N°12 I DECEMBRE 2018

CONDUIRE LA TRANSFORMATION NUMÉRIQUE DE L'ENTREPRISE

SMART DSI®

DOSSIER
Agilité, DevOps, gestion & gouvernance

INTERVIEW
RGPD : comment gérer une cybercrise ?

DECRYPTAGE
La transformation culturelle est en marche

PERSPECTIVES
La Blockchain et la gestion des identités

L'ETUDE A RETENIR
La Digital Workplace en 2022

www.iTPro.fr

« SUR ITPRO.FR, NOS EXPERTS VOUS ACCOMPAGNENT AU QUOTIDIEN POUR VOUS AIDER À TIRER LE MEILLEUR PROFIT DE VOS ENVIRONNEMENTS IT… »

Sur iTPro.fr, 7 chaînes d'informations et de formations des meilleurs experts en technologies informatiques d'entreprise, par les éditeurs de la revue SMART DSI.

9 chaînes informatiques

4,200 Dossiers et Guides exclusifs
7 Flux RSS, Newsletters hebdos
Videos & Webcasts
Fil d'actualités

Un savoir technologique unique, une base de connaissances exclusive pour vous accompagner dans la gestion et l'optimisation de vos environnements IT Professionnels.

Des ressources exclusives

Enjeux DSI
Cloud Computing
Collaboration & mobilité
Exchange Server
IBM i

Bénéficiez d'une richesse éditoriale incomparable… connectez-vous !

iTPro.fr

Un Club Abonnés

Des services réservés aux abonnés de la revue, en complément des dossiers publiés dans SMART DSI.

Suivez-nous sur **Twitter** : @iTProFR

Partagez sur **Facebook** : www.iTPro.fr

La bibliothèque éditoriale du site iTPro.fr est constituée de plus de 4200 dossiers technologiques signés par les meilleurs experts francophone et internationaux sur les thèmes de la définition, de la gestion et de l'optimisation des environnements IT basés sur les principales technologies informatiques d'entreprise en terme d'infrastructure serveurs, réseaux, plate forme de collaboration, mobilité d'entreprise et de virtualisation.

ÉDITO

La « Cybersécurité » attitude !

Au cœur de la transformation digitale, les nouvelles solutions et méthodes sont des accélérateurs incontestables à l'innovation, au changement de nombreuses pratiques et à l'évolution des mentalités. Agilité, gouvernance, DevOps, Cloud, autant de mots qui agitent les équipes IT et les différents métiers.

Il va sans dire que la gouvernance des technologies de l'information prend le pas. Ne devient-elle pas la clé de la stratégie et de la culture du service IT qu'elle doit faciliter ? Prendre le temps de la réflexion sur la structure et les objectifs s'impose pour affiner au mieux la gouvernance qui ressemble à votre entreprise !

Mais ce n'est pas tout, en cette fin d'année, les défis sécuritaires s'enchaînent. Les cyber-attaques, de plus en plus ciblées, se complexifient, les risques persistent et se multiplient. La consolidation de la sécurité est essentielle, le business en dépend fortement. Toutefois, plus de la moitié des PME françaises n'ont pas encore renforcé leurs mesures de sécurité numérique. Le manque de sensibilisation est révélateur, d'autant qu'il faut désormais compter avec les nouvelles réglementations comme le RGPD ...

De plus, à l'heure de l'explosion du nombre de machines connectées, de l'Internet des Objets, des services Cloud, des applications mobiles, n'en doutons pas, les cyber-pirates explorent finement toutes les failles de ces nouveaux environnements pour infiltrer les systèmes.

Poursuivons sur la lancée d'indicateurs très intéressants ! A la question, quelles sont les technologies identifiées comme porteuses d'opportunités ? La palme revient au Big Data et l'analyse des données (47%), suivis par la cybersécurité (39%), le Cloud, l'Intelligence Artificielle, et l'automatisation ... (1).

N'oublions pas, face à ces enjeux majeurs, si la collaboration IA-homme est une réponse, l'être humain garde le contrôle en prenant la décision finale.

Très bonne lecture et excellentes fêtes de fin d'année !

Sabine Terrey
Directrice de la Rédaction
sterrey@itpro.fr

(1) Source Kaspersky Lab Novembre 2018

SMARTDSI

N°12 I DECEMBRE 2018

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, Kevin Trelohan, 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 – Mathieu Le Gal
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

Agilité, DevOps, gestion et gouvernance

LES POINTS CARDINAUX DES TECHNOLOGIES DE L'INFORMATION ?

> Par Didier Danse

La mise en place de systèmes informatiques a pour but de fournir des outils adéquats pour supporter, optimiser ou faire évoluer des métiers et des pratiques. L'outil n'est qu'une partie de solution qui se doit de comprendre notamment une documentation adéquate, tant sur les besoins du métier que sur les processus utilisés lors de la mise en place de cette solution.

A cela s'ajoute la surveillance autour de la production des résultats et de la manière d'y arriver. Pour y arriver, il est nécessaire de garantir la transparence sur les processus, les éléments en entrée mais aussi sur les points de contrôles en place.

Du côté des métiers, il est demandé de s'adapter rapidement aux besoins des clients et des utilisateurs par tous les moyens, parfois au détriment de toute gouvernance.

Réagir rapidement ou rester en totale conformité avec les règlements et les règles de gouvernance en vigueur et risquer de perdre des opportunités à proprement parler, voilà un dilemme qu'il est fréquent d'entendre. Mais existe-t-il vraiment un dilemme ? Nous essayerons d'y répondre au travers de ces quelques lignes.

- 1 -

La gouvernance des technologies de l'information

Souvent confondue avec la gestion des technologies de l'information, sur laquelle nous reviendrons un peu plus tard, la gouvernance des technologies est l'ensemble des pratiques et moyens de gestion et de régulation des systèmes d'information.

Ces pratiques et moyens ont pour but de s'assurer du comment les investissements sont utilisés dans le but de créer de la valeur, de servir le client, d'améliorer les performances des processus en place et de contrôler les risques.

Il s'agit également de clarifier les aspects financiers, notamment les coûts, ainsi que l'organisation globale du département IT et les besoins en solutions et compétences. Ces derniers doivent en effet permettre au département de fonctionner sur le long-terme.

Certains départements seront en recherche de compétences techniques fortes, d'autres favorisent l'innovation. La gouvernance peut notamment donner des recommandations en termes de technologies, permettant notamment de favoriser la mobilité interne ou de technologies plus à même de répondre à des besoins spécifiques du métier. Ainsi, la gouvernance est l'outil de la stratégie et de la culture du département IT qu'elle doit faciliter.

Plus concrètement, la gouvernance définit comment se prennent les décisions majeures, qui a la responsabilité de le faire et sur base de quelle information. Chaque entreprise dispose d'une gouvernance qui lui est propre et qui tient compte de sa structure et de ses enjeux et objectifs.

Les règles sur la gestion des risques font également partie de la gouvernance.

En effet, on peut imaginer qu'une application pour téléphone soit délivrée sur le marché avec l'un ou l'autre souci, connu ou non mais il n'est cependant pas concevable qu'un avion ou un appareil médical puisse être commercialisé avec le même niveau de risque.

De par les aspects couverts, la gouvernance permet l'évaluation, la sélection, la hiérarchisation, le financement et la supervision de la mise en œuvre. Selon l'IT Governance Institute, l'ensemble de ces activités peuvent être regroupées en 5 piliers fondamentaux: l'alignement stratégique, la fourniture de valeur, la gestion des risques, la gestion des ressources et enfin la mesure des performances.

La mise en place d'une gouvernance peut se faire de différentes manières, notamment en fonction de la taille et de la structure de l'organisation IT. Dans des entreprises de taille moyenne ou grande, c'est un programme de « gouvernance des technologies de l'information » qui s'en assure.

Ce programme est généralement en charge de définir le référentiel de bonnes pratiques alignées avec besoins et contraintes de l'entreprise mais aussi de l'assurance qualité, notamment au travers d'audits.

La gouvernance définit comment se prennent les décisions majeures et qui a la responsabilité de le faire

Il existe de nombreux référentiels de bonnes pratiques de gouvernance sur le marché. C'est notamment le cas de COBIT (pour « Control Objectives for Information and related Technology ») qui est le référentiel le plus utilisé pour gouverner. A la lecture de la documentation COBIT, le pourquoi de l'investissement est omniprésent.

Le cas d'affaire (Business Case) en est d'ailleurs un élément clé. D'autres référentiels fournissent ce genre de bonnes pratiques, notamment ITIL au travers de la Stratégie et de la Conception et fait également des propositions sur la gestion des technologies de l'information.

- 2 -

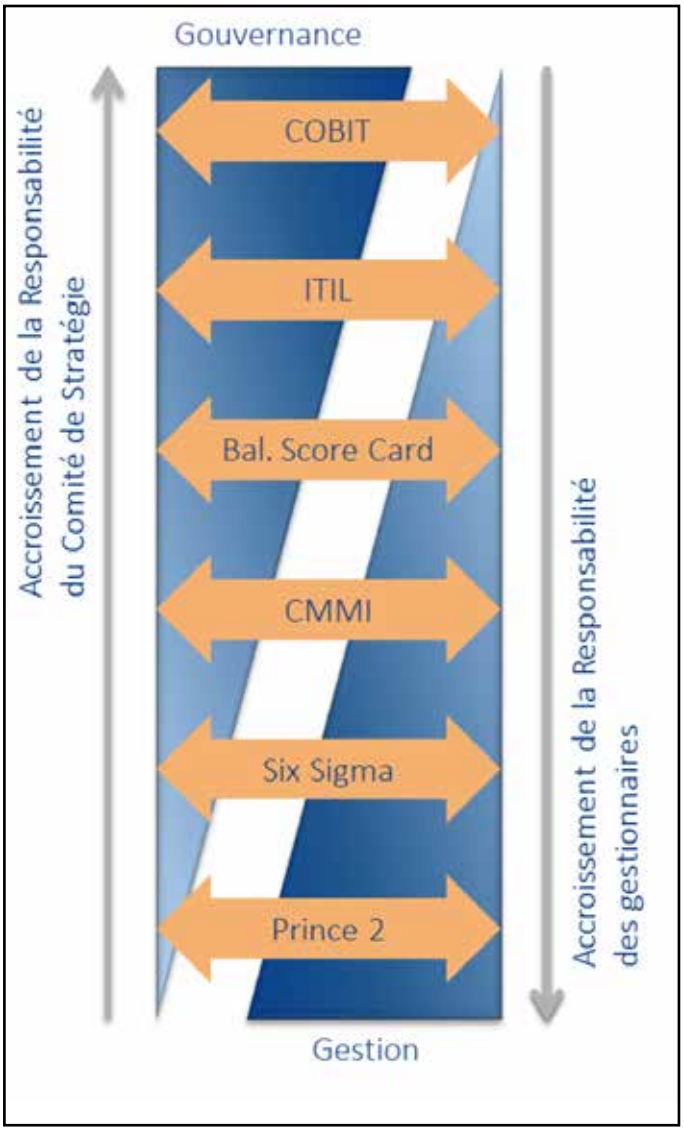
La gestion des technologies de l'information

La gestion des technologies de l'information définit comment atteindre l'excellence opérationnelle, en tant compte de l'ensemble des éléments en entrée mais aussi des points de contrôle intermédiaires.

Nous l'avons déjà entrevu, un grand nombre de référentiels coexistent, chacun ayant un périmètre et un objectif différents avec des balances différentes entre gouvernance et gestion comme on peut le voir sur la figure ci-dessous.

Ainsi, de par sa découpe temporelle dans laquelle les opérations ont une place prédominante, on pourrait alors considérer ITIL comme étant un référentiel purement de gestion IT. Cependant, on remarque également que régulièrement, le « pourquoi » au cœur de la réflexion et la stratégie, qui sont des éléments de la gouvernance. ITIL se focalisera principalement sur la fourniture de services efficaces et efficients et non sur une gouvernance globale autour de plusieurs services.

La notion d'autorité déléguée est fortement présente au sein de l'ensemble du référentiel ITIL, niveau qui est généralement défini par la gouvernance. Dans l'ensemble des processus ITIL, des points de contrôles sont suggérés voire fortement recommandés depuis la définition du besoin jusqu'à l'implémentation du changement adéquat.



C'est à la gouvernance de donner un cadre de réflexion et de compréhension pour indiquer le niveau attendu autour de ces contrôles mais aussi sur le fonctionnement de la délégation de l'autorité. Ce n'est pas le seul cas où la gouvernance est en charge de clarifier certains éléments de la gestion puisqu'elle couvre notamment la gestion des risques, l'alignement stratégique, les technologies et bien d'autres.

- 3 -

L'agilité

L'agilité a pour but de permettre une réaction rapide face aux besoins évolutifs de l'entreprise, dont les enjeux peuvent être multiples, tout en réduisant les temps nécessaires à la conception, la promotion et la diffusion des offres répondant à ces besoins. Les maîtres mots de l'agilité sont adaptabilité, flexibilité, réactivité et anticipation.

Ainsi, pour être agile, il s'agit de promouvoir une culture de changement et de collaboration où l'erreur est permise et dans laquelle le client et l'utilisateur ont une place prédominante. C'est dans un tel contexte favorable que la demande pourra y être accueillie. Le développement des potentiels et compétences prend une place importante dans la capacité d'être agile puisque l'humain est au centre du sujet, bien avant les processus.

Dans l'IT, l'agilité doit notamment permettre de démontrer rapidement la valeur d'une solution ou d'un service. Encore faut-il que ce service soit rendu. C'est le point de départ que certains peinent à atteindre. Ensuite, ce service pourra évoluer dans le temps en faisant de l'amélioration continue.

Une telle approche n'est possible que si l'agilité fait partie intégrante de l'organisation IT et qu'elle s'applique à tous les domaines, notamment l'agilité financière permet d'utiliser l'argent au moment opportun en favorisant des coûts d'opération à des coûts d'investissements.

De manière concrète, les différentes méthodes agiles recommandent d'inclure l'ensemble des parties prenantes dans les discussions afin de s'assurer que le besoin réponde à un besoin opérationnel réel et donc s'assurer que la solution soit utile.

Dans un tel cas, il n'est pas nécessaire de produire des documentations volumineuses puisque la solution sera d'autant plus adaptée à ce besoin. C'est d'ailleurs pour cette raison que l'on entend régulièrement « je suis en mode agile, je n'ai pas besoin de documentation ». Comme on peut le voir, l'agilité ne s'improvise pas. Il s'agit avant tout d'être organisé pour permettre le changement.

- 4 -

Dev(Sec)Ops

Bien que le message de l'agilité soit assez simple à comprendre, le terme « agile » est le reflet d'un grand nombre de difficultés qui peuvent être rencontrées durant la vie d'un produit ou d'un service. Tout d'abord, le nombre de déploiements impacte le temps investi sur ceux-ci. Pour répondre à cela, il s'agit de tenir compte, dès les phases de la conception et d'implémentation, des exigences non fonctionnelles telles que la montée en charge, la gestion des versions, des mises à jour et des accès afin de favoriser des déploiements rapides.

Toujours est-il qu'il est nécessaire de tenir compte de la réalité sur le terrain, ou plutôt dans les bureaux. De par leur fonction, les responsables des opérations (ops) cherchent avant tout à favoriser la qualité. Les coûts et les délais sont alors deux paramètres parfois mis de côté. Les développeurs (dev) quant à eux étant généralement contraints par le temps et les budgets, puisqu'il faut livrer vite et pour pas cher, ce qui peut impacter la qualité à un moment ou un autre.

Les maîtres mots de l'agilité sont adaptabilité, flexibilité, réactivité et anticipation

En effet, la réduction des temps telle que préconisée par l'agilité, ne s'accompagne que peu d'accroissement du budget alloué. Pourtant la qualité ne peut être impactée. Dans ce cas, qu'est-il possible de faire ? Automatiser un maximum d'opérations. Mais alors qu'en est-il des points de contrôle ? Sont-ils toujours assurés ?

C'est dans ce contexte que DevOps prend son sens. DevOps n'est ni plus ni moins qu'une culture. Une culture où l'ensemble des intervenants dispose d'une compréhension voire de compétences fortes sur l'ensemble des activités du périmètre couvert par l'équipe.

Concrètement, les développeurs apprennent comment sont gérés les systèmes tandis que les gestionnaires systèmes apprennent les bases du code et l'ensemble apprend des notions de sécurité et de gestion de projets et chacun intervient, quel que soit le domaine sur lequel se porte la réflexion. Mais au-delà de cet apprentissage, il s'agit également de profiter des compétences en proposant notamment des solutions à la croisée des mondes comme : « Infrastructure as Code ».

La vocation du DevOps c'est de permettre le déploiement régulier des applications en lieu et place d'un déploiement massif. Les tests s'effectuent au plus tôt, dans un environnement techniquement proche de la production, en lieu et place de les effectuer après un déploiement massif.

Dans la mesure du possible, ces tests seront effectués dans les phases en amont, permettant de détecter les potentiels problèmes au plus tôt, notamment lors du passage d'une version à l'autre. L'application, une fois dans l'environnement de production, est monitorée et génère des résultats compréhensibles par tous.

Aux aspects de déploiement et de maintenabilité, il s'agit également d'y attacher les notions de sécurité, de traçabilité et d'audit (sec, le chainon additionnel du DevOps pour en faire du DevSecOps), qui sont également pris en compte dès les phases de conception.

Comme nous pouvons le voir, la culture DevSecOps doit être soutenue par des outils adéquats : référentiel de besoins, gestion des sources, compilation automatique, tests et déploiements automatisés mais aussi outils de monitoring.

En effet, pour réduire le temps, il s'agit de comprendre et pour comprendre, il s'agit d'avoir des informations à analyser. Les outils ne sont pas les uniques solutions pour favoriser DevSecOps.

De nouveaux modèles d'utilisation sont en effet exploitables dans le même but. IaaS permet de disposer de ressources au moment utile, notamment lors de phase de tests. IaaS tout comme SaaS permettent aux équipes informatiques de s'abstraire de nombreuses problématiques techniques et de revenir aux fondamentaux : la valeur produite par le service !

- 5 -

La gouvernance et la gestion au service de l'agilité et de DevSecOps

Nous venons de le voir, DevSecOps peut être vu comme une réponse au besoin d'agilité qui préconise explicitement de fournir le service ou le bien au plus tôt et de le faire évoluer de manière régulière. Cependant pour permettre une telle approche, un certain nombre d'exigences doit être respecté, notamment en termes de gestion et version des sources.

DevSecOps, dans la mesure du possible, suggère de définir les méthodes et techniques nécessaires dès la phase de conception afin de permettre aux équipes de réduire le temps investi sur des problématiques à faible valeur ajoutée. DevSecOps ne peut dès lors pas s'improviser au niveau d'un projet et requiert une culture de collaboration et de changement, permettant alors d'exploiter le capital humain, nécessaire à toute innovation

Mais pour être efficace dans l'amélioration continue, il s'agit de disposer des informations utiles. Des catalogues d'informations sont alimentés avec les informations résultantes des différents processus faisant partie du référentiel de gestion, tel qu'ITIL. ITIL qui, quant à lui a pour but de standardiser les approches et de fournir des métriques adéquates.

L'amélioration continue telle qu'elle est entendue dans l'agilité est par ailleurs présente au sein d'ITIL avec le Continual Service Improvement. Ainsi un service peut-être pourra évoluer point par point, permettant de démontrer sa valeur à chaque instant, permettant alors d'adresser les préoccupations, d'augmenter la confiance et de prendre des leçons pour l'itération suivante.

La mise en place d'outils permettant l'automatisation d'activités techniques permet de profiter du meilleur des deux mondes puisqu'on peut imaginer que les outils de déploiement fournissent l'information dans les catalogues d'informations et ce de manière automatique.

En effet un grand nombre d'informations doivent simplement d'être loguées afin d'alimenter les catalogues d'information tandis que certaines de ces informations telles que les changements majeurs, sont approuvées selon les processus ITIL.

Enfin, la gouvernance se doit de mettre un cadre et des règles autour de tout cela, dans le but de favoriser cette culture de changement et collaboration.

Cela est rendu possible, notamment en exigeant un rapport d'activités commun à l'ensemble des intervenants qui indique les risques métier en lieu et place d'un rapport d'activités contenant des problématiques techniques disséminées dans les différents rapports fournis par les différents intervenants. DevSecOps n'est possible que si l'ensemble des intervenants ne parlent que d'une seule voix, qu'ils font partie d'un même ensemble.

En un mot, les référentiels de gouvernance et de gestion se veulent être des fondations solides pour favoriser la culture DevOps et promouvoir l'agilité de l'IT vis-à-vis des équipes métier.

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

Le collectif « Impact AI » : l'Intelligence Artificielle au service de l'humain

Un mouvement Collectif a ainsi été lancé en mars 2018 (loi Association 1901) avec une trentaine d'organisations en France « pour réfléchir et agir sur l'impact de l'Intelligence Artificielle et sur ce qu'il faut faire pour une AI responsable » notamment avec des algorithmes transparents, ce qui s'intègre dans l'engagement d'actions pour l'IA for Good (santé, accessibilité, économie sociale et solidaire, missions humanitaires ...).

Observatoire, Education & IA for Good

Différents groupes de travail œuvrent déjà en ce sens sur quatre domaines.

Observatoire. Orange a mis en place une initiative, le Digital Society Forum, plateforme collaborative ouverte pour mieux appréhender la vie numérique, « les enjeux sociétaux sur l'impact du numérique sont majeurs ». Le dispositif s'articule autour du travail d'acteurs (sociologues, universitaires ...), d'événements et d'une présence dans toute la France (ateliers). Cette plate-forme va coproduire des contenus et les publier.

Des rendez-vous experts et ateliers collaboratifs & participatifs en régions vont mettre à disposition toutes les informations dans un esprit de culturation.

Pour une IA responsable, Cécile Wendling, Group Head of Foresight (Axa) ajoute « nous allons lancer une librairie virtuelle de ressources en ligne, disponible à tous, en anglais et français, et où tout le monde peut contribuer ». L'IA doit être inclusive et non discriminante, l'objectif est bien de détecter les jeux de données biaisés.

Education. Sujet large car il y a urgence à former tout le monde ! Les trois approches se basent sur les ateliers initiations dès le plus jeune âge (unicité ...), la cartographie des formations diplômantes (public plus avancé) et l'évolution & transformation des métiers aujourd'hui pour apporter un champ de compétences, garantir l'employabilité et faciliter les passerelles.

IA for Good. L'ensemble des organisations contributrices du collectif vont participer en identifiant des projets dans l'économie sociale et solidaire et en mettant à disposition les ressources et compétences nécessaires pour aider à utiliser au mieux l'IA.

Le CESIN
LA CYBERSÉCURITÉ EN TOUTE CONFIDENTIALITÉ

Le 6ème congrès du CESIN à Reims, est chronologiquement le dernier événement de l'année de la profession. Regroupant les visions et les voix des hommes et des femmes en charge quotidiennement de la cyber-protection des entreprises et des institutions, il trace la voie des tendances et des préoccupations.

Le congrès annuel du CESIN a eu lieu les 4 et 5 décembre à Reims, pour le Champagne bien sûr, mais surtout pour parler de cybersécurité en toute confidentialité. C'est la 6ème édition de ces rencontres devenues en quelques années, un rendez-vous incontournable des responsables de la sécurité des systèmes d'information.

Chaque année à Reims, au cœur de la Champagne, les membres du CESIN échangent, analysent, réfléchissent aux enjeux du moment, un peu à l'écart du tumulte parisien mais pas totalement coupés de leurs entreprises.

Dans une tonalité essentiellement club de réflexion et de partage d'expériences et de problèmes, le CESIN fédère des RSSI et représentants de plus de 500 entreprises et administrations. Pour le moment, car le potentiel est à l'échelle de la croissance du marché numérique : énorme.

La résilience au sein des systèmes IT

Cette année la préoccupation principale, le thème central de l'événement a été la résilience dans la sécurisation des systèmes IT.

La résilience IT est cette capacité d'un système à absorber une perturbation, à se réorganiser et à continuer de fonctionner de la même manière qu'avant la survenance de la perturbation. Pour le monde de la

cybersécurité c'est aussi la résilience en cas de crise, la résilience du CyberSOC et la résilience dans le traitement des vulnérabilités, etc.

Il est certain que la gestion proactive des vulnérabilités est un des points essentiels de la protection en cybersécurité. Elle passe par les scans de vulnérabilités et les actions de remédiation à mettre en œuvre auprès des autres entités de la DSI : prod, infra, dev, hébergement, bureautique, etc.

L'impact des attaques par phishing sur les processus opérationnels de SOC/CERT et l'amélioration de la résilience lors de la gestion de crise ont été clairement illustrés dans les interventions de RSSI d'Opérateurs d'Importance Vitale.

Ils ont insisté sur les besoins d'industrialiser les mises à jour des systèmes, d'optimiser la gestion de crise, d'identifier les inventaires (sujet cité par presque tous les orateurs).

La gestion de crise & le SOC

Parmi les conclusions : ''la gestion de crise doit être interne à l'entreprise, mais le SOC est de plus en plus externalisé, notamment pour bénéficier de l'expérience d'experts, pour fédérer opérationnellement des expériences vécues de surveillance, de gestion d'incidents et last but not least pour faire face à la pénurie de ressources''.

Et, au final comme le dit Alain Bouillé, président du CESIN, le SOC externe est en soi une réponse à la résilience de la gestion de la sécurité.

Industrie, énergie et transports ...

Un autre point intéressant du CESIN 2018, la sécurité est devenue un sujet de premier plan pour l'industrie, pour le secteur de l'énergie, pour les transports, etc. On a l'impression que cette année nous avons moins parlé de finance et banque et plus de cybersécurité de la vie quotidienne. Tant mieux !

L'Internet des Objets, des capteurs reliés à l'Internet, notamment dans l'industrie et les transports introduit des nouveaux risques. Les 7 milliards de produits connectés via Internet passeront à 30 milliards d'objets équipés de capteurs et connectés, à l'horizon de 2020.

C'est la raison pour laquelle le marché de la cybersécurité est estimé à 248 milliards de dollars en 2023 contre 153 milliards en 2018 (source Les Echos).

La migration vers le Cloud ?

Enfin, ce qui se dégage du Congrès est l'importance fondamentale des processus continus de surveillance, d'analyse, d'identification des signaux faibles, de collecte et conservation des logs, dans un environnement certes outillé (SIEM, scans de vulnérabilités, flux de threat intelligence, analyse des données non-structurées, réputation, etc.) mais nécessitant fortement des analystes compétents.

La sécurité est un voyage pas une destination, un processus continu et régulier, adaptatif et prévisionnel, appliqué à un environnement de données protéiforme, évolutif et changeant. D'où l'importance de l'humain, depuis le cyber analyste jusqu'à l'ingénieur sécurité.

La conclusion du Congrès est celle donnée par le sondage rapide en Live pendant le congrès du CESIN: qu'est-ce qui pourrait rendre votre entreprise plus résiliente ? 81% des RSSI interrogés pensent que la migration du SI vers le Cloud favorise l'amélioration de la cyber-résilience.

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

Special Report

Maintenir une cyberdéfense à toute épreuve

Numérique et business sont indissociables aujourd'hui. Les perspectives d'évolution du chiffre d'affaires d'une entreprise sont à l'image de ce que peut proposer un monde totalement interconnecté et où tout est devenu « scalable » à souhait.

Pour une direction d'entreprise, il y a bien sûr le métier, mais il faut aussi compter sur le cœur technique de celle-ci, qui devient clairement son système d'information (SI). Son savoir-faire et sa valeur ajoutée sont quant à eux composés par les données qui y sont générées ou qui y transitent.

Une indispensable défense à quatre temps

Pour le PDG (le COMEX de façon générale), il est impensable de ne pas avoir de stratégie de sécurité, toutefois certains facteurs rendent plus difficile sa mise en œuvre.

On peut notamment citer un « time to market » accéléré par les technologies Cloud, le manque de compétences en sécurité en interne ou encore, un budget dédié inadéquat.

Pourtant, le ransomware WannaCry aura coûté à lui seul environ 92 millions de livres au National Health Service (NHS) britannique en divers coûts : interruption de services puis mises à jour des systèmes (ce qui implique deux phases, à savoir pendant et après l'attaque avec la restauration de systèmes).

Aujourd'hui, il faut effectivement envisager l'attaque en 4 temps : Prédire, prévenir, détecter et répondre. Les moyens de défense doivent naturellement prévenir mais il arrive que la menace ne soit détectée que lorsqu'elle est en cours d'action.

Ensuite, il faut pouvoir la nettoyer et s'assurer que cette dernière n'est pas restée cachée au sein des machines (ordinateur comme serveur) sur site comme dans le Cloud… Au risque d'obtenir une note salée comme l'a vécu le NHS dernièrement !

C'est d'ailleurs de cette manière qu'est organisée la gamme de produits de l'éditeur ESET, spécialiste européen de la sécurité informatique. Positionné en challenger dans le Magic Quadrant du Gartner pour les plateformes de protection Endpoint, il propose des produits qui agissent sur les 4 aspects : en prévention puis pendant et après l'exécution.

Une conformité à respecter dans le temps

Le risque Sécurité informatique est loin d'être négligeable d'autant qu'il faut compter sur les nouvelles réglementations (RGPD, NIS ...) à l'échelle européenne comme locale et qui obligent le COMEX à déclarer certains types de perte de données. Il est donc nécessaire que les directions d'entreprise mettent en œuvre une politique de sécurité adaptée.

Certaines solutions de sécurité aident à maintenir ce niveau de conformité. Ainsi, l'offre multicouches ESET agit sur les quatre paliers et pourra donc arrêter une menace en cours qui se serait infiltrée en l'arrêtant sur le deuxième voire le troisième niveau.

Des défis sécuritaires en croissance permanente

Selon une étude du cabinet d'analystes ESG, 79% des professionnels IT et sécurité des SI pensent que la cybersécurité en entreprise (en opérationnel, gestion, compétences...) est encore

plus compliquée aujourd'hui qu'elle ne l'était deux ans auparavant.

En cause ? On note l'augmentation du nombre de malwares (120 millions de nouvelles souches en 2017) combinée à un niveau de complexité plus important, mais également le nombre de nouvelles initiatives IT au sein de l'entreprise (Cloud computing, transformation digitale, applications IoT...).

On peut aussi y ajouter les cyberattaques ciblées (les attaques visent de 80 à 90% du temps un seul appareil selon ESG) ou encore le nombre croissant de matériels connectés au réseau.

Trafic réseau chiffré, Clouds hybrides (privé/public) sont autant d'autres raisons qui complexifient davantage la tâche des professionnels alors même que le budget Sécurité est en hausse pour près de 92% des entreprises, ceci ne règle pas le manque de considération envers la cyber-sécurité des métiers, ni le manque de ressources humaines dans ce secteur.

Adopter la « *Sécurité as a Service* » de haut vol pour compléter sa défense

Alors comment motiver ses équipes et faire le choix de la bonne stratégie quand on est COMEX ? Il est clair qu'au sein de l'entreprise, un certain nombre de CxO (CISO, CSO, CDO) sont nommés pour résoudre ce type de problématiques.

Pour autant, le CEO (et le COMEX d'une façon générale) est directement concerné par la moindre défaillance sécuritaire. Les récentes cyberattaques ont largement prouvé qu'une seule d'entre elles suffit pour impacter lourdement un business.

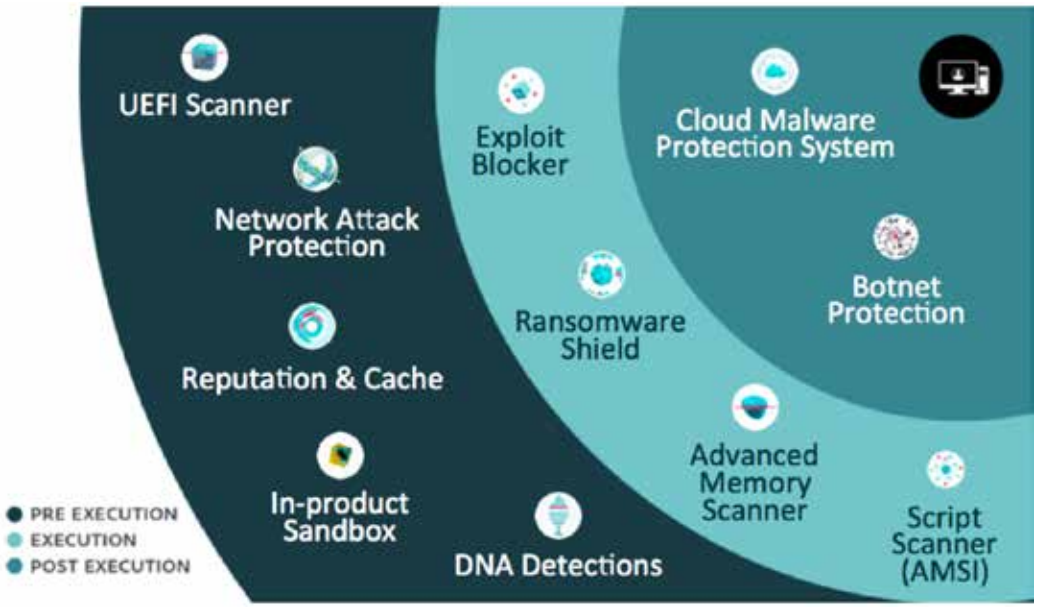
Et ce n'est pas faute d'avoir pris le parti d'investir dans la sécurité la plupart du temps. Il devient difficile pour les entreprises pourtant préparées d'être présentes sur tous les fronts. Sans compter qu'une attaque complexe exige des compétences pointues pour se défendre.

La « *Sécurité as a Service* » peut devenir une solution en faisant appel aux spécialistes de haut vol qui sauront venir soutenir les équipes internes d'une entreprise pour combattre, analyser, nettoyer voire mettre en place une solution rapidement.

Ces services peuvent également être souscrits auprès d'un MSSP. Celui-ci accompagne la création de la stratégie de sécurité de façon globale et l'applique au quotidien. Toutefois, lorsqu'une attaque complexe est en cours, il arrive que des compétences pointues et additionnelles en la matière soient requises pour le soutenir.

Certains acteurs du marché de la sécurité comme ESET ont su répondre à ce genre de nouveaux besoins de services de sécurité. « C'est pour cela que nous avons fait évoluer nos offres en y intégrant de nouveaux services adaptés à ce genre de situation comme Deployment and Upgrade, Threat Hunting, Threat monitoring et tout récemment Threat Intelligence » nous confirme Benoît Grunemwald, Directeur des Opérations France.

Protection multicouches : de multiples remparts



IA et Machine Learning essentiels contre les menaces

La cyber-menace évolue et il devient de plus en plus difficile d'arrêter la multiplication d'attaques notamment quand celles-ci sont ciblées et complexes.

En dépit de l'arsenal de protection installé, l'humain restera toujours le dernier rempart car c'est bien lui, et lui seul, qui est capable d'analyser et de détecter les menaces effectives.

L'institut AV-Test recense plus de 700 millions de variantes de malwares sur 2017 dont 120 millions ont été classées comme nouvelles.

Ces chiffres vertigineux montrent à quel point il est difficile pour les spécialistes de détecter toutes ces attaques en temps réel et ce même longtemps après ladite attaque.

L'IA (pour Intelligence Artificielle) couplé au Machine Learning (automatisation des tâches de base grâce à des patterns) semble être la solution au problème.

Ces deux technologies permettent de réduire le nombre de menaces à traiter par l'analyste (en limitant le nombre d'attaques qui auraient été mises de côté) et aident l'analyste à remplir sa mission dans des délais acceptables. Intégrer de l'IA et du Machine Learning au sein de produits ou de services demande cependant beaucoup d'expériences.

La base de données est l'une des clés de voûte de ce système et permet d'alimenter les algorithmes d'Intelligence Artificielle, bien que celle-ci ne se consolide pas en un jour, ni même en un mois voire une année !

La qualité de la base de données dépend de la pertinence des modèles choisis pour organiser les données. Par exemple, la société ESET alimente sa base de données depuis 30 ans.

Un Ecosystème nécessaire

A destination des SOC, par l'intermédiaire de fournisseurs de sécurité managée, les services de Threat Intelligence ESET s'appuient sur une épine dorsale commune : les flux techniques.

Ainsi, des Global SI ou des MSSP (Thalès, Orange Business CyberSecurity, Airbus CyberSecurity, Atos...) peuvent intégrer dans leurs offres autant des données sur les menaces que des services d'analyse à la demande ou de forensic.

Humain, Blog et LiveGrid : un cocktail d'expertises

ESET propose plusieurs sources d'informations qui facilitent l'accès aux connaissances dans le domaine de la Sécurité.
La première « WeLiveSecurity » : un blog dont le succès est dû à la qualité des informations qui y sont proposées, dont notamment les dernières tendances en termes de cybersécurité, les recherches en cours sur les menaces actives ainsi que des conseils en éducation de la sécurité.
La seconde source est ESET LiveGrid. Près de 110 millions d'appareils renvoient des informations à cette base et tous les clients d'ESET peuvent en profiter en temps réel.
Et pour finir : les experts d'ESET. Ils n'ont plus à faire leurs preuves et se déplacent même dorénavant au sein des entreprises pour soutenir les équipes internes lorsque celles-ci ont besoin de compétences pointues.

Fondée en 1992, la société ESET est spécialisée dans la conception et le développement de logiciels de sécurité pour les entreprises et le grand public (avec respectivement les rangs de 4ème et 5ème mondial). Pionnier en matière de détection proactive des menaces véhiculées par l'Internet, ESET est aujourd'hui le leader dans ce domaine. Il est désigné comme l'unique Challenger dans le Magic Quadrant 2018 de Gartner, catégorie Endpoint Protection Platforms*.

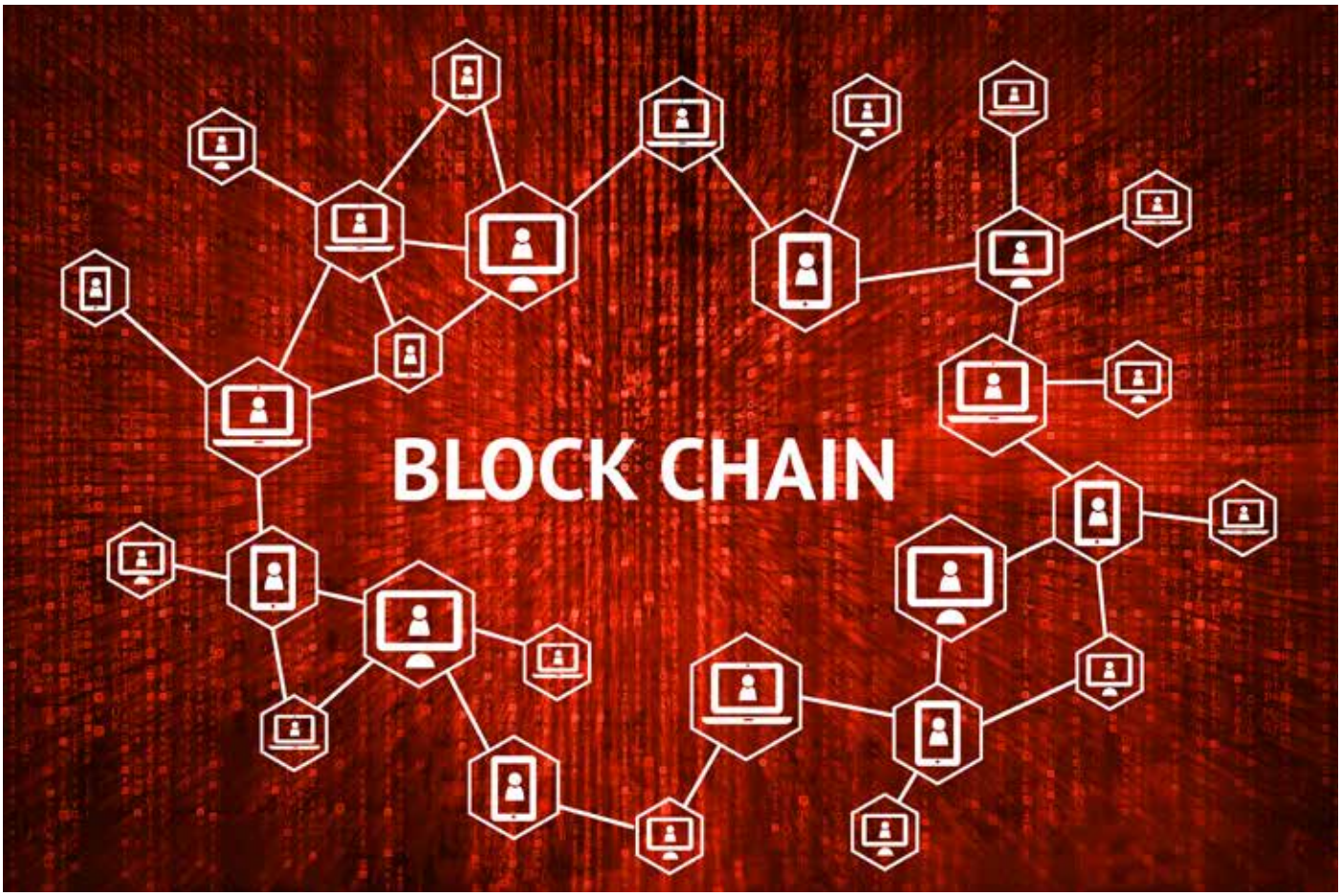
À ce jour, l'antivirus ESET NOD32 détient le record mondial de récompenses décernées par le laboratoire indépendant Virus Bulletin depuis 1998. Les solutions ESET sont reconnues et appréciées par plus de 110 millions d'utilisateurs dans le monde.

www.eset.com

La technologie Blockchain

LE FUTUR STANDARD DE LA GESTION DES IDENTITÉS ?

Ceux qui me connaissent déjà savent que je suis spécialisé dans deux domaines : La cybersécurité des systèmes d'exploitation et des annuaires ainsi que la gestion des identités. Quand je commence à parler de la Blockchain à mes interlocuteurs habituels, ils commencent à me faire de gros yeux, « Mais pourquoi donc nous parles-tu de la Blockchain ? » - « Quel est le rapport avec la gestion des identités ? » - « Toi aussi tu succombes à la mode, tu nous parles de la Blockchain ! ».



L'objectif est ici de répondre à ces interrogations bien naturelles et de fournir des pistes pour comprendre pourquoi et comment la Blockchain va transformer le métier des spécialistes de la gestion des identités.

L'objet de cet article n'est pas de vous décrire en détail ce qu'est la Blockchain, vous trouverez très facilement sur Internet de nombreux articles de vulgarisation traitant de ce sujet, l'objectif est ici de vous expliquer en quoi cette technologie est potentiellement une révolution dans le domaine de la gestion des identités.

Pour bien comprendre cela, commençons par comprendre rapidement les principes généraux de la technologie Blockchain.

Les caractéristiques de la Blockchain

Le principe de la Blockchain est caractérisé par les éléments suivants (figure 1 ci-contre).

Microsoft a réalisé un excellent Livre Blanc (en Français) vous permettant de découvrir les principes généraux de la Blockchain et les impacts sur

les différents métiers en entreprise, car vous l'avez compris, les principes fondateurs de la Blockchain sont particulièrement intéressants pour de nombreux métiers dans l'entreprise (gestion des contrats, traçabilité, transport, etc.).

Ce livre blanc est accessible sur cette adresse : https://aka.ms/blockchain-entreprise – je vous conseille très vivement sa lecture, c'est un point de départ idéal.

De plus, je vous conseille un site pour « tester » en ligne la technologie Blockchain et surtout comprendre son fonctionnement de manière très visuelle : https://blockchaindemo.io (figure 2).

Pour finir notre introduction à la Blockchain, il faut savoir qu'il existe plusieurs « versions » de cette technologie, chaque version de cette technologie amenant des subtilités de fonctionnement, de sécurité et de performance à son usage. Je citerai, sans être exhaustif : Ethereum, Quorum, Corda, BlockStack, etc.

Certaines « versions » sont plus appropriées en fonction des usages et des objectifs métiers liés à l'implémentation de cette technologie, mais finalement, les principes fondateurs restent et demeurent identiques.

Figure 2 : interface du site blockchaindemo.io

Le BaaS (Blockchain as a Service)

Le principal frein à l'usage de la Blockchain dans une entreprise est représenté par deux évidences.

- La barrière technologique à l'entrée : en effet, mettre en œuvre une application métier basée sur la Blockchain n'est pas si évident pour une entreprise qui n'a aucune expérience dans ce domaine
- Le manque de consultants capés sur ce sujet : les formations universitaires ne sont pas encore à jour sur ces sujets et les vrais spécialistes sont pour la plupart des autodidactes. Les compétences sont actuellement très rares (et donc très chères) sur le marché

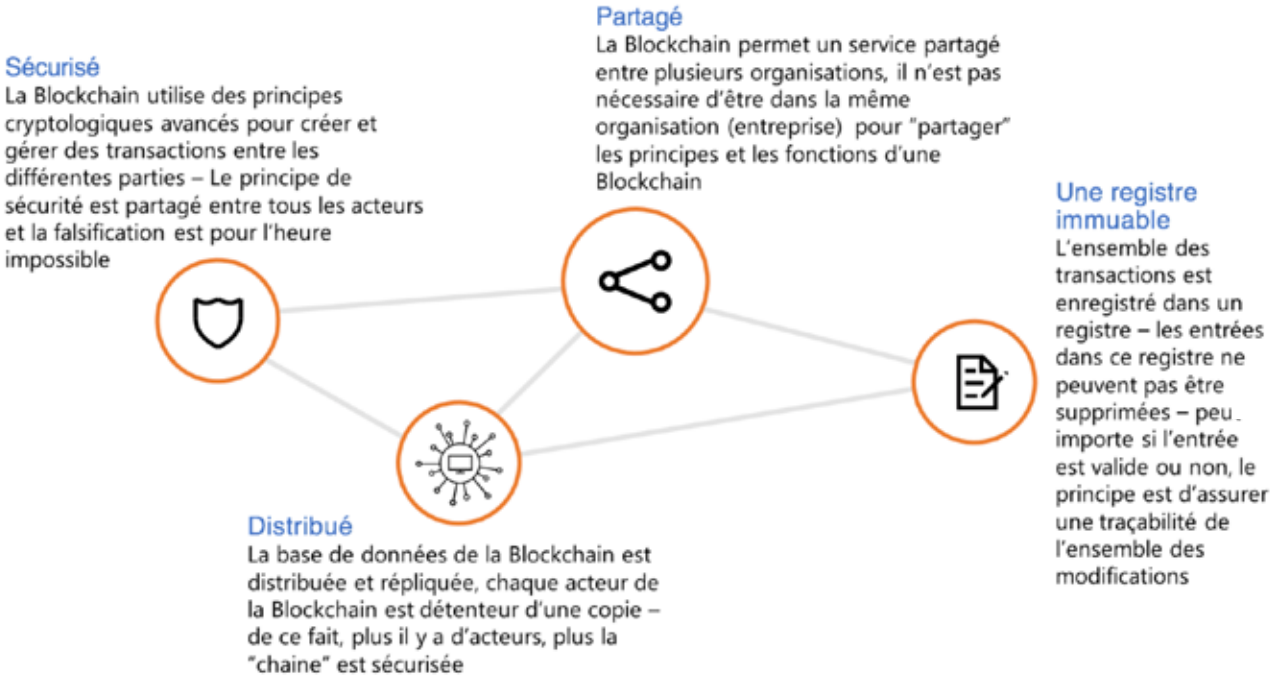


Figure 1 : les principes de la Blockchain

C'est pourquoi les principaux acteurs IT du marché développent actuellement des offres de Blockchain as a Service qu'ils insèrent petit à petit dans leur offre de Cloud public – l'objectif est de rendre le « ticket d'entrée » à la technologie plus accessible à l'ensemble des organisations. Nous pouvons citer comme exemples les offres suivantes :

- Microsoft Azure Blockchain Service
- IBM Blockchain Platform
- Amazon Blockchain Templates
- Alibaba BaaS
- Oracle Blockchain Cloud Service

Comme souvent en ce qui concerne les services Cloud aux entreprises, les deux leaders dans le domaine du BaaS restent sans conteste Microsoft et Amazon.

Si vous voulez tester la technologie, je vous conseille vivement d'utiliser ces services afin d'évaluer si cela correspond à vos attentes, c'est le moyen le plus simple et le plus sûr d'accéder à la Blockchain et de comprendre son application sur les différents métiers de l'entreprise.

Pourquoi utiliser la technologie Blockchain dans le cadre de la gestion des identités ?

Sécurisé, partagé, distribué et immuable... Avouez que cela ressemble à un rêve pour toute organisation voulant implémenter des principes de gestion des identités !

En effet, les caractéristiques intrinsèques de la Blockchain sont particulièrement adaptées aux problématiques de gestion des identités, donc il semble naturel de constater que de nombreuses initiatives ont démarré pour adapter l'usage de la Blockchain dans le cadre de cet usage.

En effet, depuis des années, nous essayons d'intégrer diverses technologies pour assurer les principes d'authentification et d'autorisation, nous pouvons lister : les annuaires centralisés, CAS, Kerberos, la fédération d'identité, OpenID Connect, les cartes à puces, le MFA, le no-password, et la liste est encore très longue ! Imaginons maintenant une technologie fondatrice permettant d'éliminer tous freins naturels à l'usage des identités, c'est finalement, la promesse de la Blockchain. (voir figure 3)

Il reste à noter que la technologie Blockchain peut s'adapter à plusieurs niveaux de participation de chaque individu ou de chaque machine participant à la Blockchain, permettant ainsi d'ajuster la participation de chaque « identité » au fonctionnement globale de la Blockchain.

- Node : ordinateur qui participe au réseau de la Blockchain et qui est capable d'envoyer ou de recevoir des transactions
- Full node : ordinateur qui réalise les mêmes opérations qu'un 'node' mais qui possède également une copie des différentes transactions réalisées dans la Blockchain
- Master node : ordinateur possédant les différentes transactions mais possédant également des données additionnelles sur les transactions non confirmées et sur les « erreurs » – il faut voir le master node comme une espèce d'arbitre sur

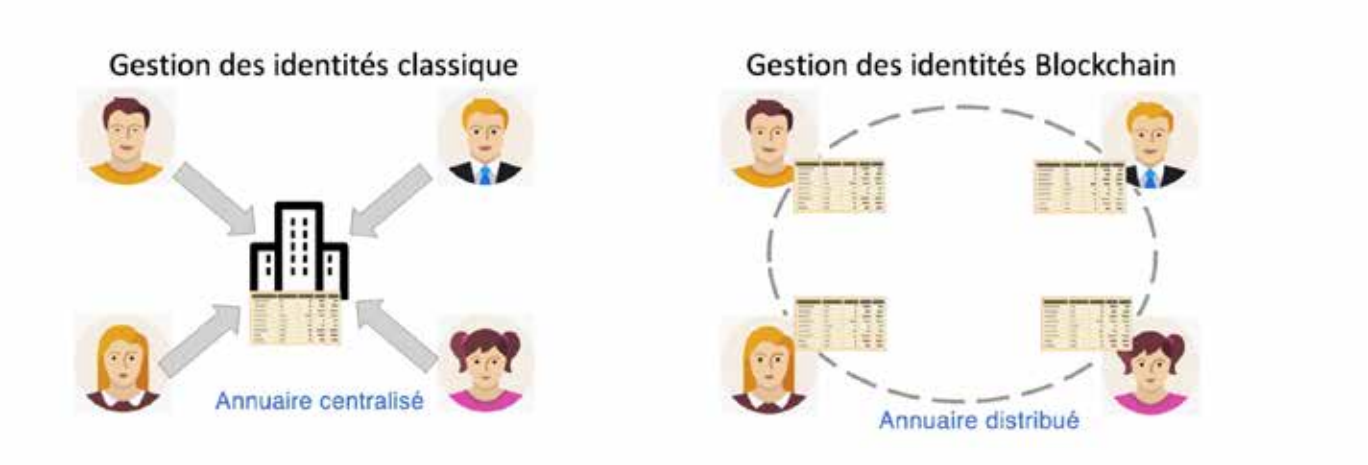


Figure 3 : gestion des identités classique et basée sur la Blockchain

les transactions permettant d'avertir les autres nodes du réseau

Comme vous le voyez, nous pouvons mélanger le principe de distribution avec un principe d'arbitrage centralisé en cas de conflit – cette architecture est bien évidement particulièrement adaptée à la gestion des identités.

Globalement la technologie Blockchain adaptée à la gestion des identités permettra de répondre aux problématiques suivantes :

- Construire une plateforme universelle de gestion des identités
- Réduire les activités de fraude et d'usurpation d'identité
- Partager des identités entre des organisations diverses
- Permettre à un individu de créer et gérer sa propre identité
- Remplacer les « usernames » et les « passwords »

Il est notamment très intéressant de constater que cela permet d'utiliser des identités dans un contexte Entreprise (identité Business) mais aussi dans un contexte Gouvernemental (identité du Citoyen).

Pour compléter votre approche afin d'appréhender comment la Blockchain peut aider votre organisation dans le domaine de la gestion des identités je vous conseille la lecture de ces deux articles (en anglais) :

- "How to use Blockchain technology for Identity": https://bit.ly/2L0RIVU
- "How Blockchain can solve identity management problems": https://bit.ly/2EfSxKu

Des initiatives multiples autour de la gestion des identités

- **La Decentralized Identity Foundation**

Une organisation tente actuellement de fédérer et structurer les approches de gestion des identités au travers de la Blockchain, il s'agit de la DIF (Decentralized Identity Foundation) – cette organisation travaille à définir les nouveaux standards en termes de gestion des identités, en adoptant un modèle basé sur la Blockchain, vous pouvez consulter leur site sur cette URL : https://identity.foundation/

Les membres de cette organisation sont principalement des acteurs prédominants dans le monde de la gestion des identités et des accès, mais aussi des startups investissant ce sujet : (figure 4)

- **lifeid.io**

La startup lifeID, basée à Bellevue, non loin de Seattle tente de créer un framework OpenSource permettant à une organisation commerciale ou gouvernementale de créer un service de gestion des Identités basé sur la Blockchain. Ils utilisent la technologie ArcBlock.

Je dirais que leurs travaux portent principalement sur la gestion des identités du côté gouvernemental, leur idée fondatrice est de proposer un protocole basé sur la Blockchain en éliminant tant que possible les problèmes de performance liés aux transactions.

- **Microsoft**

Microsoft est extrêmement actif dans ce domaine. Plusieurs sources vous permettront de comprendre dans quelle direction le géant de Redmond se dirige :

- Microsoft COCO Framework : L'objet de ce Framework dédié à la Blockchain est de renforcer les principes de sécurité : https://bit.ly/2B6PwYr
- Livre Blanc « Decentralized Identity » : Un livre blanc succinct mais permettant de décrypter les avancées de Microsoft en la matière : https://bit.ly/2PkcAvX
- Le kit de développement (SDK) de Microsoft sur la technologie Blockchain : https://bit.ly/2zd1EXm

Mon sentiment est que Microsoft a détecté dans la technologie Blockchain un moyen évident de résoudre de nombreux problèmes liés à la gestion des identités traditionnelle, de nombreux articles, des offres Cloud, des SDK, tout cela nous prouve un investissement massif de l'éditeur.

- **Les projets de recherche universitaire**

De nombreux sujets de thèse se sont emparés de cette technologie et de son application dans le domaine de la gestion des identités. De plus, de nombreux laboratoires étudient l'association du modèle de la Blockchain avec certains principes mathématiques ou de probabilité pour améliorer la fiabilité ou le modèle décentralisé du mécanisme.

Nous pouvons citer notamment des projets de recherche visant à coupler la technologie Blockchain avec les concepts de « Preuve à divulgation nulle de connaissance » - Pour aller plus loin dans ce domaine, je vous conseille la lecture d'un article Wikipédia sur ce sujet : https://bit.ly/2zFThEb

J'espère que la lecture de cet article vous aura éclairé sur les intérêts de la Blockchain en termes de gestion des identités. C'est un sujet neuf, je vous l'accorde, mais tout spécialiste sérieux de l'IAM doit suivre ces évolutions de façon étroite.

Les entreprises que je rencontre n'ont pas souvent réalisé des projets en production, néanmoins de nombreux projets de « preuve de concept » sont en cours, le train est lancé.

Et si la Blockchain Identity devenait votre prochain critère de succès dans votre activité Business ? Pensez-y de façon très sérieuse.

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)
Ensaignant à l'ESGI et à l'Université de Grenoble

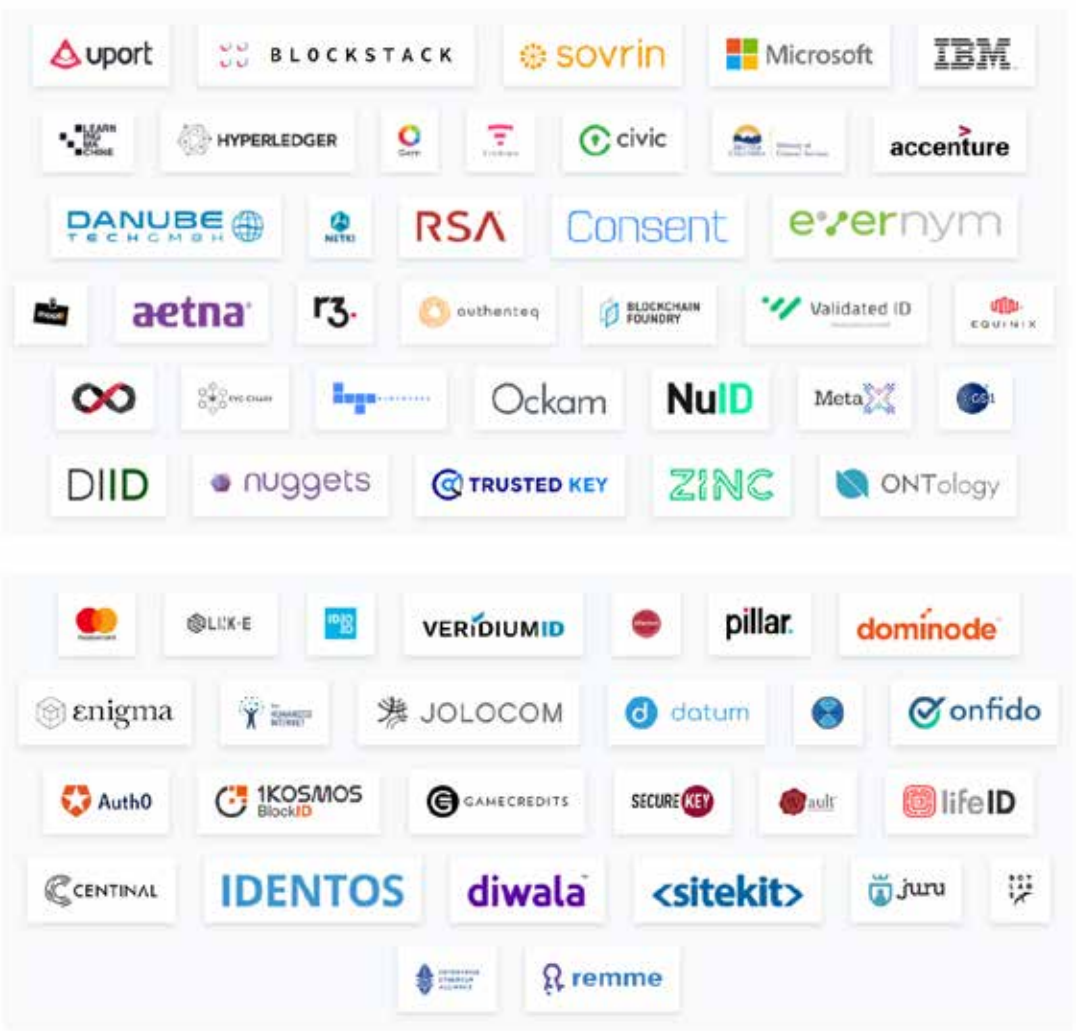


Figure 4 : membres de la Decentralized Identity Foundation (DIF)

Digital Workplace

iCD&R

Intranet - Communication Interne - Collaboratif - RSE

Le Salon de la DIGITAL WORKPLACE, de l'Intranet, de la mobilité, du Travail Collaboratif & du RSE

19*, 20 et 21 mars 2019 (à partir de 14h)

Paris Expo

Porte de Versailles

En partenariat :

iTPro.fr SMARTDSI

En parallèle :

documation

data intelligence forum expo

SOLUTIONS RH Ressources Humaines

eLearning expo

Gold Sponsor :

Jalios catalyseur d'intelligence collective

www.salon-intranet.com

Comment consommer différemment
LA CYBERSÉCURITÉ

A l'heure de l'entreprise hyperconnectée, l'ancien modèle de la sécurité en entreprise n'est plus en phase avec les nouveaux environnements et l'avenir est profondément bouleversé. Comment accéder, évaluer et adopter rapidement les nouvelles technologies et se doter de nouveaux moyens pour contrer les cybermenaces permanentes ?

Palo Alto Networks veut accélérer la transformation des entreprises et s'en donne les moyens. Résultats, acquisitions, produits, croissance ... une stratégie à la hauteur des défis. Entretien avec Alexandre Delcayre, Directeur, Systems Engineering, Southern Europe, Russie et Israël.

Des acquisitions riches de sens

Après Secdo (détection & remédiation), puis Evident.io (compliance) en mars 2018, l'acquisition de Redlock (sécurité analytics pour le Cloud public & visibilité & remédiation) en octobre, offre aux clients des capacités d'analyse de sécurité dans le Cloud et complète la stratégie globale de la société « pour asseoir son leadership en termes de sécurité dans les Cloud publics ».

L'objectif est bien d'avoir des fonctions multi-cloud de data analytics et maximiser l'approche Intelligence Artificielle (corrélation entre les données & détection sur les menaces), « la synergie est bonne, nous ajoutons une brique détection et remédiation automatisée à la brique conformité ».

Il est, ainsi, aisé de livrer au client les éléments non conformes et lui proposer les actions correctives dans son instance.

On retrouve ici la volonté du CEO de Palo Alto Networks, Nikesh Arora, de « devenir le leader en termes de cybersécurité dans les environnements multi-cloud ».

Security Operating Platform = répondre aux besoins des entreprises

Quatre points clés caractérisent cette plate-forme, les voici résumés.

Notons d'ores et déjà la visibilité totale qui permet de comprendre le contexte global de l'attaque. Puis vient la réduction de la surface d'attaque.

En effet, les fonctions sont intégrées nativement dans l'architecture pour avoir un meilleur contrôle sur les applications, utilisateurs, contenus des données utilisées.

La prévention rapide et coordonnée des attaques connues, notamment sur les différents éléments composant l'attaque (poste du travail, réseau, Cloud) est essentielle.

La détection et prévention des menaces inconnues avec une automatisation native simplifie les process, « sans automatisation, on ne suivra pas la cadence, et les systèmes hautement automatisés sont complémentaires à l'humain ».

Alexandre Delcayre

Les défis des RSSI

Les préoccupations des RSSI sont nombreuses. Si leur rôle a évolué, les derniers rapports révèlent un grand changement avec une demande forte en visibilité et conformité, « l'inquiétude est réelle face aux nouveaux challenges d'autant que l'accélération vers le Cloud élargit la flexibilité mais augmente les surfaces d'attaques ».

Ainsi, l'approche de Palo Alto est d'apporter plus d'intelligence et d'automatisation au niveau des services fournis pour développer l'analyse comportementale et simplifier la vie des clients, « en s'orientant vers une plate-forme de sécurité globale agile et hautement automatisable, les mécanismes doivent automatiser la prévention, la détection et la remédiation ». Il est impossible de créer des règles pour tous les cas de figures mais « amener l'IA, le machine Learning et l'automatisation est vital pour s'adapter aux adversaires ».

Quid de la Cyber Trust ?

Même s'il existe des dénominateurs communs, les enjeux ne se situent pas au même niveau selon la taille des entreprises.

Il faut donc se recentrer sur la notion de « trust » : façon d'organiser l'entreprise, de gérer les services, d'interagir avec les fournisseurs et tiers, et gérer le risque, « les entreprises sont invitées à y penser fortement, avec la réglementation européenne notamment, d'autant que le niveau des menaces augmente, elles sont obligées de revoir les process et règles en termes de gouvernance de données ».

La Digital Identity est un autre point clé, « on remarque une accélération par rapport à la manière de gérer et d'encadrer le fonctionnement et la sécurité autour de l'utilisateur ».

Enfin, la confiance dans les infrastructures, utilisateurs, fournisseurs prend le pas, « il faut préserver la chaîne de confiance externe et interne (propriété intellectuelle) ».

> Par Sabine Terrey

Identités et le défi sous-estimé
D'UNE INTÉGRATION OFFICE 365

Lors de la fusion ou de l'acquisition de sociétés, la question de l'intégration des systèmes d'informations se pose. Dans la plupart des cas plusieurs scénarios sont possibles.

Le plus logique mais parfois le plus compliqué, se trouve être la fusion, le second dit intégration généralement plus rapide consiste à interconnecter ce système d'informations via des approbations mutuelles entre les différents environnements. Dans les deux cas il faudra, à un moment, établir une cohabitation, une coexistence des systèmes qui permettra rapidement aux utilisateurs des filiales acquises de pouvoir accéder aux applications métiers du groupe.

Généralement, cette coexistence n'est pas un but en soi, il s'agit plutôt d'une étape transitoire qui permet aux forces de vente, aux responsables métiers d'intégrer directement les applications du groupe. Cette coexistence devra ensuite céder la place à une véritable fusion qui peut comprendre à terme la suppression du système d'informations de la nouvelle filiale.

L'objectif dans ce cas est d'obtenir, à travers un annuaire unique, des services homogènes pour le groupe (messagerie, intranet, portails collaboratifs, téléphonie, etc.).

Outre la migration des données, la question des identités va alors se poser. Sans Identité, pas de projet de migration.

Dans l'environnement Microsoft, l'annuaire technique de l'entreprise est représenté par l'Active Directory. Lors de l'acquisition de nouvelles sociétés la question se pose donc d'intégrer l'ensemble de ses utilisateurs, leurs stations de travail, leurs serveurs mais parfois leur environnement Office 365 vers les infrastructures du groupe. Le premier chantier qu'il faudra donc adresser est sans nul doute l'identité. Combien de compte utilisateurs sont à reprendre ? Comment sont gérés les comptes de sous-traitants, quelle est la politique de gestion des identités dans la nouvelle filiale ?

Sans la définition du projet de fusion ou d'intégration des identités, les autres services ne pourront pas migrer.

C'est le premier chantier qu'il faudra adresser. C'est précisément ce que nous vous proposons d'étudier

Les scénarios possibles

Il existe en réalité 2 grands scénarios envisageables lorsqu'une acquisition de société se produit.

L'intégration

Le premier scénario dit d'intégration, part du principe que l'environnement de cette nouvelle société va perdurer. Dans ce cas, les identités d'annuaire devront être conservées et devront être synchronisées vers Azure AD si le groupe possède un environnement Office 365. La mise en place de relations d'approbation entre ces deux environnements permettra de pouvoir facilement partager des ressources, via des processus d'authentification mono ou bidirectionnel.

Ce scénario peut bien évidemment se répéter, permettant aux nouvelles acquisitions, de rapidement intégrer les ressources du groupe.

C'est parfois le cas lorsque la société rachetée conserve sa propre identité ou ses propres marques. Dans ce cas, l'intégration est simple, les utilisateurs conservent leur identité propre, leur adresse de messagerie, leur identifiant de messagerie instantanée etc...

D'un point de vue architecture, les deux forêts coexistent de part et d'autre avec des serveurs contrôleurs de domaine déployés dans chaque agence respective. On notera au passage que ce mode de fonctionnement peut cependant poser quelques soucis de mobilité lorsqu'un utilisateur du groupe tentera de se connecter depuis un réseau de la filiale.

Sans la définition du projet de fusion ou d'intégration des identités, les autres services ne pourront pas migrer

Dans notre cas, les processus de synchronisation des annuaires comme Azure Ad Connect vers Office 365, prennent en charge ces scénarios, et sont parfaitement adaptés à ces situations.

Malgré cela, et malgré cette relative simplicité, des adaptations sont souvent souhaitables et entreprises, comme par exemple, l'homogénéisation des adresses de messagerie, l'uniformisation du nommage des ressources comme peuvent l'être les salles de réunion, les listes de distribution, les groupes de sécurités. L'objectif est alors d'offrir aux utilisateurs un annuaire unique et homogène dans lequel ils pourront se repérer et adresser des ressources entre les diverses entités.

Cette intégration, peut être également améliorée si les deux entreprises possèdent notamment des systèmes de messagerie basés sur les mêmes technologies comme Microsoft Exchange.

Dans ce cas, des interactions dites « riches » sont possibles comme le fait de pouvoir rechercher les plages libres occupées des collaborateurs situés dans une autre filiale. Plus simplement si le groupe a choisi la messagerie Exchange Online de Microsoft, les identités de la filiale étant synchronisées, il sera alors assez simple de migrer les données de messagerie de cette dernière vers ce nouvel environnement.

Dans ce scénario, les processus de Gestion des Identités et des Accès (IAM) du groupe seront également mis à jour. Ils devront prendre en compte a posteriori ce nouvel environnement, et pouvoir l'adresser lorsque que des nouvelles identités devront être créées ou supprimées. Cela passe généralement, par une remise aux normes du groupe de ce nouvel annuaire, en "populant" notamment des identifiants uniques (Matricules, Identifiant) sur les objets tels que les comptes utilisateurs, les comptes sous-traitants etc... Là encore, l'objectif n'est de ne pas faire disparaître l'annuaire de la filiale mais bel et bien de l'intégrer dans les processus de gestion d'identité du groupe.

La fusion

Le second scénario que nous nommerons fusion, consiste à considérer que l'annuaire de la filiale acquise, a pour objectif de disparaître. Seules les données utilisateurs seront reprises, les identités propres à l'environnement filiale devront par conséquent être ignorées des processus de synchronisation. Dans la plupart des cas, l'ensemble des utilisateurs ainsi que leurs stations de travail et les ressources serveurs (pour ne citer que celles-ci) devront migrer vers l'environnement Active Directory du groupe.

Ce scénario est bien évidemment plus complexe, plus long mais l'intégration à terme sera plus aboutie. Tout le monde sera intégré dans la seule et unique forêt Active Directory du Groupe.

Dans ce cas précis, la question est donc de savoir comment réaliser cette fusion d'identité, tout en intégrant la migration des données s'y rattachant. Là encore, sans identité pas de projet de migration.

Comment, par conséquent, intégrer les données d'une nouvelle société dans l'environnement Office 365 & Active Directory d'un groupe, sans synchroniser ses données d'annuaire, sachant que les données et leur accès sont intimement liés ?

La première des choses à faire, est de créer dans l'environnement destination (environnement Groupe) ces mêmes identités et de les synchroniser le cas échéant dans l'environnement Office 365. Une clé commune devra être établie entre les deux environnements

d'annuaire pour s'assurer qu'une relation de type un à un pour les comptes utilisateurs notamment peut être établie. Les utilisateurs posséderont deux comptes, un dans leur forêt d'origine, un dans la forêt du groupe.

Dans la plupart des cas, la création de ces nouvelles identités se fait en fonction des normes en vigueur du groupe ainsi, il n'est pas rare que le formalisme des noms de connexion soit différent vis-à-vis de la filiale.

Si le groupe utilise Office 365, le nom de connexion des utilisateurs (UPN) sera généralement identique à leur adresse de messagerie principale (@agency.com par exemple), ce qui obligera la filiale en cas de relations d'approbation bidirectionnelle à ne plus l'utiliser au profit de l'annuaire groupe. (Suppression de l'UPN dans la forêt source en cas de relation d'approbation bidirectionnelle).

Sans identité pas de migration !

Pour des questions d'accès aux ressources des agences, la création de ces comptes utilisateurs, devra également prendre en compte leur ancienne identité et plus particulièrement ce que l'on nomme le Sid History. Ce Sid History permettra aux utilisateurs devant utiliser leur identité au sein du groupe de continuer à avoir accès à leurs anciennes ressources comme par exemple les services de fichiers.

Comme l'annuaire de l'agence doit disparaître, et par conséquent ne doit pas être synchronisé vers 0ffice 365, il va être également nécessaire de récréer l'ensemble des groupes de sécurité et de distribution hérités vers l'annuaire du groupe en prenant soin là aussi de conserver leurs Sid History (Groupe de sécurité uniquement).

La plupart des entreprises en profite souvent pour les renommer de façon à ce qu'ils suivent la nomenclature en vigueur, (on parle alors de transposition des données d'annuaire plutôt que de duplication). Comme le scenario de fusion est un processus qui va durer, le temps que toutes les stations de travail intègrent la nouvelle forêt, cette transposition devra être maintenue pour permettre le déplacement des ressources vers ces nouvelles identités.

Une fois cette transposition mise en place et maintenue, le déplacement des ressources peut avoir lieu. Ce dernier devra s'appuyer et prendre en compte cette transposition d'identité pour modifier les autorisations héritées et les remplacer par les identités du groupe.

C'est ce que font généralement les outils de migration en intégrant comme Sharegate une table de correspondance des identités dans le cadre de la migration des ressources Sharepoint qu'elles soient hébergées sur site ou sur 0ffice 365. (Migration Tenant à Tenant)

Une fois migrés les utilisateurs connectés avec leurs comptes dans la forêt du groupe retrouveront leurs accès sur leurs sites Sharepoint.

Pour la migration des boîtes aux lettres & des dossiers publics, si la filiale utilise l'environnement Exchange, la migration est plus complexe et mériterait à elle seule une publication approfondie.

Cependant, en dupliquant les attributs messageries des utilisateurs de l'environnement Source, vers la forêt de destination, sachez qu'il est possible d'effectuer des déplacements de boîtes aux lettres (Move Mailbox) depuis la filiale vers l'environnement du groupe en rattachant ces boîtes aux lettres vers les identités groupe.

Ce déplacement des boîtes aux lettres ayant comme particularité la conservation de l'attribut Mailbox Guid, il permettra la mise à jour automatique du profil Outlook de vos utilisateurs vous évitant une intervention sur chaque poste de travail.

L'identité comme nous avons essayé de vous le démontrer, bien souvent sous-estimée, **joue par conséquent un rôle déterminant dans les projets d'intégration et selon le niveau de complexité, peut remettre en cause votre stratégie de migration.**

Analyser comment se feront ces fusions, ces adaptations et les conséquences de leurs modifications sur l'environnement applicatif est primordial pour construire un plan projet réaliste. Cela doit constituer une des premières étapes à prendre en compte.

Sans identité pas de migration !

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

La Digital Workplace à l'horizon 2022 ...

Collaboration, communication, mobilité, réseaux sociaux, poste de travail... Au sein d'un monde de plus en plus connecté, l'organisation des entreprises ne cesse d'évoluer pour s'adapter. Quelles seront les tendances dès 2021 ?

Un environnement intelligent centré sur l'utilisateur

La nouvelle Digital Workplace doit désormais intégrer tous les outils de collaboration et de social pour répondre rapidement aux usages des collaborateurs, en rassemblant l'e-mail, la messagerie instantanée, les médias sociaux, les applications RH, les outils de réunions virtuelles...

Les entreprises veulent disposer d'un environnement de travail souple, simple et personnalisé selon les besoins et d'une approche unique pour tous les services aux utilisateurs.

Les 5 attentes des entreprises

Si 71% des entreprises sont globalement convaincues de l'utilité du Digital Workplace (Direction - Ressources Humaines - Management), 80% ont déjà engagé leur transition vers un environnement plus numérique. Parmi les 4 principaux outils de Digital Workplace, on note :

- Office 365 - 41%
- Google Suite - 23%
- Slack - 19%
- Trello -17%.

Et pourtant des outils français innovants comme Jamespot, Jalios... répondent parfaitement aux enjeux de la Digital Workplace.

Voici les 5 attentes des entreprises

- Gagner en agilité et productivité
- Décloisonner les projets et métiers et faciliter le partage d'informations
- Replacer le collaborateur au centre de l'organisation du travail
- Accélérer l'innovation et la conduite du changement
- Permettre une meilleure collaboration des équipes géographiquement dispersées

Les 5 actions pour la Digital Workplace du futur

Pour mettre en place cette Digital Workplace du futur qui transformera la collaboration, les entreprises s'engagent dans de nouvelles démarches. Résumons les 5 actions clés :

- Désiloter l'organisation pour de nouvelles méthodes de travail collaboratif
- Identifier les usages et construire de nouveaux parcours employés
- Sensibiliser et accélérer la prise de conscience au sein de l'entreprise
- Former les collaborateurs, accompagner l'évolution des savoir-faire et savoir-être
- Faire le bon choix des outils

Source : Etude Digital Workplace - Umanis

Top 5 des enjeux de l'indispensable modernisation du datacenter

Moderniser son infrastructure informatique en adoptant une approche hybride est devenu une nécessité et, pour certains, une urgence. Une transformation dictée par 5 enjeux majeurs…

Le numérique transforme tous les usages, tous les métiers, tous les secteurs. Il impose de nouveaux rythmes beaucoup plus rapides et une agilité nouvelle. Il invite à repenser tous les processus ainsi que de nombreuses offres commerciales pour les adapter à cette nouvelle donne.

Il induit une transformation des outils, des plateformes et des technologies pour permettre aux entreprises, quelle que soit leur taille, de gagner en souplesse et en réactivité afin de rester en phase avec des marchés en pleine évolution, marqués par de nouveaux modèles économiques et de nouvelles interactions relationnelles.

D'autant que le numérique a conduit à une plus grande mobilité des personnes et une multiplication d'appareils et d'objets connectés générant un afflux massif des données qu'il faut, non seulement, pouvoir absorber, mais aussi, analyser pour en exploiter la valeur.

Big Data, mobilité, Cloud, imposent aux équipes informatiques de s'adapter, de se réorganiser et de repenser l'infrastructure de production pour soutenir ses nouveaux usages, s'aligner aux nouveaux besoins métiers et soutenir leurs initiatives tout en garantissant la conformité des processus et la sécurité des appareils, des données et des personnes.

Cette transformation numérique conduit à l'ère de l'informatique « hybride ». Elle est hybride parce qu'elle mêle étroitement ressources privées et ressources cloud publiques. Elle est hybride parce qu'elle fusionne les besoins de centralisation et la nécessité de placer de l'intelligence au plus proche des sources de données.

Elle est hybride parce qu'elle encourage IT, développeurs et métiers à mieux travailler ensemble. Elle est hybride parce qu'elle redistribue intelligemment les ressources et les applications pour allier sécurité, conformité, élasticité, et optimisation des coûts.

« L'agilité est le principal avantage de cette informatique hybride » souligne Arnaud Brozzi, spécialiste Infrastructures chez inmac wstore. « Elle permet une réactivité face aux changements rapides, ce qui est fondamental dans la digitalisation de notre business. Le mix entre clouds privés, clouds publics et des ressources On Premises aide les entreprises à gagner en agilité et à renforcer leur avantage concurrentiel ».

Pour arriver à cette agilité, il est, donc, impératif de moderniser le datacenter. Cette modernisation repose sur 5 enjeux majeurs…

1/ Consolider

La virtualisation des serveurs a offert aux entreprises une première opportunité de consolider leurs infrastructures afin de les simplifier et d'en optimiser les coûts opérationnels.

Il faut, aujourd'hui, aller plus loin. De nouvelles solutions techniques ont fait leur apparition permettant une réduction des espaces occupés par des ressources physiques au sein du datacenter.

Des technologies évolutives comme les systèmes hyperconvergés (HPE Simplivity, par exemple) ou les systèmes composables (systèmes HPE Synergy) offrent en la matière de nouvelles opportunités.

2/ Moderniser

Il est important de moderniser à la fois les équipements, les processus, et les méthodologies. La modernisation des équipements simplifie le processus de consolidation évoqué précédemment.

Elle permet, surtout, d'adopter de nouvelles approches « Software Defined » qui présentent les différentes ressources (compute, stockage, network) sous forme de pools que l'on peut allouer et désallouer à la demande et dynamiquement.

Une approche qui invite à repenser les processus d'administration et contribue à faire du département informatique un prestataire de services : en associant les ressources du cloud privé et des clouds publics, il propose un patrimoine de services d'infrastructure (IaaS), de VMs as a Service et de Containers as a Service, qui contribuent à accélérer la réalisation des projets.

La modernisation passe aussi par l'adoption de nouvelles méthodologies de développement et de déploiement pour permettre une livraison continue des applications.

3 / Automatiser

Le concept d'informatique hybride défend un modèle « low-ops » dans lequel les tâches manuelles d'exploitation sont réduites au minimum. Les composantes d'infrastructure modernes sont, désormais, intégralement pilotables par des APIs concrétisant l'idée d'une « Infrastructure as Code » dans laquelle tout est automatisé, tout est surveillé et géré de façon centralisée.

L'objectif, c'est de voir désormais les équipes IT passer 80% de leurs temps à apporter de la valeur aux métiers et à élaborer de nouvelles solutions plutôt que de passer 80% de leur temps à maintenir en état opérationnel un existant chronophage et vieillissant.

4/ Transformer (Agilité & Flexibilité)

Consolider, moderniser et automatiser ne porteront leur fruit qu'en transformant le fonctionnement des équipes et les processus organisationnels afin d'acquérir l'agilité et la flexibilité recherchées et justement permises par les nouvelles approches hybrides.

En effet, la vocation même d'une telle informatique est de permettre aisément de placer les applications sur différentes plateformes internes ou externes en fonction des contraintes de temps, des besoins d'élasticité (par exemple, en utilisant le cloud public pour absorber des pics exceptionnels et éviter de sur-provisionner les ressources internes), des besoins de proximité (être au plus proche des clients ou au plus proche des sources de données), des volontés d'optimiser les coûts, mais aussi, de mieux gérer les contraintes de sécurité.

5/ Sécuriser

La cybersécurité est devenue une préoccupation majeure de toutes les entreprises d'autant que les réglementations se font, désormais, beaucoup plus sévères et pressantes à l'image du nouveau règlement européen sur la protection des données (RGPD). La diversité et l'ingéniosité des attaques nécessitent de maintenir toujours à jour ses équipements, de centraliser les journaux pour repérer les signaux faibles grâce au Machine Learning, d'ajuster automatiquement les niveaux de défense en fonction des attaques détectées.

Encore faut-il avoir, pour cela, consolidé, modernisé, automatisé et transformé son informatique. Face à des menaces comme les ransomwares et à la diversité des risques, des solutions d'hyperconvergence comme HPE Simplivity ou des approches hybrides permettent de mettre en place très facilement des plans de continuité ou de reprise d'activité (PCA/PRA) à moindre coût, et ceci, même si l'on est une TPE ou une PME sans équipe IT.

Aujourd'hui, des fournisseurs d'infrastructure comme HPE prennent en compte ces besoins de modernisation et d'hybridité en fournissant des plateformes technologiques et des composantes d'infrastructure spécialement pensées pour favoriser la transformation numérique.

Elles offrent à la fois l'agilité, la performance et la fiabilité exigées par les métiers ainsi que la protection et la résilience imposées par les obligations de souveraineté, de sécurité et de conformité.

inmac wstore : votre partenaire de la transformation

En s'appuyant sur les grands acteurs du marché comme HPE et sur une équipe d'experts qualifiés, inmac wstore facilite et accélère votre transformation numérique. « Nos clients peuvent s'appuyer sur notre capacité d'écoute et notre force de propositions pour les conseiller, les guider et les accompagner en fonction de leurs problématiques particulières sur les multiples enjeux portés par la nécessaire transformation de leur datacenter et de leur infrastructure informatique » explique Arnaud Brozzi, spécialiste Infrastructures chez inmac wstore.

inmac wstore

www.inmac-wstore.com

RGPD

COMMENT GÉRER UNE CYBERCRISE ?

La gestion d'une cybercrise dans le cadre d'une fuite de données personnelles (RGPD) est un processus très délicat. Harmonie Technologies relève le défi haut la main. Retour sur les scénarios mis en place avec Julie Grassin, Responsable de l'offre Résilience, qui mène les projets de bout en bout.

Simuler des situations proches du réel

Harmonies Technologies accompagne les clients, enchaîne les exercices de crise et les scénarios pour aboutir au cas final, « nous organisons des exercices de gestion de crise pour entraîner nos clients à faire face à des situations de cybercrise ayant un impact sur le système d'information et sur la continuité d'activité de la société ».

« Nous simulons des situations les plus proches du réel et nous travaillons avec la cellule de crise ». La cellule de coordination, gérée par l'équipe Résilience, à l'extérieur envoie des stimuli (faux articles de presse, appels téléphoniques, fausses vidéos...), « l'interaction temps réel se met en place, on s'oriente sur différents scénarios en fonction de la façon et de la capacité de la cellule à réagir ».

Au cours de ces exercices (une dizaine par an), plusieurs scénarios sont traités selon les objectifs des clients.

Gérer les violations de données personnelles

Harmonie Technologies teste les procédures de réponse mises en place pour gérer les violations de données personnelles et entraîne le DPO en cellule de crise à faire face à ces situations, « le DPO doit notamment s'occuper de la notification à la Cnil et maîtriser le contenu du formulaire assez conséquent ». La notion des interactions est cruciale.

Ce format, alternance de réunions cellule de crise et séances de travail, est enrichissant

Julie Grassin explique « nous avons travaillé sur un exercice de crise particulier (simulation 3 jours) correspondant aux fameux 72 heures dont disposent les entreprises pour faire la notification ». Chaque jour est divisé en deux phases, une phase de réunion de la cellule de crise et une phase de travail, « ce format, alternance de réunions cellule de crise et séances de travail, est enrichissant ».

Une stratégie de communication

Pas de doute, cette stratégie doit être affinée au

plus haut niveau car la question « comment gérer la communication en 72 heures alors que les investigations techniques commencent et vont prendre du temps ... » est primordiale.

En effet, à l'issue des 72 heures, le formulaire de notification est délivré par le DPO qui collecte toutes les informations. Le service Communication produit également son plan de communication (presse, interne, réseaux sociaux, notifications directes ...).

« Cette stratégie touche un périmètre précis, évoque le nombre de personnes impactées, le type de données sorties, sans évidemment tout maîtriser au début » ajoute Julie Grassin, « c'est pourquoi les RSSI se posent la question : est-on prêt à assumer les écarts réalisés (business, exceptions utilisateurs) de la politique de sécurité quand la violation de données arrive ... ».

Julie Grassin

Une bonne compréhension entre DPO et RSSI

Les exercices, leviers très forts, révèlent « que la mission du DPO est conséquente. Même dans les entreprises très avancées sur le sujet des procédures, nous recommandons notamment au DPO de travailler avec les interlocuteurs concernés lors d'une cybercrise pour les sensibiliser en amont sur les informations requises le jour J ».

D'un langage technique de la cellule de crise, le DPO et la communication doivent vulgariser les messages et gérer la réputation de l'entreprise, « l'enjeu communicationnel est considérable, c'est un défi entre les membres de la cellule de crise et vers l'extérieur ».

En effet, avec la GDPR (General Data Protection Regulation), le public est très en attente, « nous travaillons avec les entreprises pour préparer les plans et stratégies de communication en avance».

Julie Grassin précise toutefois « on a tendance à croire que le DPO peut être le directeur de crise. Or, ce n'est pas le cas, il est déjà en charge du formulaire. Le directeur de crise doit être présent en permanence, prendre les décisions, et être à l'écoute, ce rôle ne peut pas être assumé par le DPO ».

Les interactions multi-cellules

Propagation d'une cybercrise, notification, autorité de contrôle ...comment travailler sur les données qui transitent d'un pays à l'autre ? L'objectif premier des scénarios est de commencer par des choses plutôt simples (périmètre limité, mono pays, mono cellule) pour en tirer immédiatement des leçons, mais « les difficultés arrivent très vite : les interactions multi-cellules entre les pays et les violations de données personnelles multi-pays, nous gérons donc ces points ».

On a tendance à croire que le DPO peut être le directeur de crise. Or, ce n'est pas le cas

« Nous accompagnons les clients annuellement avec des scénarios de complexité croissante ». Pour Harmonie Technologies, ces scénarios de violations de données personnelles représentent plus de 80% des scénarios d'exercices de gestion de crise.

RGPD : Règlement Général européen sur la Protection des Données

> Par Sabine Terrey

La transformation culturelle
EST EN MARCHE !

La grande conférence annuelle, Think Paris 2018, au Carrousel du Louvre, fut l'occasion de venir écouter des leaders, des innovateurs, des experts techniques en IA, Blockchain, Internet des Objets, Cloud, Sécurité ... et de disposer des clés des pour se réinventer.

Entretien avec Nicolas Sekkaki, Président IBM France, sur les nouvelles cultures d'entreprise, les profonds bouleversements digitaux, la notion d'extracteur ou créateur de valeur ...

Repenser ce que nous voulons être et faire !

Il est essentiel de faire un bilan de l'impact des technologies sur la société et les usages, sur la donnée, la sécurité, la confiance... « Aujourd'hui, nous sommes parvenus à un point d'inflexion sur le marché, les entreprises ont bien compris l'urgence de se réinventer autour de la donnée, de passer d'une culture produit à celle de l'expérience client » souligne Nicolas Sekkaki, « le changement de culture ne s'apprend pas, ne se dicte pas, mais se vit ».

La donnée est clé puisque 80% des données ne sont pas accessibles par les moteurs de recherche, « les données des entreprises sont de l'or noir, et les entreprises vont devoir en extraire de la valeur et les sécuriser ».

La donnée et l'Intelligence Artificielle transforment tous les métiers et dessinent de nouveaux usages, « la passerelle entre les métiers et technologies nous préoccupe fortement, c'est un moyen pour les entreprises de se transformer et se différencier par rapport aux plates-formes mondiales ».

La revanche des disruptés

IBM a été disrupté. Pour rappel, « il y a 15 - 20 ans, 65% de notre CA étaient liés au matériel, 35% provenaient de produits, services logiciels connexes à ce matériel. Aujourd'hui, l'activité matérielle c'est 9% de notre CA, en moins de 15 ans tout a changé. 50 % de nos nouvelles offres n'existaient pas il y a tout simplement 3 ans », d'où la rapidité de la transformation d'IBM.

« Si notre rôle est de faire des passerelles, il faut disposer de profils aux compétences métier avec une appétence technologique » complète Nicolas Sekkaki, « ceux qui comprennent les sous-jacents de cette révolution et leurs valeurs intrinsèques sont capables de créer de nouveaux modèles d'entreprise et d'innovation rapidement ».

L'Intelligence Artificielle a besoin de trois moyens pour se développer, le Machine Learning, la donnée et le savoir-faire, « notre positionnement est simple : protéger la donnée client et son savoir-faire. Nous voulons développer des technologies, les comprendre pour permettre à nos clients de les utiliser pour transformer leurs métiers ».

Derrière cette révolution cognitive, on assiste à une profonde révolution culturelle, « dans cet esprit, nous avons repensé notre implantation régionale, sur 19 sites, à Lille notamment avec 600 collaborateurs, et nous avons créé des activités de conseil qui ne cessent de croître, mon objectif est de doubler la taille du conseil et des services ».

La Good Tech

Derrière cette expression, IBM positionne la protection des données, l'IA, l'essor des compétences, le développement des métiers et des écosystèmes, les investissements...

Le changement de culture ne s'apprend pas, ne se dicte pas, mais se vit

« Il est crucial que la France s'invite dans ce débat de l'IA et participe à la création d'une conscience collective, au regard de la Tech for Education, Inclusion & Instruction notamment » ajoute Nicolas Sekkaki. Faire revenir la recherche fondamentale dans l'hexagone est urgent et se pose la question de connaître le rôle des différents acteurs pour une Tech inclusive.

Plus personne n'est prescriptif !

« On redéfinit des façons de travailler, chacun doit se réinventer et trouver sa place, car les business models évoluent de façon drastique ». Il faut se challenger au quotidien ! « le véritable changement culturel, c'est que plus personne n'est prescriptif dans ce monde d'agilité » commente Nicolas Sekkaki.

L'accès aux moyens de production est désormais accessible au plus grand nombre, IBM développe des « usines cognitives » avec des start-up afin de développer des cas d'usage (Generali, Orange Bank, Crédit Mutuel), ce qui change complètement la notion de client-fournisseur. L'échange et le partage contribuent au changement culturel, « notre rôle est d'aider les entreprises à servir leurs clients, notre génétique, c'est l'entreprise, et nous allons vers les micro-entrepreneurs, autoentrepreneurs, développeurs ... ».

Nicolas Sekkaki

Avec l'annonce du pôle scientifique et technologique de Paris-Saclay en mars dernier, IBM crée une practice et un écosystème de collaborateurs qui développent sur l'ordinateur quantique « Saclay signifie faire revenir la recherche fondamentale autour de l'IA, la donnée, la recherche appliquée et la co-innovation avec les entreprises déjà présentes sur ce plateau ».

En France, le sujet de la formation est clé, « nous voulons donner à tous, les outils, formations, expériences pour définir les métiers de demain. Au travers de la technologie, il faut casser les idées reçues, réembarquer des personnes sur le marché du travail, libérer les énergies, nous l'avons fait et nous continuons à le faire ».

> Par Sabine Terrey

L'avènement du Machine Learning
ENGINEER(ING)

Big Data, Data Science, Machine Learning, Deep Learning, algorithmes prédictifs... Cela fait maintenant plusieurs années que ces termes sont entrés dans le monde de l'entreprise. Retour sur le sujet avec Youen Chéné, CTO de Saagie.

Pour pouvoir exploiter ces nouvelles technologies, de nombreuses entreprises ont mis en place un Data Lab, mais 80% des projets Big data ou IA n'atteignent pas la mise en production. Le Machine Learning Engineering est une solution potentielle pour remedier à ce problème.

Intéressons nous à l'article d'O'Reilly (www.oreilly.com/ideas/data-engineers-vs-data-scientists) qui décrit les rôles des Data Scientists et Data Engineers et en quoi le Machine Learning Engineer pourrait être le chaînon manquant à la réussite des projets.

Quelle différence entre Data Scientist et le Data Engineer ?

De nombreuses entreprises demandent à des Data Engineers de faire de la Data Science et à des Data Scientists de gérer des infrastructures. Cela peut conduire à l'échec d'un projet, en plus de créer des tensions et frustrations au sein des équipes. Il est primordial d'identifier les rôles de chacun, leurs capacités et ainsi adapter leurs missions.

Le Data Scientist a généralement une formation en mathématiques et statistiques (parfois même en physique). Au-delà, il fait de l'Analytics et pour aller encore plus loin, il crée des algorithmes d'intelligence artificielle, le plus souvent de Machine Learning.

Il fait parler les données. Il se charge de les recouper, puis d'en fournir une interprétation claire. Le Data Scientist porte bien son nom : c'est un métier proche de celui du chercheur, mais pourtant bien ancré dans l'entreprise.

Tout comme son homologue ingénieur, il doit être en contact avec les métiers, côté business. Dans le cadre de son travail, il doit leur apporter des analyses et doit donc être familier avec l'entreprise, ce qu'elle fait et les enjeux économiques des résultats qu'il délivre. Ces résultats doivent être compréhensibles et adaptés aux métiers pour les aider dans leur prise de décision.

Une particularité que l'on retrouve chez bon nombre de Data Scientists est qu'ils ont appris à programmer par nécessité, afin de faire des analyses poussées ou pour surmonter un problème. Leur niveau n'est pas celui d'un programmeur ou d'un Data Engineer, ce qui est finalement logique puisqu'ils n'ont pas le même besoin.

Le Data Engineer a une formation en programmation, le plus souvent en Java, Scala ou Python. Il est généralement spécialisé en systèmes distribués et Big Data.

Il est responsable de la création et de la maintenance de l'infrastructure analytique qui permet presque à toutes les autres fonctions de tourner dans le monde des données.

Il s'occupe du développement, de la construction, de la maintenance et du test des architectures, telles que les bases de données et les systèmes de traitement Big Data mais donc aussi de la création de processus de modélisation des jeux de données sur l'exploration, l'acquisition et la vérification de ces derniers.

Plus concrètement, grâce à sa formation, il crée ce qu'on appelle des data pipelines. Et si cela peut sembler simple en le disant, il s'agit en fait, à l'échelle du Big Data, de faire fonctionner des dizaines de technologies ensemble. C'est d'ailleurs le Data Engineer qui choisit les technologies les plus adaptées, il se doit donc d'en avoir une connaissance accrue.

Et côté analyse de données ?

Les deux profils peuvent faire de l'analyse de données, même si le niveau de compétences du Data Scientist n'est pas le même que celui du Data Engineer. Le premier pourra réaliser des analyses très poussées quand le second maîtrise les analyses basiques jusqu'à intermédiaires.

Les deux se rejoignent aussi sur la programmation. Mais ici encore, à deux niveaux bien différents, et c'est le Data Engineer qui prend l'avantage sur ce terrain. Quand construire un data pipeline est la base du travail du Data Engineer, c'est en revanche bien au-dessus des compétences du Data Scientist. C'est aussi en cela que les deux profils se complètent, le travail de l'un supportant celui de l'autre.

Le point commun à côté duquel on ne peut passer est le Big Data bien sûr. Les Data Engineers mettent à profit leur compétences de programmation pour créer des pipelines Big Data.

La mise en production d'algorithmes de Machine Learning nécessite quelque chose en plus qu'un raisonnement purement académique

Ces pipelines servent ensuite à supporter le travail du Data Scientist qui utilise, quant à lui, ses compétences mathématiques et statistiques pour créer des produits data, concevoir des modèles et dégager des tendances. Il est donc indispensable de connaître les points forts et les limites des deux profils afin de répondre aux attentes de tous.

Un point sur les besoins en Machine Learning Engineers ?

Les Data Scientists ont, pour la majorité, suivi un cursus universitaire. Ce qui n'est évidemment pas un problème en soi peut finalement en devenir car ces profils sont souvent très attirés par la recherche et le théorique. Or, les entreprises cherchent du concret, du déploiement et de la création de la valeur. Et malgré leurs efforts, 80% d'entre elles n'y parviennent pas.

Du côté des Data Engineers, la difficulté se trouve dans le fait que cette tâche, la mise en production d'algorithmes, n'est pas tout à fait dans le descriptif de leur job. Leur rôle est davantage de gérer les les pipelines qui supportent les algorithmes de Machine Learning mais pas directement d'optimiser ces algorithmes pour leur déploiement.

La mise en production d'algorithmes de Machine Learning nécessite quelque chose en plus qu'un raisonnement purement académique. C'est pourquoi un nouveau type d'ingénieur est en train de voir le jour, le Machine Learning Engineer. Surtout présent aux Etats-Unis, ce profil tend désormais à se répandre, et constitue un enjeu qui n'est pas seulement américain.

Dans la majorité des cas, ces ingénieurs d'un nouveau genre ont une formation similaire à celle des Data Engineers. Cependant, poussés par une appétence pour les mathématiques et le Machine Learning, ils ont généralement eu un cursus croisé ou suivi des formations supplémentaires afin de pouvoir gérer aussi bien l'infrastructure que la Data Science.

Le Machine Learning Engineer apparaît donc comme le lien entre le Data Scientist et le Data Engineer. Il maîtrise les algorithmes de Data Science, mais possède aussi des compétences similaires à celle du Data Engineer pour gérer l'infrastructure qui permettra leur optimisation, puis leur mise en production.

Son profil se rapproche donc davantage d'un ingénieur que celui du Data Scientist par ses compétences logicielles. Il comprend et met en pratique les méthodes de développement ainsi que l'approche agile. Puisqu'il assure la gestion de la mise en production, ils se doit aussi de maîtriser les outils per-

mettant de maintenir un certain niveau de sécurité à l'ensemble de l'environnement.

Quelle est la definition du Machine Learning Engineering ?

Il n'existe pas encore de définition du Machine Learning Engineering puisqu'il s'agit d'une discipline à la croisée de l'ingénierie et de la Data Science encore récente et peu présente. Pour faire simple, cela comprend l'ensemble des processus qui permettent la mise en production de Machine Learning grâce à l'optimisation d'algorithmes.

Cette mission concerne donc ce qu'on pourrait appeler le dernier kilomètre de la donnée. Il pourra s'agir de réécrire en Java ou Scala le code d'un Data Scientist qui était à l'origine en R ou Python, de le mettre à l'échelle (Python vers PySpark, ou Python vers Scala Spark), ou encore d'optimiser un algorithme d'intelligence artificielle pour assurer son fonctionnement.

Elle recouvre donc toute la phase d'industrialisation qui implique, en plus de tout le reste, des tests et du déploiement continu.

Un modèle de Machine Learning nécessite plus d'attention qu'un programme informatique classique. Il peut tout à fait fonctionner et, d'un jour à l'autre, donner des résultats incohérents. Cela peut venir d'un changement dans les données, d'ajout de nouvelles données ou encore d'une attaque.

Dans tous les cas, la tâche du Machine Learning Engineer sera de gérer toutes ces failles éventuelles grâce à ses connaissances des deux milieux (infrastructure et Data Science).

La Data Fabric, est-elle l'environnement idéal pour faire du Machine Learning Engineering ?

Nous pensons que la Data Fabric permet justement de mettre facilement en production les algorithmes de Machine Learning. Elle offre les outils pour faire du Machine Learning Engineering sans avoir besoin d'un Machine Learning Engineer.

Il s'agit d'un environnement collaboratif qui va faciliter les échanges et le partage entre les Data Scientists et les Data Engineers en les faisant travailler sur des projets communs.

D'un côté, les Data Scientists vont pouvoir accéder à une plus grande quantité de données (permettant de tester la robustesse de leurs algorithmes) et intégrer les différents algorithmes qu'ils auront créés sur leurs notebooks (Jupyter, R Sutdio) grâce aux connecteurs de la Data Fabric.

De l'autre, les Data Engineers, eux, vont pouvoir créer de multiples data pipelines et y intégrer simplement les algorithmes des Data Scientists. Pour cela, ils les dockerisent tout en orchestrant les multiples technologies open-source (talend, scala, spark, Python, R, etc) nécessaires à la création des data pipelines. L'optimisation d'algorithmes ou la réécriture de code en raison de soucis de compatibilité de technologies n'est ici plus nécessaire.

Youen Chéné

Enfin, comme le démontre Saagie avec sa Data Fabric, conçue de manière à amener les pratiques DevOps dans le monde du Big Data, toutes les fonctionnalités permettant de versionner, déployer, opérer, monitorer, "rollbacker" et itérer sur les différents travaux réalisés par les Data Engineers et Data Scientists y sont présentes.

La Data Fabric se positionne ainsi comme une solution idéale pour industrialiser le Machine Learning, et orchestrer de bout en bout les projets Big Data/IA.

> Par Sabine Terrey

L'impact positif de l'Intelligence Artificielle dans l'environnement de travail

L'Intelligence Artificielle est souvent perçue négativement car elle remplacerait l'humain au travail. Et si on voyait l'IA comme un moyen d'enrichir la collaboration et la pensée humaine ?

L'IA contribue à la diversité de la pensée humaine

L'utilisation de l'IA facilite la collaboration entre les humains et les machines.

La priorité n'est-elle pas l'innovation, le gain de temps, la résolution rapide des problèmes ? Aujourd'hui, « la multiplicité, qui constitue une vision positive et inclusive de l'IA, gagne du terrain ».

90% des dirigeants s'orientent vers la diversité cognitive :

- La diversité cognitive est essentielle dans le domaine du management
- L'IA créera de nouveaux emplois (75%)
- L'IA améliorera le processus décisionnel (93%)

Le pouvoir transformationnel de la multiplicité

« L'IA est désormais perçue comme un nouveau type d'intelligence qui peut compléter les types existants que sont l'intelligence émotionnelle, sociale, spatiale et créative. Le pouvoir transformationnel de la multiplicité réside dans sa capacité à améliorer la diversité cognitive en combinant les différents types d'intelligence d'une manière nouvelle au profit de toutes les entreprises et de leurs employés. » souligne Vinod Kumar, directeur général de Tata Communications

Vers un nouveau type d'intelligence

L'IA apporte une aide à la collaboration humaine. Voici les axes d'amélioration envisagés :

- **La diversité cognitive au sein des groupes**
  La diversité de pensée produit de meilleurs résultats dans le cadre de projets. L'IA permet de créer et maintenir des groupes de travail qui favorisent cette diversité cognitive

- **Le gain en agilité, créativité et curiosité**
  L'IA améliore l'implication des collaborateurs (93%) en évaluant les compétences, les priorités en matière d'innovation et en suggérant des activités pour encourager la pensée créative à tous les niveaux

- **La collaboration humaine améliorée**
  Si la diversité des langues et cultures peut être un obstacle à la collaboration, l'IA facilite la constitution, l'organisation et la communication des équipes, à l'international (80%)

- **La création de postes**
  L'IA permet aux employés de se libérer des tâches fastidieuses et répétitives pour se recentrer sur la communication et l'innovation. Le travail est basé sur une stratégie et une grande flexibilité

Source Etude Tata Communications

Les Assises de la Sécurité 2018

ANTICIPONS COLLECTIVEMENT !

Une 18ème édition avec une envolée de contenus, d'ateliers, de keynotes, de speakers avec en ligne de mire un défi : gérer la cybersécurité au quotidien et toutes les menaces qui arrivent. Retour sur quelques acteurs présents sur l'événement.

La vigilance est la réalité des entreprises

Les Assises de la Sécurité se sont construites petit à petit avec toute la communauté de la cybersécurité, partenaires, clients, experts, car la cybersécurité est un voyage ! « 80% des offres qui arrivent seront révolutionnaires, mais ne négligeront pas les acquis ».

Le monde dans lequel nous vivons est en perpétuel changement ce qui nous impose d'être attentifs en permanence et d'échanger tous ensemble.

La mobilisation englobe les compétences nouvelles, la formation des collaborateurs, la mise en place d'un cadre juridique adapté, mais l'adaptation passe indéniablement par le développement d'un cadre moral et d'un sens de la liberté.

L'anticipation collective !

Guillaume Poupard, Directeur Général de l'ANSSI insiste « la sécurité numérique est un sujet global complexe » connecté au développement numérique. Il faut appliquer différentes règles pour se protéger face aux plus compétents et dangereux en développant une réelle approche pragmatique. La règlementation a un grand rôle à jouer.

L'anticipation, c'est examiner les produits, prestataires et services d'excellence, et bien sûr les jeunes pousses qui se développent, « nous allons continuer à qualifier les prestataires avec le label, ce qui traduit une vraie qualité » poursuit Guillaume Poupard, « et nous lançons un nouveau référentiel

- Prestataires d'administration et de maintenance sécurisées -pour compléter le dispositif » car les exigences sont élevées.

Le grand prix des RSSI

Il est un métier à l'honneur sur les Assises de la sécurité alors rappelons les grands gagnants RSSI de cette édition 2018 !

Le Meilleur Espoir est attribué à Fabien Lemarchand (Cdiscount), la Culture sécurité à Vivianne Maleterre (Haute Autorité de Santé), la Démarche Innovante à Dominique Alleron (Axa) et le prix Spécial du Jury à Stéphane Tournadre (Servier).

Gérer « intelligemment » la sécurité

Il est vital de mettre de l'intelligence dans la gestion de la sécurité, c'est ainsi que « de la même manière que les entreprises utilisent un ERP pour la gestion de leur entreprise, un CRM pour leur relation client, les entreprises doivent porter attention et utiliser un SIEM pour la gestion de la sécurité » explique Christian Pijoulat, Regional Director South EMEA, chez LogPoint.

Avoir une plate-forme pour concentrer et analyser l'ensemble des informations, remplir les obligations légales et utiliser ces éléments pour optimiser la sécurité, sont devenus des enjeux majeurs.

La sécurité au cœur des métiers

Après avoir gagné le Prix de l'innovation et Prix du public lors des Assises de la Sécurité 2017, Alsid, créée par deux anciens ingénieurs de l'ANSSI, Emmanuel Gras, CEO et Luc Delsalle, CTO, poursuit son développement et s'affirme comme un acteur incontournable de la sécurité.

Suite aux retours et besoins des clients (plus de 2,5 millions d'utilisateurs dans 6 pays), aux travaux R&D, et à la connaissance des scénarios d'attaques, Alsid for Active Directory arrive en force, tout début 2019, « ce produit reste spécialisé Active Directory, cœur de notre métier, mais on étend complètement les cas d'usages de notre solution » précise Emmanuel Gras.

Avant, nous nous adressions principalement au RSSI en lui donnant une idée de la conformité et sécurité de son système ». Aujourd'hui, Alsid étend ce concept aux équipes SOC, équipes dédiées aux réponses à incidents, équipes Threat Hunter, et équipes tests d'intrusions internes.

Les hackers raffolent des comptes à privilèges ...

« Nous voulons réduire la surface de risques des comptes à privilèges et des accès » explique William Culbert, directeur France & EMEA, Bomgar (BeyondTrust dès janvier 2019).

En effet, sur 81% des cyberattaques, les comptes à privilèges sont ciblés par les pirates.

« De plus, les chemins d'accès, qui concernent l'accès au serveur, aux bases de données, au parc informatique, sont fondamentaux et doivent être sécurisés ». Beaucoup d'attaques proviennent aussi des endpoints.

Bomgar vient ainsi ajouter à son portfolio des outils de containerisation des applications « au lieu de donner les droits administrateurs au côté endpoint des utilisateurs, on donne juste les droits nécessaires pour faire un travail précis ».

L'Intelligence Artificielle pour l'aide à la décision

IBM avance concrètement sur le sujet de l'Intelligence Artificielle en France, «nous avons une vision assez précise des critères à respecter pour l'IA : la robustesse des systèmes, la transparence, l'équité ou fairness. Notre approche est d'aider à développer des systèmes IA dans lesquels on peut avoir confiance » avance Hugo Madeux, directeur de l'entité Sécurité

L'IA développée par IBM donne des éléments à l'être humain pour comprendre le cheminement, la forme de raisonnement et fournir un certain nombre de preuves de ce qui a été fait afin de prendre la décision.

Il faut éliminer tous les biais dans les développements IA. L'être humain est décideur, s'appuie sur une aide, garde le contrôle et prend la décision finale.

Les nouveaux usages

En tant qu'acteur de l'IAM (Gestion des Identités et des Accès), Ilex mène d'une main de maître le volet identité et le volet accès.

« D'abord l'identité numérique c'est-à-dire la matérialisation numérique d'un utilisateur d'un système d'information », donc la gestion du cycle de vie de cette identité pendant que la personne travaille dans l'entreprise.

« Evidemment autour de l'identité, on ne peut passer sous silence les notions de droits d'accès, l'habilitation, la règlementation, le contrôle, l'audit ... » explique Olivier Morel, Deputy General Manager.

De plus, avec la couche access management, on touche au cœur de métier d'Ilex avec l'authentification, le SSO, le contrôle d'accès logique.

L'explosion de la cybersécurité et la transformation digitale nous amènent directement aux nouveaux leviers et usages, « la mobilité est un facteur très influençant de nos technologies, les utilisateurs travaillent sur mobile, tablette ... La digitalisation de l'entreprise oblige à parler des identités internes et externes, celles des clients, des citoyens, des abonnés ... ».

La Security Fabric pour transformer la sécurité

Avec une approche très silotée de la sécurité, on touche rapidement aux limites du système. Selon une étude du CESIN, on compte environ 11 solutions de sécurité dans une entreprise (consoles, produits, formations, évolutions...), « ce qui rajoute une complexité incroyable qui est l'ennemi de la sécurité » explique Christophe Auberger, Directeur Technique France, Fortinet.

Fortinet propose une solution d'intégration de toutes ces solutions et fonctions autour d'un framework, la Security Fabric, « cela fonctionne avec nos produits, ce qui permet de les intégrer, les automatiser et d'apporter des synergies, mais aussi avec des produits tiers. Cette Security Fabric est ouverte ».

Les entreprises viennent se plugger sur cet environnement et ont le même niveau de service que les produits natifs Fortinet ».

> Par Sabine Terrey

Le DevOps
UN ENJEU DE CULTURE ET DE PROCESS

Le DevOps est un enjeu crucial de la transition numérique des organisations. Sydney Rabsatt, Vice President Product Management chez NGINX décrypte l'approche DevOps

Le DevOps est annoncé comme un enjeu clé de la transformation digitale des entreprises, pouvez-vous expliquer pourquoi ?

Le DevOps est essentiel pour la transformation digitale puisqu'il illustre comment délivrer des applications modernes. L'équipe chargée des applications est responsable de délivrer des expériences utilisateurs optimisées et différenciées qui garantissent d'avoir une interaction adéquate pour le consommateur à tout moment. L'équipe DevOps, elle, permet à ces applications d'être livrées de manière aussi dynamique que l'exige les entreprises.

Comment accompagner les initiatives DevOps des entreprises ? Que préconisez-vous ?

Il faut d'abord avoir conscience qu'il ne s'agit pas seulement d'embaucher et de former des collaborateurs. Le DevOps est un changement profond de culture et de process.

Ainsi, les entreprises doivent prendre à bras le corps leurs nouvelles priorités et activités et adopter un process de développement d'applications adéquat, qui leur permettra de réussir.

Souvent, on constate que les équipes de DevOps ont des difficultés à tisser une chaine complexe (et fragile) d'outils pour livrer leurs applications.

Ainsi, les entreprises se tournent vers des solutions telles que NGINX afin de les aider à rationaliser le nombre de pièces mobiles nécessaires à la livraison de leurs applications, le tout avec une intégration fluide et simplifiée à leurs process.

Quelles sont les perspectives et futures tendances du DevOps pour 2019 et les années futures ?

Parmi les grandes tendances, on peut citer la consolidation et la simplification du DevOps. Aujourd'hui, on assiste à une démultiplication des outils dans le domaine applicatif, et les fournisseurs de Cloud ont déjà commencé à intégrer nombre de ces derniers dans leurs plateformes.

Toutefois, je pense que les entreprises vont les utiliser avec précaution, et qu'elles vont continuer de chercher des solutions leur offrant une flexibilité et une portabilité à long terme (même si elles ont choisi un seul fournisseur de service Cloud au départ).

Les entreprises vont aussi commencer à réduire la complexité de leurs process et le nombre d'outils auxquels elles font appel. En effet, alors que leurs outils gagnent en maturité (ou sont acquis et fusionnés avec d'autres), ils vont inévitablement se chevaucher.

Sydney Rabsatt

Ainsi, il est prévu que les grandes entreprises se concentrent sur des solutions polyvalentes, durables, et cohérentes qui permettront de s'éloigner des solutions complexes et fragiles enchainées à travers de multiple outils et intégrations de fournisseurs.

> Par Sabine Terrey

Le déploiement de Teams
ET LA CONDUITE DU CHANGEMENT

Microsoft Teams est depuis un an le nouveau produit phare de Microsoft. Tout comme Slack, il existe dorénavant une version gratuite non liée à un compte Office 365, permettant à tous de découvrir les formidables fonctionnalités proposées...

Un Hub d'applications

En ETI, PME ou Association, le déploiement de Teams se fait manuellement par l'utilisateur, qui en se connectant la première fois sur teams.microsoft.com, va télécharger l'application.

Dans les moyennes et grandes entreprises, les équipes informatiques préfèrent souvent gérer le déploiement comme elles le font pour Word, Excel ou PowerPoint, en déployant un package msi avec leurs outils de déploiements type SCCM ou autres.

Teams est un HUB d'applications : on y retrouve SharePoint, OneDrive, Word, Excel, PowerPoint, OneNote mais présenté d'une manière plus efficiente pour l'utilisateur.

L'intérêt de l'utilisateur

Selon ma propre expérience, présenter les applications Office 365 en partant de la page d'accueil Office.com n'est pas la meilleure approche car les utilisateurs s'y perdent dès les premières minutes et le constat est souvent le même : « Office 365 c'est trop compliqué ! »

En effet, si l'on souhaite présenter une à une toutes les applications, de plus en plus nombreuses, il est nécessaire d'y consacrer un minimum de temps. Malheureusement aujourd'hui, les utilisateurs n'ont pas ce temps. C'est pourquoi ils n'adhèrent pas ou peu à Office 365.

150 EXPOSANTS - 76 CONFÉRENCES & TABLES RONDES - 30 ATELIERS

CLOUD COMPUTING WORLD EXPO

SOLUTIONS DATACENTER MANAGEMENT

IoT world

2 jours pour moderniser vos infrastructures et services IT, et vous convaincre des enjeux de l'IoT.

Réservez dès maintenant votre badge gratuit !

20 - 21 mars 2019
PARIS EXPO
PORTE DE VERSAILLES

www.cloudcomputing-world.com
www.datacenter-expo.com
www.iot-world.fr

En partenariat avec : iTPro.fr SMARTDSI

Le premier réflexe serait de désactiver les applications du profil des utilisateurs de manière à avoir une page d'accueil plus simple, cependant nous sommes de nombreux consultants et/ou experts Microsoft à déconseiller fortement cette pratique.

Il est donc nécessaire de repenser la méthode de présentation de ces produits pour répondre aux questions des utilisateurs « quel est mon intérêt ? » et « à quoi cela va me servir concrètement ? »

Pour que l'adhésion soit immédiate, il ne doit pas y avoir un délai trop important entre la présentation de Teams et la mise à disposition de ce service. Les utilisateurs sont maintenant habitués au « Shadow IT » et trouveront une solution de contournement si cette mise à disposition n'est pas immédiate ou anticipée.

Les méthodes de travail

La première chose à faire avant de commencer la présentation, est de questionner les utilisateurs sur leurs méthodes de travail et les défis qu'ils souhaitent relever :

- Comment vais-je pouvoir finir plus vite mes tâches ?
- Comment passer moins de temps à répondre à toutes les sollicitations que je reçois ?
- Comment justifier ma charge de travail ?
- Comment vais-je pouvoir facilement créer une communauté sur l'innovation ?
- Comment homogénéiser nos pratiques de communication/RH au sein du groupe ?
- Ma fille est malade ce matin, puis-je travailler de la maison ? etc...

L'animateur ou « change manager » n'a plus qu'à laisser faire les utilisateurs. Les laisser faire ? oui, c'est bien aux utilisateurs de procéder aux manipulations. L'animateur est là pour fournir les indications et leur permettre d'apprendre par eux-mêmes.

Au préalable, il demande aux utilisateurs de venir à cette présentation avec leur pc portable et de se connecter à teams.microsoft.com. Une fois arrivé sur Teams, il ne reste plus qu'à leur faire installer l'application et adapter les manipulations selon les réponses et défis indiqués précédemment.

La réunion de présentation ne doit pas dépasser 30 minutes.

Ne pas freiner l'adhésion au projet

Pour que cette méthode fonctionne, la première conduite de changement doit être menée auprès de vos équipes informatiques.

Si l'on souhaite autoriser les utilisateurs à créer des équipes Teams, il faut former au préalable les administrateurs, ce sont eux les premiers ambassadeurs.

Par méconnaissance, ils s'interrogent généralement sur la manière de garantir le fonctionnement d'Office 365 si tout le monde dans l'entreprise peut créer une équipe Teams. Un script PowerShell est donc souvent utilisé pour interdire la création d'équipes Teams, hors il s'agit justement d'un frein à l'adhésion du projet, l'utilisateur n'ayant pas accès aux fonctionnalités de Teams.

Les équipes qualité et méthodes peuvent jouer le rôle de référent métiers et doivent également être formées en priorité avec les administrateurs. Ensemble, ils pourront mettre en place des règles de bonnes pratiques comme

- le nommage des équipes
- la création de modèles d'équipes en fonction des usages
- les règles d'archivage et de suppression des équipes non utiliséed
- les règles d'échanges entre utilisateurs

Ces règles, une fois rédigées, sont diffusées aux utilisateurs au même titre que la charte de sécurité informatique.

Vous n'avez pas appliqué cette méthode ? Rien n'est perdu. Il est encore possible d'intervenir sur la gouvernance des équipes Teams ainsi que leur nommage.

J'espère vous avoir fourni quelques clés pour vous permettre de déployer Teams dans votre entreprise et faire adhérer vos équipes !

> Par Kevin Trelohan
Consultant Freelance chez Dev-DS

Transformation digitale
QUEL EST LE DEGRÉ DE MATURITÉ DES ENTREPRISES FRANÇAISES ?

Le Digital Transformation Index 2018 révèle des indicateurs clés : 30% des décideurs français craignent tout simplement que leur entreprise ne devienne obsolète d'ici à 5 ans ... Eclairage sur la disruption, les difficultés de rebondir, obstacles et défis avec Erwan Montaux, Director, Large Entreprise Team, Intel et Sébastien Verger, CTO Dell EMC France

« La transformation digitale ne se fait pas de façon uniforme, les investissements sont évidemment bien différents entre les grands groupes ou les PME » souligne Erwan Montaux.

Les entreprises évoluent au risque d'être « disruptées » par des digital natives « qui n'utilisent pas la technologie pour leurs besoins, mais la technologie est le fondement même de leur business », et cela touche tous les métiers, transports, santé ...

D'ailleurs, « dans le Top 500 des entreprises en 2008, 45% (monde) n'en font plus partie et ont été disruptés ».

Le retard de la France

La France accuse un retard : 4% des entreprises sont qualifiées de Digital leaders face aux 60% qui investissent peu ou pas du tout dans cette transformation digitale.

Plus précisément, 25% sont en retard et n'ont pas de plan digital (Digital Laggards), 36% suivent (Digital Followers), font peu d'investissements mais planifient, 18% évaluent (Digital Evaluators) et font des projets, 17% ont un plan digital mature (Digital Adopters) et sont au début de l'implémentation.

Cependant, la prise de conscience est réelle, « le mouvement est lancé depuis 2016, on voit moins de retardataires et de Followers que d'Evaluators et d'Adopters » commente Sébastien Verger.

« L'évolution est intéressante depuis 2 ans, les discussions avec les clients tournent autour de l'angle d'approche de la transformation ».

Les questions changent aussi, les entreprises se demandent « comment on connecte ce qui n'est pas connecté pour avoir des prises de décision plus informées » ajoute Erwan Montaux. En effet, que l'on parle de digital, d'Intelligence Artificielle ou autres, c'est toujours au service du client

Les obstacles majeurs des décideurs

Pour les décideurs, il est très difficile de se transformer, 86 % font face à des obstacles majeurs et seulement 27% pensent qu'ils seront précurseurs. Les entreprises s'inquiètent aussi de ne pas pouvoir répondre aux futures demandes des clients.

« En 2016, l'Index révélait parmi les freins, la disponibilité, la connaissance et l'appréhension de la technologie. Aujourd'hui, on note un vrai virage puisque le frein N° 1 est l'insuffisance budgétaire et le manque de ressources » explique Sébastien Verger. Parmi les freins, retenons

- Manque de budget et de ressources

- Manque de savoir-faire et expertise interne

- Sécurité des données et cyber sécurité

- Manque de maturité, d'alignement et de collaboration interne

- Organisation en silos

- Les lois et changements législatifs

- Un trop-plein d'informations

Le Top des investissements

La cyber sécurité remporte la palme des investissements suivie de l'Intelligence Artificielle et des environnements multi-cloud, de l'Internet des Objets. « Etude après étude, on voit une réelle montée en puissance de l'IA, 70% des entreprises ont investi ou vont investir dans les deux ans dans l'IA » complète Sébastien Verger. La donnée se retrouve au cœur des investissements.

Source Etude mondiale Dell Technologies & Intel – 42 pays - Eté 2018 - France : 150 dirigeants

Comment augmenter les budgets DE CYBERSÉCURITÉ DES RSSI EN TROIS ÉTAPES

Pour 95 % des entreprises, il existe un écart entre la culture de cybersécurité actuelle et celle qu'elles souhaiteraient avoir[1]. Face aux violations de données, les investissements dans la cybersécurité ne sont jamais suffisants.

Le RSSI doit hiérarchiser les ressources disponibles, en fonction des risques potentiels, pour justifier des investissements supplémentaires nécessaires auprès de l'équipe dirigeante.

Comment justifier la pertinence de ressources supplémentaires auprès des supérieurs ? Voici 3 étapes à suivre[2].

Vérifier, évaluer et planifier

Les RSSI doivent commencer par vérifier la bonne affectation des ressources actuelles pour contenir les menaces et résoudre les vulnérabilités.

Recourir à des évaluations régulières sur les risques que présentent ces vulnérabilités et leur capacité actuelle à contenir une cyberattaque est essentiel.

Les RSSI définissent les postes spécifiques nécessitant des efforts et des investissements supplémentaires.

Une veille quotidienne permet de se tenir informé des dernières recherches et des violations de données sévissant dans le secteur, pour cerner les faiblesses de l'organisation.

Parler aux dirigeants

L'étape suivante consiste à parler aux dirigeants. Les RSSI peuvent commencer par résumer les menaces potentielles et expliquer les démarches pour y faire face, tout en démontrant l'utilisation des technologies et ressources humaines existantes. Il est conseillé d'éviter les termes techniques au profit de scénarios concrets (incidents de cybersécurité mentionnés dans la presse).

Pour démontrer la pertinence des besoins, les RSSI peuvent se reposer sur plusieurs mesures :

- le temps moyen de détection et de correction
- le nombre d'incidents et de vulnérabilités décou-

verts par rapport au nombre corrigé

- les économies réalisées grâce aux correctifs
- le temps moyen entre les incidents survenus dans le passé

Il faut souligner les failles qui rendent l'entreprise vulnérable, et déterminer les ressources nécessaires à déployer pour les corriger.

Fournir un plan détaillé sur l'utilisation du budget additionnel

La dernière étape consiste à fournir un plan sur la manière dont le RSSI utilisera un budget additionnel pour réduire :

- les risques identifiés (ressources, personnes, technologies)
- les délais
- le coût financier

Il faut estimer le retour sur investissement de sécurité (ROSI, Return On Security Investment) attendu, pour prouver l'efficacité en termes d'équilibrage du risque et des coûts.

Pour calculer le ROSI, il faut se baser sur la réduction directe des pertes financières, en quantifiant dans quelle mesure le nouveau projet atténue les risques. Les RSSI démontrent les avantages apportés à l'entreprise, via la réduction des coûts, l'augmentation des revenus ou la valorisation de la société sur le marché.

Les dirigeants ne sont pas influencés par de vagues promesses de sécurité ou des prédictions aléatoires sur les menaces actuelles et à venir.

Il est essentiel de fournir des données fiables, démontrant comment une cybersécurité renforcée favorise la pérennité d'une organisation.

Les RSSI doivent bien connaitre le marché et les objectifs de l'organisation, afin d'identifier les risques les plus critiques et mettre en avant les bénéfices qui parleront aux conseils d'administration

1 - ISACA
2 - Source Pierre-Louis Lussan, Country Manager France, chez Netwrix

Les talents du directeur financier de demain

La fonction finance intègre multiples compétences : expertise dans la visualisation des données et capacité de réfléchir au-delà du cadre comptable et financier.

Si 34 % des tâches financières sont gérées par la technologie, en 2021, 45 % seront automatisées.

Une évolution des compétences

- Rapprochement des compétences financières et des compétences numériques, statistiques, opérationnelles et collaboratives
- le data storytelling est une compétence essentielle
- le pilotage de la transformation opérationnelle est la clé

Les nouveaux talents

Voici les 4 qualités requises de la fonction finance

- comprendre comment collecter des données
- en extraire des informations clés
- être plus ouverts d'esprit pour mieux collaborer endosser le rôle de conseiller en stratégie auprès des autres dirigeants

Les 4 conseils clés

Découvrons les conseils issus de cette étude.

- **Devenez un « capteur intelligent » des évolutions du marché**
  En mesurant les impacts de la disruption, l'apport de l'innovation et la valeur que génère l'ensemble de l'écosystème
- **Créez un storytelling autour des données**
  En jouant un rôle essentiel dans l'éducation, l'encadrement, et la communication des données aux actionnaires et dirigeants
- **Oubliez les « process »**
  Comme les P2P (Procure to Pay), O2C (Order to Cash) ou R2R (Record to Report) qui vous dévient des objectifs de résultats
- **Ne vous limitez pas à la fonction finance**
  Et trouvez de nouvelles façons d'allouer les ressources, de mesurer les résultats et tirer parti des compétences

Etude Accenture - The CFO Reimagined : from Driving value to building the digital enterprise

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

METSYS

Laissez-vous guider !

Pour en savoir plus, scannez ce QR code

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