N°13 I MARS 2019

CONDUIRE LA TRANSFORMATION NUMÉRIQUE DE L'ENTREPRISE

SMART DSI®

DOSSIER
La proposition de valeur

INTERVIEW
Comment s'adapter aux nouvelles exigences des espaces de travail ?

EXPERT
Les microservices sont-ils l'avenir des applications en entreprise ?

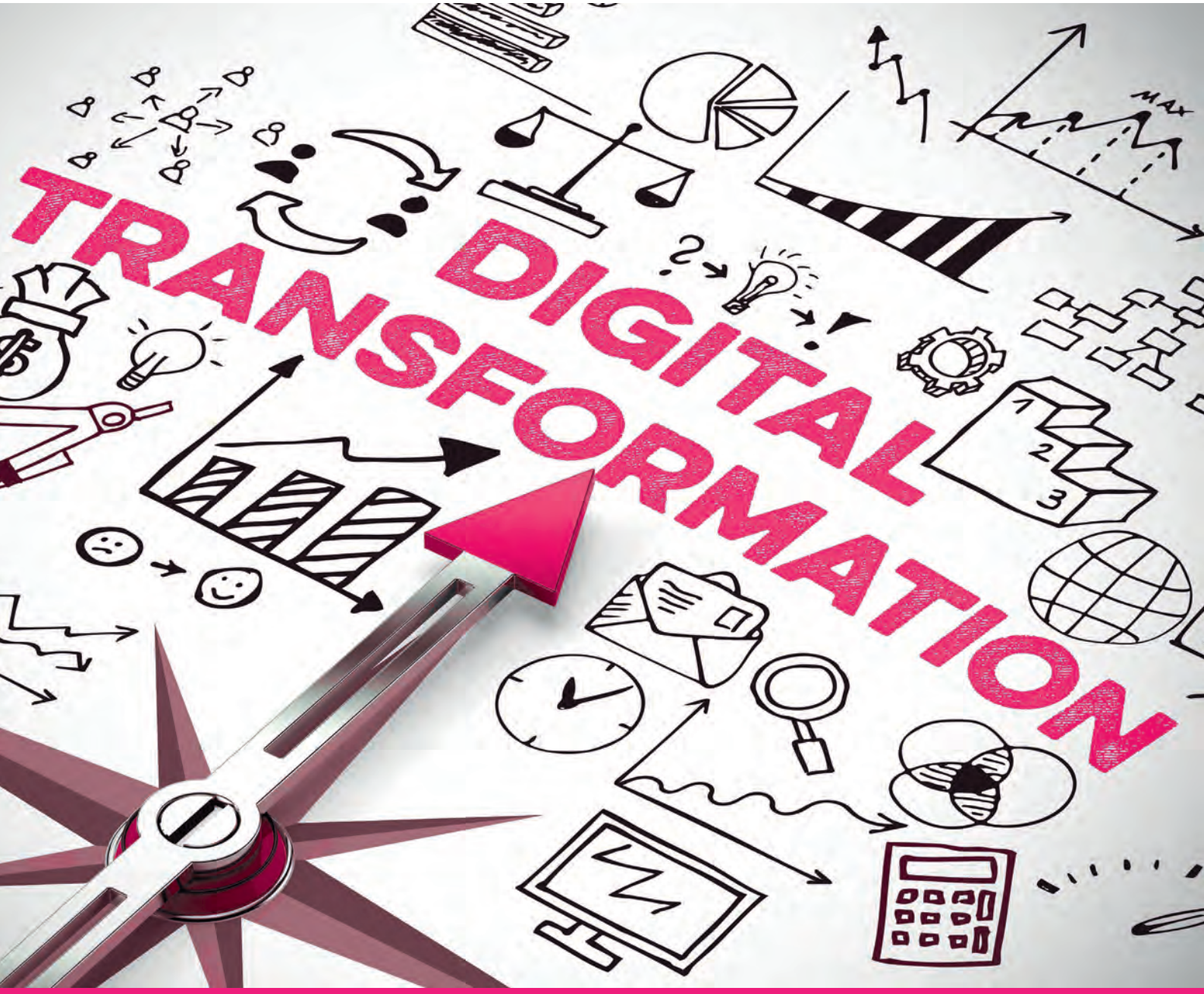
INTERVIEW
Blockchain : apporter des garanties sur les données

L'ETUDE A RETENIR
2019 - 2021 : Les 5 tendances d'un monde post-digital

vmware

Insight

AGILITÉ, CLOUD, AUTOMATISATION, RECENTRAGE SUR LA DONNÉE, INNOVATION…



Comment relever les défis de la transformation numérique ?

Découvrez nos avis d'experts sur https://fr.insight.com/learn

Suivez-nous @Insight_FR

Contactez-nous : info.fr@insight.com

L'accélération des stratégies digitales !

Il est de bon ton, chaque début d'année, de voir fleurir les bonnes résolutions face au marché qui se complexifie! Et pour les appuyer en 2019, revenons sur quelques tendances clés qui vont accélérer la transformation digitale des organisations. C'est ainsi que six éléments majeurs entendent impulser des changements informatiques au sein des démarches digitales des entreprises[1].

Prise de risques et ambition, écosystèmes d'informations et confidentialité des données, plates-formes de nouvelle génération et informatique en périphérie à savoir IoT, intelligence artificielle, réalité augmentée & virtuelle, blockchain, mais aussi data centers partagés dans le cloud public, Intelligence artificielle et Machine Learning pour de nouvelles sources de revenus ! Voici donc 6 points cruciaux envers lesquels nous devons porter toute notre attention et notre vigilance.

Et pour compléter notre approche, regardons d'un peu plus près les DSI qui continuent de croire en cette transformation puisque 82% s'adaptent et fournissent un important investissement personnel pour rester compétitif face à la concurrence[2].

De plus, pour développer plus amplement leur leadership, les DSI se remettent sans cesse en question et continuent d'élargir leur champ de vision social et digital afin d'y puiser toute leur inspiration ! Retenons trois indicateurs clés, vous verrez, le DSI n'hésite plus à s'impliquer en

- *lisant des rapports d'analystes & médias - 53%*
- *utilisant activement les réseaux sociaux (Twitter et LinkedIn) - 43%*
- *changeant fréquemment ses responsabilités au sein de l'entreprise - 34%*

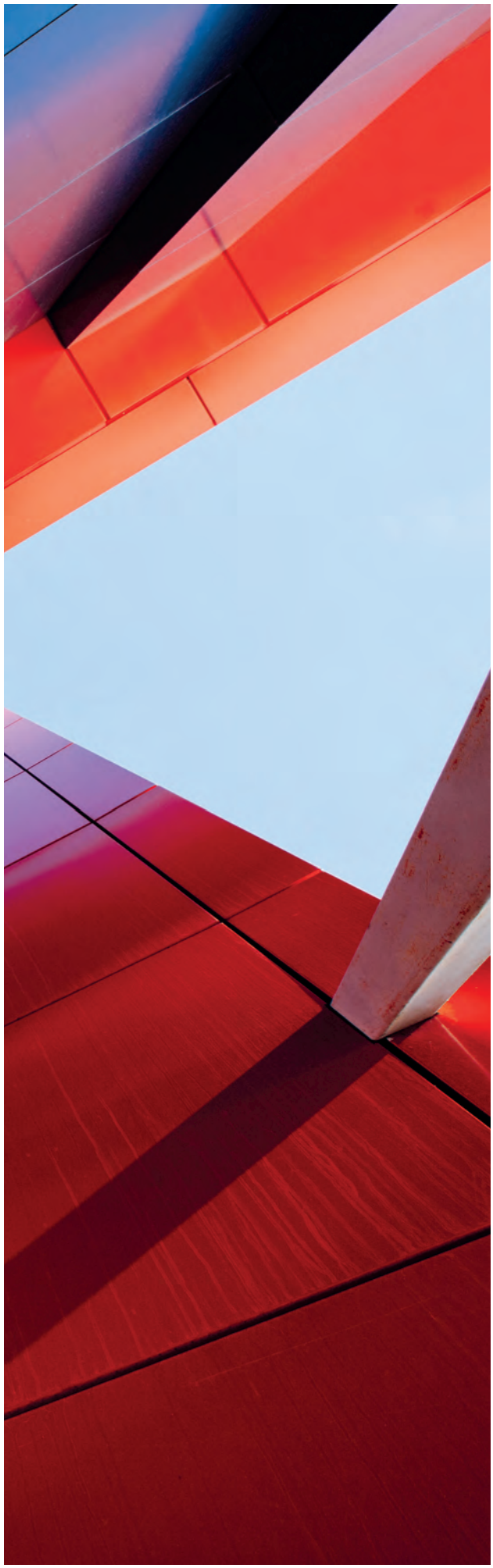
En outre, communiquer avec la direction pour justifier de la pertinence des investissements IT et miser sur la notion de valeur et de flexibilité sont désormais les priorités.

Il est ainsi devenu urgent de se focaliser sur ce qui peut être réellement entrepris et réalisé pour influencer votre « entreprise apprenante »[3], anticiper et rester dans la course !

Très bonne lecture !

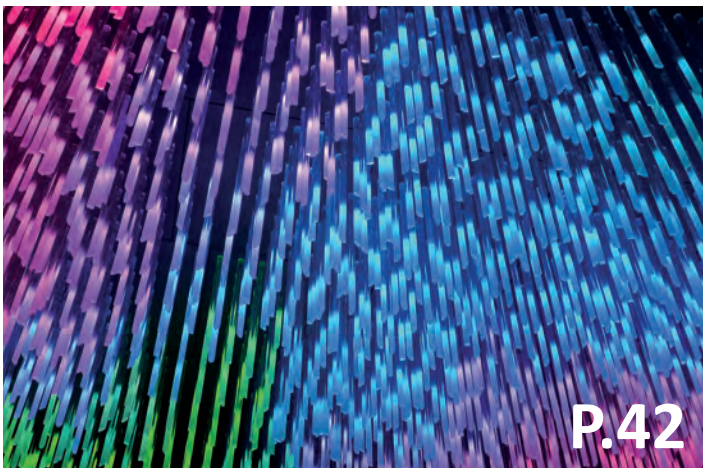
Sabine Terrey
Directrice de la Rédaction
sterrey@itpro.fr

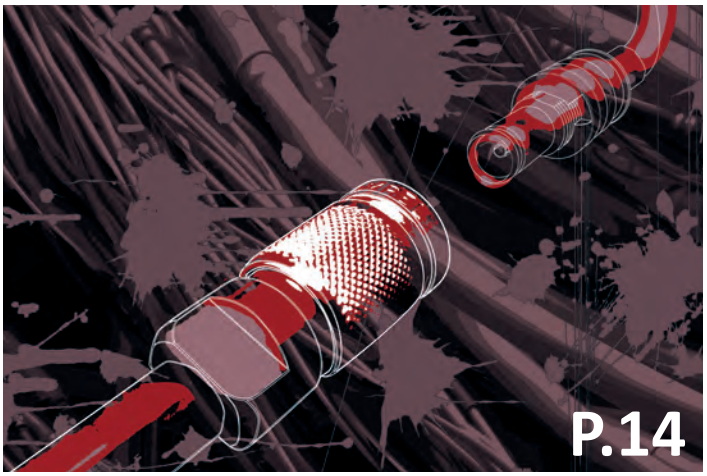
1 - Source DXC Technology janvier 2019
2 - Source Citrix & OnePoll décembre 2018
3 – Référentiel de la maturité digitale 2018-2019 IBM



SMARTDSI

N°13 I MARS 2019






P.32


P.12


P.36

SMARTDSI

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

Comité de rédaction associé à cette édition
Didier Danse, Théodore-Michel Vrangos, Sylvain Cortes, Sabine Terrey, Jeff Angama, Christopher Glémot, Philippe Paiola, Cédric Bravo, Laurent Teruin

Régie Média & Publicité - Com4Médias
Christophe Rosset – Directeur Commercial
christophe.rosset@com4medias.com
Tél. 01 39 04 24 95

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 – Philippe Deslandes
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

La proposition de valeur,
VECTEUR DE LA CONCEPTION DE SERVICES ET PRODUITS INFORMATIQUES

> Par Didier Danse

Pour certains, la proposition de valeur se confond avec le slogan ou les activités marketing, minimisant une démarche globale de réflexion et de conception aux aspects promotion et communication qui en résultent. Les mots ne sont pourtant que la représentation d'un état d'esprit et d'une approche utilisés lors de la conception d'un produit ou d'un service. Pour d'autres, la proposition de valeur ne fait qu'un avec la création de valeur. Bien que liés entre eux, ces aspects s'avèrent pourtant très différents. Une compréhension des objectifs et des enjeux de ces deux concepts est un avantage non-négligeable.

Dans le domaine informatique, la proposition de valeur est bien souvent omise, souvent de manière involontaire. Alors que les sociétés de service se doivent de promouvoir leur capacité à délivrer, cet aspect est parfois minimisé en intra-entreprise. Bien que les fonctions et services support, dont fait partie le service informatique, ne gèrent pas de rentrées financières directes, ils fournissent bien de la valeur. Dans ce contexte, la proposition de valeur claire s'avère d'autant plus importante.

- 1 -

Focus sur la création de valeur

Que sont la création de valeur et la proposition de valeur ? En quoi sont-elles différentes ? La création de valeur est l'ensemble des bénéfices qui émergent de la production d'un bien ou la délivrance d'un service. Quant à la proposition de valeur, il s'agit de l'ensemble des méthodes et outils permettant d'exprimer ce que le bien ou le service amèneront à l'utilisateur de celui-ci, de manière similaire à ce que la vision et la mission indiquent vers quoi tend une collectivité et comment elle se positionne pour y parvenir.

Pour faire simple, la proposition de valeur est l'élément externe de la stratégie autour d'un bien ou d'un service qui est en lien avec les clients et leurs besoins et attentes tandis que la création de valeur sur la chaîne de valeur est interne et repose sur ses activités et ses opérations. Les uns sont des facilitateurs pour les seconds. Avoir une offre bien ficelée permet de générer du profit. Générer du profit permet l'investissement et ainsi de la création de valeur durable dans le temps. Ainsi, le bien proposé ou le service rendu se doit de répondre à un besoin et ce pour un tarif qui convient.

Chacune des composantes de la chaîne de valeur se doit de créer de la valeur directe ou indirecte. Il est très souvent nécessaire de valoriser les opérations : Quels sont les gains financiers ? Comment la charge de travail est-elle impactée ? La création de valeur peut, en effet, s'appuyer non seulement sur des rentrées financières mais aussi sur la réduction des coûts associés, l'optimisation des façons de travailler ayant pour but de réduire les pertes. Cette valeur peut prendre différentes formes, notamment la valeur sociale, qui se transposera dans le ressenti et le bien-être ou encore l'environnement et l'économie locale. Des changements dans la gestion quotidienne management peuvent également créer de la valeur. En effet, pour créer de la valeur, l'innovation peut être apportée à toutes les étapes de la chaîne de valeur.

Pour innover, il important de lister les parties prenantes au sein d'une chaîne de valeurs, chacune avec une implication et un poids relatif dans la création de valeur. Pour faire partie de la chaine de valeur, chaque maillon doit avoir une proposition de valeur adéquate.

- 2 -

L'adéquation de la proposition de valeur avec le besoin

Lorsque l'on parle de définir les objectifs et le fonctionnement d'un système ou d'un service informatique, différentes approches peuvent être utilisées. Ainsi entend-on régulièrement que le produit ou le service doit répondre à la demande formulée, ce qui nous amène à utiliser des véhicules plus confortables afin d'affronter les éternels bouchons sur la route et à passer du diesel à l'électrique, son remplaçant nommé. Il s'agit d'une réponse à la demande énoncée d'améliorer un confort ou de fournir des alternatives à l'utilisation d'énergies fossiles mais non une solution au problème de fond, qu'il s'avère parfois plus dur à exprimer par bien des gens.

Les organisations innovantes vont plus loin dans leur approche en répondant non plus aux exigences ou aux spécifications exprimées mais bien en étant à la recherche des problèmes réels et de solutions véritables avec comme conséquence de régulièrement remettre en question les habitudes et les croyances, qui sont bien souvent des barrières à l'acceptation. Une réponse efficace et durable à un besoin requiert de clarifier la promesse de valeur, c'est-à-dire comment la solution répond à un besoin en répondant à ces trois questions :

- Quel est le problème à résoudre ?
- Qu'est ce qui rend la solution unique ?
- Comment mesurer le résultat fourni par cette solution ?

Généralement, les problèmes à résoudre prennent source parmi un des 4 obstacles courants : le manque d'argent, la difficulté d'accès, l'insuffisance de compétences et le manque de temps. On notera qu'aussi bien les besoins et attentes que les solutions varient selon les profils ciblés et les solutions à ces problématiques et attentes peuvent être dès lors très différentes. De ce fait, plusieurs propositions de valeur peuvent cohabiter, une par produit et segment de clientèle. La mesure du résultat doit permettre de mettre en avant non seulement les aspects financiers mais aussi les savoir-faire acquis, l'amélioration de la capacité, des relations et des apprentissages.

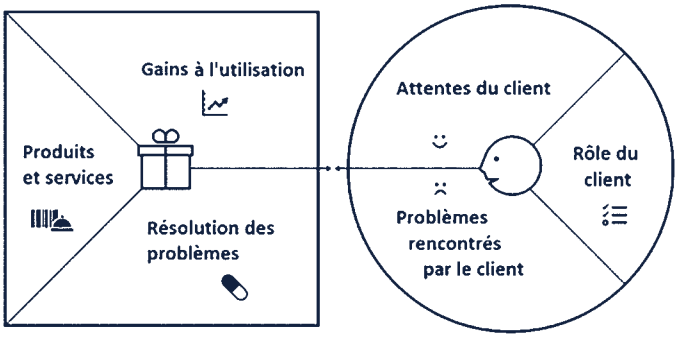
- 3 -

Le canevas de la proposition de valeur

Pour structurer la démarche mais aussi la réponse, le canevas de la proposition de valeur est l'outil adéquat.

La première partie du canevas porte sur le client. Il s'agit en effet de lister les bénéfices attendus et les aspirations du client, qui sont rassemblées sous le terme attentes. A cela s'ajoutent la liste des problèmes rencontrés par le client mais aussi ses frustrations. Enfin, il est nécessaire de définir le rôle du client pour indiquer ce qu'il veut faire ou ressentir.

En regard des problématiques à résoudre, sont explicitées les solutions proposées une fois la réflexion portée. Ainsi pour chaque catégorie précitée au sein du bloc client, les réponses sont regroupées en trois catégories: la manière de résoudre les problèmes listés précédemment, les gains à l'utilisation envisagés ainsi que les produits et services qui permettent d'atteindre les objectifs précédemment cités.



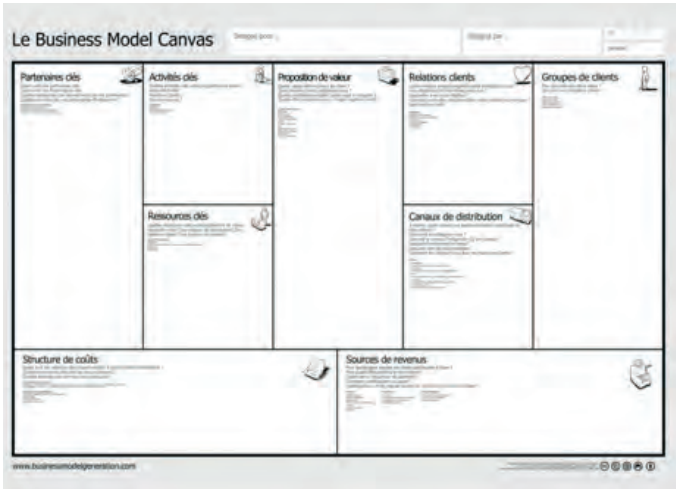
Les gains peuvent être multiples : productivité, design et ergonomie mais aussi accessibilité, nouveauté, performance, customisation, prix, réduction des coûts et des risques.

Prenons un exemple de solutions répondant à des problématiques dans un domaine donné : afin de réduire le nombre de paiements à effectuer lors d'un trajet en train (problème), une application mobile (produit) permet de payer le billet de train mais aussi le parking ou le bus pour se rendre à la gare (gain). La mise à disposition d'un petit déjeuner de qualité (gain et ressenti), à un prix réduit, inclus dans le billet, et qu'il est possible de prendre en amont ou lors du trajet (résolution du problème), permet de compléter la démarche de recherche de gain de temps (problème) et de minimiser les coûts (problème).

- 4 -

Le canevas *Business* Model

Le *pourquoi* peut être complété en décrivant le comment, à savoir les techniques et outils utilisés pour fournir le bien ou le service, c'est-à-dire comment la proposition de valeur sera délivrée à la cible. Le canevas *business model* se prête à la clarification des activités, des partenaires, des ressources, des coûts et des revenus mais aussi ses canaux de distribution :



Nous ne le détaillerons pas ici mais il était important de le citer tant il complète le canevas Proposition de valeur. Pour la petite histoire, le canevas *Proposition de valeur* est la résultante d'une adaptation du canevas *Business Model*. Ses concepteurs ont dû remettre en question leur démarche et leurs connaissances pour aboutir à un produit répondant mieux aux besoins, ce qui montre que l'ouverture permet de répondre de manière innovante à une problématique donnée.

- 5 -

L'agilité au service de la proposition de valeur

De nombreuses méthodes existent pour concevoir une proposition de valeur, avec notamment le *Design Thinking* mais aussi ses variantes telles que le *Creative Problem Solving*. Ces méthodes d'innovation et de recherche de solutions partagent toutes un certain nombre de caractéristiques : La pluridisciplinarité des forces en présence, l'aspect itératif de la conception, la remise en question permanente et la progression par la preuve.

Il est nécessaire de s'assurer que le produit ou le service soit désirable, réalisable mais aussi viable. Pour ce faire, il important d'inclure les utilisateurs dans le processus mais aussi les fournisseurs des technologies et des fonctions support pour valider la viabilité économique et organisationnelle, que ce soit sur les aspects managériaux et des ressources humaines.

Afin de répondre efficacement à une problématique, il s'agit tout d'abord de l'identifier. Ainsi, il est important de ne pas se limiter lors de l'énumération des différents points lors des phases de conception, tant pour les problèmes que les solutions. L'identification du problème réel permet de faciliter l'identification d'une solution à proprement parler. En proposant des manières innovantes de répondre à ces problèmes qui sortent de l'ordinaire, la solution devient unique.

Les étapes de l'approche itérative peuvent être énumérées de nombreuses manières. Le *Creative Problem Solving* propose la démarche suivante :

1. *L'identification des problèmes et attentes* : cette étape est la combinaison de deux actions qui se répètent, à savoir écouter et reformuler un besoin jusqu'à le rendre positif, motivant et ambitieux, le plus important étant que le besoin exprimé soit partagé. Différentes techniques se prêtent à la démarche. Cette expression de besoin est reportée dans le canevas de proposition de valeur
2. *L'analyse fine des données* : sur base du besoin identifié, la collecte d'informations peut s'avérer utile afin d'évaluer la portée du besoin mais aussi de rendre le besoin factuel et valider les idées et solutions lors des étapes suivantes. Ces informations sont généralement annexées à la définition du besoin
3. *La définition d'objectifs* : elle permet de répondre à ce que l'on veut résoudre et peut être formalisée dans le canevas *proposition de valeur*

4. *L'émergence des idées-pistes* : plusieurs techniques existent pour permettre de voir émerger des idées innovantes avec notamment le brainstorming qui se doit de respecter une durée donnée et avec un rythme soutenu. De cette manière, les idées non réfléchies émergent. C'est souvent au sein de ces idées que se trouvent les futures innovations

5. *La sélection des idées sur base de critères spécifiques* : Une fois les pistes identifiées, ne retenir que celles qui peuvent être viables mais aussi qui respectent l'ensemble des critères tels que la durée potentielle avant la mise à disposition de la solution, la viabilité financière ou encore le respect de la culture, des objectifs et des ambitions actuelles ou futures de l'entreprise

6. *La transformation des idées en solutions innovantes et réalistes* : en effet, s'il n'est pas possible de démontrer la valeur après une courte période, il est nécessaire se questionner sur la pertinence de la solution

7. *L'adhésion des interlocuteurs et réalisation de la solution* : la validation de la solution par l'ensemble des interlocuteurs est nécessaire pour améliorer l'adhésion générale autour du bien ou service. Pour cela les solutions doivent être présentées sous la forme d'un message clair quelle que soit la technique de communication utilisée telle que le jeu ou encore le dessin

8. *La planification de la mise en œuvre* : cette mise en œuvre peut respecter une approche plutôt classique mais elle peut également proposer une démarche innovante, apportant de la valeur complémentaire au produit ou au service fini.

Comme on peut le voir, les méthodes suivent un ensemble d'étapes précises, tel un processus structuré et structurant. Il s'agit pourtant d'une méthodologie heuristique, c'est-à-dire basée sur la découverte et il s'avère peu probable de prédire les inputs qui seront utilisés à chaque étape et il est normal et régulier que le processus retourne à une étape précédente. Dans tous les cas, il s'agira de s'assurer que des temps de pause soient présents afin de se questionner sur les étapes précédentes et la manière de les mener. Il est fréquent que ces démarches n'aboutissent pas à la mise en œuvre d'une solution.

A chaque étape, différentes techniques peuvent être utilisées avec notamment l'*A/B testing*, ne laissant aux interlocuteurs que deux choix possibles. Cette technique fait partie des plus simples à mettre en œuvre mais aussi des plus efficaces. Elle devra cependant être exécutée plusieurs fois afin de voir émerger une orientation claire.

De par la combinaison de l'agilité, du canevas *proposition de valeur* et des techniques de co-création, la valeur du bien ou du service n'en sera que plus élevée et répondra d'autant plus aux problèmes du segment de marché cible.

> Par Didier Danse
IT Manager - Collaborative Platforms and IT Tools

Business Intelligence : les 10 grandes tendances en 2019

Quelles tendances et technologies façonneront le secteur de la Business Intelligence en 2019 ? Une approche moderne de la BI exploite le potentiel des données.

Une Intelligence Artificielle transparente

Compréhension des données, automatisation de la prise de décisions, fiabilité des recommandations... L'essor d'une IA capable de présenter les modèles de machine learning de manière transparente est essentiel. Des modèles plus transparents, une documentation ou un historique sont attendus pour augmenter la confiance.

Le langage naturel pour humaniser les données

Les fournisseurs de solutions BI intègrent le langage naturel aux plates-formes, pour des interfaces et visualisations plus naturelles. Il faut comprendre l'intention de l'utilisateur et faire progresser le dialogue : interagir avec une visualisation permet d'approfondir les analyses !

La contextualisation des données

Des fonctionnalités analytiques mobiles et intégrées, des extensions de tableau de bord et des API sont proposées : les analyses intégrées placent les données et informations au cœur des workflows, les extensions de tableau de bord permettent d'accéder à des systèmes externes, et les analyses mobiles permettent l'accès aux données.

L'aspect social

Le mouvement Data for Good révèle le potentiel altruiste du partage de données. Grâce à la flexibilité du cloud computing, les ONG et organisations à but non lucratif développent des environnements de données élaborés : création de plates-formes dédiées au partage, collaboration entre associations, dialogue pour renforcer la confiance.

Les codes de déontologie

Règlementations, confidentialité, partage des données personnelles... certaines professions sont déjà régies par un code de déontologie, et une réflexion pour ces principes aux pratiques analytiques est en cours. Selon le Gartner, le nombre de CDO pour qui la déontologie fait partie de leurs responsabilités a augmenté de 10 points entre 2016 et 2017.

Les plates-formes BI modernes

La gestion de données est primordiale et les processus de curation de données (capture, nettoyage, définition et harmonisation de données disparates) convergent avec les plates-formes BI pour une gouvernance adaptée.

Le nouveau langage des entreprises

La visualisation de données est clé : la mise en récit pour communiquer le cheminement évolue avec la culture analytique. Cette approche participative partage les responsabilités entre le créateur d'un tableau de bord et le public, facilite les discussions, la communication et la mise en pratique de nouvelles idées.

L'adoption de l'analytique

Pour générer un impact sur les activités, les équipes de direction doivent mesurer la manière dont la plate-forme BI est utilisée : communautés internes d'utilisateurs pour booster l'engagement.

Démocratie des données & data scientist

Les data scientists doivent posséder des connaissances en machine learning et statistiques avancées, participent à l'application des résultats aux problématiques métier, communiquent avec la direction et collaborent avec les utilisateurs.

Migration de données dans le cloud pour une BI moderne

La migration vers le cloud offre flexibilité, scalabilité, et coût total de possession réduit. Le cloud permet également de capturer et d'intégrer facilement différents types de données.

Source Tableau Software

La cybersécurité,
CLÉ CACHÉE DE LA TRANSFORMATION DIGITALE

On assiste, depuis quelques années déjà, à la perte de pouvoir des acteurs classiques de contenus au profit des acteurs de la transformation digitale tels qu'Accenture ou encore Cap Gemini.

Chaque camp se déplace vers l'autre. Publicis rachète Sapient pour, comme d'autres géants de la publicité tel qu'Omnicom l'ont fait, tenter de "connecter la data", combinant la création dynamique avec la technologie, dans le but de délivrer des expériences personnalisées à grande échelle.

Une technologie multicanal ominiprésente...

Advertising Age, la bible de la communication, a sacré Accenture premier réseau digital mondial. La stupeur et une certaine crainte de se faire avaler tout cru par ces nouveaux gourous de l'ère digitale, se sont alors emparées des acteurs historiques, les WPP, Omnicom et Publicis qui régnaient jusqu'alors sur le secteur. En effet, la transformation digitale d'aujourd'hui et de demain est bien plus précise et plus profonde, œuvrant au cœur des métiers des entreprises, couvrant l'expérience des utilisateurs et clients, au sein des fonctions transverses telles que la RH ou la finance. Casser les silos, faire le lien entre la connaissance du client via la data, une création marketing qui s'adapte au contexte et aux personnes ; le tout à travers une technologie multicanal omniprésente.

Au-delà donc des technologies et *user experiences*, au-delà des modes de fonctionnement comme le cloud et les réseaux sociaux, la cybersécurité - la protection adaptative des informations - est une composante plus qu'indispensable.

Eviter une catastrophe financière et d'image

Partager des données est essentiel au fonctionnement de l'entreprise. Par exemple, partager à travers des big data des fonctions marketing ou CRM externalisées dans le cloud, impose une réflexion technique de sécurité en amont, nécessite la mise en place d'outils et de fonctions de sécurité comme les CASB pour les flux cloud ou les DAM pour la protection et la traçabilité des informations fines des bases de données.

La cybersécurité doit être partout afin d'éviter à l'entreprise une catastrophe financière et d'image. Prenons l'exemple des réseaux sociaux et de la messagerie, épine dorsale de transmission des marques vers les internautes et consommateurs. Le durcissement de la réglementation en matière de protection des données personnelles, d'abord en Europe puis certainement dans un avenir proche aux USA et en Asie, impose des mesures de protection des données, d'anonymisation, de stockage avec des contraintes techniques à respecter, etc. Les outils et les processus de sécurité peuvent et seront aussi utilisés dans la lutte contre les *fake news*, grâce à l'authentification des émetteurs de données et aux techniques de protection des marques (DMARC par exemple).

Phishing et ransomwares

La digitalisation de la société de consommation oblige les gestionnaires des réseaux sociaux et les opérateurs telcos à lutter également contre le phishing, le canal d'attaques des pirates et autres ramsomwares. *Clean-pipe* ou *clean-services* - de nombreuses appellations existent pour décrire les options de sécurité informatique de nettoyage - utilisent différentes techniques comme les sandbox (pour déjouer les menaces des messages et des pièces jointes avant leur distribution dans les boîtes de messagerie des utilisateurs), les processus de CyberSOC (Security Operations Center), les processus et scans de gestion des vulnérabilités, etc.

Des systèmes de paiements

Autre aspect important dans la course à la digitalisation de notre société : la prochaine grande étape pour Facebook, Instagram, Tencent, Whatsapp, etc. est l'intégration des systèmes de paiement. Quel système de paiement pourrait exister sans sécurité (chiffrement, authentification, etc.) ?! La non prise en compte au plus haut niveau de ces aspects impliquerait en cas d'incident, la déstabilisation du réseau social. Mais, la cybersécurité couvre aussi les cryptomonnaies, bâties sur le principe de la signature électronique. Tencent et Telegram utilisent déjà les systèmes décentralisés de cryptomonnaies.

L'ère digitale en toute sécurité

Enfin, le cloud est par définition le socle de fonctionnement de l'ère digitale, la base conceptuelle et fondamentale des réseaux sociaux, avec l'export continu des données et leur hébergement. Toutes les offres de services, d'apps en mobilité, de e-commerce, etc. s'appuient sur le cloud. Alors, le cloud sans cybersécurité, sans traçabilité des accès aux données, sans chiffrement des données, sans étanchéité des données des utilisateurs, sans surveillance et filtrage des données sortantes de l'entreprise et partageables avec divers opérateurs de services (marketing, pub, paiement, etc.) est inconcevable.

Dans l'ombre de la réussite des services digitaux se trouve donc obligatoirement et de manière croissante la cybersécurité.

Il y a ceux qui la négligent, pour la plupart par légèreté ou incompréhension des enjeux. On dit qu'un minimum de 10% du budget IT et digital de l'entreprise doit aller à la sécurité. Il y a ceux, la grande majorité, qui investissent sérieusement, proportionnellement à leurs projets IT et de digitalisation et qui l'utilisent aussi comme argument commercial et marketing.

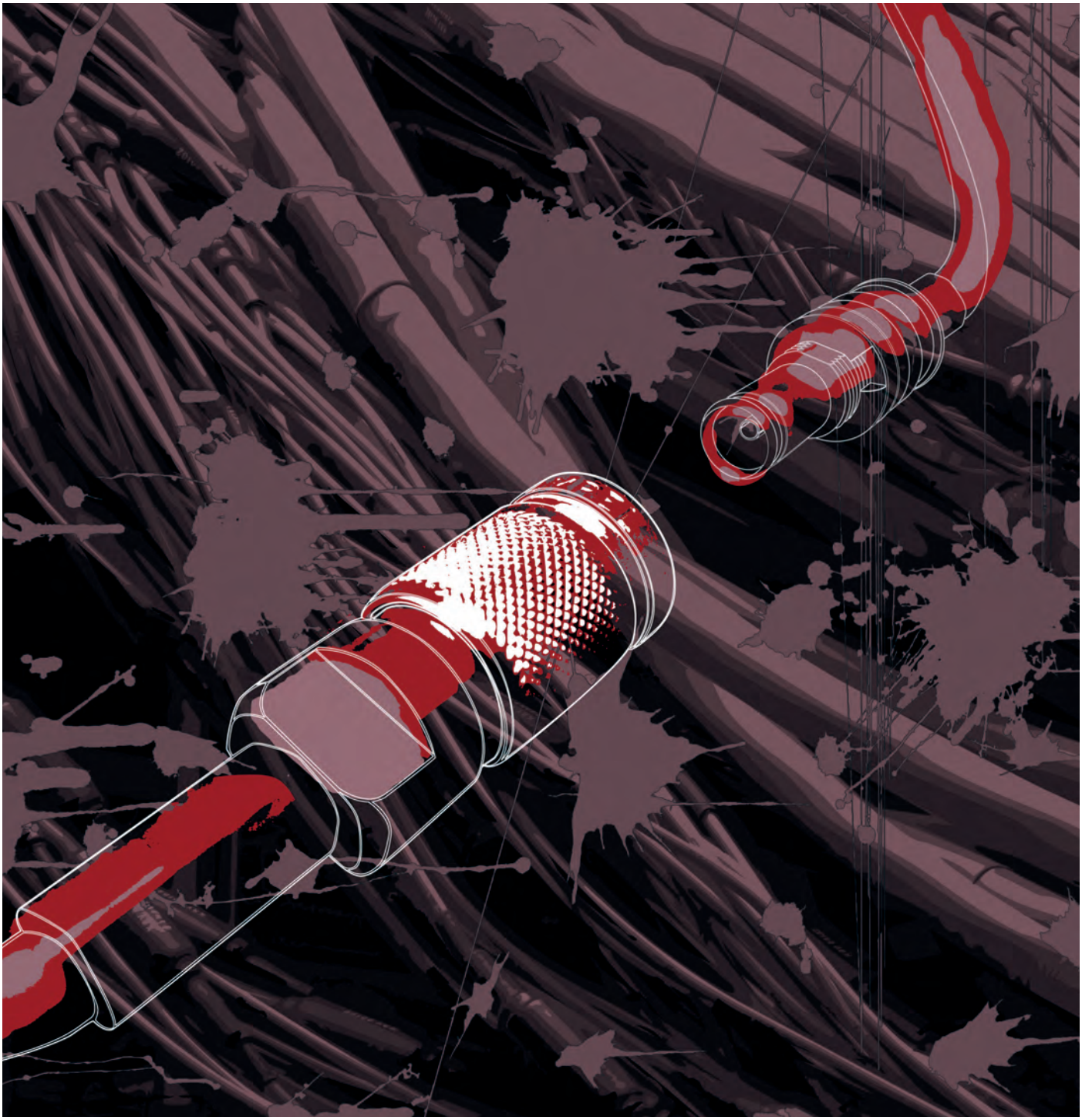
Ce sont souvent ceux dont la direction générale est directement impliquée et motivée, ceux qui se sont rendus compte à travers des exemples vécus, du formidable potentiel de l'ère digitale en toute sécurité.

> Propos de Théodore-Michel Vrangos, co-fondateur et président d'i-Tracing, recueillis en exclusivité par la rédaction de Smart DSI

L'enjeu de la connexion internet
POUR RESTER COMPÉTITIF

Trop d'entreprises en France n'ont pas d'accès internet haut débit. Alors, dans ce cas, comment pallier ce manque, accélérer l'accès au très haut débit sur l'ensemble du territoire et répondre aux besoins ?

ICOW, spécialiste de la technologie 4G pour un usage professionnel, vient d'annoncer LanLink, une solution qui offre aux entreprises non couvertes par la fibre, une connexion internet haut débit stable et un firewall administrable à distance. Entretien avec David Coiron, CEO et co-fondateur d'ICOW.



David Coiron

« La couverture du territoire est aujourd'hui très inégale et le plan France Très Haut Débit qui promet une couverture totale du territoire pour 2022 risque de ne pas être tenu ». Pouvez-vous nous en dire plus ?

Il convient de rappeler qu'en France, l'accès à Internet est considéré à « très haut débit » dès que le débit est supérieur à 30 Mégabits par seconde. A ce jour, seules la fibre et la 4G+ (et encore davantage la 5G) permettent d'obtenir des débits supérieurs à 30Mb/s.

Il est bien évidemment illusoire de croire que la fibre sera déployée sur 100% du territoire d'ici 2022, sachant par exemple qu'à peine 30% des PME françaises sont actuellement raccordées à la fibre selon une étude récente de l'Idate. De très nombreuses entreprises ne bénéficieront certainement jamais de la fibre étant donné leur isolement géographique.

Aujourd'hui, la 4G (et bientôt la 5G) est une technologie alternative qui permet de connecter au très haut débit les entreprises. Bien que les opérateurs fassent de gros efforts et accélèrent le déploiement des antennes relais 4G, il me semble illusoire de penser que les entreprises pourront bénéficier de débits atteignant au moins 30Mb/s sur l'ensemble du territoire d'ici 2022.

Pour obtenir une utilisation optimale de la 4G, il faudra assurer un déploiement de qualité et éviter tous les facteurs qui pourraient dégrader la qualité du réseau (saturation par un nombre de connexions élevées, relief naturel ...)

Ainsi, il faut garder à l'esprit que la connexion internet est devenue critique à la gestion de l'activité de la plupart des entreprises avec l'explosion des applications Cloud, l'échange de pièces jointes de plus en plus volumineuses, les interactions en visioconférence, etc.

Les entreprises ne peuvent pas attendre 2022 pour espérer peut-être avoir une connexion internet digne de ce nom et rester compétitives.

Un mot sur votre offre qui devient donc une réponse à la fracture numérique et ses points clés ?

Nos solutions permettent d'obtenir le meilleur de la 4G, afin d'offrir aux entreprises une connexion performante, fiable et stable.

Nous accompagnons nos clients dans la sélection des réseaux opérateurs les plus performants en fonction de l'adresse d'utilisation de la solution. En effet, la couverture 4G offerte par les opérateurs est très inégale en fonction d'une adresse ou d'un site donné. Nous sélectionnons donc les réseaux 4G les plus performants en fonction du lieu d'utilisation de nos équipements, afin de leur garantir un réseau d'au moins 20 ou 30 M/sec, ce que nous sommes parvenus à faire dans 98% des cas.

Nos équipes de R&D ont conçu un routeur double opérateur, qui permet à nos clients non seulement de s'appuyer sur le réseau le plus performant en fonction de l'endroit où ils se trouvent et de leurs besoins, mais également de bénéficier d'un réseau de back-up en cas de défaillance momentanée ou prolongée du réseau principal. Ce que ne peuvent pas fournir les routeurs 4G traditionnels.

Grâce à la mise à disposition d'une antenne externe déportée, nous pouvons également améliorer très sensiblement la qualité de la connexion 4G. Dans les cas les plus sensibles l'antenne externe peut même être fixée à l'extérieur du bâtiment afin de bénéficier de la meilleure connectivité possible.

Enfin, nous fournissons une IP Fixe qui permet par exemple de pouvoir connecter notre équipement à un firewall afin de pouvoir monter un tunnel VPN pour bénéficier d'une connexion sécurisée ou encore d'interagir à distance avec des équipements tels que des caméras, TPE, etc.

Comment assurer les enjeux de continuité de services et de haute disponibilité pour l'entreprise ?

Notre routeur double opérateur permet d'offrir un back-up automatique intégré en cas de perte de signal de l'opérateur principal. Les entreprises ont la garantie de bénéficier d'une continuité de services optimale. Le taux de disponibilité de nos équipements est en moyenne de 99,9%.

En plus des fonctionnalités décrites jusque-là, notre offre bénéficie de services managés : la connexion est supervisée en temps réel et nos clients disposent d'un accès à une hotline capable d'intervenir immédiatement sur du support de niveau 3. Nous pouvons réaliser à distance toutes les opérations de configuration nécessaire.

> Par Sabine Terrey

Décryptage de la cybersécurité des annuaires

Les récents événements survenus chez certaines entreprises françaises nous rappellent la nécessité pour l'ensemble des organisations de mettre en œuvre un plan de Cybersécurité particulier pour les annuaires.

En effet, que ce soit pour des attaques persistantes (APT) ou pour des infections via des ransomware/ cryptovirus les faiblesses de la configuration actuelle des annuaires offrent aux attaquants un terrain de jeu fantastique afin de mettre à mal les systèmes informatiques de nombreuses organisations.

Au travers de cet article, nous allons donc réviser les éléments nécessaires à mettre en œuvre pour implémenter un minimum de sécurité en fonction de l'annuaire utilisé.

Les différents types d'annuaires

Nous n'allons pas ici revoir ce qu'est un annuaire ou l'utilité de celui-ci, nous considérons que nos lecteurs avertis possèdent déjà la connaissance minimale pour appréhender ces concepts. Il reste néanmoins à analyser les différents types d'annuaire utilisables par les organisations – en effet depuis quelques années, notamment via l'arrivée des technologies Cloud, les concepts d'annuaire ont évolué vers de nouveaux paradigmes avec des particularités techniques et fonctionnelles.

Les annuaires locaux

Nous parlons ici de l'informatique « classique », sur les réseaux privés des organisations. Nous trouverons classiquement deux types d'annuaire : l'annuaire Active Directory et l'annuaire LDAP.

- L'annuaire Active Directory

L'annuaire de Microsoft est vraisemblablement l'annuaire de le plus utilisé dans le monde, il est précisément ce que l'on nomme un Service d'Annuaire. Concurrent un temps de Novell Directory Services (NDS), il a gagné depuis longtemps le combat et s'est déployé dans de nombreuses organisations. En effet, depuis l'année 2000, quelle que soit la taille de l'organisation, son utilisation est quasi systématique afin de gérer les différents éléments informatiques (utilisateurs, groupes, stations de travail, serveurs, imprimantes, stratégie de mot de passe, etc.) nécessaires à la production dans les entreprises.

Pourtant sa criticité n'est pas toujours claire dans l'esprit des managers. En effet, il est invisible à la plupart des utilisateurs, son usage n'est pas toujours appréhendé par certains responsables IT - bref, il fait le travail dans l'ombre, sans broncher et sans attirer la lumière.

Une étude réalisée en 2015 par ITSM Daily démontre que seulement 58% des managers IT interrogés considèrent Active Directory comme un élément critique de leur patrimoine informatique, cela en dit long sur la méconnaissance de l'importance vitale d'Active Directory au sein des organisations de toutes tailles.

- Les annuaires LDAP

Nous rangerons dans cette catégorie une grande diversité d'annuaires. En effet, nous appelons communément « annuaire LDAP » un annuaire qui est compatible avec le protocole d'interrogation LDAP (Lightweight Directory Access Protocol). En effet, à l'origine LDAP est uniquement un protocole d'interrogation, il a ensuite évolué vers un modèle de données, essayant de définir un standard sur la nature des objets créés et stockés dans ces annuaires. Nous pouvons donc maintenant déclarer qu'un « annuaire LDAP » est défini à la fois par un protocole standardisé d'interrogation mais aussi par la façon dont les objets sont créés, stockés ou répliqués.

Néanmoins attention, il existe une grande diversité d'implémentations ou de fonctionnalités selon les fournisseurs : OpenLDAP, IBM, redhat, Oracle, etc. Il faut donc garder à l'esprit que chaque annuaire peut posséder ses propres spécificités. Les annuaires LDAP sont très souvent utilisés dans les organisations pour gérer les profils utilisateurs (profiling) et les groupes d'accès pour les applications internes, en effet, la souplesse de LDAP se prête particulièrement bien aux spécificités et aux besoins applicatifs variés.

Les annuaires cloud

Nous évoquons ici la nouvelle catégorie d'annuaires qui est apparue avec la progression régulière de l'usage des services Cloud dans la plupart des organisations.

- Les annuaires DIRaaS (DIRectory as a Service)

L'idée des annuaires DIRaaS est de proposer à terme l'ensemble des fonctions et des usages proposés actuellement par un Service d'Annuaire, mais dans le Cloud public. Une façon simple de le définir serait d'imaginer un service SaaS permettant de remplacer Active Directory et l'ensemble de services fournis. Bien sûr cela n'est pas simple, et il y a encore de nombreux manques fonctionnels, néanmoins trois solutions majeures se détachent sur ce marché :

> *Microsoft Azure Active Directory*

Attention, Azure Active Directory n'est pas techniquement un annuaire Active Directory dans le Cloud, l'homonymie porte effectivement vers une grande confusion dans l'esprit de nombreuses personnes.

De plus, il est important de ne pas confondre les différents niveaux fonctionnels de cette solution. Globalement, Azure Active Directory propose deux types de services : un service de DIRaaS qui est donc un annuaire en mode SaaS et un service de Identity as a Service (IDaaS) qui est plutôt un service de SSO et de fédération en mode SaaS. Attention, il s'agit ici d'une simplification drastique de ce qu'est Azure Active Directory, mais il est primordial ici de distinguer les fonctions s'apparentant à un annuaire (ce que nous allons couvrir ensemble) des fonctions s'apparentant à un service de SSO.

> *OneLogin Unified Directory*

Acteur américain du Cloud, OneLogin propose lui aussi deux niveaux fonctionnels, un niveau DIRaaS et un niveau IDaaS. Comme pour Microsoft, nous n'évoquerons ici que les éléments fonctionnels liés à la partie annuaire. Il existe deux différences majeures avec l'environnement fonctionnel de Microsoft : la volonté de porter des fonctions classiques d'annuaires locaux directement vers le Cloud, comme par exemple l'intégration d'une fonction Radius as a Service et, l'implémentation de fonctionnalités avancées de synchronisation d'annuaires directement accessibles en mode SaaS. Ces fonctionnalités de synchronisation ne seront pas étudiées ici, car il s'agit de fonctions apparentées à ce que proposent les outils IAM du marché, ce qui est en dehors du spectre de notre article.

> *JumpCloud Directory Services*

JumpCloud a un positionnement particulier sur le marché. En effet, il ne fournit que des services de DIRaaS ! Cet acteur ne tente pas de se positionner activement sur les fonctions de SSO mais il réalise un focus sur le fait de fournir une solution SaaS permettant globalement de remplacer Active Directory : Annuaire d'entreprise, gestion des authentifications utilisateur, gestion des stations de travail et des serveurs, service RADIUS, service LDAP, stratégie de mot de passe, remplacement des GPOs, gestion des clés SSH, etc. Il est intéressant de noter que JumpCloud intègre également des fonctionnalités dédiées aux DevOps et se définit comme un « pure player » DIRaaS.

- Les annuaires V-LDAP (Virtual LDAP)

La notion d'annuaire LDAP virtuel n'est pas récente, mais l'idée est ici de migrer vers un service SaaS les fonctions portées actuellement par un annuaire LDAP local en remplacement de celui-ci.

> OneLogin Virtual LDAP Service

Implémentation d'un annuaire LDAP en mode SaaS.

> JumpCloud LDAP-as-a-Service

Implémentation d'un annuaire LDAP en mode SaaS.

Sécuriser les différents types d'annuaires

Nous allons donc maintenant parcourir les différents moyens de sécuriser les différents types d'annuaire, en fonction de leur nature intrinsèque et de leurs particularités.

Sécuriser Active Directory

Comme vu précédemment, la sécurisation d'Active Directory est très souvent la pierre angulaire de tout processus de Cybersécurité consciencieux. En effet, l'importance d'Active Directory dans les organisations est telle que toute coupure de service amènerait inévitablement à un arrêt de production massif au sein de la DSI et des métiers.

Il existe deux documents extrêmement utiles pour comprendre et implémenter de façon organisée la Cybersécurité de l'annuaire Active Directory :

- ANSSI, document en Français – « Recommandations de sécurité relatives à Active Directory » : **https://bit.ly/2Kjpu8u**
- Microsoft, document en Anglais – « Securing privileged Access Reference Material - Active Directory administrative tier model » : **https://bit.ly/2J6mLC7**

Le document de l'ANSSI fournit aux organisations françaises un excellent point de départ à la sécurisation Active Directory. Il décrit de façon précise les fonctions critiques à paramétrer au sein d'Active Directory tant sur la partie design que sur la partie objets. C'est à la fois un recueil de bonnes pratiques et des pistes concrètes pour les organisations souhaitant vérifier leur niveau de sécurité vis-à-vis d'Active Directory.

A titre d'exemple, on retrouvera dans ce document des éléments techniques extrêmement précis comme la liste des évènements Active Directory à surveiller dans une infrastructure classique : voir figures 1 et 2.

21ST EDITION ★ **09/12 APRIL** 2019 MARRIOTT PARIS RIVE GAUCHE

The **place to be** for a preview of the **Next Big Thing in Telecom**

+40 Exhibitors

+150 Speakers

+1500 Participants

MPLS+SDN+NFVWORLD ★ PARIS 2019

CISCO HUAWEI JUNIPER NETWORKS NOKIA

ciena COMARCH Netcracker RAD silverpeak VERSA NETWORKS ZTE ADVA ARISTA DELTA

infinera Mellanox metaswitch Quali NETWORKMINING Spirent Telco Systems velocloud ipinfusion

BISDN Calnex ECI ERICSSON INTRACOM MEINBERG Microsemi SEIKO Lanner tail-f osiHardware

aethra ARRCUS EKINOPS exaware inmanta ixia NETCOPE netrounds NoviFlow

More info: www.uppersideconferences.com



	ID	Fournisseur	Description
Haute	4610 (514)	Security-Auditing	Un package d'authentification a été chargé par l'autorité de sécurité locale
	4614 (518)	Security-Auditing	Un package de notification a été chargé par le gestionnaire de comptes de sécurité
	4618 (522)	Security-Auditing	Un évènement de sécurité surveillé est survenu
	4649 (552)	Security-Auditing	Une attaque par rejeu a été détectée
	4719 (612)	Security-Auditing	Une stratégie d'audit a été modifiée
	4765 (669)	Security-Auditing	Un SID History (historique d'identifiants uniques) a été ajouté à un compte
	4766 (670)	Security-Auditing	Une tentative d'ajout d'un SID History a échoué
	4794 (698)	Security-Auditing	Une tentative d'activation du mode de restauration AD a échoué
	4964 (868)	Security-Auditing	Un compte membre d'un groupe surveillé s'est authentifié
	1102 (517)	Eventlog	Le journal d'audit a été effacé

Fig 1. Extrait du document ANSSI « Recommandations de sécurité relatives à Active Directory »

R16 - Priorité 4

De manière générale, afin d'éviter un risque de rebond entre les forêts, le filtrage des SIDs doit toujours être activé sur une relation d'approbation liant deux forêts. Lors des opérations de migration, cette fonctionnalité peut être désactivée temporairement.

Fig 2. Extrait du document ANSSI « Recommandations de sécurité relatives à Active Directory »

Mais aussi, des recommandations de type « hygiène » : voir figure 2

Le document de Microsoft va lui réaliser un focus sur une méthodologie de design Active Directory nommée « Tier-model ». Pour faire simple, il est possible de découper les éléments informatiques « reliés » à l'Active Directory selon trois catégories :

- **Tier 0** : Les contrôleurs de domaine Active Directory ainsi que les machines nécessitant un compte de service avec des droits « Domain admins »
- **Tier 1** : Les serveurs membres (serveurs de fichiers, serveurs applicatifs, certains serveurs d'infrastructure, etc.)
- **Tier 2** : Les stations de travail. Certains designs incluent également dans Tier 2 tous les serveurs nécessitant une authentification interactive d'un compte utilisateur standard comme les serveurs Citrix ou RDS par exemple. Voir figure 3.

Le principe fondateur du design en Tier-Model est de séparer les zones d'administration.

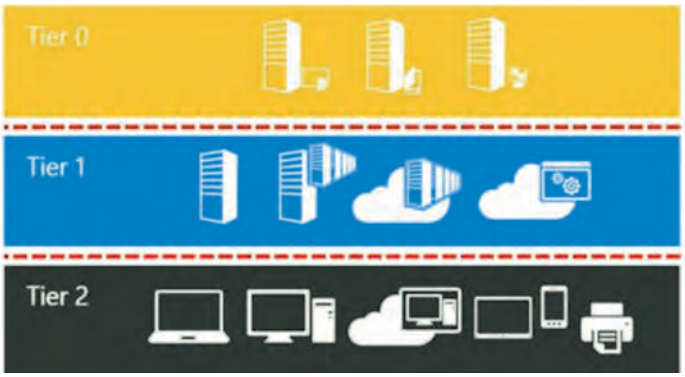


Fig 3. Découpage du Tier-model. Extrait du document Microsoft « Securing privileged Access Reference Material - Active Directory administrative tier model »

Le principe fondateur du design en Tier-Model est de séparer les zones d'administration. Par exemple, un compte d'administration appartenant au groupe « Domain Admins » n'aura pas le privilège de réaliser une authentification interactive sur une machine appartenant à Tier 2. Pourquoi ? Imaginons qu'un compte appartenant au groupe « Domain Admins » puisse s'authentifier sur une station de travail, cela signifie qu'une trace (mot de passe en mémoire, cache du hash du mot de passe administrateur,

etc.) sera alors présente sur la station de travail, si cette station de travail est par la suite infectée par un Malware, celui-ci pourra ainsi s'exécuter dans un contexte « Administrateur du domaine »... Imaginez, un crypto virus ayant accès à absolument n'importe quoi dans votre entreprise : les serveurs de fichiers, la base de données Active Directory, etc... oui, cela peut faire très mal. Voir figure 4.

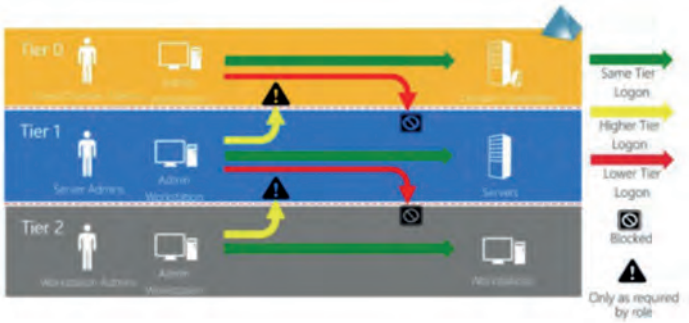


Fig 4. Restriction de l'ouverture de session entre les Tiers. Extrait du document Microsoft « Securing privileged Access Reference Material - Active Directory administrative tier model »

L'idée est donc de paramétrer ces différentes zones afin qu'elles soient isolées d'un point de vue privilèges. Le compte administrateur d'une zone ne pouvant pas interagir avec les autres zones. Les administrateurs de chaque Tier ne pouvant administrer que les machines appartenant à ce même Tier. Voir figure 5.

Comment savoir si mon Active Directory est sécurisé et non sensible aux attaques ?

C'est une question importante, et malheureusement le chemin vers la réponse peut s'avérer très complexe.

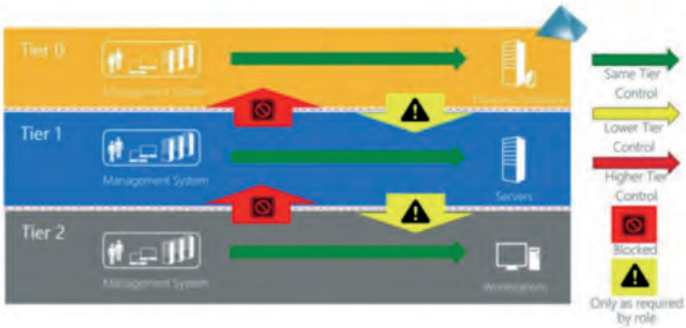


Fig 5. Restriction du contrôle de chaque Tier. Extrait du document Microsoft « Securing privileged Access Reference Material - Active Directory administrative tier model »

Une partie de la réponse provient forcement de la « vieillesse » de votre Active Directory. Il est certain que la plupart des designs Active Directory antérieurs à 2014 ne prennent pas en compte ces nouveaux éléments de paramétrage essentiels liés à la protection contre les malwares de différentes natures. Si votre déploiement est antérieur à cette date et que vous n'avez rien modifié depuis concernant les aspects gouvernance des services et des données Active Directory, il y a potentiellement danger. Un audit s'impose.

La sécurisation d'un annuaire LDAP sur site ou d'un service V-LDAP en mode SaaS diffère très peu.

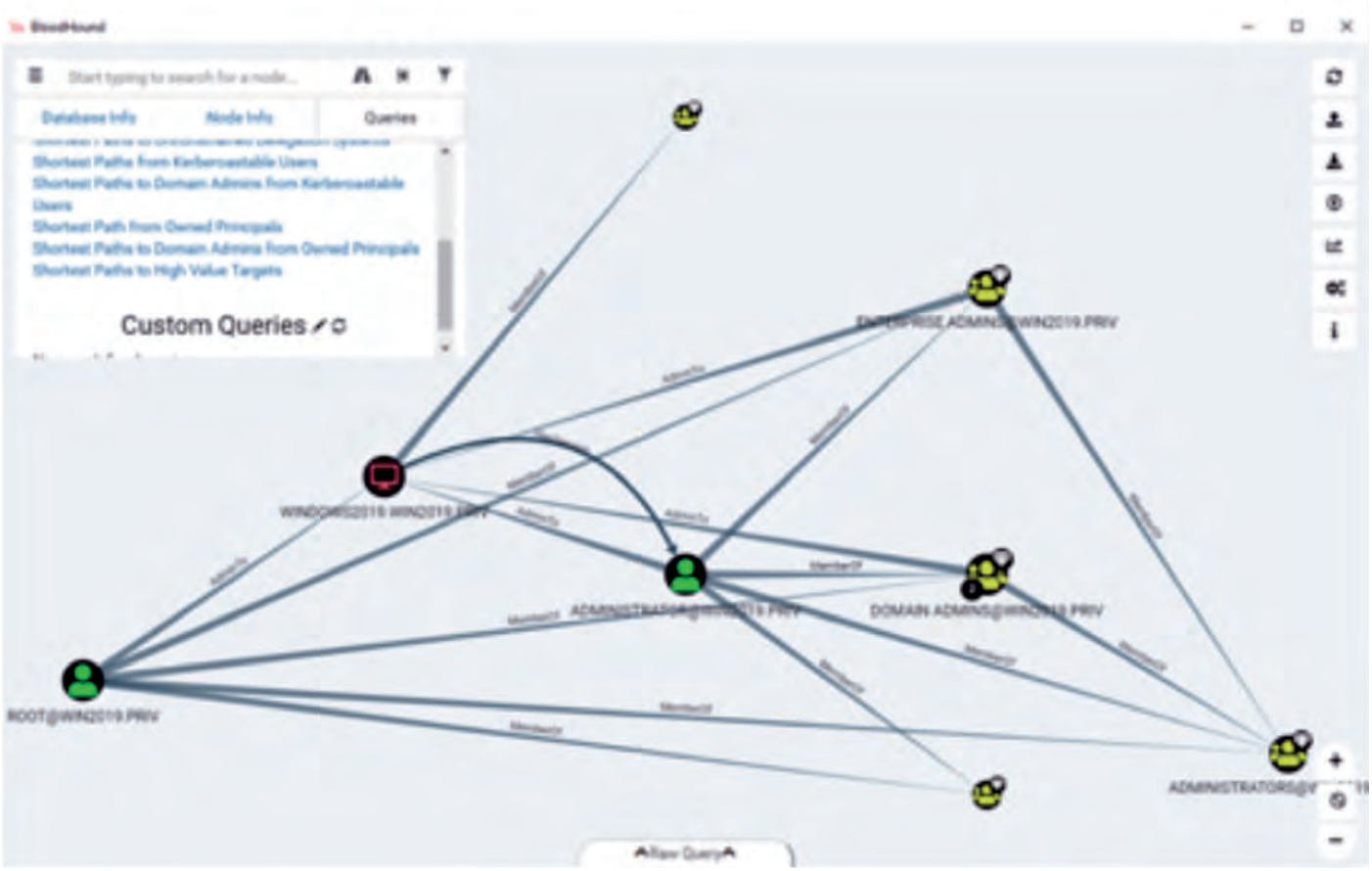


Fig 6. Interface de BloodHound évaluant les chemins d'attaque via Active Directory entre une source et une cible

Pour compléter l'approche, je vous conseille principalement l'usage de deux outils : BloodHound (outil gratuit) permettant notamment d'évaluer les chemins d'attaque ainsi que Alsid (outil commercial) permettant aux entreprises d'évaluer leur risque et d'obtenir la liste des modifications à réaliser dans Active Directory pour ne plus être en situation d'un arrêt de service potentiel – A noter, Alsid a reçu le prix de l'innovation aux Assises de la Sécurité 2017, ce qui n'est pas rien pour une jeune pousse Française !

Pour finir, PingCastle (outil avec un version gratuite et une version commerciale) peut s'avérer un excellent couteau suisse pour analyser les fragilités de son environnement Active Directory. Voir figure 6.

Sécuriser LDAP et V-LDAP

La sécurisation d'un annuaire LDAP sur site ou d'un service V-LDAP en mode SaaS diffère très peu, les bonnes pratiques inhérentes aux annuaire LDAP « classiques » sont généralement applicables aux annuaires LDAP en mode Cloud.

Voici les éléments importants à mettre en œuvre ou à vérifier :

- *Un annuaire LDAP supporte généralement deux méthodes d'authentification* : l'authentification « simple Bind » et l'authentification « SASL ». Dans le cas de l'authentification « simple BIND », il convient d'activer TLS pour obtenir un chiffrement sur le réseau lors de l'authentification et de la transmission du mot de passe (si l'annuaire LDAP sert à authentifier des utilisateurs avec un couple login/password). L'usage de SASL augmente naturellement le niveau de sécurité, car il implique l'usage de TLS, mais il faudra aussi générer et distribuer des certificats X.509 utilisés lors de la phase d'authentification.
- *Stockage des mots de passe dans un format non-réversible* : si cette option est celle par défaut dans les annuaires V-LDAP en mode SaaS, il faut s'assurer qu'il s'agit bien du paramétrage par défaut dans son environnement LDAP local. D'une manière plus large, il convient de vérifier la politique de mots de passe et les algorithmes de chiffrement utilisés lors du hash du mot de passe utilisateur.
- *Vérification des listes de contrôle d'accès* : c'est un sujet très large, mais il faut absolument vérifier à quels attributs les utilisateurs ont accès en lecture et en écriture. Malheureusement beaucoup d'organisations se contentent de l'installation et du paramétrage par défaut, or il s'agit généralement de configurations trop « ouvertes ».

De la même façon, il faut vérifier les accès attachés aux utilisateurs en mode « anonymous » et s'assurer d'un minimum de visibilité des objets et attributs dans cette situation.

La sécurisation des annuaires DIRaaS suit les règles de sécurité élémentaires inhérentes à l'usage de l'ensemble des services cloud.

Sécuriser DIRaaS

La sécurisation des annuaires DIRaaS suit les règles de sécurité élémentaires inhérentes à l'usage de l'ensemble des services cloud. Voici les éléments importants à mettre en œuvre ou à vérifier :

- *Activation de l'authentification à plusieurs facteurs (MFA)* : Activer le MFA pour les utilisateurs du service, que ce soit via une application intégrée au service DIRaaS ou via des moyens plus traditionnels tels que le SMS ou des tokens physiques. A ce propos l'ensemble des fournisseurs de DIRaaS semblent se convertir à l'usage de FIDO 2 en tant que protocole d'authentification préféré. Microsoft est très actif sur ce sujet, suivi de très près par OneLogin.
- *Usage des fonctionnalités de RBAC en liaison avec des attributs de l'annuaire* : les annuaires DIRaaS permettent la création de rôles afin de gérer le contrôle d'accès aux ressources ainsi qu'au service lui-même. Ceci permet de définir de manière extrêmement fine ce qu'un utilisateur donné a le droit de réaliser ou non dans l'annuaire DIRaaS. Sur ce point, l'expérience trop complexe des annuaires locaux (Active Directory ou LDAP) a permis d'améliorer considérablement la façon dont les fournisseurs ont modélisé les systèmes de contrôles d'accès. Il est notamment extrêmement facile d'associer des rôles à des attributs utilisateur, il suffira alors de créer un utilisateur avec des valeurs spécifiques dans certains attributs pour lui associer des rôles même complexes.
- *Vérifier la sécurité et la cohérence des annuaires sources* : le modèle de provisionnement des utilisateurs dans un annuaire DIRaaS peut être associé à deux réalités techniques : (1) provisionnement depuis une base RH, on se retrouve alors dans un contexte « classique » IAM ou (2) un provisionnement depuis un annuaire technique tel que Active Directory. Dans le premier cas, la qualité des données est sous responsabilité du personnel RH et l'on peut considérer que les informations sont bien formatées et à jour. Dans le deuxième cas, le risque est de synchroniser dans l'annuaire cloud des informations qui sont non-complètes ou non-conformes car étant la représentation d'un héritage de l'informatique locale. Ce point est extrêmement important, il ne faut pas synchroniser d'informations depuis son annuaire Active Directory vers un annuaire DIRaaS si la qualité des données n'est pas au rendez-vous, un projet de migration vers DIRaaS commence très souvent par un projet d'hygiène Active Directory ou LDAP !
- *Utiliser les outils d'authentification adaptive et d'intelligence artificielle pour encore améliorer l'expérience et la sécurité des utilisateurs* : la plupart des fournisseurs de DIRaaS sont en mesure de proposer des scénarios adaptifs à l'environnement ou au comportement de l'utilisateur pour proposer un scénario d'authentification en corrélation avec le contexte de sécurité de celui-ci. Nous rêvions de tels scénarios pour les annuaires locaux, nous pouvons en profiter dans le monde du Cloud ! Par exemple, il est ici possible de ne demander une authentification forte (MFA) que si on constate un comportement « inapproprié » de l'utilisateur, cela permet d'ajuster au mieux le niveau de sécurité en fonction des actions, de la zone géographique, des rôles d'administration de l'utilisateur, de la qualité de son périphérique, etc.

La sécurité en général consiste à ce qu'il est raisonnable de faire ou pas, en ayant une approche pragmatique des solutions techniques.

Au travers de cet article, nous avons réalisé ensemble un rapide parcours sur les chemins de la Cybersécurité associée aux annuaires, il ne s'agit ici que d'une introduction. Gardez à l'esprit que la sécurité en général consiste à ce qu'il est raisonnable de faire ou pas, en ayant une approche pragmatique des solutions techniques en fonction de son contexte. Néanmoins, la sécurité des annuaires est une spécialité bien à part dans le monde de la Cybersécurité, choisissez donc soigneusement les professionnels que vous faites intervenir sur ces sujets.

N'hésitez pas à suivre mon blog ou me contacter si ces sujets vous intéressent, l'échange et le partage de la connaissance sont la base de nombreux succès !

> Par Sylvain Cortes

Architecte Expert IAM & CyberSecurity
@sylvaincortes
sylvaincortes@hotmail.com
Blog:www.identitycosmos.com
MicrosoftMVP(Identity & Access)
Enseignant à l'ESGI - Enseignant à l'Université de Grenoble - Enseignant au CNAM

Teams : UN BON CANDIDAT DIGITAL WORKPLACE AMÉLIORANT LES PERFORMANCES DE L'ENTREPRISE

« Plus de trois quarts des entreprises pensent que l'évolution de leur stratégie Digital Workplace, de leur processus et des technologies sont très importantes pour leur performance globale. »
(The Workplace Evolution » Harvard Business Review Analytic Services)

Dans un contexte de transformation numérique, le « Digital Workplace » (l'espace de travail numérique) est l'évolution des modes de travail vers plus d'agilité, de mobilité, de simplicité et de productivité grâce aux nouvelles technologies en entreprise.

Intérêts du Digital Workplace

Avez-vous des employés qui se plaignent de recevoir trop d'email, de faire trop de réunions ? Ces symptômes traduisent peut-être le besoin d'outils numériques du Digital Workplace.

Le Digital Workplace est généralement incarné par l'intranet de l'entreprise ou par une suite d'outils collaboratifs ou communicatifs.

Quelle est la différence entre un Intranet et un Digital Workplace ?

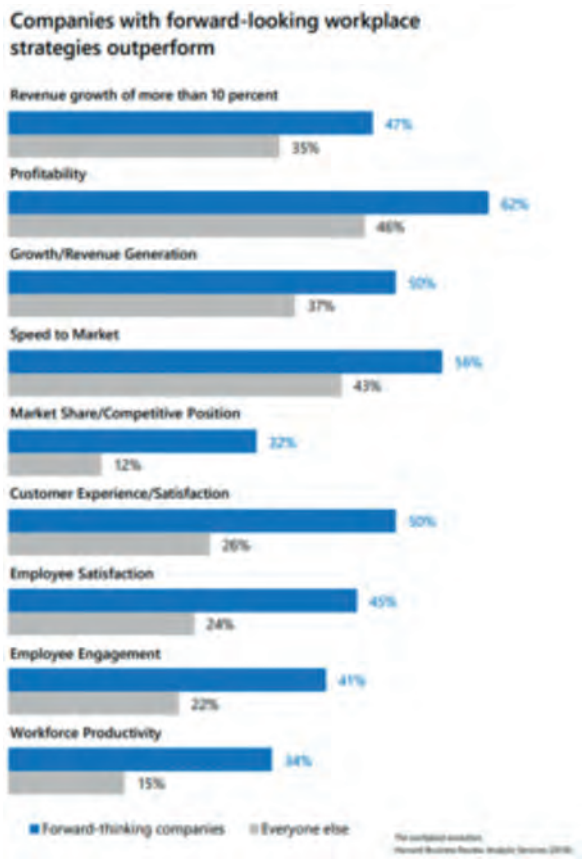
Les critères d'un Digital Workplace par rapport à un site intranet sont :

1. **Simple d'utilisation et utile** : l'interface doit être simple d'accès pour un utilisateur mature numériquement ou non. La présence d'applications métiers intégrées dans le système facilitant ainsi l'adoption
2. **Mobile** : accéder à l'information, collaborer en situation de télétravail
3. **Social** : connecter les utilisateurs entre eux afin de faciliter les échanges horizontaux et le partage de l'information. La partie sociale est généralement couverte par des outils tels que les Réseaux Sociaux d'entreprises : Workplace par Facebook, Yammer par Microsoft. Cependant nous verrons que ces outils requièrent une conduite du changement importante
4. **Ouvert** : laisser libre court à l'innovation, aux idées
5. **Intelligent** : une expérience personnalisée pour l'utilisateur (exemple : les ressources humaines voient des articles différents du département finance)

Les entreprises ayant une stratégie de « Modern Workplace » (environnement de travail numérique moderne) en tirent les bénéfices suivants : leurs bénéfices augmentent plus, elles sont plus réactives à leur marché, les employés sont plus engagés, satisfaits et productifs :

Le Digital Workplace est généralement incarné par l'intranet de l'entreprise ou par une suite d'outils collaboratif.

Figure 1 – Les entreprises en avance sur les stratégies modern Workplace surpassent les autres



Le Digital Workplace facilité avec Teams

« Microsoft Teams est une application qui permet de créer, partager et collaborer en équipe à partir d'un ordinateur, d'une tablette ou d'un téléphone portable. Sur une plateforme commune, et personnalisable, il est ainsi possible de combiner des discussions en groupe, des réunions en visioconférence, des notes et des pièces jointes » (Wikipédia)

Tracy van de Schyff parle d'outil catalyseur dans cet article https://www.valointranet.com/blog/general/why-microsoft-teams-is-the-ultimate-user-adoption-catalyst/, car sans le savoir, l'utilisateur utilise une panoplie d'outils auparavant compliqués à appréhender tels que Microsoft SharePoint (le couteau suisse Intranet et de gestion électronique de documents).

Gartner annonce l'outil comme celui devenant aussi commun qu'Outlook pour l'email.

Comment fonctionne Teams ?

Chaque équipe Teams est un groupe de personnes avec un but commun dans lequel l'utilisateur peut :

1. Discuter avec un ou plusieurs collègues (via le mode conversation comme dans Skype) ou autour de sujets communs dans des canaux de conversations (channel)
2. Collaborer sur des documents depuis son mobile ou ordinateur
3. Réaliser des web conférences, partager son écran, appeler en voip, faire des conférences enregistrées pour les employés

Une adoption à deux vitesses

Dans le domaine privé ou des startups, les employés utilisent plus naturellement des outils orientés autour de la conversation, des documents et de la collaboration synchrone (l'email étant asynchrone).

Ces outils plébiscités des générations « Millénial » (génération 1978-1994) et surtout des startups sont arrivés petit à petit dans les grandes entreprises via par exemple l'outil **SLACK** (2013) ou plus intensément depuis la sortie de **Microsoft Teams** (2017). Microsoft a annoncé une transition en 3 ans (en 2017) pour le remplacement de **Skype for Business**. Le challenge pour les employés des grandes entreprises est de s'habituer aux nouveaux concepts de canaux etc.

Les employés utilisent plus naturellement des outils orientés autour de la conversation, des documents et de la collaboration synchrone.

Plus qu'un outil, un projet d'entreprise

Bien que l'outil ne requiert pas de compétences informatiques avancées pour l'installer, il faut voir un déploiement de Microsoft Teams (et comme tout outil de la suite Microsoft 365) comme un projet à part entière afin de cadrer les objectifs d'utilisation, l'architecture de l'information, les règles d'organisation (gouvernance) et la conduite du changement.

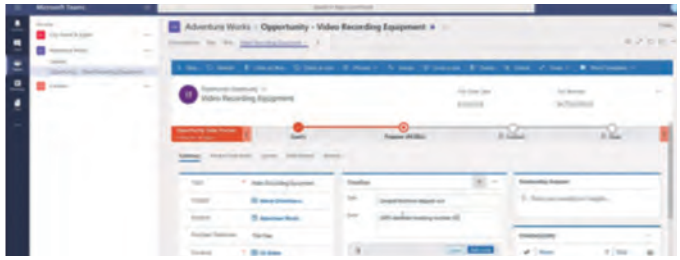
Beaucoup de déploiements Office 365 (suite de service, dont Teams) sont sous utilisés ou deviennent une usine à espace de collaborations fantômes.

Des applications métiers pour l'adoption

L'outil dispose de connecteurs vers une multitude de plateformes existantes :

Onglets pour Teams

Ces intégrations permettent à ce Digital Workplace de réduire le besoin de changer d'applications qui fait perdre en concentration et productivité.



Intégration d'un CRM dans Teams

Afin d'augmenter l'adoption de l'outil, embarquer des applications métiers dans l'outil est un atout : Application de notes de frais, gestion de planning, allocation de ressources, les possibilités sont infinies car la plateforme permet aux développeurs de déployer des applications dans l'intranet SharePoint et au sein de l'outil Microsoft Teams.

Ne pas négliger la sécurité des données

Microsoft Teams, comme beaucoup d'applications, a des données stockées partout dans le monde. Les données sont dans des Cloud privé et Cloud public managé, SaaS, applications héritées, bases de données, systèmes et processus.

Fait intéressant, 69% des entreprises estiment que la protection, la confidentialité et la conformité

des données relèvent de la responsabilité du fournisseur de services Cloud. En réalité, la plupart des contrats de fournisseur de services de Cloud disent le contraire. En conséquence, l'entreprise est responsable de ses propres données !

La criticité des données dans Teams est au niveau des documents partagés. Ceux-ci sont stockés dans l'outil Microsoft SharePoint qui peut être sauvegardé par des solutions de sauvegarde moderne telles que Veeam Backup for Microsoft Office 365.

La sauvegarde des données est nécessaire car bien qu'Office365, la suite hébergeant Microsoft Teams, est un service Cloud, la responsabilité de Microsoft

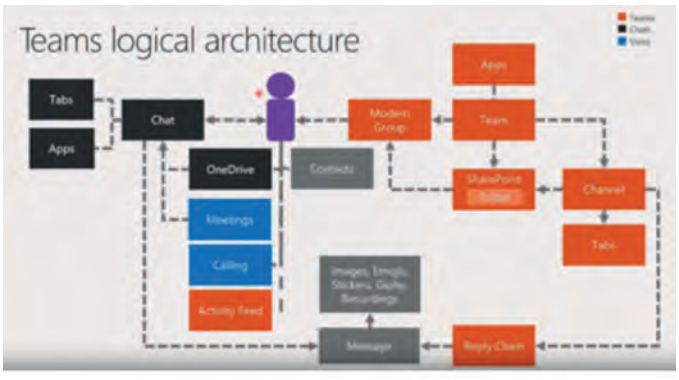
Russ Kerscher - https://collab365.community/office-365-shared-responsibility-model/

s'arrête à la gestion de l'infrastructure. En cas de virus, erreur de manipulation etc. le client garde la responsabilité de ses données.

Les spécialistes sont régulièrement confrontés à cette question : Comment restaurer des données stockées dans Microsoft Teams ? Premièrement, le mot « stocké » n'est pas le terme à associer à l'outil. Microsoft Teams stocke différents types de données au sein de différents types de services ou d'applications.

Microsoft a indiqué que la solution Teams fonctionnera comme un « hub » de travail, dans lequel tous les services et les données sont réunis. Concernant la partie VoIP (voix sur IP), cette dernière sera intégrée dans Teams. Le travail de collaboration via Teams repose sur des données partagées ou créées. En conséquence, il est primordial de protéger ces données.

Architecture logique de Microsoft Teams :



Localisation des données digérées au travers de Teams :

Pour le moment, aucune API ne permet de sauvegarder les métadonnées (onglets, connecteurs installés, conversations etc.) de Microsoft Teams. Le seul moyen de restaurer des données à partir de Microsoft Teams consiste à les restaurer vers n'importe quel emplacement puis à les restituer dans le Digital Workspace.

L'importance des données a pris de l'ampleur dans tous les aspects de nos vies numériques. Le besoin de solutions et services capables de garantir leur disponibilité puis de les « hygiéniser » a également augmenté. Dans cette nouvelle réalité où les données sont dispersées, garantir leur disponibilité devient à la fois beaucoup plus critique et difficile. Les DSI rencontrent des difficultés notamment pour localiser et gouverner l'ensemble de leurs données (structurées et non structurées). Sans un plan de sauvegarde solide, il est complexe de pouvoir récupérer les données avec certitude en cas de panne, d'attaque, de perte ou de vol. Les techniques relatives à l'analyse prédictive aident à acquérir un avantage concurrentiel et à améliorer les performances de l'entreprise.

Concernant les mises en conformité, de nouvelles réglementations telles que la GDPR entrent en vigueur impliquant chaque Nation. Aujourd'hui, il est primordial que ces données soient disponibles 24h/24 et 7j/7 pour les services et les utilisateurs. La disponibilité repose sur des mécanismes basés sur des règles dans lesquelles les données sont souvent déplacées manuellement afin d'optimiser les coûts et les performances. La disponibilité de demain doit évoluer vers un modèle plus autonome dans lequel le système réagit et s'adapte automatiquement à tout changement significatif lié au comportement des données, des applications ou des utilisateurs, où que ce soit dans l'entreprise.

Nous pensons que Microsoft Teams a les bons atouts pour répondre aux besoins d'un bon nombre d'outils du Digital Workplace. Ne pas oublier la gouvernance, formation et sécurisation de l'information dans tout projet de déploiement.

> *Jeff Angama, Consultant Technique SharePoint & Office 365 chez Monaco Digital https://about.me/jeff.angama*

> *Christopher Glémot, Team Leader Protection & Gouvernance des données chez Monaco Digital - Veeam Vanguard www.original-network.com*

FIC 2019
LA CYBERSÉCURITÉ SOUS TOUS SES ANGLES

Conférences, ateliers, Strategy challenge, Bug Bounty Live, démonstrations, prix de la start-up, prix du livre Cyber, et bien d'autres encore... Les 22 et 23 janvier, au Grand Palais à Lille, tous les ingrédients étaient réunis pour faire du FIC 2019, 11ème édition, une réussite !

Le FIC stimule l'innovation, et à cette occasion le nouvel accélérateur de CEIS Lab a été annoncé. Le FIC, c'est aussi un ensemble d'espaces où chercheurs et experts en sécurité, étudiants partagent, échangent et se retrouvent confrontés à des scénarios d'attaques en environnement réel. Retours d'expériences garantis pour lutter contre la cybercriminalité!

Le FIC rassemble ainsi différents acteurs publics et privés, et plusieurs pays sont représentés : institutions publiques, grandes entreprises et acteurs majeurs de la sécurité.

Les préoccupations des entreprises

L'effervescence sécurité « cyber » était au rendez-vous et tous les acteurs s'accordent à dire que l'événement prend de l'ampleur. Les clients finaux sont présents. Le FIC est une étape importante, et les conversations sont constructives avec un retour aux basiques : est-ce que mon inventaire est à jour, est-ce que j'ai une disponibilité à 100% de mes actifs ? à mesure que les attaques se complexifient.

Autre sujet, l'accompagnement des organisations. Thierry Casier, Senior Manager Audit & Pentest chez Harmonie Technologie commente « la sécurité dans le Cloud reste un thème essentiel, avec en ligne de mire la maturité des entreprises en terme de gouvernance et de maitrise technique. Le sujet de la sécurité autour de l'IoT gagne en vitesse et commence à inquiéter ! ».
La prise de conscience est réelle. Toutefois, Alexandre Stoica, Presales & Consulting Director chez T-Systems, ajoute « les clients veulent avoir des vues précises sur la sécurité de leurs systèmes. Les tests de vulnérabilité et de pénétration deviennent des outils clés »

Les enjeux sont forts à tous les niveaux. « Si l'analyse de risque, le RGPD, les systèmes de surveillance, détection, SOC sont de vrais sujets pour les entreprises, les problématiques autour de l'IoT industriel émergent » confirme David Leporini, Directeur des activités IoT chez Atos.

Les certifications ANSSI

Guillaume Poupard, Directeur Général de l'ANSSI a profité de l'événement pour annoncer des certifications. Orange Cyberdefense, Sogeti et Sopra Steria ont obtenu la qualification Prestataires en Détection d'Incidents de Sécurité (PDIS), et peuvent ainsi adresser les Opérateurs d'Importance Vitale (OIV), qui doivent faire appel à des prestataires conformes aux référentiels d'exigence de l'ANSSI. D'autres sociétés sont en cours de validation. Cette reconnaissance est un gage de confiance de la part des autorités

« Orange Cyberdefense est très fier d'avoir obtenu cette certification et d'être dans la première vague des lauréats. Nous œuvrons au quotidien, avec nos 1 300 experts, à rendre plus sûr l'écosystème du numérique en innovant et en s'alliant à des partenaires reconnus. Cette labellisation renforce notre conviction d'être un acteur essentiel pour protéger les OIV et notamment ceux dans le secteur de l'Industrie qui sont particulièrement stratégiques » commente Michel Van Den Berghe, Directeur Général d'Orange Cyberdefense.

Autre avancée : la qualification SecNumValid certifie la sécurisation du Cloud et Oodrive ouvre la voie.

76% des ETI ont déjà subi une attaque...

Les entreprises doivent faire face efficacement au risque cyber. 76% c'est le chiffre avancé dans une étude Bessé & PwC mars 2018, pour les ETI ayant été confrontées à une attaque en 2017. La menace cyber est comprise mais comment traduire cette prise de conscience en actes au niveau stratégique ? Moyens financiers mais aussi compétences et talents, les enjeux sont majeurs.

A mesure que la digitalisation se développe, « la vulnérabilité des infrastructure s'accroît », il faut engager des démarches et une approche sur-mesure du risque. Selon Bessé, « il faut lisser le risque financier par voie de transfert au marché de l'assurance ». Mais, au-delà de la voie assurancielle, les organisations doivent prendre le chemin de la cyber résilience.

La mixité dans la Cybersécurité !

Une rencontre au détour des allées, avec l'association CEFCYS, Le Cercle des Femmes de la Cybersécurité et notamment sa présidente, Nacira Salvan, nous prouve une fois encore la présence des femmes dans les métiers de la cybersécurité.

Cette association veut promouvoir et faire progresser la présence et le leadership des femmes dans les métiers relatifs à la sécurité des systèmes d'information (développeuses, RSSI, formatrices, CTO, analystes, consultantes, CEO, auditrices...). Les femmes travaillant dans ce domaine et celles qui aspirent à y travailler sont évidemment les bienvenues, sans oublier les hommes qui souhaitent faire progresser la présence et l'impact des femmes dans ces métiers.

Le RSSI part-time

Le « RSSI part-time » concept lancé en 2018 chez I-Tracing répond à un réel besoin. « Si l'entreprise n'a pas les moyens ou la volonté d'avoir un collaborateur plein temps en tant que RSSI, la problématique sécurité et le besoin fonctionnel (roadmap sécurité...) restent primordiaux », explique Laurent Charvériat, cofondateur et Directeur Général.

C'est pourquoi i-Tracing met à disposition la fonction et l'expertise RSSI dans un mode de fonctionnement temps partagé et une équipe peut intervenir pour différentes filiales d'un groupe. L'assistance RSSI est aussi proposée pour compléter le rôle du RSSI.

Laurent Charvériat

RISK &Me pour PME & ETI

« L'idée est de capitaliser sur notre savoir-faire dédié aux grands-comptes (gouvernance, gestion de crise, accompagnement...) dans les projets et conseils de prévention des risques cyber pour proposer cette plate-forme au marché des PME » commente Xavier de Korsak, Président Directeur Général, Harmonie Technologie.

Ce marché est d'autant plus en demande que la contrainte de mise en conformité (RGPD) est forte, « une mention légale sur un site ne signifie pas être conforme ». Le service en bêta test sera ouvert en avril, pour 6 mois, cette phase permettra aussi de tisser des partenariats.

Xavier de Korsak

Une mise à l'état de l'art !

Aujourd'hui, la majorité des projets dans le secteur public et le secteur privé, « c'est essentiellement la mise à l'état de l'art des solutions de sécurité (notamment RGPD), nous avons une approche disruptive depuis 10 ans, nous consolidons des services de sécurité sur une même plate-forme pour simplifier la vie des RSSI et des équipes de production, et apporter plus d'efficacité » souligne Raphaël Bousquet, Vice-Président EMEA South, Israël et Russie, chez Palo Alto Networks.

C'est un fait, les clients n'acceptent plus d'avoir 15 couches de solutions dans leur datacenter pour gérer la sécurité. L'évolution s'oriente vers un déploiement de solutions de sécurité virtualisées dans le Cloud privé ou public.

Raphaël Bousquet

L'évolution s'oriente vers un déploiement de solutions de sécurité virtualisées dans le Cloud privé ou public.

Une chaîne linéaire dynamique et unique

L'offre Tanium est partie d'un constat simple : les organisations publiques ou privées ont énormément investi ces vingt dernières années pour la croissance, la transformation digitale et les acquisitions.

En contrepartie, qu'en est-il de la complexification de l'organisation informatique, « la migration vers le cloud, les applications métiers, la multiplication des couches, environnements et terminaux... » soulèvent divers problèmes.

Une chaîne linéaire dynamique qui permet d'avoir une visibilité à 100% des actifs.

Afin d'éviter précisément les nombreux agents qui viennent solutionner un problème particulier, les équipes et architectures dédiées, les multiples réponses, sans référentiel unique de données, il faut s'orienter vers la simplification.

Après 5 ans de R&D, en 2012, Tanium propose « une chaîne linéaire dynamique qui permet d'avoir une visibilité à 100% des actifs, de poser des questions et avoir des réponses en temps réel, et déployer des actions à la même vitesse » explique Dagobert Levy, VP Europe du Sud, chez Tanium. Sur la plate-forme, des contenus ont été ajoutés au fur et à mesure (détection des comportements anormaux, des incidents, réponse à incidents, conformité, visibilité, inventaire, patch...) pour devenir le référentiel de données unique pour l'entreprise.

Dagobert Levy

> Par Sabine Terrey

Ethique numérique et expériences immersives en 2019

Quelles sont les tendances émergentes qui vont avoir une incidence sur les stratégies en matière de projets, d'innovation et de technologie ?

Ethique numérique, by-design, retenons les 3 pistes à suivre. En effet, il faut « un nouvel état d'esprit de la part de tous - dirigeants, employés et consommateurs »

1 - Un monde numérique plus éthique

L'IA et l'automatisation créent de nouveaux enjeux éthiques qui concernent toute l'entreprise. Pour preuve :

- 89% des dirigeants (monde) ont déjà été confrontés à un dilemme éthique : utilisation des technologies intelligentes et l'automatisation
- 87% ne sont pas préparés à répondre aux préoccupations éthiques actuelles

2 - Intelligence & design

L'association du design et de l'analyse des données permet de créer des produits et services plus personnalisés pour répondre aux attentes des clients et des employés.

Selon le CISR de la MIT Sloan School of Management, les entreprises offrant une meilleure expérience aux employés ont

- plus de résultats business
- plus d'innovation
- une rentabilité supérieure de 25%

Des responsables d'entreprises font travailler ensemble les data scientists et les créatifs pour créer des équipes multidisciplinaires.

3 – Des expériences sans limites

Le monde évolue vers une société exclusivement mobile, expérience « en mouvement », physique et virtuelle.

Créer ces expériences immersives « sans limites » nécessite un nouvel état d'esprit et un renouvellement de l'architecture informatique.

Source Etude Avanade Trendlines

Comment s'adapter
AUX NOUVELLES EXIGENCES DES ESPACES DE TRAVAIL

Une plate-forme de réunions pour les espaces de travail modernes ! Toute entreprise en rêve... BlueJeans relève le défi avec son service cloud qui connecte postes de travail, appareils mobiles et équipements vidéo des salles de réunion à une même visioconférence.

Matthieu Douvenou, Responsable grands comptes chez BlueJeans nous livre son expérience terrain et répond aux exigences des environnements de travail d'aujourd'hui.

Tous les cas d'usage de collaboration à distance

Créée en 2009, BlueJeans, société privée basée en Californie, a développé son activité en Europe dès 2014 (650 employés aujourd'hui dont une équipe dédiée d'une dizaine de personnes en France) pour répondre aux défis actuels des communications unifiées et collaboration des DSI.

Plusieurs organisations ont déjà été séduites par l'offre, au-delà des comptes américains, Linkedin, Starbucks, citons en France, Criteo, Pernod Ricard....

« La réunion à distance est notre cœur d'activité, et notre solution historique Meetings vient faire de la consolidation dans les grandes entreprises ». BlueJeans consolide ainsi les outils d'audio conférence, les sujets de web conférence et de visio conférence, le tout dans une seule plate-forme Cloud, et répond à tous les cas d'usage de collaboration en réunion à distance.

Plus seulement perçus comme de simples gestionnaires de technologies, les DSI sont désormais responsables devant les utilisateurs.

Events démocratise la communication

En complément, « notre offre, Events, autour de l'événementiel permet de réaliser des webcast vidéos à distance. Le marché de l'évènementiel est un marché en pleine transformation, d'un mode assisté et marché de niche avec des prestataires bien ciblés, nous passons à un mode où la communication est en train de se démocratiser, nous avons de plus en plus de demandes pour des solutions en self-service ».

BlueJeans se positionne au niveau de l'événementiel, « le middle manager peut faire sa communication vers son groupe » avec une solution qui s'adapte à tous les niveaux d'audience de 100 à 25 000 participants, et qui fait la liaison avec Meetings. Les DSI sont évidemment challengés sur ce type d'outils pour adresser tous les cas d'usage de la communication.

Matthieu Douvenou

Agnosticité, audio et analytique

Meetings entend se différencier de la concurrence. Aujourd'hui, deux approches émergent, celle de la consolidation (suite unique). En ce sens, BlueJeans s'est associé avec Microsoft pour une offre complémentaire et co-développée sur l'interopérabilité avec le monde de la visio conférence, « l'offre BlueJeans Gateway, 100% Cloud, hébergée dans Azure permet à un client de déployer Teams en plate-forme de collaboration et de réunions, dans une approche consolidation, tout en gardant un niveau d'interopérabilité avec ses investissements de visio conférence, gage de pérennité ».

Avec l'approche « Best of breed », la solution choisie vient s'intégrer avec l'écosystème de l'entreprise et apporte de la valeur sur l'aspect « réunions ». Les apports clés BlueJeans sur cette partie sont réels. Agnosticité et compatibilité, « c'est-à-dire notre indépendance avec l'ensemble du matériel dans l'entreprise, notre solution s'intègre avec divers outils Cisco, Polycom, Lifesize..., acteurs historiques du monde de la visio conférence ».

Autre point fort, l'audio, « dans une conférence, l'audio est primordiale, grâce à notre partenariat, la technologie Dolby Voice est intégrée dans la plate-forme BlueJeans, suppression du bruit de fond, séparation des voix, correction des niveaux sonores... ».

Enfin, l'analytique, « plus seulement perçus comme de simples gestionnaires de technologies, les DSI sont désormais responsables devant les utilisateurs. Ils ont besoin d'outils qui mesurent la satisfaction et le niveau de services apporté aux utilisateurs ». La couche analytique, intégrée dans la plate-forme, donne des indicateurs de performance sur le niveau de ressenti des réunions et évalue l'expérience.

Enfin, côté sécurité, « si les DSI sont challengés à ce sujet, nous avons la responsabilité et la maîtrise de l'ensemble de notre réseau, et sommes certifiés SOC2 ». L'ensemble des flux audio et vidéo sont chiffrés.

Smart Meeting...

Quelle valeur peut-on apporter autour des réunions ? La R&D réfléchit à l'amélioration de la productivité en réunion et notamment « à la prise de notes intelligente et la retranscription de la réunion en quelques minutes, ces axes seront des axes de différenciation pour BlueJeans dans un marché qui se consolide et nécessite de la valeur » conclut Matthieu Douvenou.

> Par Sabine Terrey

Et si nos clients
N'AVAIENT PLUS LE CHOIX ?

S'ils n'avaient plus connaissance du fournisseur de service cloud hébergeant leur Système d'Information ?

Historiquement, un client a toujours le choix et le dernier mot. S'il veut transférer le maintien en conditions opérationnelles de tout ou partie de son système d'information vers un cloud public (Azure, AWS, Google Cloud Platform, etc.) ou un cloud privé, il a toute latitude pour acter cette décision stratégique.

En tant que partenaire, nous proposons de manière plus ou moins objective les différents fournisseurs de services cloud public, comparons les fonctionnalités, les prix, le niveau de disponibilité de chacun, et nous recensons les compétences internes du client.

Nous arrivons souvent après la bataille : les commerciaux des fournisseurs de services cloud ont déjà fait pencher la balance vers tel ou tel hébergeur cloud, et le client, même s'il souhaite un avis objectif, a déjà pris sa décision, inconsciemment, bien souvent entre Amazon Web Services et Microsoft Azure. Le partenaire l'accompagne dans sa phase de migration, puis forme ses collaborateurs à cette nouvelle technologie.

Et si tout cela, c'était avant ?

Appelons ce concept Système d'Information Volatile ou SIV, en attendant un acronyme faisant l'unanimité.

Imaginez une entreprise...

Imaginez une entreprise qui n'aurait plus connaissance du fournisseur de solution cloud gérant son système d'information. La DSI transférerait en amont à un partenaire une partie de son système d'information, contenant par exemple son domaine Active Directory, son pare-feu, son antivirus, ses applications métier, ses standards de sécurité... tout cela transposé à des services cloud : machines virtuelles, WebApps, bases de données.

Le partenaire déploierait l'infra de manière... nomade et volatile. À tout moment, en fonction de critères tels que la latence ou le prix, l'infrastructure du client serait déplacée, de manière manuelle ou automatique, vers tel cloud public ou privé.

Aucune indisponibilité ne serait à déplorer car l'infrastructure cloudifiée serait dupliquée. Les frontières seraient invisibles pour l'utilisateur et l'accès au système d'information s'effectuerait de manière transparente pour le client.

Appelons ce concept Système d'Information Volatile ou SIV, en attendant un acronyme faisant l'unanimité. Le client transférerait donc la gestion de son infrastructure à un tiers, sans s'occuper de l'adéquation entre ses compétences internes et le cloud cible. Une bonne dose de confiance serait nécessaire, mais le retour sur investissement serait bien présent.

Déploiement multi-cloud

À le lire sur l'écran, cela semble attrayant et simple mais comment mettre en œuvre un tel service ? C'est ici que Terraform entre en jeu : cette solution permet de déployer des infrastructures à l'aide de fichiers de configuration (d'où l'appellation "Infrastructure as a code"). Ecrite en Go, elle fut créée en 2014 par un certain Hashimoto, fondateur de l'entreprise HashiCorp.

Désormais, un partenaire peut organiser à l'avance des déploiements d'infrastructures via un simple script, et ceci indépendamment de la plateforme cloud cible, telle qu'AWS, Azure ou un cloud privé. La simplicité des deux langages de programmation supportés, HCL (HashiCorp Configuration Language) et JSON, en fait un outil incontournable pour toute entreprise voulant proposer un service de SIV. HCL a une structuration facilement appréhendable pour tout administrateur, c'est un atout de taille. De plus, Terraform gère les versions des infrastructures déployées, afin de pouvoir revenir en arrière rapidement en cas d'erreur.

Dernier avantage de la solution, Terraform est un logiciel open source dont le code est disponible sur GitHub. Grâce à une communauté active encadrée par HashiCorp, les ajouts de fonctionnalités sont réguliers. Afin d'appréhender la solution, des exemples de déploiement par fournisseur de cloud sont disponibles depuis le lien ci-dessous :

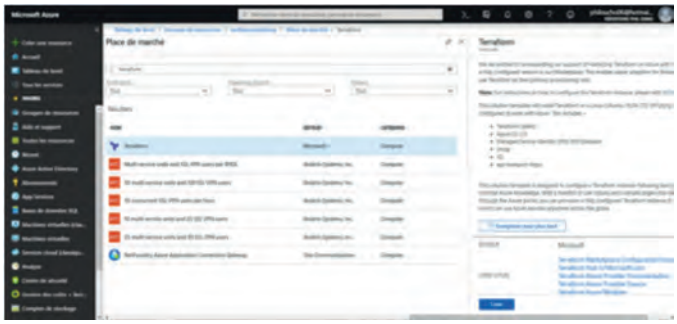
https://github.com/hashicorp/terraform/tree/master/examples

Par exemple, le code suivant initie une connexion vers un abonnement Azure et crée un groupe de ressources dans la région East US sur lequel une balise est définie :

```
provider "azurerm" {
subscription_id = ""
client_id = ""
client_secret = ""
tenant_id = ""
}
resource "azurerm_resource_
group" "myterraformgroup" {
name = "nomdugroupederessource"
location = "eastus"
tags {
environment = "Terraform Demo"
}
}
```

Terraform est disponible depuis le MarketPlace Azure, l'intégration de la solution ayant été effectuée au préalable par Microsoft.

Libre à vous de créer maintenant des ressources telles que des machines virtuelles, des WebApps, des bases de données, en quelques lignes, depuis Azure vers d'autres cloud publics ou privés !



L'IA fait son entrée

Imaginons maintenant une intelligence artificielle qui analyserait constamment le cours du dollar, qui comparerait le prix des ressources en fonction du fournisseur de services cloud, qui analyserait les SLA associés, les fonctionnalités utiles à nos clients, les changements juridiques, ainsi que le temps de réponse de leurs systèmes d'information ... Une fois le meilleur fournisseur de services cloud détecté à un instant T, l'IA basculerait les systèmes d'information, en s'appuyant sur une technologie éprouvée telle que Terraform. Des paramètres sensibles pourraient être pris en compte par l'IA dans sa décision, tels que la localisation géographique des données, critère souvent essentiel.

Ainsi, le client ne saurait plus où son système d'information est hébergé, ni comment le gérer, mais il aurait la certitude qu'il est hautement disponible, et ceci au meilleur prix. N'est-ce pas finalement ce que nos clients souhaitent ?

Qui proposera ce service innovant en premier ? Un partenaire ? Une entreprise existante ? Ou bien un nouveau venu dans l'univers de l'IT ?

La révolution du Système d'Information Volatile géré par une IA est en marche... et techniquement, tout est prêt pour qu'elle apparaisse !

La révolution du Système d'Information Volatile géré par une IA est en marche.

En tant que Cloud Solution Architect spécialisé sur Microsoft Azure, MVP (Most Valuable Professional), P-Seller (Partner Seller) et Microsoft Certified Trainer, Philippe PAIOLA travaille chez Capgemini. Il forme également des professionnels sur les technologies Microsoft (Azure, Windows Server 2012, Windows 10...) et enseigne en IUT et école d'Ingénieurs. Il possède plus d'une dizaine de certifications Microsoft. Ainsi, ses compétences techniques s'allient à son expérience pédagogique pour fournir aux lecteurs une lecture décalée du cloud public. Vous pouvez le contacter sur son courriel : philippe.paiola@gmail.com.

Les Microservices SONT-ILS L'AVENIR DES APPLICATIONS EN ENTREPRISE ?

Depuis quelques années, les microservices ont fait couler beaucoup d'encre au travers de nombreuses success story chez les grands acteurs de l'économie numérique.

Avec la montée en puissance de la containerisation dans les entreprises, on recommence à entendre parler de ce terme comme le nouveau graal, la prochaine étape de l'évolution de nos applications.

Avant de décrire plus précisément ce que sont les microservices, commençons par tordre le cou à certaines idées reçues.

"Je déploie des applications en container donc je fais du Microservice."
Non, il ne suffit pas de découper une application en différents "modules" et de les containeriser pour pouvoir parler de microservices. Au plus, on ne fait que reproduire une architecture "n tiers" avec des containers.

"Les Microservices sont des containers."
Non, si la containerisation est bien adaptée aux architectures microservices, il est tout à fait possible d'envisager d'autres "contenants" (ex : des machines virtuelles ou des web apps).

"Les Microservices sont de "petits services" web.
Oui, mais il est abusif de réduire les microservices à de "petits services" s'échangeant des requêtes REST ou SOAP, c'est bien plus que cela.

Bien qu'il n'existe pas de définition normalisée des architectures microservices, Martin Fowler, auteur reconnu et pionnier dans le domaine, les décrit comme « *Un style d'architecture qui partage des caractéristiques communes avec les aptitudes de l'entreprise* » (Organisation, Processus, Management).

En ce sens, les architectures microservices ne peuvent se résumer à une infrastructure technique ou une manière d'organiser l'exécution de son code applicatif. Les microservices sont une combinaison de modèles techniques et organisationnels destinés à apporter une réponse à des questions stratégiques. Comment construire des applications ultra résilientes et conserver une capacité d'innovation et d'adaptation à des échelles massives ?

Qu'est-ce qui définit une architecture microservices et qu'est-ce qui la différencie d'une architecture classique ?

La réponse à cette question s'articule en deux axes indissociables. Un axe technique (Architecture, Technologie, Patterns) et un axe organisationnel (Processus, Organisation, Management).

Une architecture spécifique héritée des SOA

Certes, les architectures microservices sont constituées de multiples "petits services", mais elles répondent à des patterns spécifiques qui les différencient d'une architecture "n tiers" classique. Les architectures microservices partagent de nombreuses caractéristiques avec les architectures SOA (Service Oriented Architecture).

Pour Steve Jones, CTO de CapGemini, les architectures microservices ne sont qu'une approche orientée "Delivery" d'une SOA bien conçue.

Communication asynchrone et API Gateway
Les architectures microservices disposent de concepts similaires aux SOA comme un "Bus de message asynchrone" permettant de gérer la communication des différents modules. L'API Gateway est un pattern essentiel permettant de répondre à l'éclatement de l'application en de multiples "endpoints". Cet élément permet d'exposer aux consommateurs une API uniforme de manière sécurisée.

Scalabilité et résilience
Un autre pattern essentiel des architectures microservices est sa capacité à répondre à la charge de manière différenciée. Plutôt que de déployer de nouvelles instances d'une application, seuls les services sollicités sont déployés puis détruits dès que la charge est redescendue.

Les architectures microservices prônent un modèle basé sur la "résilience" plutôt que sur la "robustesse". Le crash d'un processus ne peut entraîner la disparition du service, son existence étant assurée au travers de multiples réplicas, créés et détruits à la demande.

Monolythe VS Microservices
On oppose souvent les architectures microservices (modulaires) avec le modèle classique "Monolithiques".

Architectures Monolythiques vs Microservices (Source https://www.nginx.com/blog/introduction-to-microservices)

Imaginez votre application monolithique comme un train composé de wagons représentant vos différents modules. Dans le cas où l'un des wagons aurait un problème, il y a de fortes chances pour que votre train déraille. De même, si vous devez effectuer une modification sur l'un des wagons, vous devrez procéder à la livraison d'un train complet. Comme cette opération est lourde, vous allez attendre un nombre de modifications suffisant pour justifier le lancement d'un nouveau train. De même, si un seul des wagons est plein, vous allez probablement devoir déployer un ou plusieurs nouveaux trains.

Par opposition, une application microservices est plutôt comme une flotte de véhicules Uber. Le crash d'un véhicule n'a pas d'incidence sur le service tant qu'un nombre suffisant de véhicules identiques est disponible. Si un type de véhicule est trop demandé, il suffit d'en rajouter en circulation. De même il existe des patterns permettant de mettre à jour les véhicules sans perturber le service (Blue Green deployment, Canary Release etc.)

Bien sûr, ce modèle nécessite une application pensée et développée dans ce sens, mais cela ne suffit pas. Pour en tirer parti il faut avoir adopté un modèle organisationnel particulier.

Un modèle organisationnel, une gouvernance et des outils spécifiques à mettre en place

C'est l'aspect le plus difficile pour les organisations qui souhaitent évoluer vers des modèles applicatifs "cloud natives". Pour les entreprises qui appliquent un modèle ITIL "serveur centrique" depuis de nombreuses années, cela peut représenter un cap difficile à franchir. Les architectures Cloud natives sont "Service Centrique". Ce seul aspect induit une véritable évolution de la gouvernance d'un SI.

Les architectures microservices nécessitent une grande maturité technique. Il ne s'agit pas seulement d'être doté des bons outils (CI/CD), encore faut-il disposer de la culture (DevOps) permettant de les mettre en œuvre de la bonne manière.

Live and let die
La création et la destruction d'instances, parfois en quelques minutes d'intervalle sont incompatibles avec une vision "analytique" visant à stocker l'ensemble de ces informations dans une CMDB. Si cette notion garde son sens, il faut revoir le niveau de détail et la définition des "Configuration Item" à un niveau "service".

La vélocité de livraison, l'aspect clef des architectures microservices
L'un des principaux atouts des architectures microservices est leur capacité intrinsèque à maintenir un flot continu de livraisons.

A fur et à mesure qu'une application classique grossit, sa base de code devient de plus en plus importante. Les modifications deviennent de plus en plus complexes et coûteuses à implémenter. La fréquence des livraisons ralentit, et ce, d'autant plus vite que les demandes de changements s'accumulent.

Les architectures microservices sont une manière de segmenter une application en différents modules indépendants disposant de leur propre base de code.

Pizza & Product teams
Un microservice ne peut être géré que par une seule équipe clairement identifiée et disposant d'une autonomie étendue. Contrairement à une équipe projet qui a un début et une fin, cette équipe existe aussi longtemps que le service existe. Elle est responsable des évolutions, du déploiement et du support.

Parce qu'elle est autonome dans le déploiement, elle n'a pas à attendre le passage d'un "batch" pour voir ses modifications apportées en production.

Le terme « Pizza Team » nous vient de Jeff Bezos (PDG Amazon) et signifie que l'équipe doit pouvoir être nourrie par une ou deux pizzas. Cette taille réduite est le garant d'une productivité maximale (partant du principe de nombreuses fois éprouvé que la productivité d'une équipe chute de manière importante au-delà de 9 personnes).

Quelques conclusions et vérités...

Il n'est pas possible de traiter ce sujet de manière exhaustive dans un seul article tant il est vaste et complexe. Nous pouvons cependant tirer quelques conclusions et rétablir quelques vérités permettant d'y voir un peu plus clair.

Culture DevOps et outils adaptés
La mise en œuvre d'une architecture microservices requiert de hautes compétences techniques et une grande maturité de la culture DevOps. L'infrastructure sous-jacente doit être entièrement automatisée (raison pour laquelle la plupart des applications microservices sont créées dans le Cloud Public) et dotée des outils permettant la mise en œuvre des concepts de Continuous Integration / Continuous Deployment (CI/CD) et d'Infrastructure as Code (IaC)

Gérer la complexité d'un système distribué
L'ADN d'une application microservices réside dans le couplage faible des différents modules. Cette caractéristique implique une distribution de l'information et un mode de communication asynchrone. La gestion et l'évolution d'un tel système est extrêmement complexe et nécessite de fortes compétences.

GreenField ou BrownField ?
Le découpage en microservices est un exercice périlleux très structurant pour le futur de l'application. Les choix effectués lors de la création d'une application devront être assumés dans le temps alors que de nombreuses hypothèses n'ont pas encore été éprouvées par la réalité du terrain.

Pour ces raisons, de nombreuses voix s'élèvent pour disqualifier les architectures microservices dans le cadre d'une création. Une application "microservices" étant infiniment plus complexe à maintenir (il faut parfois créer ses propres outils pour assurer le MCO).

Une architecture ne devient pertinente qu'à partir du moment où votre application est devenue trop lourde et trop complexe à maintenir d'un seul bloc et que cela devient un problème stratégique pour l'entreprise.

Quand on entame la migration d'une application vers une architecture microservices on parle parfois de "peler l'oignon". On va enlever une à une les couches de l'application en identifiant les services à sortir jusqu'à ce que le code d'origine ait totalement été remplacé.

Un choix stratégique

Dans un monde où toute entreprise est destinée à devenir une "software company" (dixit Satya Nadella, CEO Microsoft). L'utilisation des architectures microservices doit être évaluée au regard d'impératifs stratégiques.

- La nécessité d'innover ou de pénétrer de nouveaux marchés
- La nécessité d'aligner les objectifs métiers et l'outil informatique
- La nécessité de changer les structures de gouvernance de l'IT pour permettre des prises de décisions rapides
- La nécessité de s'adapter plus rapidement aux conditions du marché
- La nécessité de défendre son marché contre des concurrents disruptifs

L'utilisation des architectures microservices doit être évaluée au regard d'impératifs stratégiques.

Ces choix sont souvent une question de survie pour les entreprises concernées. En conséquence, si vous n'avez pas encore commencé à mettre en œuvre ce type d'architecture, il y a peu de chance que vous en ayez réellement besoin.

Cependant, si les concepts DevOps, CI/CD et les pizza teams sont des composantes récurrentes des architectures microservices, ces pratiques conservent toute leur valeur dans un modèle plus classique.

Rien que dans ce domaine, il y a déjà fort à faire pour gagner en agilité et en productivité !

> Cédric Bravo
Cloud Solution Architect

LA CYBERSÉCURITÉ DE DEMAIN !

**Beaucoup de challenges s'annoncent pour 2019, Cloud, Internet des Objets, OT...
Décryptage avec Loïc Guézo, Stratégiste CyberSécurité Europe du Sud chez Trend Micro.**

La migration vers le Cloud

Pour certaines organisations, le défi de la migration est toujours là, « tous les clients se situent à des degrés variables du dispositif de Cloud hybride, et leur objectif à l'horizon 2020-2025, c'est vraisemblablement 80 à 90% de leur infrastructure Cloud. Notre challenge 2019 est d'accompagner les clients dans cette transformation numérique, en leur confiant les briques de sécurité qui sont de leur responsabilité ». Avec le Cloud et le modèle de responsabilité partagée au niveau sécurité, le fournisseur de services Cloud doit contractuellement un certain niveau de sécurité, puis, une fois livré, le client a, lui aussi, une charge sécurité dans les couches supérieures.

« Ce modèle de responsabilité, variable selon les fournisseurs, doit s'intégrer dans l'existant en pleine transition vers le Cloud ». Le modèle de sécurité choisi doit savoir adresser de manière unifiée et efficace, les machines legacy dans le datacenter, les machines modernes en mode virtualisé et intégrer les nouvelles applications indifférenciées, « notre produit Deep Security aide à relever ces défis et permet d'intégrer des fonctions sécurité, intégrité, anti-malware... sur des serveurs physiques, serveurs virtualisés ou des instances du Cloud public, voire avec des extensions sur les containers, le tout avec une seule console de gestion ».

Ainsi, face au renouvellement technologique et au « retour du poste de travail » avec des modules inexistants il y a encore dix ans, Trend Micro a annoncé Apex One, nouvelle mouture de la solution de sécurité pour les endpoints en entreprise. Apex One propose, via un seul agent logiciel, un large panel de fonctions de détection, de remédiation et d'investigation.

Loïc Guézo

OT & IoT : de nouveaux horizons ...

S'ouvrent aussi de nouveaux paysages et avec eux, de nouveaux besoins à savoir l'OT (Operation Technology) pour la numérisation des systèmes industriels, et l'Internet des Objet / 5G.

Côté OT, fin 2018, Trend Micro a créé avec Moxa, spécialiste de solutions de communication industrielle et réseau, une joint-venture de portée mondiale TXOne Networks, pour répondre aux exigences de sécurité des environnements IIoT (IoT industriel), autrement dit la fabrication intelligente, les villes intelligentes, l'énergie intelligente... et relever les défis du monde de l'OT !

Trend Micro noue des partenariats avec des fabricants de composants de base (notamment en Asie) autour de l'IoT, « nous leur fournissons un kit logiciel de fonctions de sécurité, charge à eux d'intégrer ces composants logiciels dans leurs produits pour qu'une fois manufacturés, ces produits bénéficient des fonctions de sécurité by design ». Les secteurs automobile, télécom sont évidemment largement concernés !

Et l'entreprise a d'ailleurs profité du Mobile World Congress (MWC) de Barcelone pour dévoiler Trend Micro Consumer Connect, suite logicielle de sécurité qui va aider les opérateurs télécoms à mieux protéger les clients et optimise la protection des objets connectés contre les menaces connues et inconnues en appliquant une couche virtuelle de sécurité. De plus, avec l'arrivée de la 5G, les opérateurs télécoms auront l'opportunité de renforcer la protection des clients.

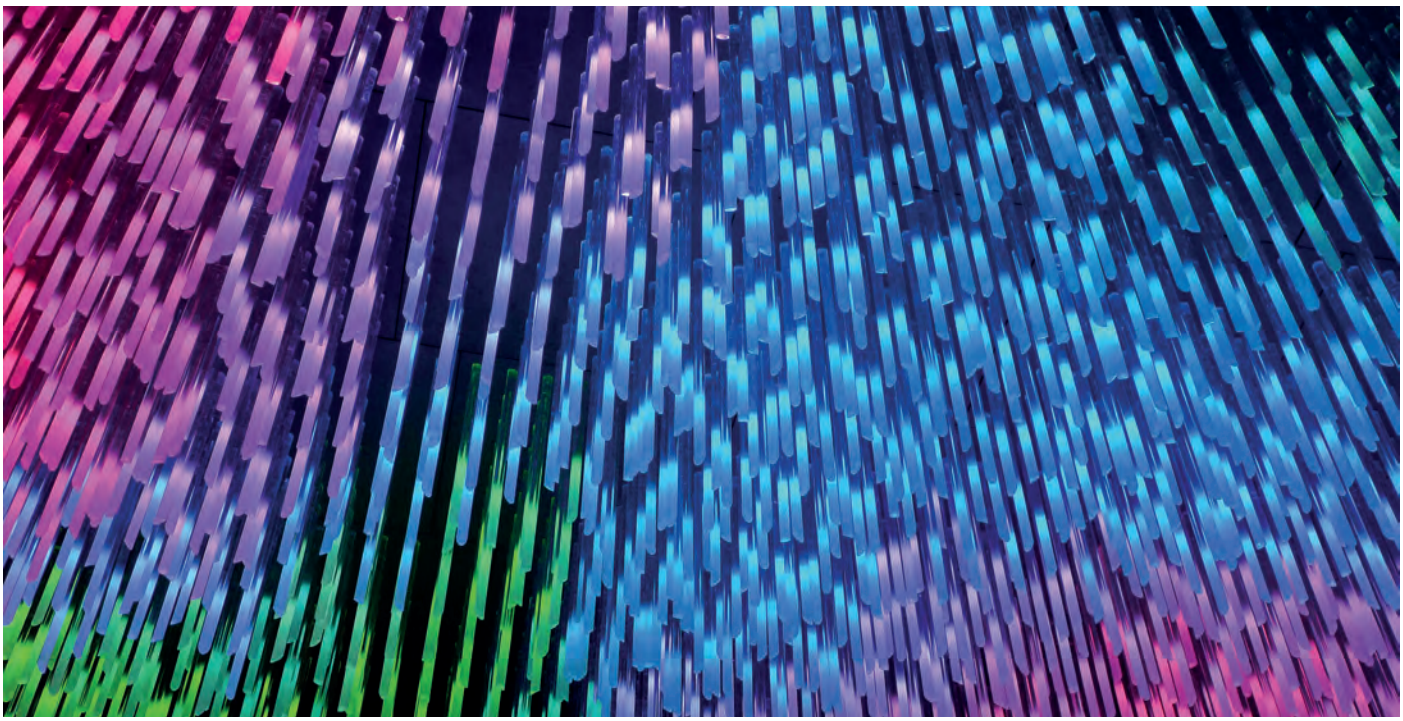
> Par Sabine Terrey

Comment intégrer rapidement
VOS FILIALES DANS OFFICE 365

L'intégration des environnements de messagerie Exchange quelles que soient leurs versions vers Office 365 est le lot courant des sociétés à croissances externes devant rapidement intégrer des environnements divers et variés bien souvent dans des délais très courts.

Nous verrons qu'il existe plusieurs niveaux d'intégration selon la stratégie retenue à court ou moyen terme et que les niveaux de complexité technique peuvent varier, selon l'environnement de transition et l'outillage retenu.

L'objectif de cet article est, par conséquent, de préciser les différentes étapes d'intégration, les risques inhérents et les outillages possibles pour ce genre d'opérations.



Intégration et cohabitation

L'acquisition d'une nouvelle entité va potentiellement générer des changements importants au niveau de son système d'information, et ce, au profit de la maison mère. Les applications métiers de la filiale vont être abandonnées au profit des applications « Corporate ». Le premier sujet adressé par cette contrainte métier va concerner l'identité.

Première brique permettant l'authentification des utilisateurs vers le système d'information et les applications métiers, l'ensemble des identités est, bien souvent, créé rapidement introduisant la notion d'un double compte pour les utilisateurs de la filiale.

Les utilisateurs de la filiale acquise se connectent alors traditionnellement à leurs environnements puis de nouveaux, sont authentifiés par celui de la maison mère. Cette double authentification peut être partiellement transparente pour les accès Microsoft s'il est possible d'établir des relations de confiance entre les forêts Active Directory respectives.

La plupart du temps la mise en place de ces relations d'authentification permet aux nouveaux comptes créés de conserver l'accès aux anciennes ressources Microsoft mais toutes les applications métiers ne savent pas gérer ces relations de confiance. Elles demanderont, alors, aux utilisateurs une connexion additionnelle avec le compte de la maison mère.

Une des questions importantes à se poser est la question de la cible définitive.

Devrez-vous à terme conserver l'environnement de compte de la filiale ou au contraire, devrez-vous le faire disparaitre au profit de celui de la maison mère ?

- **Dans le premier cas (Conservation)**, on ne parle pas véritablement d'intégration mais de cohabitation. Les deux environnements Active Directory vont cohabiter sur le long terme, se faire confiance et les utilisateurs des deux mondes resteront dans leurs domaines respectifs.
- **Dans le second (Intégration)**, le système d'information de la filiale doit être « soluble » dans celui de la maison mère. Les stations de travail vont être intégrées dans la ou les forêts de la maison mère et les données de messagerie devront migrées vers le tenant 0365 de cette dernière.

Le diagramme suivant (1) décrit la façon dont sont organisés les services d'envoi dans un scénario où le domaine Corporate est partagé par la maison mère et deux autres filiales (Filiale-1 & Filiale-2). Dans ce scénario, la maison mère et la filiale 1 possèdent toutes les deux un tenant 0365.

Le service de récriture d'adresse est présent sur un serveur Edge Exchange. Ce service n'existe pas encore sur l'environnement Microsoft Exchange Online.

Pour la réception, les équipements de la maison mère devront rester en en place et devront réacheminer les messages pour les utilisateurs de la filiale vers leur tenant. Cette redirection peut être faite de deux façons.

La première consiste à faire du routage par le biais de l'annuaire, le second est une simple configuration SMTP via les services de réécriture d'annuaire.

Etape 1 : Donnez l'impression

Dans le cas d'acquisition, une des problématiques est de permettre rapidement aux personnes de la filiale de pouvoir envoyer avec le même domaine SMTP (ex :@coporate.com) que celui de la maison mère. Cela revient à partager un espace de nom SMTP sur plusieurs entités (la maison mère et la ou les filiales) ce qui vous allez le voir n'est pas forcement évident, surtout si la filiale utilise Exchange Online.

Si la filiale que vous devez intégrer vient avec son Tenant 0365, il ne vous sera pas possible d'étendre le nom de votre domaine SMTP sur ce dernier. Ceci en raison d'une limitation fonctionnelle qui limite l'usage d'un nom de domaine à un seul et unique Tenant 0365.

Pour l'envoi, il vous faudra, par conséquent utiliser un service de réécriture d'adresses depuis votre filiale. Service, qui va convertir tous les messages envoyés en tant que @filiale.com en @corporate.com. Pour des questions de sécurité nous vous conseillons d'acheminer ce flux sortant vers les équipements de messagerie de la maison mère ayant la responsabilité déclarée sur internet (SPF, MX) d'envoyer et de recevoir les messages. Vous éviterez ainsi que vos messages soient considérés comme Spam.

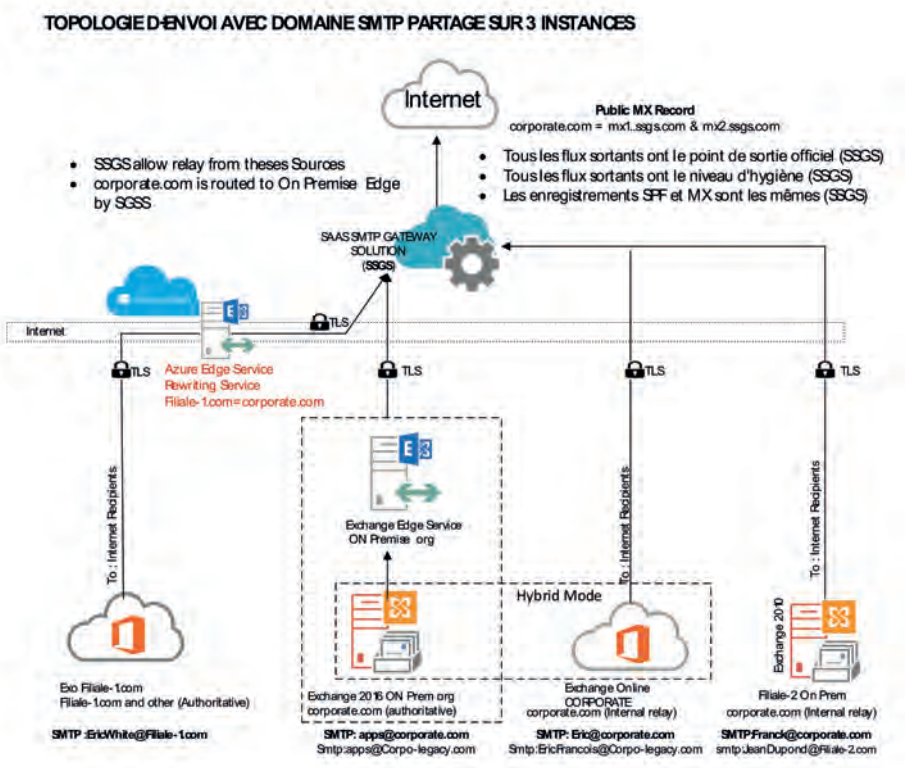


Schéma 1

- **Routage par le biais de l'annuaire :** Dans ce cas, des entrées dans l'annuaire de la maison mère sont créés (« Mailuser » ou Contact de messagerie). Ces entrées d'annuaire de messagerie portent l'adresse SMTP corporate (Ex : john.doe@corporate.com) mais également une adresse de redirection (Target Address) Exemple john.doe@filiale-1.com. Cette adresse

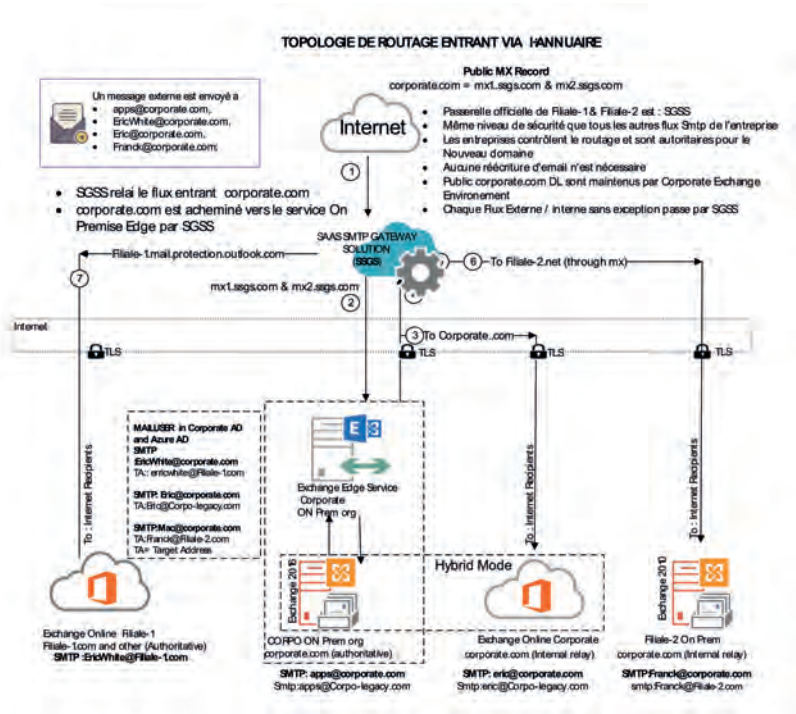


Schéma 2

de redirection sera utilisée par Exchange online ou Onpremise pour acheminer le message dans la boîte aux lettres de la filiale. Ce système peut être utilisé avec plusieurs filiales en même temps si celles-ci ne portent pas le même nom de domaine SMTP. Voir schéma 2. L'intérêt d'utiliser des objets de type mail user (Utilisateurs AD avec extension de messagerie), permet aux utilisateurs de la filiale de disposer d'un compte utilisateur dans l'environnement Corporate et par conséquent de pouvoir se connecter aux diverses applications métiers qui utilisent l'annuaire Active Directory.

Les applications métiers de la filiale vont être abandonnées au profit des applications « Corporate ».

- **Routage par configuration** : Le routage par configuration consiste à utiliser le serveur Edge pour réécrire les adresses dans le sens inverse de l'envoi. De @corporate.com à @filiales.com.

Le diagramme précise une topologie de routage entrant basé sur l'annuaire et l'utilisation de « Target Address » et de ces fameux « Mailuser ».

Ces deux solutions fonctionnent parfaitement et sont documentées par Microsoft. J'ai cependant une petite préférence pour le Routage par le biais de l'annuaire car d'une part, il s'inscrit plus adroitement dans le scénario d'intégration que le premier (nous verrons pourquoi par la suite) puis il permet d'autre part, la création de listes de distribution gérées par la maison mère au sein de son Exchange online (la cible définitive ne l'oublions pas) adressant des boîtes aux lettres des deux environnements.

Quoiqu'il en soit ce « renommage à la volée » va donc permettre de donner l'illusion extérieurement d'une intégration mais ne doit être considérée que comme un pis-aller temporaire. Une étape avant l'intégration ou plutôt la dissolution de l'entité filiale dans l'environnement de la maison mère.

C'est l'étape 2, celle qui va impliquer de rattacher aux comptes de la filiale déjà présents dans l'environnement de la maison mère (Les fameux « mail users » cités plus haut), les ressources et les accès hérités. Comme le scénario de départ est de supprimer l'environnement Active Directory de la filiale, vous ne devez pas synchroniser ce dernier dans l'Azure AD Corporate. Si vous le faites pour migrer dans Office 365 les ressources associées, celles-ci resteront liées à la forêt locale. Cette dernière devra par conséquent rester en production ce qui n'est pas l'objectif.

L'étape 2 consiste à préparer l'intégration et comporte deux chemins possibles.

L'étape suivante donc consiste à s'assurer que pour chaque compte présent dans la filiale correspond un compte dans l'environnement Corporate, son clone en quelque sorte que nous nommerons pour des raisons de praticité : Surrogate

L'étape 2, qui est conséquente, consiste à préparer l'intégration et comporte deux chemins possibles. Le premier consistant à s'appuyer sur les fonctions d'Azure AD connect pour effectuer cette fusion d'identité, le second consistant à s'appuyer sur des outils tiers.

Mais nous verrons cela dans la partie 2 à venir.

> Laurent TERUIN
lteruin@hotmail.com
https://www.linkedin.com/in/laurent-teruin-96708b34/

HOUAM

Avoid complexity

TeamSync

TeamSync rend transparent **l'échange des documents, données et metadonnées.**
En temps réel, synchronisez vos espaces collaboratifs pour tous vos projets inter-entreprises, quelles que soient vos plateformes

GoodMeeting

GoodMeeting est **LA solution qui simplifie la réservation et la gestion des salles de réunion en entreprise.**
Disponible pour Exchange, Office365, Smartphones et tablettes

CloudAuditor

Avec CloudAuditor, **auditez** l'activité, **gérez vos licences, rapportez l'utilisation de toutes vos applications Cloud**, que ce soit pour Office365, OneDrive, Box, Dropbox ...

HOUAM C'EST AVANT TOUT

LA SIMPLICITÉ

www.houam.com

Microsoft Azure · Office 365 · SharePoint · Exchange

NOUS CONTACTER

Téléphone : + 33 (0) 1 40 903 148
Email : contact@houam.com
Site internet : www.houam.com

BLOCKCHAIN :

APPORTER DES GARANTIES SUR LES DONNÉES

Entretien avec David Leporini, Directeur Sécurité IoT, chez Atos pour évoquer des sujets porteurs à savoir les signatures électroniques, la Blockchain, l'Internet des Objets...

David Leporini

L'indispensable signature électronique !

Atos s'est emparé du sujet et se focalise notamment « sur la signature électronique qualifiée et à distance » c'est-à-dire, la signature avec le consentement de l'utilisateur à valeur probante « sans nécessairement avoir un dispositif de signature qualifiée au niveau du poste de travail » commente David Leporini. En termes de facilité d'usage et de déploiement, il est intéressant de migrer la partie contrôle de l'usage de la clé sur un serveur centralisé.

Ainsi, côté serveur, l'enjeu est essentiel, « la personne signataire garde le contrôle exclusif de sa clé comme si, cela se passait en local et on permet à l'utilisateur authentifié d'avoir le contrôle de sa

clé ». Un module d'activation est intégré « sur un module hardware de sécurité (HSM) certifié qui garde le contrôle à distance de la signature, cette base de confiance permet de vérifier qu'il s'agit de la bonne personne ».

Atos travaille avec un certain nombre d'industriels et entend donc accompagner les fournisseurs de services de confiance dans le déploiement de ces services pour permettre une signature jusqu'à un niveau qualifié.

Blockchain : faire émerger les bons cas d'usage

L'expérimentation permet de dégager les cas d'usage pertinents, « on note déjà quelques mises en production Blockchain, qui vont sans doute s'accélérer en 2019. L'outil spécifique va venir complémenter des systèmes déjà en place, avec l'automatisation de certains processus ».

L'approche Blockchain d'Atos pourrait s'orienter ainsi « si la Blockchain devient un outil IT pour des cas d'usages appropriés (au-delà des cryptomonnaies) quels sont les enjeux sécurité et comment y répondre ». Certes, on note différents modèles de Blockchain, cependant le modèle industriel est le modèle collaboratif d'entreprises, « ainsi, un cas d'usage est partagé par un certain nombre d'acteurs qui veulent collaborer (supply chain, partage de données...)», mais cela reste très compliqué en termes de gouvernance (base de données centralisée)

Dans cet esprit, il s'agit de s'appuyer sur le partage automatisé d'une base de données, et pour sécuriser l'ensemble, « la Blockchain apporte un certain nombre de propriétés et garanties sur un modèle de confiance global ». Puis des identités sont générées. « Atos développe des outils qui permettent de sécuriser ces développements avec une vision cyber de la mise en œuvre de solutions Blockchain » souligne David Leporini, « nous testons aujourd'hui les cas d'usage, dès que ces technologies seront utilisées en production, les problématiques cybersécurité vont se poser ».

« On peut justement faire le lien avec la signature électronique car on embarque dans les mêmes modules de sécurité, les mêmes serveurs sécurisés, ce qu'on appelle les nœuds Blockchain ». Il s'agit de l'infrastructure que chaque entité va devoir déployer pour maîtriser les identités, sécuriser l'échange d'informations et inscrire de manière contrôlée les données sur une Blockchain, « nous apportons une solution unifiée et uniforme ». La Blockchain apporte la garantie et la pérennité que les données ont été signées.

Quid des problématiques IoT ?

Outre l'analyse de sécurité et de risques, le RGPD, les systèmes de surveillance et de détection, les problématiques Internet des Objets s'emparent des entreprises, notamment dans l'industrie automobile, « l'industriel va toucher le grand public, avec des enjeux forts, comme la prise à distance d'un véhicule connecté ».

Atos vient, par ailleurs, d'annoncer, la suite de sécurité Horus pour les systèmes de transport intelligents (ITS), qui sécurise les communications des véhicules connectés. « La sécurité des véhicules est au cœur des enjeux des services Smart City qui améliorent la sécurité routière et l'efficacité du trafic. La suite de sécurité Horus pour ITS permet aux véhicules de communiquer de manière sécurisée avec leur environnement. Elle permet également aux constructeurs automobiles et aux fournisseurs d'applications Smart City de relever efficacement les défis de leur secteur » précise David Leporini.

> Par Sabine Terrey

Cybersécurité en France : 6 violations par mois et par entreprise

94 % des entreprises françaises ont subi des violations de sécurité lors des 12 derniers mois.

Un haut degré de sophistication

Les indicateurs à prendre très au sérieux :

- 91 % signalent une augmentation du volume des cyberattaques :

  22% ont constaté une augmentation du volume d'attaques de 25%, 34% une augmentation de 26 à 50%, 23% une augmentation de 51 à 100%. 12% ont signalé une augmentation de plus de 100%

- le nombre des attaques a augmenté de plus de la moitié au cours de l'année passée (35%)

- 94 % constatent des menaces de plus en plus sophistiquées

Le nombre moyen de violations par organisation est de 5,81

- 59 % des organisations ont subi au moins cinq violations

- 1 entreprise sur 10 signale au moins 10 attaques

Face à ce constat, 89 % prévoient d'augmenter leur budget de cyberdéfense en réponse à l'accumulation de menaces.

Les attaques par hameçonnage dans le viseur

Le ransomware est à l'origine de 19 % des violations au sein des entreprises françaises. Le facteur humain joue également un rôle clé : les attaques par hameçonnage sont à l'origine d'une violation sur six en France.

Threat Hunting

Des mesures actives de chasse aux menaces ou « threat hunting » ont été mises en place (73% - plus spécifiquement 35 % au cours des 12 derniers mois)

Les mesures de threat hunting

- renforcent globalement les défenses (95%)

- améliorent leur posture défensive (56%)

Source Etude Carbon Black & Opinion Matters - janvier 2019

UNE FEMME EN ZONE DE GUERRE

LE NOUVEL ALBUM PHOTO DE RSF

REPORTERS SANS FRONTIERES
POUR LA LIBERTE DE L'INFORMATION

2019 – 2021 : les 5 tendances d'un monde post-digital

Connaissez- vous le pouvoir du DARQ ? Décryptage des principales tendances technologiques qui vont façonner le futur des entreprises au cours des 3 prochaines années.

Les réseaux sociaux, la mobilité, l'analyse de la data et le cloud sont désormais au cœur de l'activité technologique des entreprises (79%). Les entreprises doivent se différencier une fois la maturité digitale atteinte : voici les 5 tendances à prendre en compte :

1 - Le pouvoir du DARQ...

Ces 4 technologies vont réinventer des secteurs d'activité :

- Distributed Ledger Technology (DLT)
  Les registres distribués (blockchain...) facilitent les transactions et la collaboration à grande échelle et sans intermédiaires
- Artificial Intelligence (AI)
  Essentielle dans l'optimisation des processus et les prises de décision : 41 % citent l'IA en N°1
- Extended Reality (ER)
  La réalité étendue crée de nouvelles expériences générant un engagement plus important
- Quantum Computing
  L'Informatique Quantique propose des approches pour résoudre les problèmes de calcul les plus difficiles (cybersécurité ..)

2 - La Connaissance client exponentielle

Les données recueillies sont une base de connaissances vivantes pour comprendre les nouvelles générations de clients et leur proposer des expériences uniques : les données démographiques numériques identifient les besoins non satisfaits des clients (83%)

3 - Les Talents Augmentés

Il faut tenir compte de la nouvelle façon de travailler : pour 71 % des dirigeants, les employés ont une maturité digitale supérieure à celle de leur entreprise.

4 - L'écosystème !

Plus les entreprises sont tournées vers leur écosystème, plus les connexions les rendent vulnérables. Les grandes entreprises collaborent avec leur écosystème pour proposer les meilleurs produits, services et expériences, mais seuls 29 % des dirigeants déclarent connaitre les mesures de conformité et de résilience des partenaires en matière de sécurité.

5 - Saisir les besoins clients sur l'instant

La technologie crée un monde d'expériences à la demande personnalisées. Chaque opportunité doit être considérée comme un marché unique et éphémère sur lequel se positionner : selon 85 %, la personnalisation et la livraison en temps réel sont les facteurs concurrentiels les plus importants.

Source Accenture Labs et Accenture Research. Vision Technologique Accenture

COMEXPOSIUM DC consultants | @ReadyForIt_2019 | ready-for-it.com

METSYS

Laissez-vous guider !

Pour en savoir plus, scannez ce QR code

Paris - Rennes - Nantes - Tours - Lille - Lyon - Toulouse
www.metsys.fr