N°5 I MARS 2017

CONDUIRE LA TRANSFORMATION NUMÉRIQUE DE L'ENTREPRISE

SMART DSI®

DOSSIER

GDPR : La protection des données en Europe

STRATEGIE

La mobilité en entreprise en 2017

DECRYPTAGE

Comprendre les objets connectés

L'ETUDE A RETENIR

Maîtriser la donnée : l'enjeu des Directions métiers

www.smart-dsi.fr

2017 : question de sécurité !

En ce début d'année, la sécurité est au cœur de toutes les attentions. Qu'il s'agisse d'environnements professionnels mais aussi de services de l'Etat avec les élections présidentielles, le challenge sécuritaire préoccupe.

Le sujet est d'autant plus sensible qu'une autre échéance approche rapidement : mai 2018. Cette date résonne avec la GDPR (General Data Protection Regulation), cette fameuse réglementation européenne sur la protection des données. Et là, il y a urgence. Depuis son entrée en vigueur en mai 2016, tout s'accélère pour les DSI ou tout devrait, pour le moins, s'accélérer en entreprise, puisqu'aucune n'échappera à la loi ! Au-delà des contraintes, ne faut-il pas y voir une opportunité de repenser la sécurité des données personnelles et de se poser les bonnes questions ?

A l'heure où la mutation digitale permet à tous d'être mobiles et rend possible un accès permanent aux données, les risques sont évidemment bien plus importants. Les données véhiculant nombre d'informations de grande valeur et confidentielles poussent les entreprises à se repositionner face au défi sécuritaire. Les conformités légales et le choix d'offres techniques doivent s'accompagner de mesures juridiques et organisationnelles. Gérer la mobilité est devenu une priorité d'autant que la transformation numérique repousse les limites et décuple les projets mobiles.

Ainsi, prendre le temps de faire le point sur la cybersécurité est une résolution 2017. Cyberespionnage, cyberadversaires, surveillanceware, des mots qui ne doivent pas écarter les fondamentaux. En effet, au-delà de la mise en place d'une stratégie de la gouvernance, les enjeux passeront, notamment, par une adaptation des solutions, par la formation et sensibilisation des collaborateurs et par une prise de conscience de la nécessité d'une Direction des risques.

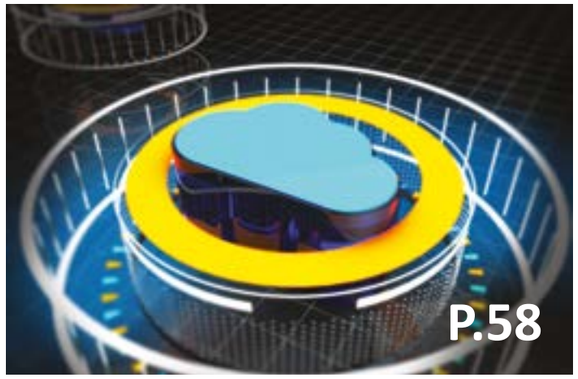
La sécurité touche, finalement, le cœur même de toute innovation. Par conséquent, la DSI n'en finit pas de multiplier les missions et décrypter les tendances technologiques sur lesquelles il faut absolument parier en 2017 !

Très bonne lecture !

Sabine Terrey
Directrice de la Rédaction
sterrey@itpro.fr

SMARTDSI

N°5 I MARS 2017



SMARTDSI

Rédaction
Pour joindre les membres de la rédaction
redaction@smart-dsi.fr

Comité de rédaction associé à cette édition
Loïc Duval, Théodore-Michel Vrangos, Fabrice Di Giulio, Juliette Fauchet, Marie Varandat, Loïc Thobois, Laurent Teruin

Régie Média & Publicité - Com4Médias
Renaud Rosset – Directeur Conseil
renaud.rosset@com4medias.com
Tél. 01 39 04 24 80

Abonnements
Smart DSI - Service Abonnements
BP 40002 - 78104 St Germain en laye cedex
Tél. 01 39 04 24 82 - Fax. 01 39 04 25 05
abonnement@smart-dsi.fr

Conception & Réalisation
Studio C4M – José Agaramunt
conseil@com4medias.com

SMART DSI est édité par IT PROCOM
Directeur de la Publication : Sabine Terrey

IT PROCOM - SARL de Presse au capital de 8.000 €, siège social situé : 10-12 rue des Gaudines, 78100 St Germain en Laye, France. Principal Actionnaire : R. Rosset Immatriculation RCS : Versailles n°438 615 635 Code APE 221E - Siret : 438 615 635 00036 TVA intracommunautaire : FR 13 438 615 635

N° ISSN : 2494-9701 - N° CPPAP : 0518 T 93059
Dépôt légal : à parution - Imprimé en France par IMPRIMATUR 87400 St Léonard de Noblat

Site officiel : www.smart-dsi.fr

MS Cloud Summit Paris 2017
PARI REUSSI

Pas d'annonce produits mais des cas d'utilisation et des présentations techniques.

Avec son axe résolument technique et usage des solutions Cloud et Hybride de Microsoft, le MS Cloud Summit Paris 2017 a trouvé son public. Ici pas d'annonce produits, mais des présentations techniques et des cas d'utilisation.

800 participants en 2 jours

Carton plein pour cette première édition du MS Cloud Summit Paris 2017. Laurent Cayatte, président de Metsys et partenaire de cet évènement, savoure « **C'est une réussite ! 800 participants sur les deux jours de conférences et nous avons même été contraints de refuser du monde** ».

Installé au centre de conférences New Cap à Paris, du 23 au 25 janvier, le MS Cloud Summit Paris 2017 n'est pas un événement comme les autres.

Ici, **les speakers sont des experts techniques, des architectes, des développeurs, des consultants, des datascientists** tous spécialistes de l'environnement Microsoft.
« Ici, vous ne croiserez pas de directeurs marketing ou de commerciaux venus faire la promotion de leurs offres ».

Un événement monté par cinq communautés Microsoft

A l'origine de cet événement, cinq communautés créées autour de l'offre de l'éditeur de Redmond : AOS, Agile.net, AZUGFR, CMD et GUSS. « Leur objectif : créer un événement pour partager de l'information technique et usage autour des solutions Cloud et Hybride de Microsoft » déclare Laurent Cayatte. En d'autres termes se différencier des emblématiques Tech Days ou MS Experiences très orientées offres et produits. Laurent Cayatte se souvient « il y a une quinzaine d'années, Microsoft organisait dans ses locaux rue de l'université, IT Pro, un événement centré sur la technique. L'idée, aujourd'hui, est de reprendre ce concept ».

Au MS Cloud Summit, **les interventions sont techniques, cas d'applications et sans langue de bois.** Les speakers n'ont pas hésité à aborder les difficultés rencontrées lors des déploiements des solutions. Des discours qui plaisent à l'auditoire.

2 conférences plénières et 72 ateliers

Animés par des indépendants ou des experts issus d'Entreprise de Services du Numérique (ESN), 72 ateliers se sont enchainés autour d'Azure, d'Office 365, de SQL Server 2016, de SQL Server sur Linux, de Docker, de SCCM, de SharePoint ou encore d'Exchange. Microsoft a, quand même, fait une brève apparition lors des plénières, avec notamment la présence de Julia White, Vice-President Azure and Security marketing Microsoft Corporate, venue des Etats-Unis pour assurer la deuxième conférence plénière « Nous sommes très fiers. Cela prouve l'intérêt que porte Microsoft à l'axe choisi par le MS Cloud Summit Paris 2017 » se réjouit Laurent Cayatte.

Avec ce type d'événement, tous les partenaires de Microsoft espèrent gagner en visibilité et créer un véritable écosystème pour échanger et partager leurs expériences et leur savoir-faire.

Holoscent
PLACE A LA REALITE MIXTE OLFACTIVE

Avez-vous entendu parler du duo « réalité mixte » et « hologrammes olfactifs » ? Un binôme qui s'en donne à cœur joie ! Eclairage.

Présentée à Paris fin janvier, l'expérience « HoloScent » a reçu un accueil tout à fait favorable du public.

Quand l'expérience mêle la réalité mixte et les hologrammes...

Une toute nouvelle expérience de réalité mixte composée d'hologrammes olfactifs vient de voir le jour. Développé par Synergiz, entreprise de services numériques, spécialisée en interfaces naturelles, et Exhalia, pionnier du marketing olfactif, « HoloScent », dispositif multi-sensoriel vous donne la possibilité de visualiser des éléments virtuels dans un environnement réel et d'y associer différentes odeurs particulières.

Une immersion sensorielle

S'appuyant sur les lunettes Microsoft HoloLens et le collier connecté olfactif Exhalia, « HoloScent » renforce et « booste » l'univers et l'expérience utilisateur en développant et activant en même temps plusieurs sens comme la vue, l'ouïe et l'odorat.
Et les champs d'application ne manquent pas, entre cosmétique et parfumerie, en passant par l'alimentaire jusqu'à la santé, tout comme les cas d'usage proches de la conception et du marketing ! Encore une expérience à suivre de près !

GDPR

Le Règlement Général Européen sur la Protection des Données

IL EST PLUS QUE TEMPS DE S'Y METTRE !

> Par Loïc Duval

LES BONNES PRATIQUES DE LA RÉGLEMENTATION EUROPÉENNE SUR LA PROTECTION DES DONNÉES

La GDPR est là... Et bien trop de DSI, bien trop d'entreprises, en ignorent jusqu'à son existence ! Pourtant aucune d'entre elles n'y échappera. Bien plus qu'une loi contraignante, la GDPR est une invitation à de bonnes pratiques et un ensemble d'opportunités...

Entrée en vigueur le 25 mai 2016, la nouvelle réglementation européenne sur la protection des données, ou General Data Protection Regulation (GDPR), concerne tous les organismes collectant, gérant ou stockant de la donnée. Les entreprises ont deux ans au maximum pour se mettre en conformité, soit jusqu'en mai 2018. Mais vu l'ampleur du chantier, 15 mois ne seront pas de trop !

- 01 -

Nouvelles règles et des concepts existants étendus

En soi, et notamment en France où les données personnelles sont déjà très protégées par diverses réglementations, la GDPR ne bouleverse pas fondamentalement la donne. En tout cas, pas pour les grandes entreprises déjà soumises à des règlementations fortes. Comme le souligne Fabrice Lorvo, avocat associé du Cabinet FTPA, « la GDPR est un outil très utile dans le conflit entre le droit européen applicable aux internautes de l'UE et le droit américain revendiqué par les GAFAs. Aux USA, le concept de donnée personnelle n'est pas reconnu. C'est une marchandise ».

Pour autant, la GDPR introduit quelques notions nouvelles en matière de gestion des données personnelles dont notamment le droit à l'oubli, c'est-à-dire la possibilité pour chaque individu d'exiger la suppression de ses données des bases d'une entreprise. Surtout, elle impose à toute entreprise de respecter des données qui, finalement, ne leur appartiennent pas. Elle les invite à se poser des questions que nombre d'entre elles ont, jusqu'ici, refusé de se poser : quelles sont les données à caractère personnel que nous récoltons ? Qui y a accès ? Ces données sont-elles suffisamment protégées pour être inexploitables en cas de vol ou de brèche dans nos défenses cyber-sécurité ?

La réglementation s'applique à toutes les entreprises, y compris les organisations hors Union Européenne (UE) mais qui font des affaires avec l'UE ou utilisent des données personnelles de ressortissants de l'UE.

Elle impose, aussi, la nomination d'un DPO (Directeur de la Protection des données) dans toutes les entreprises traitant des données personnelles et réaffirme le principe de « minimisation » selon lequel les données collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Elle impose aux entreprises d'obtenir le consentement de l'utilisateur avant toute collecte d'informations personnelles en précisant dans quel but cette collecte a lieu et d'avertir les utilisateurs en cas de modification des finalités de cette collecte.

- 02 -

Des enjeux financiers colossaux

Enfin, dans les évolutions notables, il faut encore ajouter la responsabilité juridique directe des entreprises et l'obligation de signaler toute violation de données, dans les 72 heures suivant la constatation, à l'autorité européenne.

Si les données sont insuffisamment protégées et sont potentiellement exploitables par le pirate, l'entreprise est aussi tenue – par le biais de son DPO – de notifier la fuite aux personnes concernées. Combinées à la loi de modernisation de la justice autorisant notamment les actions collectives en justice, ces nouvelles dispositions signifient que la moindre fuite ou non-respect de la GDPR peut coûter cher, très cher même.

En effet, les clients pourront intenter des actions collectives contre les entreprises ne respectant pas la réglementation ou qui n'auront pas su protéger leurs données.

Par ailleurs, la moindre violation fera forcément le buzz sur Internet, détruisant au passage l'image de la société.

Et n'oublions pas les sanctions prévues par la réglementation : jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial pour une non-conformité, le montant le plus élevé étant retenu.

Enfin, cerise sur le gâteau, gageons que les assureurs vont s'inviter à la danse en réévaluant leurs primes d'assurance à la mesure du risque encouru.

- 03 -

Pas de conformité sans gouvernance des données

Face à de tels enjeux, on peut s'étonner du manque d'empressement des entreprises à se conformer à la réglementation. Une étude réalisée par Symantec auprès de 900 entreprises françaises montre en effet que 22% d'entre elles estiment qu'elles ne seront pas prêtes en mai 2018. De fait, l'empressement n'est, probablement, pas la seule explication quand on connait l'ampleur du chantier. Pour protéger les données personnelles, les entreprises doivent en effet savoir où elles sont. Or, pour des raisons à la fois historiques et organisationnelles, les données sont souvent éparpillées dans le système d'information et dupliquées dans différentes applications (CRM, ERP, logistique, etc.). Elles sont aussi parfois incomplètes ou erronées.

En d'autres termes, la première étape d'une mise en conformité consiste à établir une cartographie des gisements de données existants. Forte de cette connaissance, l'entreprise pourra alors classifier ses informations par degré de sensibilité et établir des règles de protection en établissant des droits d'accès, en appliquant du chiffrement lors des échanges mais aussi au niveau du stockage et de l'archivage, en masquant ou anonymisant une partie des données pour les rendre inexploitables en cas de violation ou encore en mettant en place des routines de suppression pour se conformer à la réglementation sur le droit à l'oubli.

En résumé, la mise en conformité est impossible sans une gouvernance des données. Gouvernance qui soit dit en passant doit impliquer tous les collaborateurs de l'entreprise ainsi que les fournisseurs. Il suffit d'un commercial transportant des données personnelles sur un ordinateur portable ou encore d'un prestataire utilisant des jeux de données réelles pour tester une application pour faire courir un risque à l'entreprise...

Pour chaque donnée personnelle, les entreprises devront documenter un PIA (ou en Français EIVP -Étude d'impact sur la Vie Privée -) analysant l'impact en cas de brèche.

Les entreprises devront également nommer un DPO (Data Protection Officer) qui servira d'interface entre l'entreprise et l'autorité de régulation (La CNIL). Contrairement à l'ancien « CIL » au profil technique proche de la DSI, le DPO doit être en relation directe avec la Direction Générale et posséder un profil à la fois juridique et technique. Il doit pouvoir s'appuyer sur un comité de gouvernance associant DSI et métiers. C'est à lui d'avertir la CNIL en cas de fuite en fournissant les PIAs nécessaires. La CNIL décidera alors, selon les mesures mises en œuvre, du risque réel et imposera à l'entreprise non seulement les sanctions financières mais également l'obligation de porter la fuite sur la place publique.

- 04 -

Un chantier et des opportunités

La GDPR est donc un chantier auxquelles aucune société ne peut aujourd'hui échapper. L'effort dépend évidemment de la taille de l'entreprise. Mais contrairement à une idée fréquemment répandue, il n'est pas hors de portée des PME. « Face à la GDPR, il existe une segmentation par rapport à la taille de l'entreprise et aux ressources » explique Laurent Heslault, Security Strategist chez Symantec. « Au niveau des grands comptes, il y a ceux qui sont déjà soumis à des réglementations souvent bien plus contraignantes que la GDPR et sont déjà bien équipés face à ce qu'ils appellent le 'mille-feuille règlementaire'. Ils ont déjà les équipes et les compétences. Et puis il y a les entreprises et industries multinationales qui n'étaient pas encore confrontées à ce genre de réglementation contraignante et qui vont devoir mettre en place des compétences.

C'est un très gros projet à plusieurs mois qui ne s'improvisera pas. Enfin, il y a les TPE et PME, où l'identification des données personnelles ira généralement assez vite. L'important pour elles sera davantage que ses solutions Cloud soient conformes.

Elles devront aussi trouver des partenaires qui les aideront à se mettre en conformité et leur fourniront le DPO. »

Bref, la GDPR est là et bien là. Et les entreprises ne peuvent plus s'offrir le risque de l'ignorer plus longtemps. Elles doivent prendre cette règlementation comme autant d'opportunités à saisir : celle d'améliorer la confiance de ses clients en ses services, celle de se poser la question de la valeur des données récoltées, celle de repenser la sécurité des données à caractère personnel comme confidentiel.

La révolution des compétences

L'efficacité des technologies ne doit pas sous-estimer l'investissement dans le capital humain.

Prendre en compte les outils de l'ère digitale est une chose, acquérir en permanence le savoir-faire et les compétences pour s'adapter en est une autre. Il en va de la responsabilité des dirigeants, de la compétitivité des entreprises et des talents de demain.

Accélérer les rythmes de formation

Les compétences dites « humaines » à savoir l'esprit critique, la créativité, et l'intelligence émotionnelle sont des sources de valeur parfois sous-estimées. En doublant le rythme auquel les employés acquièrent toutes les compétences nécessaires, la part des emplois menacés par l'automatisation pourrait être réduite :

- de 10 % à 4 % aux Etats-Unis
- de 9 % à 6 % au Royaume-Uni
- de 15 % à 10 % en Allemagne

Prôner le numérique positif

L'impact du numérique sur le travail est positif pour 87% des employés (78% en France).

Les robots, l'analytique et l'intelligence artificielle les aideront

- à être plus efficaces (74% Monde - 67% France)
- à acquérir de nouvelles compétences (73 % Monde - 67% France)
- à améliorer la qualité de leur travail (66 % Monde - 56% France)

Investir dans le capital humain

Développement du self-service, importance des contacts humains, gestion de situations émotionnelles et de situations imprévues, capacités à développer de l'empathie ou de l'autorité, pour ne citer que ces critères. Les compétences humaines prennent leur essor et les collaborateurs sont conscients de la nécessité de la formation, de l'appropriation des technologies numériques et du repositionnement des tâches. Il faut repenser le travail pour tirer parti du potentiel humain.

Les dirigeants doivent se réinventer et imaginer différemment leurs manières de motiver, récompenser et soutenir les collaborateurs. Des facteurs liés au bien-être, à l'implication, à la qualité de vie, et à la reconnaissance sont devenus des indicateurs clés.

Le digital pour former au digital

Plusieurs pistes peuvent être évidemment envisagées. Il en est une importante à savoir capitaliser sur l'état d'esprit actuel basé sur l'apprentissage permanent et utiliser le numérique pour former à grande échelle.

E-learning, MOOC, technologies portables « wearable » pour former en temps réel sur les lieux de travail, logiciels intelligents pour la formation personnalisée, recommandations et aide dans les besoins d'apprentissage des collaborateurs.

Etude Accenture Strategy. Enquête en ligne fin 2016 en Allemagne, France, Italie, Turquie, au Royaume-Uni, aux Etats-Unis, Brésil, en Australie, Inde et au Japon, auprès de 10 527 professionnels (dont 1 023 en France) représentant différents domaines de compétences et de générations.

Les enjeux français
DE LA CYBERSECURITE EN 2017

Le grand avantage du FIC (Forum International de la Cybersécurité) est qu'il a lieu en janvier ; cela donne une vision en perspective de l'année qui commence. Mais prévoir est incertain, chaque année ayant son lot de surprises…

La 9ème édition du FIC en 2017 a été un franc succès. Surtout le premier jour avec une forte affluence. Sans vouloir comparer l'événement lillois aux Assises de la sécurité qui se tiennent à l'autre bout de la France, cet événement de la cybersécurité devient le kick-off de début d'année, facile d'accès, gratuit et proche de Paris. En phase avec la croissance du secteur de la SSI, l'édition qui vient de se terminer a vu plus d'exposants et plus de visiteurs. Historiquement axé sur les secteurs public et militaire (on y voit d'ailleurs un florilège d'uniformes de toutes origines), le salon a mis en avant autant les éditeurs/constructeurs que les sociétés de services, conseil, ingénierie, audit, formation. A ce propos l'ANSSI, l'Agence Nationale de la Sécurité des Systèmes d'Information, a fêté sa première promotion de formateurs-sensibilisateurs à la sécurité labélisés SecNumedu. Une Agence, avec ses deux stands, très active sur tous les plans : du label France Cybersécurité au programme de certification PDIS (Prestataires de Détection d'Incidents de Sécurité) en passant par le renforcement des liens européens ou les conseils pour la mise en œuvre d'un SOC.

Le FIC 2017 a démontré, par sa montée en puissance, la prise de conscience des entités et organismes d'Etat.

La cybersécurité 2017

L'année 2017, avec les élections présidentielles et législatives, est bien délicate "cybersécuritairement" parlant pour les Services de l'Etat et particulièrement pour l'ANSSI. Une élection présidentielle, c'est l'élection d'une personne, une cible unique. Elle est plus facile à attaquer, à dénigrer, d'en manipuler l'image, que de viser un parti politique avec des centaines de représentants. La cybersécurité est au cœur de ce danger pour la démocratie.

Le vol des données des partis, candidats et sympathisants, le vol et la divulgation des emails, la fabrication des faux mails compromettants, la manipulation des informations, le dénigrement anonyme et exponentiel avec le levier des réseaux sociaux, les attaques à l'intégrité des informations, les attaques en DDoS, le piratage des sites, etc. sont des dangers autant pour les équipes des candidats que pour les partis politiques. Les médias aussi, ainsi que les instituts de sondages, dont on sait les fragiles équilibres financiers, devraient prendre ce risque au sérieux et investir en hommes et solutions pour protéger leurs ressources informatiques.

Pour notre métier, l'exemple de la présidentielle américaine a été un coup de tonnerre. Plus de hacker boutonneux bidouillant à distance depuis son garage mais de véritables structures étatiques de pirates informatiques. Selon les services secrets américains, les auteurs de l'attaque étaient entraînés, financés et encadrés par le service de renseignements de l'armée russe. Les révélations sur le piratage de la messagerie du directeur de campagne d'Hillary Clinton et le rapport de la CIA accusant Moscou, montrent que la cyberattaque lors de la présidentielle américaine est un acide corrosif caché, rongeant la démocratie et la société américaine. Selon les services secrets américains, le paroxysme des cyberattaques était tel, que le 31 octobre, à quelques jours de l'élection, Barack Obama a appelé Poutine pour le menacer sur ces véritables actes de guerre.

Un sujet sensible

En France, le sujet est plus que sensible. Les structures des partis politiques sont légères, à l'image de PME avec de nombreux prestataires peu sensibles à la protection des informations, peu armés en amont et incapables de faire face à une cyberattaque.

Cette situation est aggravée par le manque de compétences techniques opérationnelles en SSI en France. La pénurie d'ingénieurs fait déjà très mal et les perspectives sont encore plus sombres. Les coûts augmentent, la disponibilité diminue. Peu d'ingénieurs rapidement compétents dans un environnement techniquement complexe, lié à la nécessaire transversalité technologique de la sécurité des systèmes d'information.

Car pour protéger un périmètre, il faut de la sécurité IP, de la sécurité du stockage, de la virtualisation, de la sécurité des identifiants, de l'OS hardening, de l'analyse post incident, de l'archéologie des logs, du bigdata appliqué à la sécurité, du monitoring des bases de données, etc.

Cette situation de pénurie s'aggrave et risque de freiner la croissance du secteur avec notamment une flambée des rémunérations sans réévaluation du prix des services. Déjà en 2017, plus encore en 2018, l'IA et le machine learning appliqués à la cyber surveillance apporteront de l'oxygène aux prestataires des services de cybersécurité. Assisterons-nous à la robotisation du traitement de la cyber surveillance ? Ou à l'émergence de SOC robotisés ?

L'externalisation

La complexification de la sécurité SI couplée au manque de ressources va pousser les entreprises à externaliser leur surveillance et leur SOC. La tendance 2017 est déjà là : après les OIV (opérateurs d'importance vitale) et les grands groupes, de plus en plus d'entreprises, ont contractualisé cette externalisation.

Le danger des données dans le cloud et leur exportation à l'extérieur de l'entreprise, souvent à l'insu des RSSI et DSI, par des applications en mode SaaS est un axe hautement sensible.

Le risque d'aspiration frauduleuse des données est bien réel. Cette menace constante exige une attention particulière ; les WAF (Web Application Firewall), les PAM (Privileged Access Monitoring), les coffres-forts de mots de passe pour l'authentification renforcée et la traçabilité, sont parmi les solutions inscrites dans les projets 2017. Ces solutions couvriront aussi les IoT et surtout les infrastructures industrielles de contrôle-commande/SCADA.

On ne peut terminer ce succinct tour d'horizon sans citer les conformités légales qui vont coûter temps et argent aux entreprises. La plupart des éditeurs présents au FIC citent à chaque phrase le règlement européen GDPR (General Data Protection Regulation), dont l'application par toutes les entreprises est prévue au 2ème trimestre 2018.

Rappelons la conformité LPM (Loi de Programmation Militaire) pour les entreprises concernées, mais aussi et toujours PCI DSS (avec ses craintes financières), et les conformités réglementaires sectorielles pour la finance, les jeux en ligne, les télécoms, etc.

> Propos de Théodore-Michel Vrangos, cofondateur et président d'I-TRACING, recueillis en exclusivité par la rédaction de SMART DSI.

Bon, maintenant que
J'AI OFFICE 365, JE FAIS QUOI ?

Partie 3 : Trois choses à ne surtout pas faire

Série d'articles sur la gouvernance à la fois technique et fonctionnelle de Office 365. Le thème central est « comment faciliter l'adoption et améliorer la productivité ».

Gouvernance version 3.0 : Conformité & Sécurité

La notion de conformité est à peu près aussi vague que celle de gouvernance.

Il s'agit d'un besoin métier, entendez donc par-là que chacun aura des besoins différents à ce sujet. Exemple très simple : demandez autour de vous ce qu'est un document confidentiel et comptabilisez le nombre de réponses différentes pour vous faire une idée de la complexité de la tâche. Car oui, la mise en place d'un plan de conformité est complexe et nécessite une profonde réflexion préalable, au même titre qu'un plan de gouvernance.

J'ai commencé à aborder ce point il y a trois ans avec mes clients, lors de leur passage sur Office 365 (ou sur SharePoint on premises). Si la mise en place d'un plan de gouvernance sonnait comme une évidence malgré parfois le manque de recul qu'ils pouvaient avoir, je me suis souvent retrouvé confronté à l'argument imparable : « nous ne sommes pas mûrs pour cela ».

Problème, aujourd'hui cet argument ne tient plus car on demande justement aux entreprises, ou organisations au sens large, d'être prêtes à cela. Pis, il n'est plus seulement question d'être prêt théoriquement, mais également en pratique. Pour prendre deux exemples contraignants pour les organisations, prenons la réglementation EU-GDPR ou les nouvelles prérogatives de la CNIL.

- **Dans le premier cas,** la gestion des informations relatives à la vie privée est désormais légiférée au niveau européen
- **Dans le second**, la CNIL a, désormais, la possibilité d'être proactive sur les contrôles qu'elle effectue, et les pénalités financières qu'elle peut infliger, peuvent s'élever à 4% du chiffre d'affaires mondial d'une entreprise.

Du point de vue légal, Il est donc obligatoire aujourd'hui pour les entreprises de se prémunir contre le risque d'infraction à des réglementations (on retrouve ici la notion de conformité).

Au-delà des aspects légaux, il y a toujours un point sur lequel les entreprises ne sont pas prêtes : c'est le risque de perte d'information, sensibles ou non. Ce risque est souvent négligé parce que dans la

grande majorité des cas, la source en sera humaine et sans volonté de nuire. Ce risque étant généralement situé entre la chaise et le clavier d'un poste de travail, comment mettre en place des garde-fous à la fois souples et efficaces ?

- Efficaces pour intercepter des comportements inappropriés/inattendus et gérer le facteur « Dark Data »
- Souples pour éviter une perte d'adoption de vos plateformes et la croissance du facteur « Dark IT »

Chose à ne pas faire #1 : trop brider le système

Et par extension les utilisateurs. La notion de Dark IT définit l'ensemble de processus informatiques mis en place en dehors du contrôle de l'IT, voire en dehors de sa connaissance. A trop brider un système, on ouvre la porte à la mise en place de processus parallèles car les utilisateurs ont maintenant très souvent pris l'habitude d'utiliser des outils collaboratifs publics pour leur usage personnel. Prenons par exemple un Office 365 dans lequel la collaboration est réduite à sa plus simple expression (celle d'un référentiel documentaire auquel seuls les internes ont accès). Que vont faire les utilisateurs ayant besoin de partager du contenu avec l'extérieur ? Les solutions sont nombreuses : OneDrive, Drop Box, Box, Google Drive et consorts. De là, comment s'assurer que les données partagées sont censées l'être ? Comment s'assurer de la sécurité de ces données partagées ?

Pourquoi ne pas envisager soit d'autoriser les partages externes avec les solutions natives offertes par Microsoft, soit des solutions tierces offrant plus de protection ?

Ouvrir le partage externe avec Office 365 passe par plusieurs étapes. La première consiste en une configuration des collections de sites SharePoint online qui auront cette fonctionnalité activée. La seconde, pour chaque collection de sites, consiste à définir comment le partage peut être fait :

- avec des utilisateurs externes déclarés dans l'annuaire de l'organisation
- avec des utilisateurs externes qui accéderont au partage via un lien et un compte Microsoft (live.com, outlook.com, hotmail...)
- avec des utilisateurs externes qui accèderont au contenu via des liens anonymes

Ceci a, néanmoins, des inconvénients : le premier est de ne pas pouvoir assigner la possibilité de partage externe à des utilisateurs distincts. Le second est de nécessiter plusieurs opérations de la part des externes pour accéder au contenu. Le troisième est la difficulté de monitorer clairement ces partages externes. Tout ceci peut avoir un impact négatif sur l'adoption et favoriser l'utilisation de moyens parallèles.

Avec l'apparition de Groups, de nouvelles collections de sites sont disponibles et toute la complexité de partage qui va avec. Par défaut, le paramètre de partage des collections de sites SharePoint qui font partie d'un groupe Office 365 autorise le partage avec les utilisateurs externes déclarés dans l'annuaire de l'organisation. Ceci signifie que malgré une configuration fine pouvant être faite pour SharePoint online, il est néanmoins facile d'avoir des partages externes actifs (même si relativement maîtrisés). Et donc de perdre le contrôle sur le contenu.

Chose à ne pas faire #2 : croire que le contenu est maîtrisé

Le Dark Data. Selon la définition de Gartner, il s'agit de l'ensemble des « données qui échappent à l'organisation de l'entreprise : ce qui n'est pas répertorié par l'entreprise mais par les salariés eux-mêmes qui cachent ces données volontairement ou involontairement ». Ces données, qui sont donc non structurées – du moins pas au sens de ce qu'attendrait l'entreprise –, non sécurisées, dispersées sur des emplacements potentiellement publics (serveurs de fichiers ou encore stockages cloud type OneDrive, Google Drive, Dropbox...).

Selon l'IDC (International Data Corporation), jusqu'à 90% des données des entreprises constitueraient ce Dark Data. Imaginez donc un iceberg. La partie visible : ce que vous connaissez. La partie immergée : le reste.

Prenons en exemple le cas d'un office de HLM il y a des années en arrière. Cet office mettait à disposition des quelques 12000 gardiens d'immeuble un fichier dans lequel un champ de commentaires devait être rempli avec les différentes interventions menées dans les logements (telles que des réparations électriques, plomberies, etc.). Sur dénonciation, il est apparu que ce champ contenait d'une part beaucoup d'informations relatives à la vie privée des locataires, mais également une collecte de données **subjectives** ou **d'infraction** ("alcoolique", "violence conjugale", "ancien SDF addiction boisson"...) ou relatives à la **santé** des personnes.

Pouvoir explorer ces données, les rendre intelligibles et les exploiter est une obligation pour les organisations ou entreprise. Tout d'abord l'exposition de ces données peut avoir un effet désastreux en termes d'image, voire coûteux en réparation de préjudices et amendes.

Ensuite, la dispersion de ces données peut s'avérer être une perte d'information, car si elles étaient exploitées, elles pourraient être une source de profitabilité. Imaginons le cas d'un manufacturier quelconque dont les retours clients et les opérations de service après-vente ne seraient pas connus du service de recherche et développement. Les défauts ne seraient pas corrigés – ou sur le tard – faisant traîner des coûts qui pourraient être identifiés plus tôt.

Enfin, car il est important d'identifier les données importantes de celles inutiles. Les doublons de fichiers stockés dans des emplacements différents, les données sans aucun rapport avec l'activité, etc. On peut estimer assez facilement à 30% les données qui n'ont absolument aucun intérêt pour l'entreprise. Sauf que ces données occasionnent des coûts, en termes de stockage, de gouvernance, etc. Enfin, parce que les emplacements de stockage non maîtrisés n'ont peut-être – certainement – pas le degré de sécurité requis pour la protection de certaines informations.

Outre l'exploration des données « à but lucratif », il faut aussi tenir compte du facteur sécurité. Dans tout le Dark Data figurent aussi des informations potentiellement nuisibles.

Prenons, par exemple, le cas d'un laboratoire pharmaceutique menant une étude clinique. Une fois l'étude terminée, les résultats peuvent être communiqués publiquement (du moins, dans le périmètre du laboratoire et des chercheurs) à la condition sine qua non d'avoir atteint un degré d'anonymisation affectant les participants, les médecins, le laboratoire ayant mené l'expérimentation. Seuls les résultats peuvent être rendus publics. Prenons un assistant qui masque une colonne de fichier Excel contenant les noms des personnes ayant participé aux tests, avant publication (par méconnaissance des outils, en tout bonne foi). Prenons enfin un laboratoire pharmaceutique ayant demandé l'expérimentation, qui trouve trace de ce document publié non anonymisé, et qui voit toute sa phase d'expérimentation annulée par ce simple fait. Dans ce cas, aucune volonté de nuire, mais une fuite d'information légalement inacceptable.

Pour explorer ces données, il n'y a pas vraiment d'autre choix que celui de l'analyse des documents. Il peut s'agir d'analyser les métadonnées, les modèles, des zone précises du document – entête ou pied de page par exemple – ou tout simplement d'en faire une analyse sémantique en se basant sur des règles telles que des dictionnaires, des expressions régulières, etc.

Comme pour une migration, un tel projet se compose de plusieurs phases :

1. Analyse des risques

Consiste en une phase de définition, avec les métiers, ce qui relève du risque pour l'entreprise. Par exemple, qu'est-ce qu'un document confidentiel (le nombre de réponses à cette question peut s'avérer particulièrement élevé) ? Quelle donnée est confidentielle ? Quelles réglementations doivent être suivies (CNIL, GDRP, méthodologies internes...) ? Mais également en allant au-delà de la définition des données « à risque », définir un comportement à adopter face à un cas concret. Par exemple, que faire lorsqu'un contenu confidentiel est trouvé hors de son périmètre restreint de diffusion ? Que faire si des contenus inappropriés sont trouvés dans des espaces non prévus pour les héberger ?

2. Définition des règles de recherche

Une fois que l'on sait ce que l'on recherche, d'un point de vue métier, il s'agit de le formaliser par des tests simples. Nous chassons les documents confidentiels ? Techniquement, comment cela se traduit-il ? Un pied de page avec une valeur « confidentiel ». Ou un template particulier. Ou un document contenant une référence à des mots clés précis. Ou encore ceux créés par des VIP. Ou tous les documents du service de ressources humaines... beaucoup de possibilités qui peuvent également être mixées pour définir différents niveaux de criticité (un document RH avec le nom des plus hauts dirigeants et le mot clé « salaire », au hasard). On définira également le périmètre de recherche pour chaque règle, et le type de recherche, temps réel versus planifiée.

3. Action selon les résultats de scan

Pour chaque violation, définir une action. Si la violation est une certitude et qu'une automatisation de la réaction est possible, on peut se passer d'un contrôle manuel, mais quid d'une situation qui requiert une action humaine pour analyser le risque ? Par exemple, un projet ultra confidentiel identifié

par le code « concorde » nécessite un scan large pour éviter toute fuite d'information. Concorde étant également le nom d'un avion, d'une place parisienne, un verbe conjugué, un arbitrage peut être utile et donc un processus par mise en quarantaine et gestion d'incident plus approprié.

Chose à ne pas faire #3 : croire que la technique peut tout résoudre

La sécurité est, en effet, l'affaire de tous. Et si la technique peut aider, beaucoup, il ne faut pas sous-estimer la puissance de calcul nécessaire pour scanner en continu des centaines de milliers de documents. Une grande majorité des problèmes relève, en fait, du comportement des utilisateurs, il ne faut donc pas hésiter à les impliquer dans le processus, par des formations, des rappels, etc.

Ensuite, celui qui souhaite soustraire des informations y arrivera TOUJOURS. Dès lors que l'accès aux données est possible, on peut les faire fuiter : par une photo sur un smartphone, une clé USB, une simple réécriture de mémoire d'informations confidentielles, etc.

La mise en place d'une stratégie de gouvernance de la sécurité est obligatoire désormais (elle l'était également avant, mais sous-estimée, trop coûteuse eu égard aux bénéfices, ou tout simplement jugée trop complexe).

- Les différentes réglementations internationales dissuadent de plus en plus les entreprises de ne pas mettre en place ce type de stratégie
- La responsabilité du RSSI évolue
- Les DPO (Digital Protection Officer) sont mis en place pour veiller au respect de la protection des données

La transformation est en cours, mais ce qui était un frein au choix d'Office 365 par manque de réponses à ces questions, ne l'est plus aujourd'hui. Microsoft fournit une base de protection au niveau plateforme et DLP, ses partenaires permettant d'aller beaucoup plus loin sur les terrains techniques et fonctionnels.

Le contexte étant posé, je détaillerai dans mon prochain article l'offre de protection proposée par Microsoft pour Office 365, ainsi que l'offre de certains de ses partenaires proposants des solutions ayant une couverture beaucoup plus large.

> Fabrice Di Giulio, MVP Business Solution, MCSE SharePoint et Productivité

Protéger les données des collaborateurs en mobilité

CONTRAINTES ET DEFIS

Les données numériques véhiculent un grand nombre d'informations de grande valeur, voire confidentielles. La révolution digitale permet à tous, notamment responsables et dirigeants d'être extrêmement mobiles. Ils peuvent avoir accès, en permanence, au système d'information de l'entreprise et peuvent ainsi travailler en tout lieu. Si cet accès permanent aux données de l'entreprise fait naître des réelles opportunités, il génère aussi de nombreux risques.

Les nouveaux défis sécuritaires imposent aux entreprises de se réorganiser en profondeur. Quelles sont les contraintes ? Quelles sont les bonnes pratiques à adopter ? Autant de questions auxquelles Matthieu Bourgeois, associé du département IT/ Propriété Intellectuelle du cabinet SIMON ASSOCIES a accepté de répondre.

Quelles sont les nouvelles sanctions et obligations de sécurité posées par le Règlement communautaire sur la protection des données ?

Le nouveau règlement communautaire (Règlement Général sur la protection des données – « **RGDP** ») prévoit une obligation de sécurité à la charge du responsable de traitement et du sous-traitant, comme le faisait déjà la Loi Informatique et Libertés, actuellement en vigueur, mais de manière plus précise par rapport à cette dernière puisque l'article 32 du RGDP donne une liste illustrative (c'est-à-dire non obligatoire et non limitative) des mesures de sécurité qui peuvent être mises en œuvre, à savoir :

- La pseudonymisation
- Le chiffrement
- Tout autre moyen « permettant de garantir la confidentialité, l'intégrité, la disponibilité » des données, et parmi lesquelles il faut considérer que figurent très certainement l'identification/ authentification des utilisateurs ainsi que la mise en place de contrôles d'accès avec une gestion stricte des droits.

Il s'agit là des mesures devant être mises en place « avant » l'atteinte.

« Après » l'atteinte, tout responsable de traitement devra procéder à une notification auprès de l'autorité de contrôle (la CNIL, pour la France), ainsi que, si l'atteinte engendre « un risque élevé pour les droits et libertés d'une personne physique » (on pensera, par exemple, à une divulgation non autorisée de données bancaires), le responsable de

traitement devra alors procéder à une notification à l'ensemble des personnes concernées par la violation de leurs données. A titre d'exemple, Orange a dû, il y quelques années, effectuer une notification de ce type auprès de plusieurs centaines de milliers de personnes dont les données avaient fait l'objet d'un accès par un tiers non autorisé, et cette notification avait engendré des frais, pour l'opérateur, de plusieurs millions d'euros.

Matthieu Bourgeois

Le nouveau règlement prévoit des sanctions, en cas de non-respect des obligations de mise en place de sécurité préventives ainsi que d'absence de notification lorsque celle-ci est requise, pouvant aller jusqu'à 2% du chiffre d'affaires mondial réalisé par le responsable de traitement/ sous-traitant défaillant ou 10 millions d'euros (le plus élevé des deux plafonds étant retenu).

Côté solutions de sécurisation en mobilité, comment protéger les données et les collaborateurs ?

L'entreprise devra mettre en œuvre des mesures techniques (tel que, par exemple, le chiffrement du canal de communication entre le mobile et le système d'information de l'entreprise, la conteneurisation des données accessibles via le mobile à travers un dispositif sécurisé, séparant ces données professionnelles des éventuelles autres données personnelles dans l'hypothèse où le salarié utiliserait ce mobile à des fins pro/perso...) mais également des mesures juridiques (comme, par exemple, la mise en place d'une charte informatique qui posera des règles strictes d'utilisation des terminaux nomades – tels que les mobiles, les tablettes... - et précisera notamment les règles applicables en cas de vol ou perte du terminal).

Une charte informatique présentera l'avantage d'offrir à l'entreprise des recours efficaces contre ses éventuels collaborateurs malveillants. A cet égard, une décision peut être citée : dans un arrêt du 22 octobre 2014, la Cour de Cassation a confirmé la condamnation – prononcée par la Cour d'Appel de Bordeaux – d'un salarié ayant appréhendé un grand nombre de fichiers informatiques de son entreprise peu avant de quitter celle-ci pour rejoindre un concurrent, sur le fondement de l'abus de confiance. Dans cette affaire, la présence d'une charte informatique, ratifiée par le salarié et lui interdisant toute utilisation des données de l'entreprise à des fins personnelles, n'a pas été étrangère à la solution retenue (Cour de Cassation, chambre criminelle, 22 octobre 2014, pourvoi no 13-82630).

Est-ce qu'une nécessaire réorganisation des entreprises s'impose en réponse aux contraintes réglementaires ?

Oui, sans aucun doute. Sur le plan organisationnel, il est indispensable de mettre en place un processus de pilotage de la sécurité des données, qui implique notamment :

- De dégager une classification des données à protéger, qui seront ensuite soumises à des restrictions d'accès ou d'usage adapté
- De se doter de moyens de détection des atteintes possibles, ainsi que d'outils permettant de réagir et d'en limiter rapidement les effets préjudiciables
- De nommer un Responsable de la Sécurité des Systèmes d'Informations (« RSSI ») ou équivalent, disposant de moyens humains et financiers adaptés, nouant un partenariat fort avec la direction de l'entreprise
- De mettre en place des processus visant à impliquer le RSSI et ses équipes dans tous les nouveaux projets, afin que les éventuels risques soient identifiés et donnent lieu systématiquement à une réponse adaptée

Il faudra bien entendu, aussi, impliquer le délégué à la protection des données (en anglais « Data Protection Officer », aussi appelé « DPO »), lorsque l'entreprise sera dans l'obligation d'en désigner un (ce que le RGDP exige lorsque les activités de l'entreprise « consistent en des opérations des traitement qui, du fait de leur nature, de leur portée et/ ou de leur finalité, exigent un suivi régulier et systématique à grande échelle des personnes concernées »), pour que celui-ci soit systématiquement associé aux projets mettant en œuvre des traitements de données à caractère personnel et puisse se prononcer sur leur conformité.

> Par Sabine Terrey

La mobilité en entreprise en 2017
QUELS SONT LES VRAIS ENJEUX?

Envahies par les smartphones et les tablettes, les DSI ont souvent dû gérer la mobilité dans l'urgence voire devant le fait accompli. Mais la transformation numérique a permis de redonner plus de perspectives aux projets mobiles.

En 2017, les challenges restent pourtant nombreux.

BYOD et mobilité ont quitté les Unes des magazines et sites dédiés à l'IT qu'ils squattaient, presque quotidiennement, il y a encore deux ans (et les années précédentes). La mobilité est une réalité à laquelle toutes les entreprises ont fait face plus ou moins dans l'urgence.

Elle a été l'un des moteurs de cette prise de conscience de l'existence d'une révolution numérique qui allait profondément transformer les usages et les processus des entreprises ainsi que les missions de la DSI et l'organisation des métiers.

Pourtant la mobilité est loin d'avoir abandonné le paysage informatique. Elle continue d'évoluer, bousculant les habitudes et encourageant de nouvelles approches en matière de sécurité des informations et de développement d'applications. Elle demeure un sujet clé, mais n'est qu'un volet parmi d'autres de la transformation numérique.

1 - L'évolution des usages...

La mobilité contribue aujourd'hui à redessiner l'espace de travail. Comme en témoigne l'étude Smart Workpace 2040 du CBRE, ce dernier est en passe d'être repensé pour ne plus être centré autour de l'individu mais autour des fonctions : dans la même journée le collaborateur se déplace de son « jump space » (un endroit où l'on peut rapidement se connecter au réseau de l'entreprise et travailler de façon productive) à la « creative room » (pour chercher l'inspiration à plusieurs avec tous les outils de brainstorming imaginables à disposition), de la salle de réunion collaborative à la cabine transactionnelle isolée (pour passer ses coups de fil ou appels par visiophonie en toute discrétion), tout en faisant une pause à la cafeteria où l'on vient échanger entre collaborateurs et partager les idées de façon informelle.

Cette approche est loin d'être futuriste. Elle est déjà mise en œuvre sur les campus américains de Google ou Apple par exemple, et elle est au cœur de la refonte du Campus Microsoft d'Issy-Les-Moulineaux. Nous entrons dans l'ère du « Flex Desk », du bureau flexible, opposé du bureau fixe.

Cette transformation de l'espace de travail est influencée par les nouveaux outils mobiles et elle les influence en retour.

En témoigne le succès des tablettes Surface de Microsoft et plus généralement des hybrides « 2 en 1 ». Tous les constructeurs ont désormais de tels concepts à leur catalogue et même Apple a été contraint de

céder au format avec son iPad Pro. Si ces produits ont d'abord trouvé leur audience auprès du grand public, ils intéressent aujourd'hui les entreprises. Voilà aussi pourquoi les constructeurs s'intéressent de plus en plus au concept « Continuum » de Windows 10 qui transforme un smartphone en véritable PC par simple adjonction d'un clavier et d'un écran (une idée que Samsung semble vouloir étendre à l'univers Android avec son futur Galaxy S8 si on en croit les fuites de ces dernières semaines).

Entrevu avec les Lumia 950, le concept a été vraiment inauguré par HP avec son Elite x3. Mais, il prendra sa vraie ampleur en fin d'année avec l'arrivée de Windows 10 Redstone 3 et du support des applications x86 sur processeur ARM.

Cette fonctionnalité déjà démontrée par Microsoft à plusieurs reprises pourrait bien marquer une révolution dans l'univers des smartphones tant elle colle étonnamment aux scénarios Flex Desk exposés ci-dessus.

Voilà une trouvaille technologique à laquelle les entreprises doivent aujourd'hui réfléchir et qu'elles ne doivent pas sous-estimer.

2 - L'évolution des approches...

La guerre des BYOD (Bring Your Own Device), CYOD (Choose Your Own Device), COPE (Corporate Owned, Personnaly Enabled) n'existe plus.

Chaque entreprise tend à adopter les trois approches et à les mettre en œuvre en fonction des besoins et des profils des collaborateurs. Finie l'époque de la multiplicité des solutions MDM (Mobile Device Management).

Le marché s'est condensé et les startups de la sécurité mobile ont été pour la plupart rachetées : AirWatch par VMware, Fiberlink (MaaS360) par IBM, Good Technology par BlackBerry (devenue une entreprise 100% logiciel), Zenprise par Citrix (pour XenMobile). De son côté, Microsoft a aussi beaucoup investi dans la mobilité pour enrichir (plus ou moins directement) ses offres Microsoft Intune et « Enterprise Mobility+Security ». Il n'y a guère que MobileIron à voler encore de ses propres ailes.

Le MDM a disparu au profit d'un concept bien plus large et plus cohérent : l'EMM (Enterprise Mobility Management). Au-delà de la gestion de l'hétérogénéité des smartphones et tablettes, les outils EMM adressent les problématiques de protection des données, de gestion des applications, et de supervision des accès (en incorporant de plus en plus la gestion des identités).

Des solutions qui cherchent de plus en plus à embarquer Intelligence Artificielle et Machine Learning pour automatiquement repérer les usages déviants, les actes malveillants et les attaques extérieures. C'est d'autant plus important que les menaces mobiles se sont multipliées particulièrement dans l'univers Android avec une spectaculaire croissance du nombre de malwares mais également de leur complexité (ransomware, etc.). Aucune plateforme n'est cependant épargnée (cf. XcodeGhost sur iOS) d'autant que des attaques de type Phishing sont indépendantes des plateformes et que les utilisateurs se laissent davantage berner par ces dernières lorsqu'ils sont en situation de mobilité entraînant le vol de leurs identifiants Office 365, Gmail, Paypal, Twitter, etc.

Par ailleurs, cette gestion de la mobilité et de sa sécurité s'étend désormais aux objets connectés (IoT) ainsi qu'aux « wearables » (montres connectées, suivi d'activités, etc.) dont le Gartner prédit l'entrée dans le monde de l'entreprise en 2017.

3 - De l'évolution des applications...

L'adaptation des applications métier au monde de la mobilité reste le grand challenge des entreprises. Cloud et micro-services permettent aux entreprises d'adopter des approches davantage compatibles avec la création d'applications mobiles. Parallèlement, l'intégration de Xamarin dans Visual Studio apporte aussi aux entreprises habituées aux développements « .NET » une simplification des développements cross-plateformes.

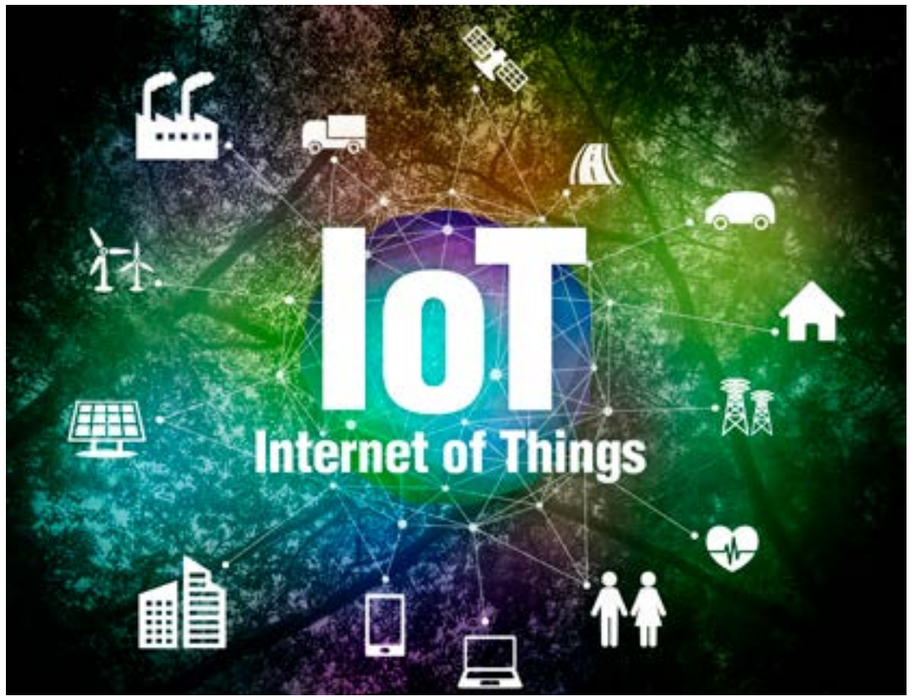
Mais d'autres solutions commencent à émerger. On voit ainsi apparaître sur le marché des solutions dites « Low Code » (très peu de code) voire carrément « Code Less » (sans code). Elles permettent aux développeurs de monter rapidement des solutions métiers connectées mais aussi, parfois, à des utilisateurs avancés de se composer leurs propres outils. Jusqu'ici monopole de quelques acteurs aventuriers et visionnaires comme Appian, App Press, AppGyver, Altova, Umajin, MobileSmith, OpenAsApp, ViziApps ou encore Mendix, le sujet commence à intéresser les géants tels que SalesForce avec sa plateforme Lightning, Google avec App Maker ou encore Microsoft et sa plateforme PowerApps.

Des solutions qui viennent compléter les autres formes de « mobilisation » des logiciels d'entreprise intégrées dans les solutions EMM comme la virtualisation des applications.

> Par Loïc Duval

Comprendre les objets connectés
REFLEXION, USAGES ET ACTIONS

Objets connectés et Internet des Objets, industrie du futur et nouveaux business numériques, données et connectivité, autant de concepts à analyser avant de se lancer dans tout projet d'autant que, selon le Gartner, il y aura 25 milliards d'objets connectés en 2020. De quoi être bien entouré !



Quel est l'impact de l'intégration des objets connectés dans la stratégie, l'écosystème, le système d'information des entreprises ? Du type d'objet, aux services et données, jusqu'aux questions éthiques, usages, énergétiques, choix des réseaux sans omettre les risques et mesures à prendre. Telle est la réflexion [1] que les entreprises doivent désormais mener avant d'aborder une démarche 'objets connectés' et entrer dans le monde de l'Internet des Objets.

L'évolution de la technologie

Les objets connectés se déploient dans tous les secteurs économiques et ce déploiement ne compte pas s'arrêter là, bien au contraire, le processus s'accélère. Si l'innovation technologique et les nouveaux usages œuvrent en ce sens, les questions vont bon train. En effet, cette technologie est tout simplement devenue une réalité.

Tout un écosystème se développe autour des objets connectés afin de répondre à l'évolution des business models de la transformation numérique. L'enjeu « Collecte des données – Connectivité » est évidemment lié à l'Internet des Objets. Toutefois, il faut dissocier les deux concepts.

Objets connectés et Internet des Objets

En effet, pour beaucoup, les objets connectés et l'Internet des Objets recouvrent le même concept. Or, « s'il est possible de définir ce qu'est un objet connecté, l'utilisation du mot de manière plurielle (« les » objets connectés) étend le concept à un écosystème dans lequel sont parties prenantes le Big Data, la sécurité, les services, les usages particuliers... C'est cet écosystème qui est aussi appelé Internet des Objets (IoT) » [2].

Un objet connecté se connecte à Internet et dialogue ainsi avec d'autres objets. L'Internet des Objets se révèle dans la puissance générée par l'interconnexion des objets par Internet. Pour le Gartner, « l'Internet des Objets est un réseau d'objets physiques, dédiés à des usages particuliers, qui embarquent des technologies pour communiquer, détecter ou interagir avec l'environnement externe selon leurs états internes. L'Internet des Objets est donc un écosystème d'objets », mais bien d'autres définitions existent.

Les Métiers et la DSI

La bataille économique des objets connectés est lancée. Avec l'Internet des Objets, les différents marchés se rapprochent et les interactions se multiplient. Les entreprises doivent repenser la gouvernance, la stratégie, la performance, la sécurité et l'accès aux données, mais aussi s'interroger rapidement sur les nouveaux marchés, les acteurs et les différents services. En outre, pour aider les Métiers à identifier les nouveaux besoins et usages, la DSI doit mettre en place un écosystème sur lequel les directions Métiers pourront s'exprimer et créer les nouveaux services.

Services, données et communication

Passons au Système d'Information. Capacité technologique et puissance de l'infrastructure d'un côté, accompagnement des Métiers par les DSI sur les bonnes pratiques à suivre, de l'autre.

Les plates-formes de services et de données sont au cœur de toutes les attentions, si la DSI n'a pas les compétences globales sur ce type de plateforme ou si le SI n'a pas la capacité de tout analyser, il est fortement recommander de se tourner vers les PME innovantes et start-up qui possèdent ce savoir-faire. Plusieurs éléments sont à considérer : le « front-end », le « back-end » sur lequel il faudra valoriser l'information des objets et réaliser des analyses prédictives, le format des données transférées et les données à caractère personnel.

Un autre aspect, tout aussi essentiel, est à prendre en compte : l'infrastructure de communication. Cette infrastructure englobera le type de communication, la couverture réseau, la consommation énergétique, le volume des données transmises, la fréquence de captation, de transmission des données, et le prix des capteurs - émetteurs.

Sécurité et recommandations

On ne peut pas parler d'objets connectés sans évoquer les risques encourus et ces risques dépendent évidemment des enjeux liés aux objets gérés par l'entreprise. Il faut donc poser quatre critères [3] :

- Si l'entreprise fabrique les objets connectés, elle doit intégrer la sécurité dès la conception
- Si l'entreprise acquiert les objets pour les déployer en interne, elle doit intégrer la sécurité au sein des processus Métiers
- Si l'entreprise recommande les objets connectés, sa responsabilité intervient envers les clients en cas d'incident de sécurité.
- Si l'entreprise s'ouvre à des objets dans une dimension BYOD, elle doit protéger les données (pertes, vols, intrusions ...)

Quant aux mesures de prévention à prendre, il faut, dans un premier temps, évaluer les différents cas d'usages et la relation de l'entreprise par rapport aux objets, mais aussi comprendre les enjeux Métiers, les risques liés aux usages et l'environnement concerné.

La complexité de l'écosystème à mettre en place autour des objets connectés est réelle, et le phénomène, étroitement lié au Big Data et traitement des données, s'amplifie au fur et à mesure du développement rapide du marché. Enfin, face aux freins, la prise de conscience des gains de productivité et du potentiel qui s'ouvrent aux entreprises, donne le ton !

> Par Sabine Terrey

(1) Le CIGREF dont la mission est de « développer la capacité des grandes entreprises à intégrer et maîtriser le numérique » vient de publier un rapport « Objets connectés, un 360 pour bien les comprendre » pour permettre aux entreprises de comprendre leur impact. Plus d'informations : http://www.cigref.fr/wp/wp-content/uploads/2016/12/CIGREF-Objets-Connectes-2016.pdf

(2) Citation du CIGREF – Rapport décembre 2016

(3) Méthodologie CARA de Wavestone : https://www.wavestone.com/app/uploads/2016/09/Objects-connectes-Securite-4D_FR_publi.pdf

Les prévisions technologiques 2017
SUR QUELLES TENDANCES PARIER

Le monde change... Vite, trop vite. L'attente est une attitude qu'aucune DSI ne peut s'offrir. Voici ces transformations technologiques à ne pas perdre de vue, en 2017, pour garder l'entreprise sur la voie de la modernité numérique.

Il n'est pas facile de suivre le rythme des innovations. Il devient même de plus en plus difficile de savoir se projeter et d'assimiler les concepts imposés par la numérisation et la nécessité de rendre chaque entreprise plus agile. On connaît les trois grandes tendances auxquelles toutes les DSI essayent, chacune à son rythme, de se conformer : Cloud, Big Data, DevOps.

Au-delà de ces grands axes s'inscrivent d'autres tendances innovantes qui vont impacter rapidement le fonctionnement des entreprises, leur capacité à communiquer avec leurs clients, leur capacité à prédire les évolutions de leurs marchés, leur capacité à suivre le rythme des nécessaires transformations.

Voici quelques sujets phares sur lesquels il faudra, en 2017, réaliser veille, prospection et effort d'anticipation.

- 01 -
Intelligence artificielle à la demande

Le célèbre CES de Las Vegas est toujours un excellent indicateur des tendances. Et si l'on devait retenir un seul et unique mot de la dernière édition, il tiendrait en deux lettres : « IA ». En 2017, nous allons « manger » de l'intelligence artificielle à toutes les sauces. Nul doute que le moindre algorithme de rapprochement de patterns ou de déduction basique sera qualifié d'IA par les départements marketing. On va nous vendre de l'IA comme on nous a vendu du Cloud et du Big Data à tort et à travers.

Au-delà du phénomène « hype », se cache pourtant une vraie réalité. Le Deep Learning autrefois restreint aux centres de recherche d'entreprises comme Microsoft, IBM et Google (dont le Deep Mind a fait les preuves de la supériorité de la machine sur l'homme en battant un champion de Go) est en train de se démocratiser. Et ceci grâce à des API facilement accessibles d'analyses vocales, d'analyses d'images, d'analyses de texte contextuelles.

Bien des entreprises ont en 2016 commencé à découvrir ce que le Machine Learning pouvait leur apporter dans leurs analyses au travers de solutions comme Azure ML, Amazon Machine Learning, ou IBM Watson Analytics (SPSS Modeller). En 2017, c'est un Machine Learning accéléré par des ASICs, des GPUs ou des FPGAs qui va s'imposer dans les Data Centers, notamment au travers des multiples Frameworks désormais à portée de toutes les entreprises (Microsoft CNTK, Caffe, Chainer, Keras, Torch, TensorFlow, Theanos ...).

Mais le Machine Learning reste une discipline différente de l'IA au sens large.

Elle englobe des sciences cognitives qui, une fois intégrées au cœur des applications, peuvent transfigurer les expériences utilisateurs, les interactions avec les clients mais également ouvrir des champs d'analyse extraordinaire en matière de santé, de surveillance de lieux, de détection des fraudes, de workflows juridiques, de commerce, etc. Bref, il est grand temps pour les DSI de se pencher sur le potentiel de Cortana Intelligence Suite (https://gallery.cortanaintelligence.com/machineLearningAPIs), des Microsoft Cognitive Services (https://www.microsoft.com/cognitive-services/en-us/), des Watson Services (https://www.ibm.com/watson/developercloud/services-catalog.html), des IBM Bluemix Services (https://console.ng.bluemix.net/catalog/?category=watson) et autres HPE Haven OnDeman APIs (https://dev.havenondemand.com/apis).

C'est en comprenant et mesurant leur potentiel que les DSI pourront lancer des projets innovants et différenciant exploitant cette IA à la demande simple à mettre en œuvre mais révolutionnaire.

L'idée : proposer des interactions plus intuitives avec vos clients et créer des produits et des services cognitifs différenciant et créateurs de valeur.

- 02 -

Assistants virtuels & Chatbots

Évidemment, l'intelligence artificielle et les services cognitifs viennent aussi transfigurer le dialogue homme-machine.

Au point que, désormais, on puisse dans certains contextes remplacer l'homme par des intelligences communicantes artificielles, des Chatbots. Ces derniers vont se multiplier en 2017 avec des SDK pour toutes les messageries en vogue : Facebook, Telegram, Kik, WeChat, Viber et bien évidemment Skype. Cela représente plus de trois milliards d'utilisateurs actifs.

Or une étude du la société Aspect montrait fin 2016 que 71% des consommateurs américains préféraient résoudre leur problème par eux-mêmes (sans interaction humaine) et que 69% interagissaient déjà au moins une fois par mois avec des Chatbots. Converser par texte avec des Chatbots « 24/24, 7/7 » devient donc progressivement une pratique ancrée dans les mœurs.

En 2017, les entreprises doivent profiter de la relative simplicité de mises en œuvre de nouveaux SDK (Microsoft Bot Framework, Howdy's BotKit, Wit.ai) pour réfléchir à l'opportunité de telles intelligences conversationnelles dans leur domaine d'activité : notifications, engagements lors de visites du site Web, supports, réservations, etc. Les champs d'application sont vastes. Mais elles doivent aussi réfléchir à leurs usages internes alors que ces Chatbots commencent à s'imposer dans des outils comme Microsoft Teams (https://msdn.microsoft.com/en-us/microsoft-teams/bots), Yammer, Skype for Business, Facebook Workplace, Slack ou HipChat.

Il est un autre domaine où ces nouvelles interactions, pour ne pas dire ces nouvelles conversations, viennent enrichir la relation entre l'homme et le numérique qui l'entoure. Les assistants virtuels comme Amazon Alexa ou Microsoft Cortana sont des services très ouverts.

Il devient dès lors possible de les intégrer dans vos applications ou vos produits - ne serait-ce que pour bénéficier de leur remarquable reconnaissance vocale - comme en témoigne la multiplicité des lampes, enceintes Bluetooth, aspirateurs-robot et autres gadgets embarquant ces assistants virtuels sur le CES 2017.

Quoiqu'il advienne, 2017 marquera une étape clé, même si nous ne sommes encore qu'au début de ces intelligences conversationnelles. Mais il n'est plus très loin le temps où l'on pourra mener une conversation avec son ordinateur...

- 03 -

Automatisations, Workflows et IoTs

L'automatisation est omniprésente. Elle est la clé du SDI et de l'évolution du DataCenter. Elle est au cœur des processus DevOps. Elle s'étend désormais à tous les métiers, même le marketing (Salesforce Automation, Marketo, Eloqua, Userfox, Outmarket...). Les Chatbots sont, d'ailleurs, en soi une forme d'automatisation. Et les IoTs sont des composantes essentielles dans toute approche automatisée.

Surtout, les DSI vont désormais devoir apprendre à se familiariser avec de nouvelles plateformes de Workflow qui permettent d'assembler les services avec une étonnante simplicité et créer ainsi des automatismes pour servir tous les besoins de l'entreprise : Microsoft Flow (intégré à Office 365), IFTTT, Zapier, Google Apps Script.

- 04 -

Des services sans serveur

Ce sera l'une des grandes tendances de l'année 2017 : le « serverless computing », autrement dit l'informatique sans serveurs. Cette approche micro-services intimement associée au Cloud permet aux développeurs de créer des services sans se soucier d'infrastructure, de déploiement et de problématique de montée en charge.

L'idée est de leur permettre de créer le plus simplement et rapidement possible des « fonctions », de les attacher à d'autres exposées via des librairies, et de les exposer sous forme d'APIs au sein d'une plateforme Cloud qui prend tout le reste en charge.

Vous gagnez en temps de développement et en simplicité de mise en œuvre sans sacrifier ni la sécurité ni la montée en charge. Les leaders du Serverless Computing se nomment Azure Functions, AWS Lambda, Google Cloud Functions et « Iron.io ».

- 05 -

Windows 10

Voilà une « prédiction » qui peut surprendre. Après tout, Windows 10 a déjà été pour nombre de services informatiques l'un des grands casse-têtes de l'année écoulée. Pourtant 2017 est encore une année charnière pour le système de Microsoft. Voici pourquoi...

* Nombre d'entreprises n'ont pas encore commencé leurs déploiements Windows 10. C'est une étape indispensable : elle affecte la gestion de la mobilité, la gestion des sécurités et les développements internes. En matière de sécurité notamment, la future version « Creators Update » apportera en 2017 des innovations remarquables comme Windows Defender Application Guard (avec une conteneurisation d'Edge) et des améliorations à Windows Information Protection (qui isole les données entreprises des données personnelles), à Windows Defender Advanced Threat Protections (pour détecter et répondre aux attaques réseau) et à Windows Analytics (gestion du parc).

* Les PC hybrides sont aujourd'hui prêts pour l'entreprise. Ils constituent aujourd'hui une réponse viable et fiable à bien des scénarios métiers. Qu'ils soient des PC à écran rotatifs ou des « 2 en 1 » à écran détachable, ils bénéficient des nouveaux processeurs Intel Kaby Lake pour associer 6 qualités essentielles : ergonomie tactile+stylet, performances, autonomie (plus de 10h), légèreté (moins de 1 Kg pour des 12 pouces), et silence de fonctionnement. Et Windows 10 est au cœur de ces appareils.

* Avec Windows 10 Creators Update débarque Windows Holographic qui est à la fois une nouvelle

couche Windows, un nouveau Shell, un nouveau Framework et de nouveaux outils de développement, tous destinés à simplifier et standardiser l'élaboration d'applications en réalité virtuelle et augmentée et font rentrer VR et VA dans l'ère de l'industrialisation. Ce qui nous amène tout naturellement au point suivant...

- 06 -

Réalité Mixte

2016 aura été marqué par l'introduction des premiers casques de « Réalité Virtuelle » et du casque de réalité augmentée « Hololens ».

2017 devrait marquer leur popularisation avec l'arrivée de modèles à moins de 300 euros.

Et si leurs applications sont aujourd'hui essentiellement ludiques, il est essentiel que les entreprises prennent dès maintenant conscience de leur potentiel notamment dans les domaines de l'immobilier, de la maintenance, de la santé, de la vente et du tourisme.

L'un des intérêts phares des nouveaux casques « Windows Holographic » annoncés chez Dell, Lenovo, HP ou Acer, est d'encourager une réalité mixte : même plongé dans un univers 100% virtuel, l'utilisateur garde (par différentes astuces graphiques) notion de l'environnement physique qui l'entoure ce qui lui permet du coup de se lever et de se déplacer.

Cette réalité mixte est aussi moins perturbante pour nos sens. Aux entreprises innovantes d'en saisir les opportunités...

> Par Loïc Duval

2017, l'année du Blockchain ?

Déjà largement investi par le domaine bancaire, le principe des Blockchains intéresse aussi l'industrie de la musique, de l'authentification d'identités ou des dépôts de brevet.

Tous les Business s'appuyant sur des certifications et des contrats sont aussi susceptibles d'être impactés par cette technologie.

L'idée des Blockchains repose sur le principe d'une base de données distribuée dans laquelle les informations sont listées séquentiellement en blocs autovérifiés et vérifiables interdisant toute altération.

Elle induit de nouveaux concepts comme celui des « Smart Contracts » qui peuvent intéresser les domaines de la santé (confidentialité du dossier patient) et des chaînes logistiques.

Jusqu'ici cantonnés à la recherche et aux PoCs, les Blockchains deviennent en 2017 accessibles à bien des entreprises avec l'apparition de services BaaS (Blockchain as a Service) chez Microsoft Azure et IBM Smart Cloud.

DSI un beau métier au coeur
DE LA TRANSFORMATION DES ENTREPRISES

Rencontre avec Robert Eusebe, un DSI moteur d'innovation qui aime relever les défis...

Directeur des Services Numériques (DSN) de la société d'ingénierie Ingerop, Robert Eusebe aime relever les défis :

après avoir piloté la transformation digitale d'Arte pendant 12 ans, cet ingénieur diplômé de CESI revient à ses premiers amours – l'industrie – pour accompagner le Groupe dans cette nouvelle ère numérique.

Transformation sociétale et nouveaux modèles économiques

« La transformation digitale va bien au-delà du numérique, explique-t-il. Nous assistons à une véritable transformation sociétale avec de nouveaux modèles économiques.

Tous les secteurs ne sont pas impactés au même

moment. Pour Arte et l'audiovisuel, c'était dans les années 2000 avec l'apparition des contenus numériques. Pour Ingerop, c'est maintenant avec le développement des smartcities, des bâtiments intelligents et bien entendu de l'Internet Of Things. J'aime les défis.

C'est le propre d'un DSI que de savoir prendre des risques et saisir les opportunités offertes par les nouvelles technologies. Cette dimension entrepreneuriale fait partie de l'ADN du DSI ».

Robert Eusebe

Convaincu d'avoir un rôle à jouer dans la transformation de son entreprise, Robert Eusebe résume son métier à deux missions fondamentales : le maintien du système d'information en conditions opérationnelles – « il faut que ça tourne ! » - et le développement ou, en d'autres termes, être moteur d'innovation.

« L'innovation n'appartient pas à la DSI. En fait, c'est l'affaire de tous. L'important c'est que chacun s'approprie la dynamique de changement de façon à créer des équipes projets multidisciplinaires, à l'origine des combinaisons originales et associations d'idées nouvelles », souligne le DSN d'Ingerop.

Son titre ? « Je n'en suis pas l'instigateur, précise-t-il, Ingerop avait déjà compris que la mission d'un DSI va au-delà de la gestion d'un parc informatique. Je suis néanmoins le premier DSN du Groupe et le titre convient parfaitement à la vision que j'ai de mon métier aujourd'hui ».

DSI, un métier en évolution

Un métier qui a bien évolué depuis son début de carrière en 1983 avec une accélération de la transformation digitale et une réduction des cycles impactant directement les systèmes d'information.

« D'un autre côté, depuis que l'homme est homme, les évolutions, le progrès ne cessent d'accélérer, le besoin d'agilité que l'on constate aujourd'hui étant la conséquence de cette accélération. De fait, la valeur d'un système d'information ou d'une organisation repose aujourd'hui sur une équation simple : sécurité x agilité ».

Ancien RSSI et responsable décisionnel d'Holcim (1996-2002), Robert Eusebe est particulièrement sensible à la sécurité des systèmes d'information et à la cohérence des données, deux fondamentaux qui participent à l'agilité du système d'information.

« La valeur d'un système d'information se mesure à son agilité et à sa sécurité »

Réactivité, agilité et sécurité

Pour renforcer la réactivité du Groupe, il a, dès son arrivée, réuni des équipes dispersées géographiquement pour constituer une DSI Groupe globale, organisée de façon très classique en trois grands services : relation utilisateurs/support, responsables de l'infrastructure et études & développement.

« Ça reste une bonne organisation, estime-t-il. Ce qui ne nous empêche pas de mettre en place du Devops pour gagner en agilité tout en renforçant la sécurité ou encore d'adopter les technologies clefs de l'agilité et de la mobilité : cloud, virtualisation du poste de travail ou SDN ».

Et d'ajouter en forme de conclusion : « Sécurité, gouvernance des données, innovation...si on reste sur ce schéma, le CDO fait partie intégrante de la DSI. Souvent nommé par une Direction Générale qui souhaite donner un second souffle à la transformation digitale, le CDO peut alors entreprendre des développements isolés, non connectés au SI de l'entreprise qu'il convient ensuite d'intégrer pour garantir une bonne expérience client ».

> Par Marie Varandat

Cyberespionnage & entreprises
QUID DES « SURVEILLANCEWARE » ?

Les appareils mobiles se situent à la frontière entre cyberespionnage et motifs criminels. Comment évaluer précisément le niveau de sophistication des attaques et appréhender les enjeux sécuritaires ? Comment intégrer la mobilité au sein de la stratégie de sécurité de l'entreprise ? Eclairage par Mike Murray, Vice-Président Recherche chez Lookout, qui revient sur ces problématiques.

Les menaces évoluent en permanence tout comme le niveau de sophistication, peut-on revenir sur le concept de "surveillanceware", qu'est-ce que ça signifie concrètement ?

Très simplement, les surveillanceware sont des logiciels malveillants qui ciblent, s'installent et infiltrent les appareils mobiles de leurs victimes (portables, tablettes) pour surveiller, espionner et exfiltrer de l'information à leur insu.

Ces surveillanceware ciblent principalement les membres et les décideurs des entreprises et des gouvernements.

Leur existence et l'étendue de leur capacité d'infiltration sans qu'elles puissent être détectées confirment l'évidence émergente que les risques de cyberattaques mobiles contre les entreprises et les gouvernements représentent aujourd'hui un véritable problème.

Prenons un exemple, qu'est-ce que ViperRAT ? quels sont objectifs des pirates ?

ViperRAT est une arme de cyberespionnage puissante. L'équipe de chercheurs de Lookout a déterminé que ViperRAT est un type de "surveillanceware" et représente une menace très sophistiquée qui peut cibler aujourd'hui non seulement des gouvernements mais aussi des entreprises. ViperRAT s'est attaqué il y a quelques temps aux Forces de Défense Israélienne. ViperRAT a la capacité de collecter les informations comme les SMS, les contacts, les documents PDF, les archives .rar, les documents de type Word, l'historique de navigation, les photos, les journaux d'appels.

En plus de collecter ces informations, l'attaquant peut prendre le contrôle de l'appareil photo du portable de sa victime et prendre des photos, enregistrer des vidéos ou de l'audio, ouvrir un navigateur et aller à un lien spécifique, écouter furtivement à un moment donné ou une période donnée à partir de l'appareil de la victime.

Avec un tel niveau d'accès aux informations, en utilisant ViperRAT, les pirates peuvent accéder à des informations confidentielles mais aussi tout savoir sur les actions et activités de leurs victimes. Une arme redoutable quand il s'agit d'espionnage industriel ou institutionnel par exemple.

Les risques de cyberattaques mobiles sont un réel problème pour les entreprises, sont-ils suffisamment pris en compte ?

Malgré une augmentation des attaques et de leur niveau de sophistication, on peut encore actuellement dire que les risques de cyberattaques mobiles sont encore sous-estimés par les entreprises mais aussi par les utilisateurs de smartphones et de tablettes. C'est un peu normal, après tout, pour caricaturer, notre smartphone est un petit appareil qui ne nous quitte jamais, qui est gardé précieusement au fond de notre poche, de notre sac à main ou que l'on tient dans le creux de la main. En plus, on est très souvent persuadé qu'il est déjà protégé car l'écran n'est pas accessible sans code d'accès ou un accès protégé par empreinte digitale.

Cependant, il faut voir les appareils mobiles comme de véritables mini ordinateurs surpuissants. Les enjeux de sécurité sont importants et doivent être pris en considération par les entreprises. La complexité de la protection d'une flotte mobile propriétaire ou bien encore des appareils mobiles personnels que les employés utilisent aussi pour travailler sont des enjeux importants pour la protection des données.

Le mobile aujourd'hui doit faire partie de la stratégie de sécurité de l'entreprise. C'est un incontournable.

Comment intégrer la mobilité dans la stratégie sécurité de l'entreprise : Quelles sont les 3 recommandations clés pour les responsables IT?

Les appareils mobiles sont aujourd'hui à la frontière du cyberespionnage, et autres motifs criminels potentiels. Les entreprises, les fonctionnaires et membres des gouvernements utilisent tous les jours des appareils mobiles pour leur travail ce qui signifie qu'aujourd'hui plus que jamais les responsables IT et de la sécurité de ces organisations doivent intégrer la mobilité dans leur stratégie de sécurité.

- Le **premier conseil** que nous pouvons donner est de comprendre que **les enjeux de sécurité mobile sont multidimensionnels.** Une stratégie de sécurité mobile doit pouvoir protéger l'entreprise sur trois niveaux : réseau, applications et systèmes d'exploitation. Il faut aussi à la fois pouvoir protéger et détecter les risques possibles et pouvoir prendre en compte la gestion des ressources en fonction du type d'appareil mobile, du lieu et /ou du profil de l'utilisateur

- Le **second conseil** est assez basique - **faites vos mises à jour** quand elles sortent ou dès que possible sur tous les appareils de votre flotte mobile. Les malwares peuvent être conçus pour exploiter des vulnérabilités du système d'exploitation de vos appareils

Mike Murray

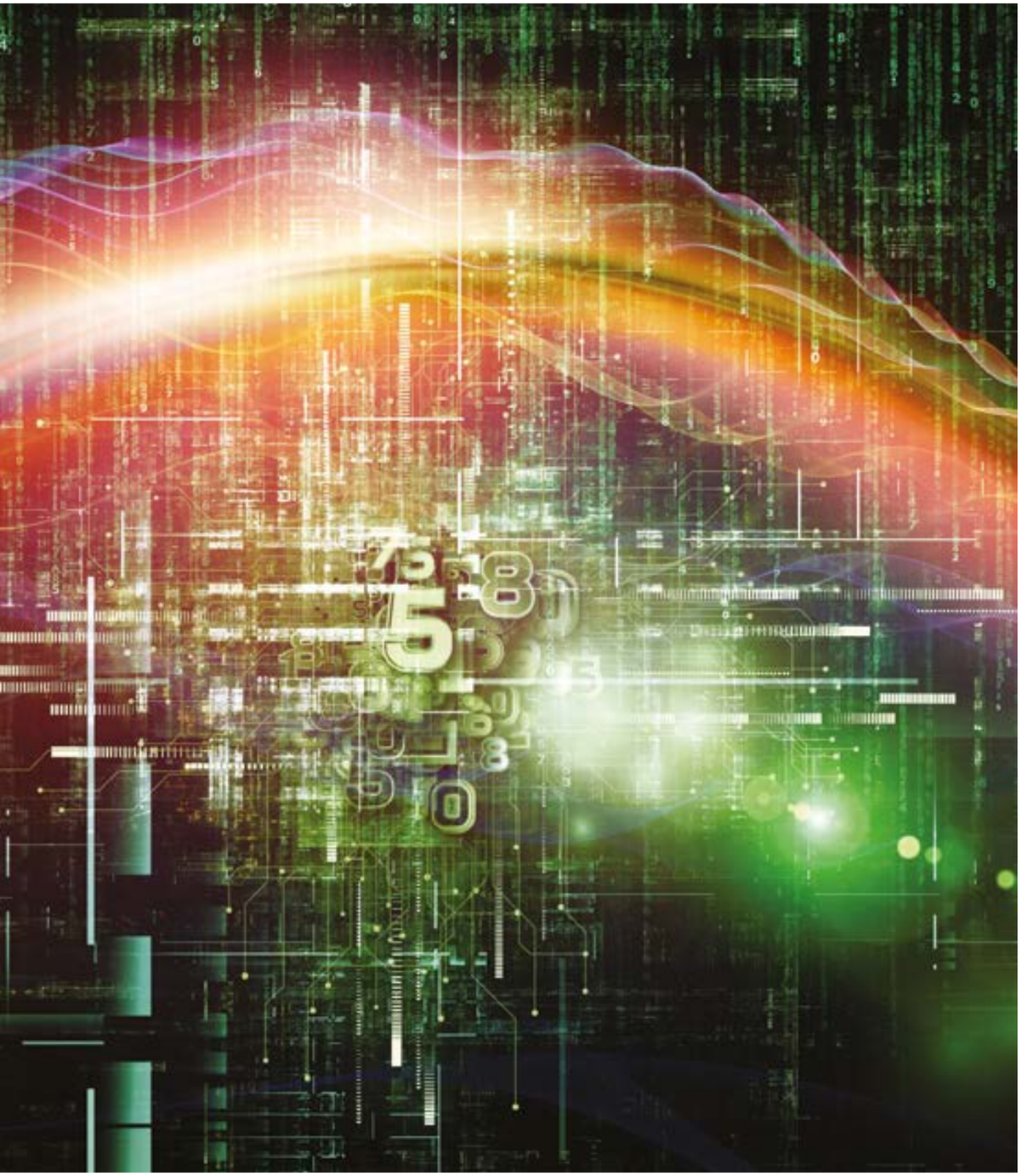
mobiles. Les mises à jour que l'on reçoit sont donc importantes car elles peuvent contenir des patchs qui permettent de sécuriser un peu mieux votre appareil mobile

- Finalement, **le troisième conseil** est de travailler à la **stratégie de sécurité mobile avec une société partenaire spécialisée dans le mobile**. Le challenge est de taille et très différent des enjeux rencontrés sur les autres infrastructures informatiques.

> Par Sabine Terrey

Pleins feux sur le Machine Learning

CONCEPT, IMPLÉMENTATIONS ET PERSPECTIVES



Le Machine Learning fait partie de ces "Buzz Word" que l'on croise régulièrement au détour des différentes actualités que l'on peut lire.

Même si les concepts généraux semblent compris et connus, ses différentes implémentations restent obscures et complexes pour ceux qui veulent commencer à l'implémenter ou en comprendre les tenants et aboutissants.

Le concept

Le concept général du Machine Learning permet de réaliser des projections à partir d'un jeu de données existant pour en déduire des résultats.

Ainsi, en prenant par exemple un jeu de données correspondant aux différentes ventes de biens immobiliers comme le prix, la surface, la ville, le type (maison, appartement, ...), la surface du jardin... il nous serait possible grâce au Machine Learning d'obtenir automatiquement un algorithme déterminant le prix d'un nouveau bien en spécifiant les mêmes caractéristiques.

Evidemment, plus il y aura de données et plus il y aura de critères dans le jeu de données sources, plus la projection sera proche de la réalité.

Les algorithmes entrent en scène

Aussi, une fois le jeu de données source obtenu, le métier de Data Scientist entre en jeu. Le Data Scientist est un expert de la gestion et de l'analyse de données.

Il détermine les indicateurs pertinents pouvant être obtenu à partir de sources de données multiples. Le Data Scientist est donc spécialisé en statistiques, en informatique et connait le contexte des données analysées. Il aura pour rôle de manipuler les données afin d'indiquer au moteur le type de résultat attendu.

Pour cela, il va pouvoir utiliser des composants de traitement mathématiques et statistiques qui vont permettre d'entraîner le moteur de Machine Learning afin qu'il détermine le fameux algorithme. Cet algorithme qui va souvent se présenter sous la forme d'une boîte noire, a pour objectif d'être utilisé tel quel. Plus concrètement, une fois l'entraînement effectué, on enregistre son résultat sous la forme proposée par l'outil c'est-à-dire un « bout de code » dans un langage quelconque ou d'un web service qui va nous permettre de consommer ce service.

C'est ainsi qu'il est important d'évaluer l'importance que peu prendre le Machine Learning dans votre Système d'Information.

Si il est utilisé dans le cadre d'une expérimentation et que le moteur ne sera pas ré-entraîné régulièrement, il n'est pas forcement judicieux de monter une infrastructure On-Premise qui ne va être utilisée que ponctuellement pour générer votre fonction. On peut, alors, se tourner vers des solutions dans le Cloud.

Si les mécanismes d'entraînement du Machine Learning font pleinement partie de votre workflow avec une réévaluation régulière des fonctions à partir de données fraîches, il devient pertinent d'imaginer implémenter des infrastructures On-Premise parmi les nombreuses implémentations existantes sur le marché.

Les usages

Aussi, pour évaluer rapidement les usages possibles du Machine Learning, Microsoft propose gratuitement son moteur d'expérience d'apprentissage automatique via sa plateforme Azure.

Elle a pour avantage de proposer une interface simple et graphique permettant à un Data Scientist d'aller à l'essentiel en masquant la mécanique sous-jacente au fonctionnement du moteur. Des éléments graphiques de représentation de la donnée ainsi que des outils de comparaison entre le résultat de l'entraînement et les données d'origine faisant partie intégrante de l'outil.

Le résultat de l'expérimentation sera alors exposé sous la forme de web service afin d'en tester le bon fonctionnement et la pertinence dans vos applications.

Si le résultat est satisfaisant, il est possible de souscrire à un abonnement afin d'utiliser ce web service directement en production.

Pour les scénarios les plus complexes, le Machine Learning peut aller beaucoup plus loin et va permettre par exemple de prendre comme source une base de données d'image qualifiée (chaque photo est accompagnée d'une description de son contenu) comme http://www.image-net.org/ pour ainsi se permettre lors de l'analyse d'une photo, de déterminer si les caractéristiques permettant d'identifier un élément (objet, personne, ...) sont réunis et ainsi les trouver automatiquement.

Pour cela, des algorithmes de construction de caractéristiques vont permettre en amont de simplifier et d'orienter le travail afin d'éviter d'avoir

à analyser des millions voire des milliards de possibilités.

Ce type d'implémentation est évidement plus complexe à mettre en place.

Trois indicateurs clés

Dans l'optique où le Machine Learning sera de plus en présent dans les entreprises, on en déduit plusieurs considérations importantes à prendre en compte pour anticiper au mieux une implémentation à court, moyen ou long termes ...

1. **Le stockage de la donnée d'entreprise** devient un élément stratégique car au-delà des capacités de traitement actuel, il faut anticiper les futurs usages de la donnée actuelle et donc archiver les données

2. **La qualité des données brutes** devient importante. Celles-ci doivent-être qualifiées et représentatives des objectifs attendus. Elles doivent couvrir l'ensemble du périmètre cible afin de ne pas induire en erreur les déductions du système d'apprentissage (Ex: Jeu de données sur les 15-25 ans alors que la projection attendue concerne toute la population)

3. **La réussite d'un projet de Machine Learning** s'appuie encore actuellement sur une contextualisation efficace du traitement du jeu de données. Cela requiert donc des compétences scientifiques importantes inhérentes au métier de Data Scientist pour permettre une amélioration continue des résultats du Machine Learning

Loïc Thobois est CTO pour la société D.T. Consulting et administrateur de la plate-forme de partage communautaire http://www.avaedos.com. MVP depuis 2004, il est passionné des technologies Microsoft et partage ses connaissances sur ce sujet depuis plus de 15 ans.

Comment devenir un « digital native » ?

Le degré d'engagement des entreprises est-il jugé suffisant ?

Devenir un « digital native »

La disruption, là où tout se joue ! Les entreprises qui prennent en compte tout le potentiel de la disruption proposent de nouveaux services et réduisent les coûts.
Afin de ne pas être distancé par les start-up et autres acteurs émergents, il faut prendre le train de la transformation numérique pour créer des opportunités.
Les technologies avancées, Cloud, analytique, nouvelles applications feront de votre entreprise un leader, tout en s'appuyant sur la rapidité et les conditions d'adoption des solutions.

Stratégie numérique & Business

A la question, quels sont les impacts de la technologie sur le business ? Les réponses sont claires.

- **Une part de marché accrue** (avec 8 fois plus de chances de l'augmenter)
- **Des délais de commercialisation réduits** (grâce aux technologies émergentes)
- **Un développement fluidifié** et une infrastructure plus flexible (par l'utilisation des conteneurs pour le développement d'applications)

Rapidité d'innovation & Réactivité

Si le contexte du business, les besoins IT et l'approche envers la technologie sont à prendre en compte, les entreprises tendent à créer des processus en réponse aux tendances technologiques (63%), d'autres paramètres sont tout aussi déterminants.
En effet, la rapidité d'innovation est considérée comme une priorité et la motivation impulsée est directement liée aux avancées de la concurrence (65%).

Maturité digitale & Objectifs métiers

Le numérique est bien plus qu'une simple évolution, il s'agit d'une transformation globale multidisciplinaire qui impacte les directions, l'organisation entière, la gouvernance, les produits, les processus, la stratégie IT, les investissements, les données.

Conteneurs & Priorités

Les conteneurs vont en ce sens et apportent des avantages architecturaux. En adoptant les conteneurs, on constate une diminution des délais de développement (de 15 à 30%), des gains de flexibilité, de productivité matérielle (entre 5 et 15%).
Malgré les freins, manque de compétences, de connaissances, immaturité des écosystèmes, l'adoption est en marche.

Etude Bain & Company - Red Hat « For Traditional Enterprises, the Path to Digital and the Role of Containers » menée auprès de 449 dirigeants, hauts dirigeants, DSI seniors et développeurs/personnel chargé des opérations IT, au sujet des conteneurs.

RSSI et digital font bon ménage

ENTRE INNOVATION, NOUVEAUX USAGES ET SENSIBILISATION

Pourquoi la transformation numérique perturbe-t-elle la sécurité ou, inversement, pourquoi la cyber-sécurité impacte-t-elle la transformation numérique ? Les Systèmes d'Informations et les données sensibles sont concernés au plus haut niveau.

Innovation et sécurité

Dans ce monde numérique où le rythme de l'innovation et des changements s'accélèrent, où la concurrence est de plus en plus oppressante et les risques de plus en plus nombreux, quelle est la perception et la réalité de la cybersécurité ?

Découvrons les résultats de la dernière enquête (1) du CESIN, Club des Experts de la Sécurité de l'Information du Numérique.

A l'ère du Cloud, du BYOD et des objets connectés, qu'en est-il du contrôle des accès, du stockage des données sensibles hors des frontières, de la sensibilisation des salariés aux bonnes pratiques, mais aussi des investissements des entreprises et de l'augmentation des effectifs dédiés à la sécurité ?

Les solutions techniques en place sont-elles adaptées aux réels besoins des entreprises ? Autant de questions à examiner.

Le risque social engineering

Les cyber-attaques ne font que progresser. Ainsi, au cours des douze derniers mois :

- 80% des entreprises ont constaté au moins une cyber-attaque
- 34% entre une et trois attaques

De plus, en un an, le nombre d'attaques a augmenté pour 46% et est resté stable pour 53%.

Quant au type d'attaques, le ransomware se place en première position (80%) du Top 3 (augmentation de 19% depuis janvier 2016), suivi de l'attaque par Deni de Service (40%) et de l'attaque virale générale (36%).

Un aspect nouveau émerge, les entreprises sont désormais confrontées à des risques

- **social engineering** (55%)
- vulnérabilités résiduelles permanentes (50%)

(Voir Schéma A)

Des solutions inadaptées aux cyber-attaques

Faces aux risques, outre les antivirus et pare-feu, de nombreuses solutions sont implémentées dans les entreprises, mais qu'en est-il de leur efficacité ?

Si les organisations s'équipent de solutions VPN (87%), filtrage web (84%) et antispam (79%), la supervision de la sécurité et l'authentification forte se placent derrière avec respectivement 50% et 48%, et seulement 26% ont souscrit une cyber-assurance.

L'efficacité des solutions est relative puisque un tiers des entreprises les considèrent inadaptées aux besoins et attaques actuelles.

Les nombreux risques du Cloud

Les entreprises estiment que la transformation numérique a un impact sur la sécurité des SI et des données (95%) et ces dynamiques impactent la gestion des données sensibles pour 89% des RSSI interrogés.

De plus, un nombre important d'entreprises (82%) ont leurs données stockées dans le Cloud, ce qui les expose à des risques liés, en particulier, à la difficulté de contrôle des accès et audit, au stockage des données dans des datacenters à l'étranger (hors droit français), au non-effacement des données, à la confidentialité vis-à-vis de l'hébergeur, à la non-restitution des données et du traitement Big Data à leur insu.

Sensibilisation & nouveaux usages du numérique

Et ce n'est pas tout. D'autres risques émergent rapidement avec les nouveaux usages du numérique à savoir

- **le BYOD avec l'utilisation de devices personnels au bureau**
- la multiplicité des devices (smartphones, tablettes…)
- l'usage personnel des devices de l'entreprise
- le télétravail et l'accès au réseau en mobilité
- les objets connectés
- le Machine to Machine
- le Big Data
- la blockchain
- le e-commerce

La sensibilisation des collaborateurs progresse, puisque 65% pensent que les salariés sont sensibilisés aux cyber-risques et plus d'une entreprise sur deux a déjà mis en place des procédures de vérification du respect des recommandations de cyber-sécurité lors de situation concrètes (audit, campagnes de faux phishing…).

La stratégie de la gouvernance

Au cours des douze prochains mois, les enjeux seront techniques, stratégiques et humains. Si les entreprises envisagent de nouvelles solutions pour se protéger et faire face aux cyber-risques, elles se tournent vers d'autres horizons.

Les trois enjeux clés seront :

- Bien analyser la gouvernance de la cyber-sécurité
- Mieux former et sensibiliser les collaborateurs
- Adapter les solutions à la transformation numérique

Sans oublier l'augmentation des budgets et des ressources, la sécurité des objets connectés, du Big Data, les modèles de sécurité collaboratives ou bien encore l'évolution des réglementations françaises et internationales et l'implication des états.

Enfin, un dernier point critique sans doute à améliorer. A la question, qui pilote la protection contre les cyber-risques dans votre entreprise ? 66% répondent sans hésiter la DSI contre 22% la direction des risques ...

Sondage OpinionWay pour le CESIN – Résultats Janvier 2017.
Étude quantitative réalisée auprès de 141 membres du CESIN, à partir du fichier membre du CESIN (280 contacts) du 10 novembre au 5 décembre 2016, selon les procédures et règles de la norme ISO 20252. Echantillon interrogé par Internet sous système CAWI.

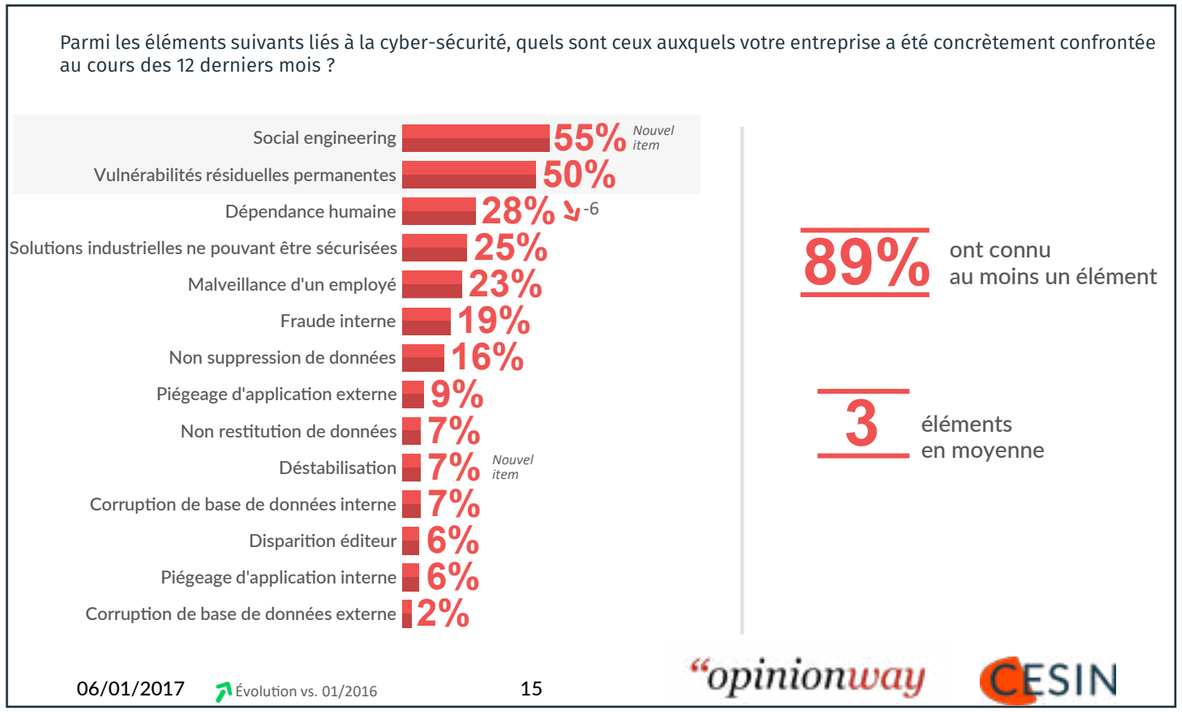


Schéma A

Comment la Cyber Threat Alliance
S'ATTAQUE AUX CYBERADVERSAIRES

A l'heure où l'amplification des attaques est quasi quotidienne et où la vigilance est de mise, abordons la mission d'une alliance bien spécifique, la Cyber Theat Alliance qui entend avant tout perfectionner les mécanismes de défense contre les cyberadversaires à l'échelon mondial. L'ex-responsable de la cybersécurité à la Maison Blanche, Michael Daniel, rejoint la CTA en tant que Président pour conduire la mission dévolue à cette entité. Nous avons posé quelques questions à Alexandre Delcayre, Directeur Avant-Vente - Europe du Sud, Russie/CIS et Israël de Palo Alto Networs, qui nous éclaire sur les missions de cette alliance.

La CTA est une initiative des spécialistes de la cybersécurité, à quels enjeux répond-elle ? Quelle est sa mission ?

La Cyber Threat Alliance, créée en 2014, a une triple mission :

- **Mettre en commun les informations** relatives aux menaces afin de mieux contrer les cyberadversaires, côté membres CTA, et de protéger les clients
- **Perfectionner la cyber-sécurité** des infrastructures informatiques stratégiques
- **Améliorer la sécurité, la disponibilité,** l'intégrité et le bon fonctionnement des systèmes informatiques

Avant sa création, chaque société ne procédait à aucun partage coordonné d'informations, ce qui avait un impact néfaste sur la capacité des entreprises clientes à mieux se défendre contre les cyberattaques, en particulier celles liées à l'augmentation de la fréquence et de la sophistication des menaces avancées ces dernières années.

Palo Alto Networks, en tant que membre fondateur de la CTA, se réjouit d'être rejoint dans cette initiative par Check Point Software Technologies Ltd. et Cisco, ce qui valide notre approche de partage coordonné d'informations, initiée il y a maintenant presque 3 ans.

Comment la CTA s'adapte-t-elle aujourd'hui pour faire face aux évolutions permanentes des cybercriminels ?

Le premier projet de la Cyber Threat Alliance, en tant qu'entité à part entière (entité à but non lucratif depuis février 2017), porte sur le développement et le déploiement d'une nouvelle plate-forme automatisée de mutualisation de la veille sur les menaces.

Celle-ci permet à ses membres d'intégrer des informations en temps réel, directement applicables à leurs produits, afin de mieux protéger leurs clients aux quatre coins du monde. Cette plate-forme optimise l'organisation et la structure des informations sur les menaces en élaborant des scénarios d'adversité, qui centralisent l'ensemble des éléments se rapportant à une campagne d'attaques donnée afin d'accroître l'intérêt contextuel, la qualité et l'exploitabilité des données.

Alexandre Delcayre

Cette approche innovante transforme une veille abstraite sur les menaces en autant de protections réellement exploitables, permettant aux membres d'accélérer l'analyse des informations et le déploiement de mécanismes intelligents dans leurs produits respectifs.

Quelles sont les pratiques de défense en cybersécurité ?

Une fois les informations relatives aux menaces partagées, chaque société met en place sa propre stratégie de déploiement. A ce sujet, nous avons une approche globale et transverse avec notre plateforme de sécurité axée sur la prévention des menaces connues ou inconnues d'où qu'elles proviennent (passerelle internet, Centre de données, Cloud public, SaaS, Poste client, IoT).

Les informations collectées via la CTA viennent enrichir notre Threat Intelligence Cloud, qui ne se limite pas à l'analyse de fichiers potentiellement malicieux mais qui inclut l'ensemble des contre-mesures et outils nécessaires à une sécurité agile, moderne et dynamique.

> Par Sabine Terrey

Les membres fondateurs
Fortinet, Intel Security, Palo Alto Networks et Symantec ont été rejoints par Check Point Software Technologies Ltd et Cisco. La CTA s'entoure de nouveaux membres affiliés, IntSights, Rapid7 et RSA, qui rallient Eleven Paths et ReversingLabs.

Accompagnement utilisateurs
ET COMMUNICATIONS UNIFIEES : UN LUXE ?

Si les communications unifiées sont en passe de devenir la norme pour les entreprises soucieuses d'optimiser les processus de décisions et faciliter la collaboration, leur acception par les utilisateurs est parfois plus délicate. Selon la vétusté de la situation de départ et la culture de l'entreprise, leur mise en place, mais surtout leur mode d'interopérabilité avec l'utilisateur peut choquer. A l'heure où l'on parle du droit à la déconnexion comment présenter ces environnements qui permettent d'être joignable 24 heures sur 24, 365 jours par an ?

Par ailleurs, l'utilisation optimale de ces fonctionnalités comme le présentiel, la messagerie instantanée, la conférence Web audio et vidéo demande un certain degré de maîtrise. Faire l'impasse d'un accompagnement utilisateur sur ce type de projet en comptant sur la capacité d'adaptation des utilisateurs : est-ce prendre un risque ? A vous de juger.

Préparer les esprits

L'introduction d'un environnement comme Skype for Business notamment en remplacement d'une solution vieillissante de téléphonie a de quoi bouleverser les habitudes. Le présentiel est l'un des points les plus sensibles dans les entreprises car il permet de connaître l'état d'un utilisateur, et notamment depuis combien de temps, il n'a pas utilisé son environnement Skype. Ce qui revient en quelque sorte à afficher dans toute l'entreprise son état de présence. L'état de présence est une information nouvelle qui inquiète parfois les utilisateurs. Un peu comme le fut l'image de la messagerie, où la communication pyramidale a fait place à une communication horizontale.

Le rôle de l'accompagnement utilisateur sera entre autres, d'expliquer comment fonctionne ce mécanisme d'état de présence, comment le gérer, pourquoi il est important d'assimiler qu'en toute circonstance, l'utilisateur garde un contrôle complet et que le fait de ne pas être connecté ne signifie pas que l'on ne travaille pas pour l'entreprise. Il sera également de rassurer sur l'utilisation de ces informations d'état de présence par les services informatiques en intégrant ces notions dans une charte commune.

L'enregistrement des échanges lors des conversations en messagerie instantanée et plus particulièrement si ceux-ci intègrent des personnes extérieures au monde de l'entreprise est souvent demandé par les services de sécurité. Aussi est-il préférable d'annoncer clairement cette mesure plutôt que de laisser les utilisateurs s'en apercevoir.

La conférence Web peut, elle aussi, poser des problèmes liés aux droits à l'image. Notamment si celle-ci est enregistrée puis utilisée à des fins de formation interne ou externe. Là aussi, il convient de préparer le terrain pour éviter toute ambiguïté.

Préparer l'entreprise

Même s'ils sont peu nombreux, certains projets de déploiement ont été stoppés net par les instances de l'entreprise car perçus comme un élément bouleversant les règles établies. Le présentiel combiné à l'omni présence du service qu'il soit sur PC, tablette et téléphone portable peut légitimement apparaître menaçant vis-à-vis du droit à la déconnexion. Il peut également être vécu comme une obligation de disponibilité en dehors des heures de travail. Présenter le projet aux représentants du personnel en précisant clairement les conditions d'usage et les limitations qui seront mises en place, aura tendance à renforcer l'adoption de la solution et contribuera parfois à clarifier, voire « dédramatiser » une situation.

La démonstration des fonctions de la solution, en prenant soin d'insister sur les options permettant à l'utilisateur de maîtriser ses statuts de disponibilités, est un point important qui aura tendance à rassurer et contribuera à une meilleure acceptation.

Former les utilisateurs aux nouveaux usages

Les communications unifiées comme la Solution Skype pour Entreprise est au regard d'un simple téléphone doté d'un cadran numérique, une véritable révolution fonctionnelle. Elle demandera un certain temps d'adaptation pour vos collaborateurs. Si aucun accompagnement n'est réalisé, un rejet est tout à fait possible, d'autant plus que votre solution va être immédiatement comparée à l'ancienne. Mais prenons un exemple cher à tous les utilisateurs : la qualité de la voix.

La solution ancestrale consistait à utiliser des lignes dédiées (analogiques) équipées de périphériques spécialisés que peu de choses pouvaient perturber. Les communications unifiées se basent sur un réseau Internet dont la bande passante est fluctuante, généralement sur des équipements divers et variés parfois inadaptés à la transmission vocale et bien souvent utilisés en mobilité. Si rien n'est fait, l'expérience de vos utilisateurs risque d'en pâtir.

Même si les messages commerciaux laissent penser que tout est réalisable tout le temps dans tous les environnements possibles, la réalité montre que ce n'est pas le cas. Organiser une conférence ne serait-ce qu'audio (et que dire de la conférence vidéo) demande un minimum de connaissances et un peu d'anticipation.

La réalisation de fiche-conseils pour l'organisation et la tenue d'une conférence Web intégrant la voix et vidéo est primordiale. Elle permettra notamment d'informer l'organisateur sur :

1 - L'anticipation dont il doit faire preuve avant d'ouvrir la conférence

- Types de participants susceptibles d'être invités (Interne / Externe/ Mobile)
- Nombre maximum de participants que la conférence peut héberger
- Téléchargement des documents de présentation
- Envoi de la présentation pour les personnes qui seront présentes uniquement en audio
- Réglage du son ou de ses périphériques audio
- Isolation vis-à-vis des bruits extérieurs
- Validation de son image (Positionnement de la Web Cam / Eclairage/ Cadrage)
- Mise en place ou suppression du Lobby d'attente
- Désactivation des microphones de tous les participants
- Passage en mode silencieux de son portable
- Etc..

2 - Les conseils qu'il doit donner lors du démarrage de la conférence

- Messages d'avertissements aux participants notamment si la conférence est enregistrée
- Conseils aux participants pour rejoindre la conférence par interface ou téléphone
- Appel audio d'éventuels participants retardataires ou ayant des soucis de connexion
- Vérification que tous les participants visualisent correctement le contenu présenté
- Activation de certains participants en tant que présentateur
- Essai son, pour vérifier que tous les participants soient en mesure de l'entendre correctement

3 - Les actions qu'il doit effectuer pendant la conférence

- Passage de relai à un autre intervenant et désactivation de son microphone
- Interaction en messagerie instantanée
- Désactivation ou activation de microphone de participants
- Vérification de la qualité du son (Option de l'interface Skype)
- Eviction d'un participant

4 - Les opérations susceptibles d'être réalisées après la conférence

- Clôture de la conférence
- Gestion de l'enregistrement de la conférence
- Mise à disposition de l'enregistrement

L'accompagnement au changement va permettre aux utilisateurs d'être informés non seulement des fonctionnalités de la solution mais également des limites de celle-ci notamment en mobilité. Votre accompagnement doit intégrer la solution en tant que telle mais également des aides à l'utilisation de solutions annexes comme peuvent l'être :

- La solution de téléphonie en place
- Les casques ou oreillettes audio (Comment basculer le son de son Téléphone vers un autre périphérique par exemple)
- Les pieuvres ou autre RoundTable
- Les tablettes de salles (Périphérique qui affiche la disponibilité de la salle)
- Les salles de visiophonie qui peuvent être connectées avec l'environnement de Communications unifiées (Exemple Polycom & Skype pour Entreprise)

L'objectif est ici de démontrer la cohérence applicative du projet et son intégration dans l'existant en faisant référence à des cas pratiques, quotidiens et récurrents. Il est important de mettre en avant les gains de temps dans l'exécution du travail et l'apport collaboratif de la solution car ceux-ci seront bien réels.

On ne manquera pas de préciser les cas d'usage dans les divers métiers de l'entreprise ainsi que les évolutions à moyen terme que vous envisagez. Exemple : « Aujourd'hui nous pouvons faire des conférences avec tous les collaborateurs de l'entreprise. Demain, nous serons en mesure de le faire avec les 300 millions d'utilisateurs Skype et ainsi renforcer notre approche BtoC».

Le risque de ne pas informer de ces nouveaux usages est important. Au mieux la solution sera sous utilisée, au pire le projet risque de ne pas dépasser le stade du pilote. Ne pas accompagner c'est faire l'impasse sur la valorisation de votre projet auprès de la Direction et limiter votre projet aux aspects purement techniques. Cela peut effectivement suffire lorsqu'il s'agit de changer d'opérateur télécom, mais lorsqu'il s'agit de moderniser les habitudes de travail de l'ensemble des collaborateurs dans le but de les faire adopter de nouveaux outils, j'en doute. L'accompagnement au changement sur un projet de communications unifiées n'est définitivement pas un luxe.

> Par Laurent Teruin, Expert, MVP Office Servers and Services

Maîtriser la donnée : l'enjeu des Directions métiers

La Data Analytics s'emballe et les compétences d'analyse des données se multiplient. Eclairage sur les défis, perspectives et risques pour toutes les fonctions clés de l'entreprise

Les données ne cessent de croître et l'intérêt pour celles-ci s'amplifie. Les entreprises n'ont plus le choix et les métiers l'ont compris, c'est en s'appropriant et en maîtrisant les données, que l'organisation augmente son levier de transformation et sa compétitivité.

Les Data Scientists deviennent essentiels, tout comme les indispensables modèles collaboratifs sur l'écosystème des données. Qu'il s'agisse de finance, du marketing, d'achats & supply chain, de ressources humaines ou bien encore des risques et de l'audit interne, toutes les fonctions de l'entreprise sont désormais concernées. A elles d'entrer dans le jeu des données.

1 – La Finance : sa transformation est d'autant plus liée à la donnée qu'elle parviendra à la valoriser. L'enjeu est de disposer de l'information financière pertinente au bon moment, d'utiliser la donnée comme levier de transformation, et d'améliorer la capacité de prise de décision.

2 – Le Marketing : le digital fait évoluer ses pratiques et usages de la donnée. Le développement de nouveaux services, de la connaissance client, de la personnalisation de la relation client sont les enjeux décisifs.

3 – Les Achats & Supply Chain : ces directions doivent comprendre les usages de la donnée en optimisant les achats et en explorant les gisements des datas.

4 – Les Ressources Humaines : elles doivent tenir compte de l'évolution des modes de travail, de la diversification des compétences, de la digitalisation des échanges pour maîtriser la donnée. Entre indicateurs de pilotage Ressources Humaines, gestion des données associées « Master Data », et approche « People Analytics », les usages doivent évoluer.

5 – Les Risques et l'Audit interne : contrôle et anticipation sont les clés de toute avancée. L'environnement de l'entreprise est exposé en permanence. Il faut donc renforcer sans cesse les dispositifs de contrôle et s'appuyer sur une démarche Data Analytics pour la gestion des risques, la rationalisation des contrôles, l'anticipation et l'identification de nouveaux modèles.

Etude Deloitte : Tendances 2017 - Data Analytics

Les 5 indices
D'UNE SECURITE INEFFICACE

Entre augmentation des cyber-attaques et complexité des processus des services IT, quel est le degré acceptable de cyber-résilience et quel est le niveau d'engagement des entreprises françaises ? Investissement, compétences et leadership fort sont les maîtres mots !

Maintenir son activité

La cyber-résilience est définie comme « la synchronisation des capacités de prévention, de détection et de réaction qui permettent de gérer une cyberattaque, d'en atténuer les répercussions et de s'en remettre ». En d'autres mots, **l'entreprise peut-elle maintenir le cap lors d'une attaque** et prévenir, détecter, contenir les menaces liées aux données, applications et infrastructure ?

Un haut niveau de cyber-résilience réduit le nombre d'attaques de données et permet de résoudre rapidement tout incident IT.

En France, les cyber-attaques posent encore problème, les chiffres sont sans appel puisque l'entreprise **n'est pas préparée à se remettre d'une cyberattaque pour 73%** et le niveau de cyber-résilience n'est pas « élevé » au sein de l'entreprise pour 79%.

Les 5 indices d'une sécurité inefficace

La complexité des procédures de l'entreprise est perçue comme un frein par 47 % des personnes interrogées.

Découvrons maintenant les 5 éléments qui nuisent à la sécurité.

1 - Le manque d'organisation et de préparation (69%), le manque de sensibilisation au risque, d'analyse et d'évaluation (52%) et l**e manque d'implication du leadership**. Ainsi, seulement 39 % déclarent que les dirigeants de leur entreprise reconnaissent le rôle de la cyber-résilience dans la réputation de la marque

2 - Le manque d'un plan de réponse aux incidents de sécurité informatique : un plan CSIRP n'est pas systématiquement appliqué dans l'entreprise (77%)

3 - L'augmentation de la durée de résolution d'un incident informatique (48%)

4 - La non-prise en compte de l'erreur humaine. Ainsi les incidents vécus impliquent une erreur humaine (pour 70%). Les incidents ou les dangers les plus récurrents sont les logiciels malveillants (70 %) et le phishing (62 %), suivis par l'erreur de communication (58 %)

5 - La négligence de la réglementation mondiale sur les données privées. Seuls 22 % estiment que leur organisation respecte scrupuleusement le règlement général européen sur la protection des données. Il y a urgence en la matière qu'il s'agisse du GDPR ou des lois internationales de chaque pays.

Les 5 clés d'une sécurité optimale

Plusieurs éléments contribuent à renforcer la cyber-résilience à savoir

1 - Un investissement dans le recrutement, la formation du personnel et dans les fournisseurs en services managés

2 - La participation à une initiative, plate-forme de réaction aux incidents, programme de partage d'informations sur les menaces. Toutefois, si le partage d'informations améliore la sécurité de l'entreprise (69%), on note des réticences, 54 % ne partagent pas d'informations sur les menaces, en raison d'absence d'avantages (55 %), de manque de ressources (29 %) ou de coûts trop élevés (29 %)

3 - La flexibilité, une équipe compétente et une bonne préparation permettent d'atteindre un haut niveau de cyber-résilience

4 - La mise en place d'un plan de de réponse aux incidents de sécurité informatique (CSIRP)

5 - La mise en place de fonctionnalités technologiques clés pour

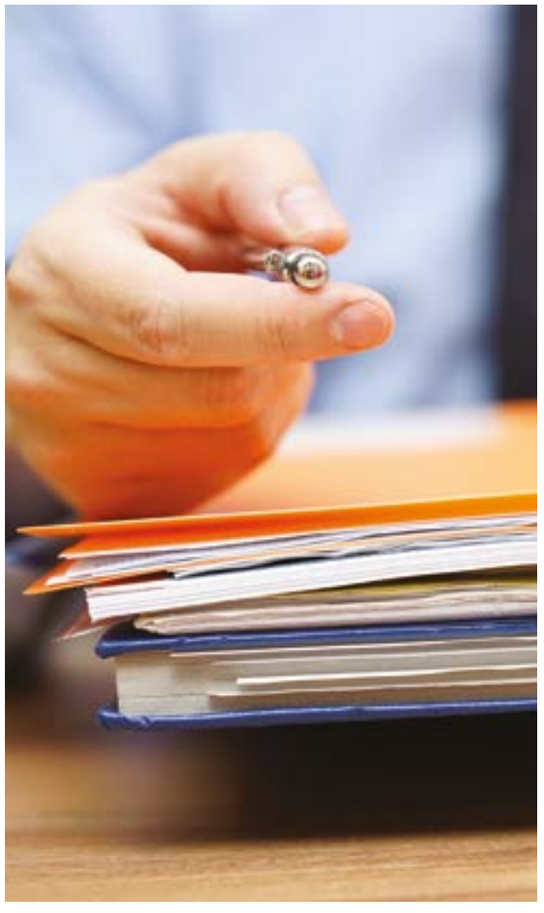
- empêcher les dispositifs non sécurisés d'accéder aux systèmes de sécurité (80 %)

- contrôler les terminaux et les connexions mobiles (77 %)

- sécuriser les données stockées dans le cloud (77 %) et contrôler les dispositifs mobiles non sécurisés, dont le BYOD (71 %).

> Par Sabine Terrey

Etude 2017 Cyber Resilient Organisation menée par l'Institut Ponemon pour IBM Resilient. 1ere édition pour la France.



L'IT hybride attire les DSI

Transformation numérique et IT hybride, un binôme stratégique

Complexité des SI, lourdeur des infrastructures mises en place, accélération des changements technologiques, que faire pour renforcer les niveaux de performance et retrouver l'agilité nécessaire aux systèmes IT ?

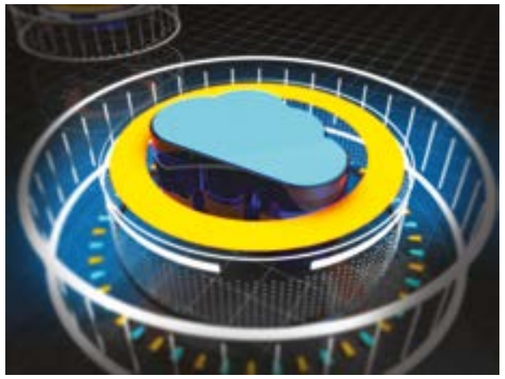
Face à la transformation numérique, la vision de l'IT hybride semble définitivement la réponse. Comment limiter les effets de disruption, le foisonnement des nouveaux entrants et la vitesse d'adoption ? Selon Carl Lehmann, directeur de recherche spécialiste de l'architecture d'entreprise, de l'intégration et de la gestion des processus métier chez 451 Group « l'IT hybride, c'est la stratégie pour y parvenir ».

Améliorer la compétitivité

Le Cloud booste la compétitivité, si la moitié des entreprises en sont convaincues, les traditionnels freins prennent le dessus, à savoir la sécurité (35%), l'intégration d'autres systèmes (32%) et de plusieurs clouds (25%). Et pourtant ! L'engouement est là puisque 63 % optent pour une démarche hybride. Tirer parti des ressources hétéroclites (cloud privé, cloud public, datacenters privés, sur site ou externalisés) reste l'objectif final.

Booster les niveaux de disponibilité

Le Cloud apporte des atouts technologiques à savoir la flexibilité (77%), de courts délais d'implémentation (66%), la facilité de déploiement (58%), la fiabilité (28%), les meilleures fonctionnalités (26%). Le business n'est pas en reste, puisque la continuité des opérations tout comme une meilleure collaboration vont dans le sens du nuage hybride !



Externaliser l'administration de l'infrastructure

Réactivité, agilité, fiabilité, cohérence, satisfaction des besoins et demandes internes, accélération de l'innovation ... les avantages de l'externalisation se multiplient.

En résumé, découvrons le petit Top 5 de l'externalisation

- Alignement sur les évolutions technologiques : 72%
- Capacité à répondre aux besoins de l'entreprise : 67%
- Rapidité à résoudre les problèmes : 57%
- Expérience utilisateur : 57%
- Accès aux compétences requises : 57%

Sans oublier la fiabilité dans la maîtrise des coûts (56%) et l'intégration des systèmes de contrôle (51%).

Etude Harvard Business Review, intitulée « Hybrid IT Takes Center Stage » et menée pour Verizon Enterprise Solutions auprès de 310 dirigeants d'entreprises et DSI du monde entier.

VOUS FEREZ LA DIFFÉRENCE

AUDIT
CONSEIL
INTÉGRATION
SUPPORT
GESTION DE PROJET
FORMATION

METSYS

PARIS • LYON • LILLE • RENNES
www.metsys.fr

Gold
Microsoft Partner

Microsoft