécurité à un groupe de travail multidisciplinaire** (juridique, RH, DSI, métiers, avec une forte implication de la direction) qui prendra soin de respecter les lois et règlements sectoriels.
2. **Réaliser une analyse des risques** pour éviter de prendre des mesures inutiles ou coûteuses, ou de ne pas en prendre là où il en faudrait.
3. **Commencer par définir la politique générale sur la sécurité de l'information**, qui est un document synthétique de haut niveau fixant les grandes orientations. Ce document sera signé par un décisionnaire.
4. **Détailler les standards de sécurité du système d'information**, qui donnent des règles précises, techniques et organisationnelles, comme la politique de mots de passe ou les critères de classification de l'information.
5. **Détailler les procédures, qui décrivent comment seront appliquées les règles**, par exemple pour gérer les incidents ou ouvrir des flux. Préciser les responsabilités de chacun et prévoir la gestion des exceptions.
6. **Formaliser le volet RH de la politique**, qui précisera les droits et devoirs des utilisateurs du système d'information.
7. **S'appuyer sur les normes (ISO 27001, 27002, 27005, 27004...)**, guides et référentiels (comme Cobit 5 ou celui de l'ANSSI). Ils apportent une aide mais ne doivent pas être des bibles.
8. **Rester pragmatique** en évitant de produire du volume ou en édictant des règles qui ne peuvent pas être respectées en pratique.
9. **Ne pas sous-estimer les mesures réactives de la politique de sécurité**. Les grands groupes se concentrent trop souvent sur les mesures de prévention.
10. **Tenir compte de la dimension internationale de l'entreprise** car chaque pays a sa culture.
11. **S'intégrer au maximum aux processus de contrôle**, notamment qualité, déjà en place dans l'entreprise.
12. **Adapter les politiques aux nouveaux usages** car la sécurité informatique doit accompagner les besoins métiers et non les freiner.
13. **Prévoir le processus d'audit** des mesures prévues dans la politique.

sensibiliser leurs employés et à mettre en place des contrôles. *« Le but n'est pas d'engager des procès mais de prendre toutes les précautions pour les éviter »*, résume Antoine Beligné.

> **Un contrat sert à prendre toutes les précautions pour éviter un procès**
> ***Antoine Beligné***
> *PSA Peugeot Citroën*

Lutte contre la cybercriminalité : un équilibre à trouver entre risques et coûts

Antoine Beligné se montre assez réaliste vis-à-vis de la cybercriminalité : *« il y a toujours un avantage à l'attaquant, qui choisit sa cible et son heure. L'essentiel est de pouvoir détecter au plus vite une attaque et de réagir en relançant les services et en conservant des traces pour comprendre et apprécier l'impact. »* Dès lors, l'attitude vis-à-vis des attaques de type MPA (Menaces Persistantes Avancées) est mesurée : l'analyse des risques montre jusqu'à quel point il faut mettre des moyens techniques et humains pour détecter ces attaques et réagir.

Et concrètement, PSA Peugeot Citroën maintient à niveau son dispositif de prévention sans engloutir des moyens inconsidérés. La cybercriminalité fait en outre l'objet d'une veille menée avec les juristes du groupe. Parmi les conclusions : en cas de lancement de procédures, il est très difficile de constituer un dossier recevable par un juge, d'autant qu'en cas d'incident, il est plus urgent de rétablir le service que de constituer des preuves. *« Pour autant, nous sommes prêts à utiliser les outils de la législation, en portant plainte auprès des autorités, même si cette simple décision peut nous éclabousser »*, ajoute Antoine Beligné.

Renforcer les moyens face à l'évolution de la réglementation

Concernant le respect de la réglementation, PSA Peugeot Citroën adapte les moyens techniques et surtout humains, en particulier en ce qui concerne les données à caractère personnel, un domaine régulé par la Cnil en France. *« Avec la réglementation européenne en cours de définition, la communication sera obligatoire en cas de perte de données à caractère personnel. On devra donc renforcer l'organisation en place pour réagir en fonction de cette réglementation »*, précise Antoine Beligné.

Quant à l'attitude face au Patriot Act américain, c'est une certaine résignation qui prédomine chez le constructeur automobile. *« Si nous installons un outil de chiffrement sur des PC et que nous entrons aux États-Unis, cet outil sera potentiellement inutile. Si l'on veut réellement cacher des données, elles ne doivent tout simplement pas passer la douane »*, résume Antoine Beligné. Quant à la future loi sur le secret des affaires, si jamais elle est promulguée, elle donnera un cadre pénal plus favorable aux poursuites mais elle imposera un alourdissement des procédures car il faudra faire la preuve pour gérer les litiges.

Pour en savoir plus

Retrouvez en vidéo
Antoine Beligné
PSA Peugeot Citroën
sur **CIO Online**

Scor prévoit un accroissement des usages liés au BYOD

Afin de maitriser les risques liés à l'informatique, la société de réassurance Scor veut mettre en place un cadre de contrôle suffisamment efficace pour protéger ses données, tout en cherchant le meilleur compromis par rapport à l'efficacité du système d'information et à la volonté d'offrir aux utilisateurs un accès depuis n'importe où. Pour gérer le phénomène du BYOD, Scor a choisi, comme L'Oréal, de déployer l'offre de l'éditeur Good Technology sur les ►

MENACES PERSISTANTES AVANCÉES : L'ANSSI CRÉE UN GROUPE D'INTERVENTION

« Les techniques mises en œuvre par les instigateurs des menaces persistantes avancées ne sont souvent pas très novatrices car il leur suffit d'une faille pour être efficaces, comme un mot de passe faible d'un seul utilisateur », prévient **Victor Vuillard, chef du groupe d'intervention à l'ANSSI**. Une fois que l'attaque a démarré, le côté persistant est le plus caractéristique. *« L'objectif est en effet de s'installer pour voler des données dans le temps »*, explique Victor Vuillard. Après un premier accès, l'attaquant tente typiquement de voler des données d'authentification et organise progressivement la compromission de dizaines voire de centaines de machines et d'équipements. Quand il a la main sur l'annuaire de l'entreprise, donc sur les mots de passe des administrateurs, il peut placer des portes dérobées à gauche à droite. En somme, il est chez lui. *« Pour le déloger, il faut comprendre comment il fonctionne, identifier les systèmes compromis et le déloger de façon cohérente, c'est-à-dire partout à la fois. En somme, il faut reconstruire le système d'information pour reprendre la main »*, résume Victor Vuillard. Compte tenu de l'ampleur de la tâche, une approche industrielle doit être mise en place. C'est l'objectif du groupe d'intervention rapide que l'ANSSI crée, sur la base de l'expérience du traitement de ce genre d'incidents. De taille modeste, ce groupe interviendra pour les attaques les plus importantes et les plus graves, auprès des administrations et entreprises de 12 secteurs clés. ■

> **Dans le Cloud, la mutualisation est une source de risques car des centaines de personnes pourraient accéder à nos équipements**
> ***Henri Guiheux***
> *SCOR*

smartphones. Elle donne essentiellement accès à la messagerie professionnelle. *« C'est une solution dont la portée est limitée mais elle est simple, non intrusive, sécurisée et rapide à mettre en œuvre »*, justifie **Henri Guiheux, RSSI de Scor**, tout en estimant que c'est une démarche temporaire, tant la pression des demandes de nouveaux services est importante. *« Les nouvelles générations voudront utiliser ces devices pour un nombre croissant d'usages, au point qu'ils remplaceront probablement les PC portables »*, estime Henri Guiheux.

Le télétravail est assez développé dans les filiales suisse et américaine de l'assureur, tandis qu'en France, il fait encore l'objet de certaines réticences. La DSI mène toutefois deux démarches complémentaires qui concernent également la mobilité. D'une part, un portail en technologie Web et Citrix permet un accès limité, mesuré et contrôlé, à certaines ressources du système d'information, à partir de PC banalisés, notamment personnels. La sécurité est assurée par une technologie d'origine RSA Technology exploitant des mots de passe dynamiques. D'autre part, des PC portables donnent un accès plus large au système d'information, avec une authentification forte biométriques et un VPN. Ils sont proposés à certains utilisateurs.

Réseaux sociaux : le filtrage va être affiné

En revanche chez Scor, l'accès aux réseaux sociaux est interdit à la demande du management. *« Mais nous sommes en train de mettre en place un nouveau système de filtrage d'URL qui permet d'identifier des catégories d'utilisation telles que le jeu, la politique ou l'usage professionnel. On pourra par exemple autoriser Facebook en fonction de son contenu »*, précise Henri Guiheux.

La question de l'e-réputation de Scor sur le Web se pose vis-à-vis de ses clients. Pour y répondre, une cellule d'intelligence économique comptant trois personnes surveille l'image de l'entreprise et des différents marchés sur lesquels elle travaille. Cette cellule s'appuie sur la solution Digimind qui surveille également les cyber-risques et les évolutions réglementaires.

Cloud : les risques sont maitrisables par contrat

Par ailleurs, Scor s'est engagé dans une démarche de Cloud privé de grande envergure, hébergé par un prestataire dans un Data enter situé en France et dont les ressources sont mutualisées avec d'autres entreprises. Le choix du Cloud était dicté par le besoin de réactivité et par l'effectif restreint de l'entreprise qui est de 2100 personnes, dont 100 à la DSI.

Or, la mutualisation est une source potentielle de risques car des centaines de personnes pourraient potentiellement accéder aux équipements de Scor. *« Nous devons nous assurer que l'on peut savoir qui est autorisé à faire quoi »*, explique Henri Guiheux. De plus, la mutualisation peut générer des risques d'attaques par rebond. *« Tous ces risques sont maîtrisables par des clauses contractuelles portant sur la confidentialité ou le plan de secours, par une gouvernance du suivi de la sécurité et par des contrôles »*, détaille Henri Guiheux. Ces contrôles prennent la forme d'audits réalisés en interne et par des demandes de conformité à la norme ISO 3402, qui concerne la protection des données à caractère personnel. Quant aux applications SaaS comme la gestion de la paie, elle est également encadrée par des clauses contractuelles. Les éditeurs donnent des garanties jugées suffisantes car aucune application du cœur de métier de Scor n'est concernée.

Scor reconnaît avoir été victime de tentatives de MPA (Menaces Persistantes Avancées). L'entreprise a en effet détecté des e-mails contenant des malwares spécifiques ciblant l'entreprise qui n'étaient donc pas reconnus via des bases de signatures, mais seulement par un moteur d'analyse comportementale. *« Ces emails ont été reçus par notre président et plusieurs personnes de la direction, qui nous ont alertés »*, ajoute Henri Guiheux.

Scor s'organise contre les MPA

A l'évidence, un travail de Social engineering avait été réalisé en amont pour identifier les personnes intéressantes. Les attaques ont été très courtes car il s'agissait seulement de tentatives, mais des semaines d'analyse ont été nécessaires pour décortiquer leur nature et leur origine géographique. Elles venaient de quatre ou cinq pays en même temps. D'autres tentatives, dans un grand nombre de pays, visaient à récupérer par email ou par ingénierie sociale, des numéros de mobiles de dirigeants. Ces attaques ont pu être repérées grâce à une communication intense entre les filiales. Elles ont été à l'origine d'un renforcement du monitoring, dans le cadre d'une démarche plus générale de gestion des risques opérationnels ►

dont les risques IT ne représentent qu'un type parmi d'autres. Afin d'éviter de travailler en silos, cette gestion des risques implique plusieurs entités : Risk manager IT, Risk managers des métiers, DSI, direction juridique, comité de protection des données et direction générale. *« Les métiers sont en première ligne, l'IT est là en support »*, précise Henri Guiheux. Parmi les décisions récemment prises, Scor lance actuellement un vaste programme de protection des données, basé notamment sur un centre de sécurité SOC (Security Operations Center) qui permettra de détecter les comportements anormaux, caractéristiques des MPA.

500 questions qui engagent l'assureur en cas de litige

Côté textes réglementaires, Scor constate une pression croissante. En tant qu'assureur, la socéité est soumise à Solvency 2, qui renforce l'obligation de bonne gestion des risques et de sécurisation des données. Parallèlement, l'entreprise est dans une démarche de certification, notamment ISO 3402, pour la protection des données sensibles, dont les données à caractère personnel des assurés. *« Cette protection des données fait l'objet d'une réglementation de plus en plus contraignante, surtout aux États-Unis et en Grande-Bretagne »*, déclare Henri Guiheux. Scor reçoit en effet des questionnaires sur la protection des données. Ils sont de plus en plus nombreux, détaillés – comprenant jusqu'à 500 questions – et engagent l'assureur en cas de litige.

Et pour ce qui concerne le Patriot Act, Henri Guiheux se montre plutôt pessimiste. Selon lui, la portée de ce texte va bien au-delà des frontières des Etats-Unis. *« Bien que notre prestataire de Cloud privé héberge notre infrastructure en France, il s'agit d'un fournisseur américain. Si le FBI faisait pression sur lui pour accéder à nos données, il parviendrait probablement à ses fins »*, estime-il. Pour autant, il n'identifie pas d'autre alternative que d'accepter cet état de fait. ■

Thierry Lévy-Abégnoli

Pour en savoir plus

Retrouvez en vidéo
Henri Guiheux
SCOR
sur **CIO Online**

PUBLI-REDACTIONNEL

MATINÉE STRATÉGIQUE

CONFÉRENCE ORGANISÉE LE 5 AVRIL 2012 PAR CIO

La virtualisation, étape vers le Cloud et le portail de services

La virtualisation des postes de travail et des Data Centers demeure au centre des préoccupations des managers IT. Les bonnes pratiques suivent la montée en puissance du Cloud. Elles ont été détaillées lors de la conférence organisée le 5 avril par les rédactions de CIO et du Monde Informatique en partenariat avec Juniper Networks, Schneider Electric, Microsoft et Veeam Software.

Sur le métier, sans cesse, il faut remettre son ouvrage. La virtualisation des ressources informatiques n'échappe pas à la règle, tant ce domaine progresse rapidement qu'il s'agisse de Cloud privé ou des environnements de travail. Les bonnes pratiques en la matière constituent la trame de la conférence stratégique organisée par les rédactions de CIO et du Monde Informatique, le 5 avril au Pavillon Dauphine, à Paris. L'événement était organisé en partenariat avec Juniper Networks, Schneider Electric, Microsoft et Veeam Software.

En ouverture, Didier Navez, Senior Advisor chez le cabinet d'analystes Forrester Research, a présenté l'état de maturité du marché de la virtualisation, des différentes technologies ainsi que leurs liens avec la mise en œuvre de Clouds privés. *« 85 % des entreprises ont virtualisé une bonne partie de leurs serveurs et 80 % d'entre elles ont mis en place des politiques qui imposent, par défaut, la virtualisation »*, a relevé Didier Navez.

Le réseau doit être optimisé pour les environnements virtuels

Dans ce cadre, les salles de serveurs occupent une position clé. Xavier Duflos, Strategic Alliance Manager chez Juniper Networks, a souligné la nécessité d'adapter le réseau au sein des Data Centers, sous l'impact de la virtualisation des serveurs afin d'accélérer les flux de données. *« Une application informatique moderne repose sur des services applicatifs correspondant à autant de machines virtuelles. Le réseau doit optimiser les multiples échanges entre ces services et l'accès aux ressources de stockage »*, a insisté Xavier Duflos.

Une préférence pour le Cloud privé

Une première table ronde a fait le point avec cinq responsables de systèmes d'information qui ont virtualisé les Data Centers de leurs entreprises, et s'engagent pour la plupart sur la voie du Cloud privé. On a ainsi pu entendre les retours d'expérience de Jean-Francois Imokrane, responsable du service Informatique de la Direction de l'information légale et administrative (DILA), Sylvie Lebenstein, Chef de département infrastructure et socle logiciel chez Renault, Jean-Michel Castanie, Director Infrastructure Strategy and Process chez Alstom et Frédéric Halimi, DSI d'EAS Industries. ▶

Dans la foulée, Eric Boucheron, Data Center Software & Security Director chez Schneider Electric, est revenu sur la création d'une infrastructure de Data Center sécurisée, automatisée et agile, sous l'effet de la virtualisation et du Cloud. Il a détaillé l'importance d'un management de type DCIM (Data Center Infrastructure Management) des ressources d'une salle informatique. *« Un bon DCIM permet une gestion du froid, des flux d'air, de l'énergie, de l'espace disponible et de la capacité réseau, tout en anticipant les problèmes, notamment grâce à une modélisation de la salle »*, a-t-il pointé.

Le Cloud privé ouvert vers le Cloud public

Dans ce mouvement global vers le Cloud, Christophe Dubos, Architecte Infrastructure et Datacenter chez Microsoft, a tracé les différentes voies, en associant infrastructure privée et publique. Le Data Center devient un centre de services, animé par un ensemble d'outils d'orchestration et de gestion. *« Ces différents composants prennent en compte les environnements virtuels mais aussi physiques, et ils supportent un modèle de Cloud hybride, associant des ressources privées et publiques »*, a-t-il souligné.

Une seconde table ronde a réuni cinq responsables IT d'entreprises ayant opté pour la virtualisation de tout ou partie de leurs postes de travail. On a pu ainsi entendre les retours d'expérience de Alain Lemoine, Directeur informatique du Cabinet Fidal, Patrick Joly, DSI de Mondial Assistance, Jérémy Verrier, responsable informatique du Technicentre Industriel de la SNCF de Nevers, ainsi que de Frédéric Halimi, DSI d'EAS Industries.

Pour clore la conférence, Olivier Robinne, Southern EMEA Director chez l'éditeur de logiciels Veeam Software, a mis en lumière le fait que si la virtualisation est une technologie banalisée, pour autant sa généralisation reste freinée par des questions de fiabilité, de performance, de délais de sauvegardes/restaurations et d'administration. « *Les problématiques de protection des données et d'administration doivent être traitées de manière simple* » a-t-il insisté, illustrant ces propos grâce à deux exemples d'entreprise ayant optimisé leurs sauvegardes en environnements virtualisés, le chimiste Arkema et l'hébergeur LinkByNet. ■

Pour en savoir plus

CIO

Retrouvez
les vidéos et les présentations de cet évènement
sur **CIO Online**

Promouvoir les logiciels libres

Jean-Luc Raffaëlli, directeur de projets stratégiques à la DSI groupe de La Poste, a toujours promu des systèmes d'information ouverts, avec un intérêt prononcé pour le logiciel libre. Universitaire, et non ingénieur, il veille à défendre la valeur du capital immatériel de son entreprise.

CIO : Vous êtes docteur et non ingénieur. Est-ce que cela change quelque chose dans une carrière ?

Jean-Luc Raffaëlli : Oui, sans aucun doute. C'est plus dur les premières années. Surtout, il y a vingt ans, il existait un grand écart entre les préoccupations des chercheurs et celles des entreprises. Cet écart, aujourd'hui, se résorbe. Et puis, au bout de cinq ou six ans d'expérience en entreprise, les docteurs ont les acquis dont on pouvait leur reprocher parfois l'absence.
Lorsqu'une entreprise mise, au départ, sur quelqu'un qui n'a pas la meilleure image, elle est bien contente, ensuite, de disposer d'un expert avec une méthode rigoureuse et une grande agilité intellectuelle. La confiance est alors établie.

CIO : Comment avez-vous débuté votre carrière ?

Jean-Luc Raffaëlli : J'ai débuté chez Altran. En quatre ans, je suis devenu consultant senior, avec le taux de facturation associé. Avec mes premières expériences en consulting, j'ai acquis la preuve que mes compétences étaient bien pertinentes.

CIO : Pourquoi vous êtes-vous intéressé à l'open-source ?

Jean-Luc Raffaëlli : Depuis très longtemps, je connais bien Linux. En fait, je suis attaché à l'ouverture. L'enfermement coûte cher : la facture gonfle très vite lorsque des projets sont freinés par la fermeture des systèmes ou lorsque l'on souhaite changer de fournisseur à partir d'un système fermé.
Au sein du groupe La Poste, l'open-source a été le sujet qui a réuni tous les métiers autour de la réduction des coûts. Puis nous avons travaillé sur le développement de la valeur. Nous avons, en fait, mené une réflexion plus globale sur le cycle de vie des systèmes.

CIO : Qu'entendez-vous par là ?

Jean-Luc Raffaëlli : Pourquoi limiter le calcul d'un retour d'investissement à deux ou trois ans ? Le système sera utilisé, en tout ou modifié, bien au delà. C'est à partir de quatre ou cinq ans que l'open-source apporte le plus de différences.

CIO : Ceci dit, l'open-source n'est pas gratuit, comment évaluez-vous les coûts ?

Jean-Luc Raffaëlli : Le gain global sur le budget d'un projet entre une solution propriétaire et une solution open-source est de l'ordre, en moyenne, de 5 %. C'est le coût de la licence. Mais la valeur est au delà du temps du projet.
C'est pour cela que nous travaillons sur la valeur dans la durée : la valeur stratégique, la valeur de pérennité, la valeur orientée utilisateur… A quoi cela sert de mettre à jour un logiciel tous les ans avec des nouveautés sans valeur d'usage ? Cela n'a aucun intérêt ! Et en plus cela a un coût. L'open-source n'a pas ce défaut de la feuille de route imposée par un éditeur.
L'open-source a pour seul objectif de satisfaire l'utilisateur, qu'il s'agisse de l'entreprise utilisatrice ou de l'utilisateur final.

CIO : Vos relations sont-elles, de ce fait, toujours tendues avec les éditeurs de logiciels propriétaires ?

Jean-Luc Raffaëlli : Certains éditeurs propriétaires font du très bon travail. Il faut juste qu'ils soient loyaux avec leurs clients. L'enfermement nous épuise. Il est, en particulier, tout à fait inacceptable de devoir payer pour récupérer des données.
Je ne sais pas toujours si les données appartiennent à La Poste ou bien si elles appartiennent à ses clients. Mais, ce qui est sûr, c'est que les données n'appartiennent jamais aux fournisseurs.

CIO : Et avec les éditeurs et prestataires du monde du logiciel libre ?

Jean-Luc Raffaëlli : Nous avons la même attitude avec tous nos fournisseurs, du monde du logiciel libre comme du monde propriétaire. Nous présentons notre démarche de gouvernance, de respect des standards, d'ouverture, etc. Nous leur demandons alors de reformuler comment les fournisseurs ont compris nos besoins.
Bien qu'éditeur, Suse, par exemple, a été capable d'expliquer de façon claire à la Direction des Achats ce qu'il apportait, notamment en pérennité. Ce fournisseur, comme d'autres (Nagios, Alterway…), nous a accompagné dans notre démarche.

CIO : Comment avez-vous défini cette démarche ?

Jean-Luc Raffaëlli : Quand je suis arrivé dans le groupe La Poste, il y a cinq ans, je venais d'un milieu très agile mais avec des processus très industriels, les télécoms. Mais tout ce qui pouvait être mis en place à l'instigation du siège était déjà mis en œuvre à La Banque Postale. Celle-ci a donc servi d'exemple.
Beaucoup de travail a été fait sur l'intégration, l'industrialisation et l'ouverture. Nous avons également voulu professionnaliser et industrialiser le travail des SSLL [Sociétés de Services en Logiciels Libres, NDLR]. Ma spécialité porte sur les thématiques amont : la gouvernance, l'architecture…

CIO : Votre démarche est-elle toujours la même ?

Jean-Luc Raffaëlli : Oui. La DSI commence par sensibiliser les directions métier aux enjeux dans le cadre de notre fonction de conseil. De la même façon, par exemple, la direction juridique sensibilise aussi chaque direction sur les préoccupations d'ordre légal. Comme exemple de sujet faisant l'objet d'une telle sensibilisation, il y a la localisation des données.
Cependant, le métier reste libre de ses choix.

CIO : Vous êtes très impliqué dans le monde associatif. Vous êtes ainsi vice-président de l'Open World Forum et parrain de l'OpenCIO Summit cette année. Quel intérêt y avez-vous pour y passer du temps ?

Jean-Luc Raffaëlli : Oui, c'est vrai, cela prend beaucoup de temps. Et ça fait plusieurs années qu'on travaille avec l'AFUL [Association Française des Utilisateurs de logiciels Libres]. C'est une suite logique à notre démarche ouverte. Nous voulons donner une visibilité à celle-ci.
Je ne peux que regretter que certaines entreprises fournissant de l'open-source soient sur des modèles plus de survie que de développement de richesse. Trop souvent, les entreprises utilisatrices ne voient l'open-source que comme un supermarché on l'on se sert sur les étagères et où on passe à la caisse sans payer. Ca ne pourra pas toujours durer. Et ce n'est pas toujours à la seule administration de payer les développements.
Beaucoup de solutions ont besoin d'investissements. Beaucoup d'acteurs ont besoin que les entreprises utilisatrices co-investissent, contribuent pour disposer de solutions ouvertes et plus performantes. ▶

DOCTEUR, CONSULTANT ET POSTIER

« Les Raffaelli sévissent à La Poste depuis 70 ans » s'amuse Jean-Luc Raffaëlli. Pourtant, ce n'est pas pour raisons familiales qu'il a rejoint cette entreprise. Docteur de l'université Paris VII avec une thèse réalisée au laboratoire LMD-Polytechnique, il a débuté sa carrière dans le conseil, chez Altran, il y a une vingtaine d'années. Il y devient consultant senior en quatre ans. Au bout de quelques années, il rejoint un opérateur télécom par soucis d'appartenir véritablement à une entreprise. Cet opérateur se construisait à l'époque et laisse ainsi un très bon souvenir à Jean-Luc Raffaëlli. Spécialisé sur des thématiques comme la gouvernance ou l'architecture des systèmes d'information, il rejoint La Poste en 2007 pour travailler avec un directeur qu'il appréciait énormément à titre personnel. Il représente son entreprise auprès du Cigref sur des thématiques comme l'Open Source et le Cloud, toujours en concertation avec les métiers. Il dirige le domaine « valorisation de la donnée » et participe aux différentes déclinaisons au niveau du système d'information de la stratégie générale du groupe La Poste. ■

Utiliser l'open-source c'est bien. Contribuer, c'est mieux.

CIO : Comment convaincre une entreprise de payer pour améliorer une solution qui va profiter également à d'autres ?

Jean-Luc Raffaëlli : Le passage de ce cap de maturité est difficile, ne le cachons pas. Mais il s'agit d'améliorer les solutions pour qu'elles satisfassent mieux nos besoins. Il y a bien entendu, comme sur tous les projets, un ROI à déterminer et il ne s'agit pas de financer n'importe quoi n'importe comment. Nous faisons cela sur des projets dont je ne peux pas vous dévoiler les détails. Il faut, pour commencer, réussir à faire formuler aux utilisateurs qui vont financer les projets les avantages de disposer d'un système ouvert.
Il s'agit, finalement, de reprendre la main sur l'histoire du système d'information pour ne plus payer plusieurs fois, par les différents clients, pour un seul investissement.

CIO : Ne payer qu'une fois, cela ressemble à la démarche de l'Adullact (Association des Développeurs et des Utilisateurs de Logiciels Libres pour les Administrations et les Collectivités Territoriales) qui développe ou fait développer en logiciels libres des solutions métier mutualisées pour les collectivités locales ?

Jean-Luc Raffaëlli : Tout à fait. L'Adullact est, de ce point de vue, tout à fait exemplaire. De la même façon, l'idée de la région Ile de France de rendre compatible Libre Office avec le cloud est excellente. C'est un investissement raisonnable pour couvrir un besoin commun à tous.
Mais la bataille de la feuille de route écrite par les utilisateurs, les clients, n'est pas encore gagnée. Pour cela, il faudrait que les clients aient une vision stratégique, prospective. La première question est en effet celle de la gouvernance et de la stratégie.
Finalement, c'est la même chose qu'avec l'Open Data : l'ouverture, le co-investissement et la co-innovation profitent à tout le monde. Et un grand groupe comme La Poste se doit de piloter l'empreinte qu'il laisse sur son environnement.

CIO : Le risque de l'open-source n'est-il pas justement l'absence de la béquille que constitue malgré tout la vision d'un éditeur traditionnel de logiciels propriétaires ?

Jean-Luc Raffaëlli : Clairement, que ce soit pour les développements ou les implémentations, une absence de méthode et de vision aura des effets pires avec de l'open-source qu'avec du propriétaire.
Mais c'est aussi parce que le vrai gain de l'open-source se fait dans la durée, la pérennité, la capacité à choisir le destin de son système d'information et les évolutions de sa gouvernance. ■

Bertrand Lemaire

VICE-PRÉSIDENT DE L'OPEN WORLD FORUM 2012

Jean-Luc Raffaëlli sera en 2012 vice-président de l'Open World Forum. Cette manifestation, dont CIO est partenaire, se déroule du 11 au 13 octobre 2012 et comprend un parcours spécifique dédié aux DSI, l'OpenCIO Summit, le 11 octobre, dont Jean-Luc Raffaëlli sera le parrain. Ces deux manifestations auront lieu à l'Eurosite George V, avenue George V à Paris.
Parmi les thèmes abordés à l'OpenCIO Summit, notons : les travaux de gouvernance menés par la DISIC (Direction interministérielle des systèmes d'information et de communication de l'État), les marchés de support, l'Open Source et le Numérique, l'Open Source et les méthodes agiles au service de la DSI... Outre le keynote d'ouverture de Jérôme Filippini (Directeur interministériel des systèmes d'information et de communication de l'État), la manifestation se base sur des témoignages de DSI comme Bruno Ménard (Directeur informatique Groupe Sanofi-Aventis, vice-président du CIGREF) et Michel Delattre (DSI Groupe La Poste).
Jean-Luc Raffaëlli précise : « *parmi les sujets abordés, il sera aussi bien question de stratégie que de manière de contribuer à la communauté, ou bien comment avoir une démarche prospective, donner une transversalité aux données en interne et en externe pour en accroître la valeur.* » ■

PUBLI-REDACTIONNEL

MATINÉE STRATÉGIQUE

CONFÉRENCE ORGANISÉE LE 27 MARS 2012 PAR CIO

Sélectionner les ressources et le pilotage pour créer de la valeur

Le pilotage économique de la DSI est une obligation pour les décideurs IT. Ils doivent alors se rapprocher des directions financières. Les bonnes pratiques ont été exposées durant la conférence organisée au Pavillon Dauphine, le 27 mars, par les rédactions de CIO et du Monde Informatique en partenariat avec HP, Wipro et Egeys.

« Pour ne pas se perdre dans de multiples couches de concepts, il faut revenir aux fondamentaux et définir clairement ce qu'est le pilotage » a martelé Francis Capdepuy, Directeur chez ISG One, maison mère de Compass, spécialiste du benchmarking. Il s'exprimait en ouverture de la conférence sur l'optimisation du pilotage des systèmes d'information organisée par les rédactions de CIO et du Monde Informatique, en partenariat avec HP, Wipro et Egeys. Il a rappelé que les métriques de pilotage des systèmes d'information reposent sur des concepts tels que l'efficacité du service, à mesurer par les utilisateurs, et son efficience, à mesurer par la DSI.

Améliorer la collaboration entre DSI et DAF

Au-delà, il est indispensable que la DSI collabore avec la Direction Administrative et Financière qui détient les clés des investissements et des ratios de performance. *« Nous avons mené une étude sur l'amélioration des relations DSI-DAF avec le cabinet américain CFO Research »* souligne Bruno Buffenoir, Vice Président Sales de HP France. Il apparaît que les contraintes de chacune des directions sont totalement différentes. Pour autant, on peut formuler un *« objectif commun, qui est de réduire le time-to-deliver, en respectant les contraintes économiques »* résume Bruno Buffenoir. Chaque direction se doit de comprendre les fondamentaux de l'autre. Au bout du compte, il convient de refondre le modèle de service de la DSI et de facturation aux directions utilisatrices.

Une externalisation à géométrie variable

Le coût est au cœur du management des ressources qu'il s'agisse de services ou d'équipes IT. Lors de la table ronde qui a suivi, il est apparu que l'externalisation est une démarche stratégique à géométrie variable dans le temps et selon les périmètres. Une tendance à ré-internaliser certaines compétences clés, qui constituent l'atout concurrentiel de l'entreprise, se faisant jour.

Cette table ronde centrée sur les bonnes pratiques en matière de Sourcing réunissait Pierre Dulon, DSI de Crédit Agricole Corporate and Investment Bank ; Patrick Franchinard, Directeur de l'activité Electronique du groupe Air Liquide en Europe ; Dominique Poussin, Secrétaire général de la DSI-RC et directeur du contrôle de gestion et de la comptabilité du GIE Agirc-Arrco et Philippe Vilandrau, Directeur des opérations de VSC Technologies, l'entité technologique de Voyages-SNCF.com. ▶

Comment réduire les coûts

Face à la pression sur la DSI, Olivier Gaspar, Directeur de programmes de Wipro, est alors intervenu pour expliquer quels leviers sont disponibles. Il a chiffré les marges de manœuvre qu'il identifie en matière d'optimisation des coûts sans nuire à la nécessaire réactivité ni négliger les risques, de type sécurité ou obsolescence technologique. Il cite un potentiel d'économies allant de 5 % à 40 % selon les domaines IT. *« La pression sur les coûts est évidemment forte en période difficile mais ne penser que réduction des coûts peut être gênant à moyen terme »* a-t-il prévenu mettant en avant la nécessité des actions de transformation, de modernisation et d'industrialisation des processus.

La DSI face à la logique financière de l'entreprise

Le rapprochement entre la DSI et la direction financière doit s'effectuer en toute transparence lorsqu'il s'agit d'arbitrage en matière de projets métiers. C'est le point de vue défendu par Jean-Claude Lebois, Président du cabinet Egeys et ancien DSI d'un grand groupe d'assurances. Pour lui, la DSI doit disposer de l'outillage ad hoc afin d'intégrer, en temps réel, la logique financière de l'entreprise malgré un environnement de plus en plus complexe. *« Dans l'assurance par exemple »* décrit-il, *« un décret sortant le 31 décembre peut être applicable au 1er janvier avec de forts impacts tant sur les métiers que sur les systèmes d'information. Il faut donc piloter en temps réel ses projets avec toutes les directions métier simultanément. »*

Au bout du compte, il n'en reste pas moins que les projets IT doivent être rentables. Comment calculer ce ROI et définir la valeur créée par la DSI ? Ce calcul est complexe, et dépend de chaque entreprise lorsqu'il s'agit de prendre en compte les coûts et les diverses formes de création de valeur. C'était l'objet de la seconde table ronde qui a réuni Georges Epinette, Directeur Général de la Stime et DOSI du Groupement des Mousquetaires ; Eric Lovisolo, Directeur financier du Printemps, Francis Massé Secrétaire général de la DGAC (Direction Générale de l'Aviation Civile) et Fabrice Portilla, contrôleur de gestion de Systalians. ■

Pour en savoir plus

CIO

Retrouvez
les vidéos et les présentations de cet évènement
sur **CIO Online**

Les dépassements de budgets et de délais des projets de PGI sont désespérément ordinaires

Les projets à base d'Oracle e-Business Suite sont confrontés à de plus longs retards que les projets SAP ou Microsoft Dynamics. C'est le résultat d'une analyse mondiale menée par Panorama Conseil et relayée par nos confrères américains de CIO.com.

Il est malheureusement fréquent de voir des projets de PGI (Progiciel de gestion intégrée) impliquant Oracle, SAP ou Microsoft Dynamics finir par prendre plus de temps que prévu par les clients de ces produits. C'est ce que révèle l'enquête publiée début juillet 2012 par Panorama Consulting, une société de la région de Denver spécialisée dans la sélection et l'implémentation de PGI. Cette société se présente comme un cabinet de conseil totalement indépendant et n'ayant aucun lien financier avec un quelconque fournisseur.

Cette enquête est basée sur 2000 réponses provenant de 61 pays recueillies entre février 2006 et mai 2012. Environ 40 % des répondants étaient en Amérique du Nord a précisé le président de Panorama Consulting Eric Kimberling lors d'un webinaire de présentation de l'étude. Environ 61 % des répondants ont déclaré que leurs projets ont duré plus que prévu, tandis que 28 % des projets ont été terminés à temps et 11 % ont été achevés plus tôt que prévu.

Les progiciels moins en cause que les projets eux-mêmes

Le progiciel employé n'est en général pas en cause dans les problèmes des projets, toujours selon l'enquête. Ainsi, seulement 4 % des répondants ont cité des problèmes de fonctionnalités fournies par l'éditeur comme étant une raison pour les retards du projet, bien que « *les problèmes techniques* » ont été invoqués par 14 %.

Un changement dans la portée initiale du projet était la principale raison des ralentissements, tel que mentionné par 29 % des répondants au sondage. « *Les questions d'organisation* » viennent ensuite avec 20 %, suivies par « *les problèmes de données* » et « *les contraintes de ressources* » avec 17 % chacun.

Une justification essentielle pour des projets de PGI est la promesse d'un retour sur l'investissement consenti en logiciels par l'entreprise. Mais l'enquête de Panorama Consulting a révélé que près d'un tiers des répondants n'avaient pas encore réalisé des bénéfices financiers en lien avec leurs projets, et une autre part de 30 % a déclaré qu'il a fallu au moins trois ans pour commencer à voir un début de rentabilisation.

Microsoft Dynamics arrive moins en retard que ses concurrents

Microsoft Dynamics arrive en tête du peloton en termes de rapidité de mise en œuvre globale, en moyenne 13 mois réels (contre 11 mois prévus) contre 17 mois (15 mois attendus) pour SAP et 18 mois (14 mois attendus) pour Oracle, selon l'enquête. Les projets SAP et Microsoft Dynamics ont donc dépassé en moyenne de deux mois le calendrier prévu, tandis que les implémentations d'Oracle subissent en moyenne quatre mois de dépassement. Ces résultats doivent cependant être considérés avec une certaine prudence, car Microsoft Dynamics tend à être mis en œuvre par les petites entreprises avec des environnements moins complexes, comme Eric Kimberling l'a rappelé pendant son webinaire. ▶

La rentabilité toujours en question

Dans l'ensemble, les répondants sont inquiets au sujet des bénéfices qu'ils peuvent retirer de leurs projets PGI. 60 % considèrent « *la disponibilité de l'information* » comme un plus, mais seulement 7 % jugent pouvoir retirer une « *baisse des coûts de main-d'œuvre.* » En outre, l'enquête proposait comme bénéfices liés à la bonne réalisation des projets PGI des items tels que « *réduire les coûts informatiques* » ou « *améliorer les relations avec les clients* » mais ces items n'ont été cités que par très peu de répondants. Panorama Consulting en déduit que « l*a sélection de ces items par un pourcentage désespérément petit des répondants implique que les avantages potentiels du PGI ont peu de chance d'être réalisés.* »

Parfois, les projets ERP vont si mal que les clients finissent par poursuivre leur fournisseur, ou vice-versa. Oracle, pour sa part, est actuellement impliqué dans un différend très médiatisé avec la Montclair State University. Epicor a également été la cible d'un certain nombre de procédures récentes. ■

Chris Kanaracus / CIO.com

Pour en savoir plus
CIO
Retrouvez
la version originale
sur
CIO.com

HUMEUR

CIO EVENEMENTS 2012

Inscrivez-vous dès à présent aux conférences 2012 sur cio-online.com

27 septembre 2012

LE DÉCISIONNEL PASSE A LA VITESSE SUPÉRIEURE

Le décisionnel à l'ère du big data et des réseaux sociaux

9 octobre 2012

AGILITE DES SYSTEMES D'INFORMATION

Les accélérateurs du changement

20 novembre 2012

INNOVATIONS ET DÉFIS 2013 DE LA DSI

L'innovation IT au service de la compétitivité de l'entreprise

SOMMAIRE N° 56 SEPTEMBRE 2012

Pour toute demande concernant CIOpdf : cio-abonnement@it-news-info.com - N° de téléphone dédié : 03 27 32 26 29

Une publication de :
IT NEWS INFO - 40 boulevard Henri Sellier 92150 Suresnes • 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
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 septembre 2106
Siret : 500 034 574 00029 RCS Nanterre