N°19 I SEPTEMBRE 2020

CONDUIRE LA TRANSFORMATION NUMÉRIQUE DE L'ENTREPRISE

SMART DSI®

DOSSIER
Connaître ses applications pour réduire les risques informatiques

INTERVIEW
Simplifier le quotidien des opérationnels de la donnée

BONNES PRATIQUES
Conseils pour améliorer sa cybersécurité dans le monde post-Covid

INTERVIEW
Comment faire travailler ensemble les Data Scientists et les Métiers

L'ETUDE A RETENIR
Téléphonie dans le Cloud : vers la maturité !

DIB France
vous facilite l'IT

SOLUTIONS WORKPLACE
INFRASTRUCTURES & SECURITE
SERVICES & INTEGRATION

Depuis plus de 30 ans DIB France s'est développée sur des valeurs fortes autour de l'écoute, la proximité et la satisfaction client, ces valeurs guident notre stratégie au quotidien et accompagnent vos projets de transformation numérique.

1992

1
équipe d'experts
à votre écoute

+20%
de croissance
en 2019

31 millions
d'euros de chiffre d'affaires
réalisé en 2019

www.dib-france.fr

Tél : 01 34 57 90 00

S'adapter au monde Covid-19 !

La crise sanitaire impacte évidemment toutes les activités et les process des entreprises. Nombre d'entre elles ont, par ailleurs, décidé d'accélérer leur transformation digitale en s'armant d'outils pour traverser au mieux cette période. D'autant que personne ne sait combien de temps précisément cette phase particulière va durer...

Alors si le monde dans lequel nous vivons, n'est plus exactement le même que celui d'avant, s'adapter rapidement pour au moins anticiper d'autres éventuelles futures crises, peut être un bon début !

Quelques recommandations sont donc bien utiles, qu'il s'agisse de conseils pour améliorer sa cybersécurité, capitaliser sur les données et en avoir une vision responsable, optimiser de nouveaux modes de fonctionnement, mesurer les stratégies Cloud, appréhender les enjeux business des décideurs, relever les défis de l'automatisation intelligente mais aussi bien évaluer les risques du passage si soudain au télétravail.

En effet, les cybercriminels savent réagir rapidement aux faits d'actualité et cherchent aujourd'hui à exploiter l'épidémie et tirer profit de l'anxiété ambiante. Dès le mois de mars, on a remarqué une augmentation significative des e-mails malveillants utilisant la thématique du Covid-19 pour manipuler les utilisateurs. D'ailleurs, les trois quarts des pièces jointes dans ces e-mails contenaient des « infostealers », type de malware destiné à voler des informations sensibles[1].

Si la crise met en lumière les inégalités d'accès aux nouvelles technologies, elle rappelle aux entreprises leurs devoirs, celles-ci semblent perçues comme les mieux placées pour construire la société demain. Ainsi, en France, 55% veulent croire à la capacité des organisations à édifier un monde meilleur pour les jeunes générations[2] ! Inspirant...

Très bonne lecture !

Sabine Terrey
Directrice de la Rédaction
sterrey@itpro.fr

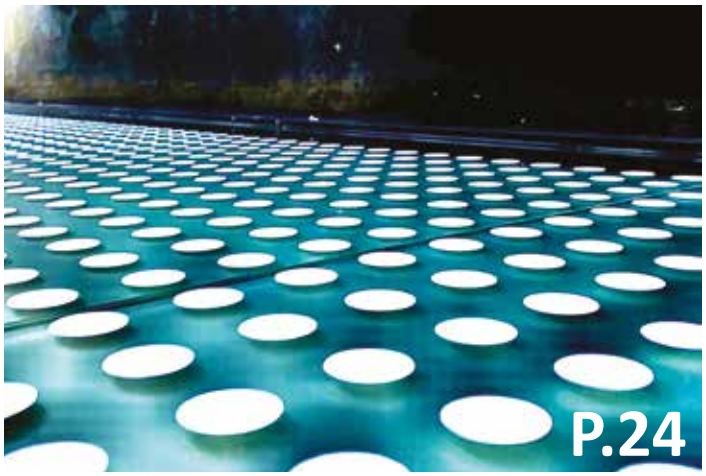
1- Source F-Secure: Attack Landscape H1 2020 Report
2- Source Salesforce -Global Campaign Stakeholder Series, Future of Work

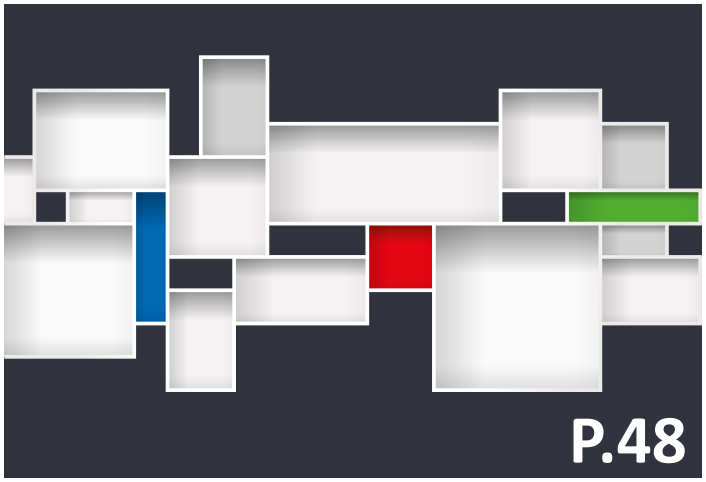
SMARTDSI
SMART DSI - ABOSIRIS
Service des Abonnements
BP 53 - 91540 - Mennecy - France
Tél. +33 1 84 18 10 50
abonnement@smart-dsi.fr
1 an soit 4 n° : 120 € TTC - TVA 2,1%

« SMARTDSI est la 1ère revue d'informatique professionnelle trimestrielle dédiée aux décideurs informatiques, aux décideurs métiers et aux professionnels des nouvelles technologies de l'information et de la communication (NTIC). La revue SMART DSI, au travers de chroniques, dossiers, études et analyses, constitue un formidable support d'informations stratégiques, de veille et de formation technologique, à l'intention des décideurs informatiques et experts métiers d'entreprise pour leur permettre de comprendre les enjeux, évaluer les perspectives et conduire, avec leurs équipes, la transformation numérique de l'entreprise ».

SMARTDSI

N°19 I SEPTEMBRE 2020





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, Laurent Teruin, Thierry Bollet.

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

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

Conception & Réalisation
Studio C4M – Philippe Deslandes
conseil@com4medias.com

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

N° ISSN : 2494-9701 - N° CPPAP : 0518 T 93059

Dépôt légal : à parution - Imprimé en France par IMPRIMATUR 87400 St Léonard de Noblat

Site officiel : www.smart-dsi.fr

CONNAÎTRE SES APPLICATIONS
POUR RÉDUIRE LES RISQUES INFORMATIQUES

> Par Didier Danse

Plus vite, plus souvent, tout en respectant de plus en plus de contraintes, voilà le quotidien des développeurs, quel que soit leur domaine d'activités. L'utilisation de composants tiers, payants ou non, s'avère alors nécessaire. Avec le lot de fonctionnalités apportées par le composant vient aussi une série de risques de sécurité ou de conformité.

Le pouvoir donné aux développeurs de déployer des applications de manière rapide sans requérir d'intermédiaire peut alors mener à un niveau de risque plus élevé que la normale. En effet, ces composants sont désormais la cible de personnes malveillantes, qui exploitent les failles connues du composant ou en y injectant du code malveillant.

La transitivité des dépendances doit d'ailleurs être prise en compte, sans quoi l'exercice s'avère totalement inefficace.

C'est alors que les équipes sécurité, généralement les premiers à détecter ces risques, font la grimace. Comment peuvent-elles être impliquées et partager la responsabilité de la sécurité de l'organisation ? Cette question, ou mieux encore sa version inclusive « Comment est-il possible de tenir compte de toutes les contraintes tout en atteignant l'objectif final, à savoir fournir des solutions utiles et sécurisées utilisables pour répondre aux objectifs de l'entreprise ? » refait à nouveau surface.

Voici alors une opportunité de donner de la visibilité et du contrôle à l'ensemble des intervenants et y inclure d'autres équipes, notamment les équipes en charge des aspects conformité. L'analyse de la composition des applications répond à ces besoins.

Identifier ...

Diverses techniques existent pour identifier des failles de sécurité, notamment l'utilisation d'outils de tests, que ce soit en statique ou en dynamique, comme nous avons pu le voir dans un précédent article.

Ce type de tests se limite cependant à ce qui est directement visible et ne permet pas d'identifier les risques légaux liés à l'utilisation d'une licence open-source ou de piloter les changements applicatifs, notamment liés à la découverte de failles de sécurité dans un composant après le passage au banc de tests.

L'identification de ces vulnérabilités requiert la conjonction de différentes sources, y compris les outils de suivi des non-conformités. Encore faut-il que la qualité soit là. En effet, il peut être simple d'obtenir des faux-positifs si ces sources s'avèrent peu fiables. C'est là que l'humain intervient pour combler les trous laissés par l'intelligence artificielle, même si celle-ci est en permanente évolution, et identifier les causes de ce faux-positif. Il faut également que l'information soit disponible en temps et heure. C'est dans ce contexte qu'en plus des bases de données partagées, de l'information exploitée par les fournisseurs eux-mêmes s'avère utile.

Par ailleurs, l'identification des licences associées aux composants s'avère plus critique qu'il n'y parait. Certaines licences requièrent en effet de publier le code source d'une application lorsque celle-ci inclut l'un ou l'autre composant. Ainsi, il est nécessaire de pouvoir identifier la licence associée mais aussi les changements apportés au composant, ces licences pouvant évoluer dans le temps.

Pour parvenir à un niveau de contrôle adéquat, il s'agit de faire l'inventaire des composants d'une application et des dépendances entre ces composants, quelles que soient l'application et la méthode de packaging, et ce y compris pour les containers ou encore le *serverless*.

La transitivité des dépendances doit d'ailleurs être prise en compte, sans quoi l'exercice s'avère totalement inefficace. Sur base de cette liste, il est alors possible de lister les vulnérabilités connues au sein de ces composants ou encore les licences associées.

... et le faire savoir ...

Avoir l'information disponible est une chose. La restituer intelligemment en est une autre. En effet, de nombreux acteurs doivent pourvoir disposer de ces données : les équipes développement, les équipes opérationnelles, la sécurité, le légal et l'équipe dirigeante, ce à quoi s'ajoutent les auditeurs et gestionnaires des licences. C'est ainsi que les systèmes en charge de l'analyse de la composition logicielle se doivent de proposer différents rapports avec des groupements et des filtres adaptés aux différents lecteurs.

En complément des filtres liés aux rapports, la navigation au sein de l'information est clé dans ce contexte. La sécurité se penchera davantage sur les vulnérabilités et le temps nécessaire au comble de ces vulnérabilités. Les équipes en charge des licences se pencheront plus sur les licences, idéalement associées au nombre d'occurrences de déploiement. Les équipes légales peuvent également analyser les différentes licences et ainsi identifier les risques qui y sont liés, et qui peuvent aller jusqu'à la publication complète du code source d'une application censée être le différentiateur de l'organisation.

Avoir l'information disponible est une chose. La restituer intelligemment en est une autre.

Il est également important de pouvoir faire des comparatifs dans le temps, que ce soit au travers de rapports fixes ou mieux encore, définis sur base de critères que chacun peut prédéfinir. Cela permet notamment d'entrevoir l'évolution dans le temps, pour un périmètre donné. Dans ce contexte, il serait fort utile de pouvoir définir des objectifs par périmètre.

... pour réagir au mieux

Maintenant que l'information est accessible, il s'agit de réagir. Réagir rapidement peut s'avérer nécessaire dans bien des cas. Pour réagir vite, il s'agit de comprendre la situation actuelle et les solutions futures. Pour cela, de nombreux fournisseurs de solutions partagent de la documentation indiquant la disponibilité de nouvelles versions ou encore des changements à proprement parler, tant dans le code que la configuration des systèmes.

Pour réagir vite, il s'agit de comprendre la situation actuelle et les solutions futures.

La seconde approche est d'avoir des automatismes, directement définis dans l'application : notifier, requérir des approbations et bien d'autres choses. Selon le système en place, cette approbation peut s'avérer une étape nécessaire, là où certains systèmes différentieront les composants approuvés des autres sans être restrictifs. L'automatisation peut d'ailleurs permettre d'approuver de manière automatique des composants sur base de critères donnés tels que le niveau de vulnérabilité et les licences utilisées. L'automatisme va jusqu'à la remédiation.

Faire réagir au plus tôt

En fonction du niveau de risque, tant au niveau de la sécurité ou du type de licences ou encore de la vie, il s'agit de notifier diverses équipes de l'évènement ou encore de simplement empêcher l'utilisation d'un composant en faute, notamment en le rendant indisponible dans son repository, pour autant que celui-ci le permette.

Le niveau de réaction doit se baser sur plusieurs facteurs dont le nombre d'utilisations des composants mais pas seulement. Les utilisateurs de ces systèmes doivent pouvoir garnir l'information déjà disponible avec des informations complémentaires, notamment le niveau de criticité des applications. Ces informations permettent alors de définir des actions en fonction de la criticité de la vulnérabilité ou le niveau d'utilisation d'un composant et surtout dans quel contexte le composant est utilisé. En effet, le risque associé à l'utilisation d'un composant est très variable d'un applicatif à l'autre. L'utilisation d'un composant dans un applicatif bancaire ou utilisant des données sensibles tels que les applicatifs médicaux rendra le niveau de criticité bien plus élevé que l'applicatif interne en charge de la réservation de matériel, bien qu'il s'agisse du même composant.

Comment choisir son outil d'analyse de la composition des logiciels ?

Pour quoi faire ?

Tout d'abord, il est nécessaire de définir une stratégie de gestion des composants, et une série d'objectifs, qui en découle.

La stratégie doit permettre, en effet, de répondre à certaines questions pour l'opérationnalisation :

- Quelle structure mettre en place ?
- Faut-il mettre en place une équipe centralisée ?
- Et dans ce cas, quel est son rôle ?
- Quelles sont les responsabilités des uns et des autres ?
- Au-delà des développeurs, quelles sont les autres équipes qui interviennent dans l'organisation ?

En effet, tous les outils ne proposent pas tous les mêmes fonctionnalités ni avec la même approche. Ainsi, certains outils s'avèrent plus adaptés à certaines audiences et cas d'utilisation. Le niveau de tolérance aux faux-positifs, liés à l'organisation, doit également être pris en compte. L'approche proposée par les fournisseurs pour réduire les faux-positifs entre également en ligne de compte.

Quoi qu'il en soit, l'outil d'analyse se doit de couvrir un maximum de cas d'utilisations et de s'intégrer avec un plus grand nombre, et ce, afin d'éviter le besoin de passer d'une application à l'autre.

Le niveau de tolérance aux faux-positifs, liés à l'organisation, doit être pris en compte.

Un élément d'un écosystème complet

L'outil d'analyse, pour être efficace, se doit de s'intégrer dans un écosystème. Certains outils excellent dans ce domaine puisqu'ils s'intègrent avec tout ou presque, là où d'autres se limitent à certains systèmes tiers, langages ou *frameworks*.

Un tel outil permet d'être exploité totalement lorsqu'il fournit de l'information directement aux développeurs, dans leur environnement de développement mais aussi au sein de leur pipeline *CI/CD*. De plus, il s'agit également de s'intégrer avec les outils tiers utilisés par les développeurs eux-mêmes, tant en entrée qu'en sortie : gestionnaire d'artefacts mais aussi les suivis des problèmes et les outils de sécurité afin de notifier directement ceux-ci de tout risque au niveau sécurité.

En entrée, les issues trackers publics peuvent s'avérer très intéressants puisqu'ils servent de référence.

En entrée, les issues trackers publics peuvent s'avérer très intéressants puisqu'ils servent de référence. En sortie, il s'agit potentiellement de publier en retour des informations au sein des systèmes tiers afin de notifier, à la communauté de développeurs, les vulnérabilités ou les problèmes de licence par transitivité.

Qui sont les acteurs sur ce marché ?

Dans le domaine de l'analyse des composants logiciels, WhiteSource, JFrog, Synopsys, Sonatype, WhiteHat, Veracode et quelques autres se partagent le marché. Par simplicité, ces types d'outils avaient été classés parmi le *Static Application Security Testing* avec des nuances (scan de références et non de code) mais il s'agit en fait de SCA (Software Composition Analysis). Cependant le SAST vise le code là où le SCA se focalise sur les associations de composants. L'idéal est un outil commun pour les deux sujets.

WhiteSource est le plus avancé si l'on en croit Forrester. Sa force est de couvrir un ensemble de besoins très larges, là où certains se focalisent sur l'un ou l'autre aspect, notamment du fait de leur présence sur des marchés de niche. Ainsi, certains favorisent la notion de dépôt ou encore le référentiel de code source auxquels sont greffées des solutions d'analyses. WhiteSource a pris l'autre pendant : s'interconnecter avec ces outils spécialisés. Sur le terrain, WhiteSource s'avère, en effet, adapté à une utilisation globale en proposant des utilisations de niveau plutôt élevé dans tous les domaines. Il faudra pousser l'utilisation de l'outil très loin pour rencontrer des besoins suffisamment spécialisés pour ne pas être couverts.

Prenons un autre exemple : JFrog, le leader dans le domaine des référentiels d'artefacts, s'avère également efficace dans le domaine, grâce au composant Xray. Pourtant, comparé aux leaders du marché, il s'avère qu'il y a de nombreuses limites puisque XRay scanne uniquement ce qui se trouve dans son propre référentiel. Ainsi, si JFrog Artifactory est l'unique référentiel, Xray devient fortement efficace. Fort heureusement, Artifactory peut se targuer d'agir en tant qu'intermédiaire pour récupérer des artefacts d'autres sources. Ainsi, il peut s'avérer parfois un peu léger quand il s'agit d'identifier au plus tôt. La combinaison des deux pourrait alors amener des résultats très intéressants, bien que l'un ou l'autre pourrait largement convenir dans des cas spécifiques.

L'agilité et la progressivité seront pourtant des facteurs clés pour permettre à chacun de comprendre et apprendre.

En plus de cela, pour réagir au plus tôt, l'intelligence artificielle et le machine learning s'avèrent plus qu'utiles. Ainsi, plus le système aura accès un maximum de sources d'informations, notamment le code source lui-même, ce qui permet d'identifier comment les composants sont utilisés, plus il pourra apprendre des risques. Si l'envie vous venait d'envisager l'utilisation de telles solutions, n'oubliez pas de vérifier que le système lui-même n'envoie pas trop d'informations vers des services tiers, ce qui pourrait compromettre l'intégrité de vos données. Un comble quand on pense que l'introduction d'un tel outil a pour but d'identifier des vulnérabilités introduites grâce aux composants open source.

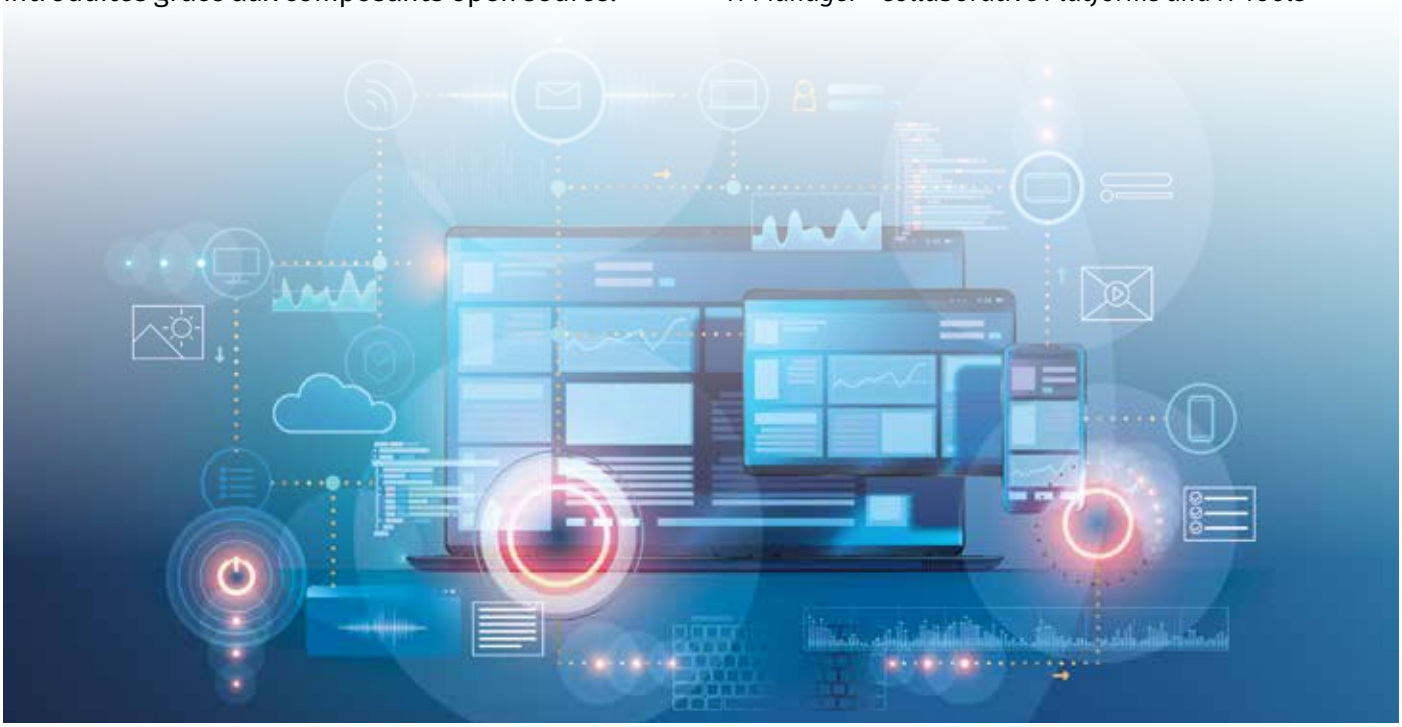
Comment démarrer une fois l'outil en place ?

L'outil a été choisi, c'est déjà une bonne chose puisqu'il permettra de rendre concrètes les actions mais aussi les résultats. Il s'agit alors de promouvoir la prise de conscience et la responsabilité au plus proche des ceux qui développement les applicatifs. Mais aussi, il s'agit de mettre en avant la collaboration entre entités, qu'il y ait une équipe centrale ou non. L'ensemble des équipes doivent partager des objectifs et non découpler les objectifs pour éviter la mise en compétition voire même la mise en opposition de celles-ci. Pour y arriver, il sera certainement nécessaire de mettre en place des formations en vue d'augmenter la connaissance des différents intervenants.

En parallèle à cela, il est nécessaire de définir des règles de gestion. On pourrait être tenté de définir l'ensemble des règles et de chercher à s'y tenir absolument. L'agilité et la progressivité seront pourtant des facteurs clés pour permettre à chacun de comprendre et apprendre.

Avant de chercher à bloquer l'utilisation d'un composant, il s'avère certainement bien plus utile d'identifier les composants et de comprendre ceux-ci pour mieux identifier les sources de risques. Encore une fois, l'accompagnement de l'ensemble des intervenants est certainement une clé importante, que ce soit par l'équipe centrale ou une équipe formée temporairement pour accompagner les autres.

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




STORMSHIELD
Le choix européen de la cybersécurité
Partenaire de confiance
pour
vous donner
la liberté
d'entreprendre
en toute sérénité
IT
OT
www.stormshield.com

Ransomware : ENNEMI PUBLIC Nº 1

Quand on parle de cybersécurité, on cite beaucoup de dangers : vol de données, d'identité, de données personnelles, fraude, espionnage, phishing, usurpation d'identité, etc. etc. Mais, l'explosion des cyberattaques par ransomware est devenue le principal problème des entreprises. Et, malgré une croissance constante des dépenses de cybersécurité, le rançongiciel fait de plus en plus de dégâts.

Un incident de type ransomware est souvent une triple peine : l'informatique est bloquée, voire détruite ; les données sont perdues ; l'entreprise paye la rançon mais ne récupère souvent rien...

Se protéger....

Certes, une attaque par ransomware est souvent initiée par du phishing, un peu à l'instar d'un virus porté par un manque d'hygiène ou des gestes barrières non respectés. Je n'oublierai jamais la détresse du dirigeant d'une PME du nord de la France, leader dans la distribution de produits auprès de professionnels et artisans, qui avait investi dans un entrepôt moderne et entièrement robotisé et doté de processus efficaces mais dont l'informatique/bureautique pour la prise de commandes, la facturation, la base des clients, etc. était restée non protégée et qui a dû arrêter son activité pendant plus d'une semaine à cause d'un rançongiciel.

Alors que les dépenses informatiques se contractent dans la plupart des secteurs et des technologies à la suite d'une pandémie et de la crise économique qui s'en suit, les dépenses mondiales en produits et services de sécurité devraient enregistrer une solide croissance en 2020, dopées par la montée des menaces de sécurité, estime IDC. Elles

« 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.

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

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

iTPro.fr

iTPro.fr

9 chaînes informatiques

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

Des ressources exclusives

Enjeux DSI
Cloud Computing
Collaboration & mobilité
Exchange Server
IBM i

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.

atteindront 125,2 milliards de dollars en 2020, soit une augmentation de 6,0% par rapport à 2019. On dépense de plus en plus pour protéger le lien restant des entreprises avec leurs clients, leurs collaborateurs et leurs partenaires.

En même temps, dans la vie des entreprises, on constate une explosion des cyberattaques par ransomware. Le rapport de cyber-assurance Beazley Breach Briefing 2020 fait état d'une augmentation des attaques par ransomware d'environ 130%. Celles connues car beaucoup restent cachées. Heureusement que le RGPD oblige les entreprises victimes d'annoncer l'incident.

S'appuyant sur des cas concrets, le rapport de Beazley répertorie 775 incidents de cybersécurité liés à un rançongiciel. Une véritable explosion, +50% au 1er trimestre 2020 par rapport au 4ème trimestre 2019 ! D'après le rapport, la progression entre 2018 et 2017, n'avait enregistré qu'une croissance de 20 %, pour ce type de cyberattaque.

Le montant des rançons...

Le même rapport évalue la somme demandée par incident à 111 605 $ en moyenne - en forte augmentation, avec le constat que plus l'entreprise est importante plus le montant de la rançon est élevé. Ce qui représente 33 % de plus au premier trimestre 2020 qu'au dernier trimestre 2019. Quant à la taille des entreprises victimes, le rapport indique que l'effectif moyen se situe entre 500 et 700 employés, c'est-à-dire en baisse d'une année sur l'autre – les attaquants visent donc des entreprises de plus en plus petites.

A propos des récentes attaques par ransomware, de grands groupes en France ont fait état (officieux) de rançons demandées de l'ordre de la dizaine de millions de dollars. Peu importe que les entreprises-victimes aient payé ou non la rançon.

Dans son récent rapport annuel sur la gestion des cyber-risques, l'assureur Hiscox indique que les pertes des entreprises ayant subi une attaque via un ransomware étaient presque trois fois plus importantes que celles qui avaient subi un incident de cybersécurité de type malware, soit 821 000 €.

Le même rapport Hiscox estime à 18% les entreprises françaises attaquées ayant versé une rançon, et 19% des victimes de ransomware assurent avoir pu récupérer leurs données « sans devoir payer de rançon. » Et les autres ??

A noter que selon Coveware, les attaques Ryuk et Sodinokibi représentent 33% de l'explosion des rançons payées durant le 1er trimestre 2020.

Que faut-il faire dans ce contexte ?

Avant toute chose, ***sensibiliser et former*** des utilisateurs de toutes professions au sein des entreprises, *l'awarness* comme disent les Anglo-Saxons, car le seul moyen de lutter contre le manque d'experts et d'ingénieurs est de remonter le niveau général de tous, de l'assistante au comptable, du chercheur au marketeur et au commercial. Le MOOC de l'ANSSI est un excellent outil de formation et sensibilisation.

Ensuite, ***se doter d'outils de sécurisation et de protection*** des vecteurs d'attaque, notamment protéger la messagerie et être vigilant dans la navigation web, car les attaquants arrivent dans la très grande majorité des cas par des mails de phishing ou des liens web.

Inutile de dire que les SOC d'entreprise sont clés dans la lutte contre les ransomwares.

Puis, ***surveiller, analyser, récolter et détecter les signaux faibles***, indicateurs de compromissions ; surveiller les postes de travail, pardon les end-points dans toutes leurs dimensions : remote/ télétravail, entreprises, smartphones, tablettes, etc. Inutile de dire que les SOC d'entreprise sont clés dans la lutte contre les ransomwares. Les grandes entreprises sont quasiment toutes organisées autour de CyberSOC dédiés, très souvent externalisés auprès de spécialistes.

Il faut aussi penser à ***inclure les maillons faibles*** comme les sous-traitants, les cabinets d'avocats, les prestataires marketing, les filiales éloignées, etc. qui souvent ne sont pas couverts. La capacité de résistance de la chaîne de protection est donnée par le maillon le plus faible !

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

LE DROIT À LA DÉCONNEXION : UN ENJEU RH

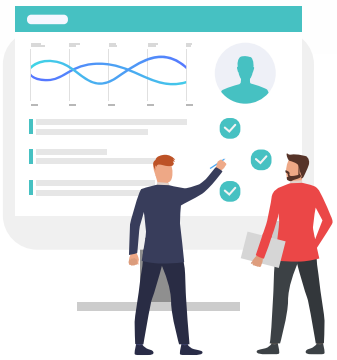
DANS UN MONDE RÉGI PAR L'IMMÉDIATETÉ,
LA DÉCONNEXION N'EST PLUS UNE OPTION, MAIS UN DROIT.

PROMODAG REPORTS PERMET LA CONFORMITÉ AVEC LE DROIT À LA DÉCONNEXION

GÉRER LA DÉPENDANCE EXCESSIVE AUX TECHNOLOGIES

LE DROIT À LA DÉCONNEXION EST UNE OBLIGATION LÉGALE

DES CHARTES DE BONNES PRATIQUES POUR LE CONFORT DES SALARIÉS



UN OUTIL AU SERVICE DES RESSOURCES HUMAINES

UNE SOLUTION DE SENSIBILISATION, D'ALERTE ET DE PRÉVENTION

PROMODAG REPORTS MAÎTRISE LE DROIT À LA DÉCONNEXION & PROTÈGE VOS SALARIÉS

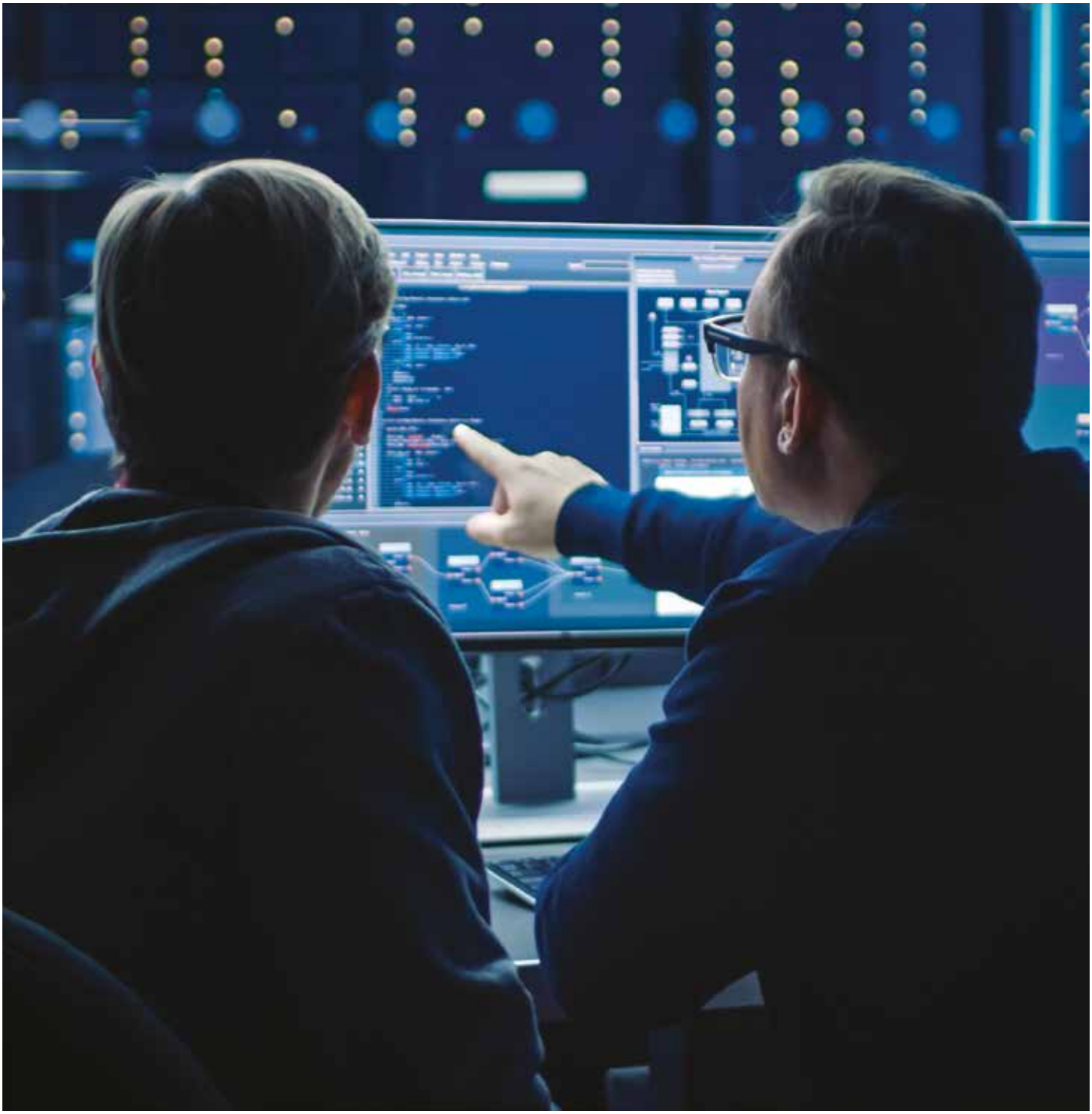
Découvrez la solution Promodag Reports

Promodag

www.promodag.fr

Quelques conseils POUR AMÉLIORER SA CYBERSÉCURITÉ DANS LE MONDE POST-COVID

Non. Je n'ai pas désiré écrire un énième livre blanc sur comment travailler à distance pendant l'épidémie de COVID. L'idée de ce papier est plutôt de comprendre les enseignements de cette période si particulière et d'en retirer les axes d'amélioration applicables au SI en termes de sécurité. Le sujet est vaste, mais tentons d'être pragmatique et concis afin de faire ressortir quelques conseils pratiques applicables par tout type d'organisation : Grande entreprise, PME, association, organisation publique, etc.



CE QUE LE COVID NOUS A APPRIS

Si l'évolution ne provoque pas le changement, la révolution l'oblige

S'il y a une seule leçon à retenir de la période COVID, c'est définitivement l'expression de la formidable capacité d'adaptation que possède toute organisation.

En quelques semaines, voire quelques jours, des millions de personnes ont pu commencer à télétravailler, des dizaines de milliers de personnes ont reçu des clés FIDO2 pour gérer l'authentification sécurisée et des milliers de serveurs RDP ou ICA ont été déployés. Qui l'aurait cru ?

Malgré les problèmes de budget et les limites techniques, les DSI ont su s'adapter, certes, parfois dans la douleur, mais restons positifs, cela a globalement fonctionné.

De plus, les « problèmes » de sécurité toujours enclins à retarder les projets traditionnels ont su être adaptés afin de répondre à l'urgence.

Nous ne le savions pas, mais l'agilité de nos entreprises Françaises est finalement exceptionnelle.

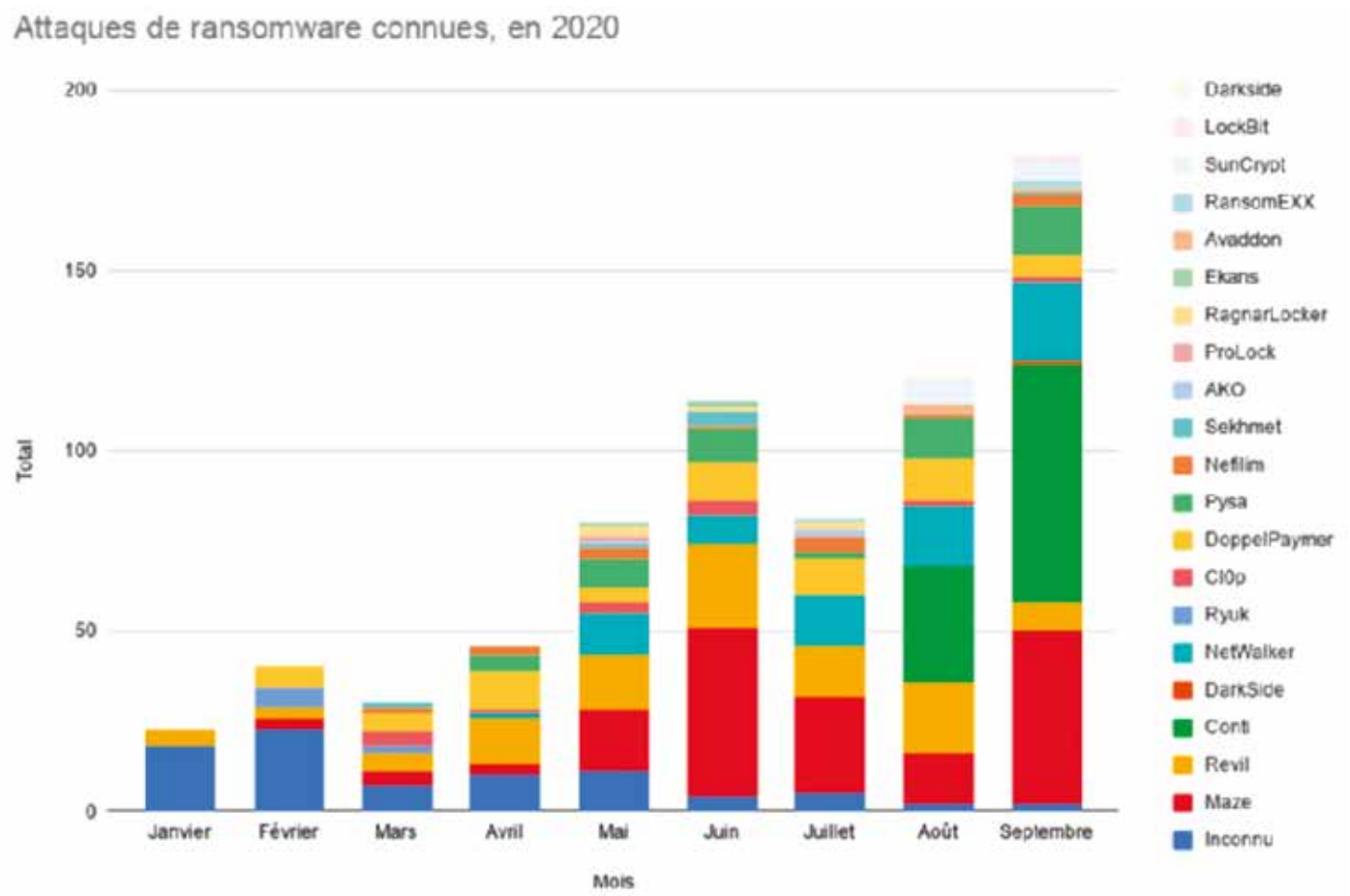
Le cyber-monde peut avoir des répercussions catastrophiques sur le monde réel

Dès le début de la crise, nous avons pu assister à une multiplication en règle des attaques provenant principalement de groupes mafieux organisés. L'objet de cet article n'est pas de réaliser une étude exhaustive de l'ensemble des risques IT pendant la crise COVID mais plutôt de mettre en lumière le fait que les attaquants n'ont aucun scrupule, l'objectif final est de « faire » de l'argent.

Il est classique de constater que les périodes propices aux cyber-attaques sont calquées sur les temps de faiblesse des organisations :

- Période de Noël en Europe
- Période de Thanks Giving aux USA
- Week-end ou vendredi soir
- Mois d'Août en France

Moins de personnes, des intérimaires non formés à l'ensemble des politiques de sécurité, multiplication des courriels promotionnels – ces périodes réunissent tous les ingrédients propices à une cyberattaque.



Source : https://bit.ly/33OGTQy

La période COVID n'échappe à la règle et nous avons constaté une augmentation drastique des tentatives d'attaques détectées.

Une image valant toujours mieux que de nombreuses explications, je vous invite à consulter ce graphique créé par Valery Marchive illustrant les attaques connues de ransomwares en 2020.

Evidemment il ne s'agit ici que de ce qui est connu publiquement, nous pouvons facilement extrapoler vers un nombre réel beaucoup plus important.

Les hôpitaux ou cliniques ne sont pas épargnés, loin de là.

Une récente attaque de ransomware sur une clinique Allemande a provoqué le décès tragique d'une patiente, faute de pouvoir accéder à certains systèmes, la patiente n'a malheureusement pas pu être opérée. Ce terrible accident nous rappelle à nouveau que les attaques de ransomware sont opérées la plupart du temps par le crime organisé, et non pas par de « jeunes hackers » avides de sensations tapis dans leur garage.

Plus d'information sur cet évènement tragique consultable ici : https://bit.ly/3j0jge4

QUE RETIRER DE CETTE PÉRIODE ET COMMENT PRÉPARER LA SÉCURITÉ DE NOS SYSTÈMES IT POUR LE FUTUR

Essayons de lister l'ensemble des bonnes pratiques ou solutions devant être implémentées maintenant pour assurer un futur plus sécurisé pour nos organisations respectives.

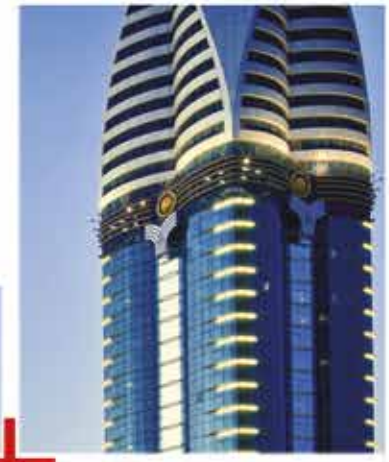
Adopter une solution anti-phishing

La première étape d'une attaque (en dehors de la reconnaissance sociale et technique depuis l'extérieur de l'entreprise) est quasiment toujours l'envoi d'un phishing contenant un lien piégé ou un document malicieux.

Evidemment avoir une solution anti-phishing ne résoudra pas tous vos maux d'un claquement de doigt, mais il est possible de réduire drastiquement le risque, il apparait qu'une solution anti-phishing reste un très bon investissement.

L'agilité de nos entreprises Françaises est exceptionnelle.

« COMPRENDRE LES ENJEUX, ÉVALUER LES PERSPECTIVES ET CONDUIRE LA TRANSFORMATION NUMÉRIQUE DE L'ENTREPRISE »



SMARTDSI

www.smart-dsi.fr

« Analyses, dossiers, chroniques pour conduire la transformation numérique de l'entreprise »

Conserver l'esprit d'initiative et d'agilité technique

Comme indiqué plus haut, l'ensemble des organisations Françaises ont fait preuve d'une résilience et d'une adaptabilité tout à fait remarquables. Il serait dommage de couper cet élan et de revenir à des postures et des méthodes peu constructives en termes de sécurité informatique.

Les points importants à retenir sont :

- **Mieux vaut couvrir 70% de son périmètre que rien du tout**

Remarque classique du RSSI pré-COVID : « je ne peux pas couvrir 100% de mon parc avec votre solution, donc je ne fais rien ». Cela parait fou, mais il s'agissait d'une attitude généralisée des responsables sécurité. La crise COVID a fait exploser ces postures, profitons-en et restons agiles

- **Ne pas avoir peur du cloud public, mais rester vigilant**

L'usage de solutions hébergées sur un Cloud Public peut générer une certaine réticence, néanmoins gardons à l'esprit que la capacité de résilience des différents fournisseurs Cloud est sans égale par rapport à ce que peut réaliser en interne une entreprise, quelle que soit sa taille. En effet, les fournisseurs de Cloud Public investissent massivement dans la sécurité de leurs systèmes et exécutent des points de contrôle en continu. Néanmoins il convient d'aborder le Cloud de manière structurée en s'assurant d'avoir une migration organisée et le déploiement des briques de sécurité minimales permettant un usage sans risques

Déployer une solution de MFA

Nous le savons tous, l'usage du mot de passe comme solution unique du contrôle de l'authentication est complètement dépassé par les techniques de hack actuelles. Il convient de déployer une solution de MFA pour tous les éléments accessibles sur un Cloud Public : Consoles des machines virtuelles, courriel, CRM, documents partagés, etc.

Très franchement, ceci n'est plus une option mais une obligation.

A nouveau il faut savoir rester pragmatique : vous n'avez pas les moyens d'équiper tous vos collaborateurs avec des clés FIDO 2 ? Pas de problème, achetez des clés FIDO 2 pour les populations à risque : Directeur financier, RH, compatibilité, comité directeur, etc. Et activer le MFA par SMS pour les autres. Mieux vaut un mot de passe + SMS que seulement le mot de passe. Ce n'est pas parfait, c'est contournable, mais vous éliminerez environ 80% des risques liés à l'accès aux données. A nouveau, 80% c'est mieux que 0%.

Il se trouve que dans 85% des cas, les malwares vont utiliser Active Directory pour passer à l'échelle.

Assurez-vous de votre bonne conformité Active Directory et surveillez-la en temps réel

Vous l'avez bien compris, les malwares sont en vogue. Et cela n'est pas près de se terminer. Il se trouve que dans 85% des cas, les malwares vont utiliser Active Directory pour passer à l'échelle, c'est-à-dire pour se répandre dans l'entreprise. En effet, les attaquants sont eux aussi pragmatiques, ils savent que vous avez Active Directory, ils savent que vous l'avez installé il y a plus de 10 ans et ils savent que vous êtes très occupé.

Contrôler votre Active Directory c'est contrôler la quasi-totalité de vos applications et données, il convient donc de protéger cette pièce maitresse en s'assurant de sa bonne conformité de configuration. Dernier conseil, même si les audits « one-shot » peuvent trouver leur place dans votre plan de sécurité, n'oubliez pas qu'Active Directory est une cible vivante soumise à de nombreuses modifications journalières, la vérité de l'audit du Lundi n'est donc pas celle du lendemain.

Utiliser un « concentrateur » de logs et d'évènements

Je n'ai pas utilisé le mot SIEM volontairement. En effet, même si un SIEM commercial du marché peut tout à fait proposer cette fonction, il existe des moyens quasi gratuits de le faire. En fonction de vos moyens investissez dans un SIEM du marché ou installez un serveur SYSLOG sur un serveur Linux ou Windows. C'est moins sexy, les fonctions sont limitées mais cela peut faire l'affaire pour débuter. Encore une fois, mieux vaut un bon serveur SYSLOG que pas de concentrateur de logs du tout.

Si vous pouvez investir dans un SIEM, faites en sorte qu'il devienne l'outil principal de votre SOC, connectez l'ensemble des systèmes de sécurité intermédiaires vers le SIEM, chaque système intermédiaire fera son travail spécifique et n'enverra que des alertes pondérées et pertinentes vers votre SIEM – si le SIEM représente l'interface quasi-unique de votre équipe SOC, veillez à ne remonter que ce qui est important, sinon vos équipes sécurité seront noyées sous les évènements et ne distingueront plus la différence entre les alertes critiques et les faux positifs.

GOODMEETING

OPTIMISEZ LA GESTION DE VOS SALLES DE RÉUNION

www.goodmeeting.fr

Quand cela est possible, appliquer la philosophie Zero-Trust même aux systèmes on-prem

Ok… Je sais… ZeroTrust est le « buzz-word » à la mode et quand on rentre dans les détails de Zero Trust il est très compliqué de comprendre ce qu'il faut faire exactement. En toute honnêteté, je suis d'accord.

Néanmoins.

Il faut comprendre que ZeroTrust est une philosophie, et non une technologie. Cette philosophie s'appuie sur plusieurs piliers, chaque consultant sécurité possède sa propre grille de lecture sur le sujet, je ne vous donnerai ici que ce je considère comme primordial à comprendre, en rajoutant un gros niveau d'abstraction afin de ne pas perdre mes chers lecteurs :

- **L'authentification ainsi que l'autorisation se décident au plus près de la donnée :** En clair, cela signifie que le contrôle d'accès doit se faire au plus proche du système qui contrôle la donnée, voire de définir des briques de contrôle propres à la donnée elle-même. Par exemple on demandera un MFA pour accéder à un document financier important à chaque fois que celui-ci sera ouvert mais on se contentera d'un mot de passe pour accéder à un document du marketing sauf si un nouveau périphérique inconnu est utilisé pour y accéder

- **ZeroTrust n'est pas que pour le Cloud :** Si les principes de ZeroTrust semblent fondés pour le Cloud, ils peuvent s'appliquer à certaines portions de vos environnements on-prem – n'hésitez pas à répertorier vos systèmes locaux et étudier comment appliquer ZeroTrust à ces systèmes, c'est tout à fait possible

- **Définir des micro-périmètres :** Un micro-périmètre est un ensemble logique de ressources, de données et de briques de sécurité. Plutôt que de vouloir gérer l'ensemble de la sécurité de façon contrainte et centralisée, l'idée consistera à définir une solution de sécurité adaptée à chaque micro-périmètre – Par exemple Active Directory peut être considéré comme un micro-périmètre dans le modèle ZeroTrust

Les contrats d'assurance ne couvrent pas tous les coûts liés au risque Cyber.

Se préparer au pire

Il est important d'anticiper les situations de crise. Pour cela, il existe des éléments de base que vous devez vérifier et maitriser le jour J, sans hésitation et sans vous poser de questions :

- **Avoir une version papier de certaines informations :** En cas d'attaque de cryptolocker, une grande partie de vos données ne sera plus accessible. Il est donc important de créer et conserver une version papier des informations primordiales que vous devrez maitriser pendant une crise de sécurité majeure : Numéros de téléphone des membres des équipes sécurité, Adresse IP, schéma du réseau, mot de passe de certains comptes importants, schéma des flux entre applications, etc.

- **Avoir contracté en amont avec un fournisseur de services spécialisé dans la réponse à incident :** Si vous subissez une attaque en règle, vous aurez certainement besoin d'aide de la part d'un spécialiste de la réponse à incident. L'idéal est d'avoir réalisé le travail contractuel en amont : renseignez-vous sur ces sociétés, rencontrez-les, et contractez une prestation de service de réponse à incident déclenchable dans un délai raisonnable. Dans ces conditions, vous n'aurez pas à vous soucier des éléments contractuels liés aux achats lors de la crise, vous aurez certainement d'autres priorités à gérer

- **Vérifier en amont votre contrat d'assurance :** il est possible que votre contrat d'assurance couvre certains risques cyber, il s'agit parfois d'une option au contrat. A nouveau l'idée est de connaitre en amont les éléments contractuels et de savoir quelles informations vous devrez fournir à votre assurance afin d'être couvert. Les contrats d'assurance ne couvrent pas tous les coûts liés au risque Cyber, mais c'est toujours bien d'avoir un peu d'aide financière ou de conseil pendant ces périodes tendues

Profitez de cette période pour revoir vos plans de sécurité et anticiper l'avenir, le monde après-COVID ne sera pas exactement comme celui d'avant, nous devons nous adapter et améliorer notre niveau de résilience afin de faire face aux crises futures.

Par Sylvain Cortes – Security Evangelist – Microsoft MVP

Blog : www.identitycosmos.com

« 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.

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

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

iTPro.fr

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

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

iTPro.fr

9 chaînes informatiques

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

Des ressources exclusives

Enjeux DSI
Cloud Computing
Collaboration & mobilité
Exchange Server
IBM i

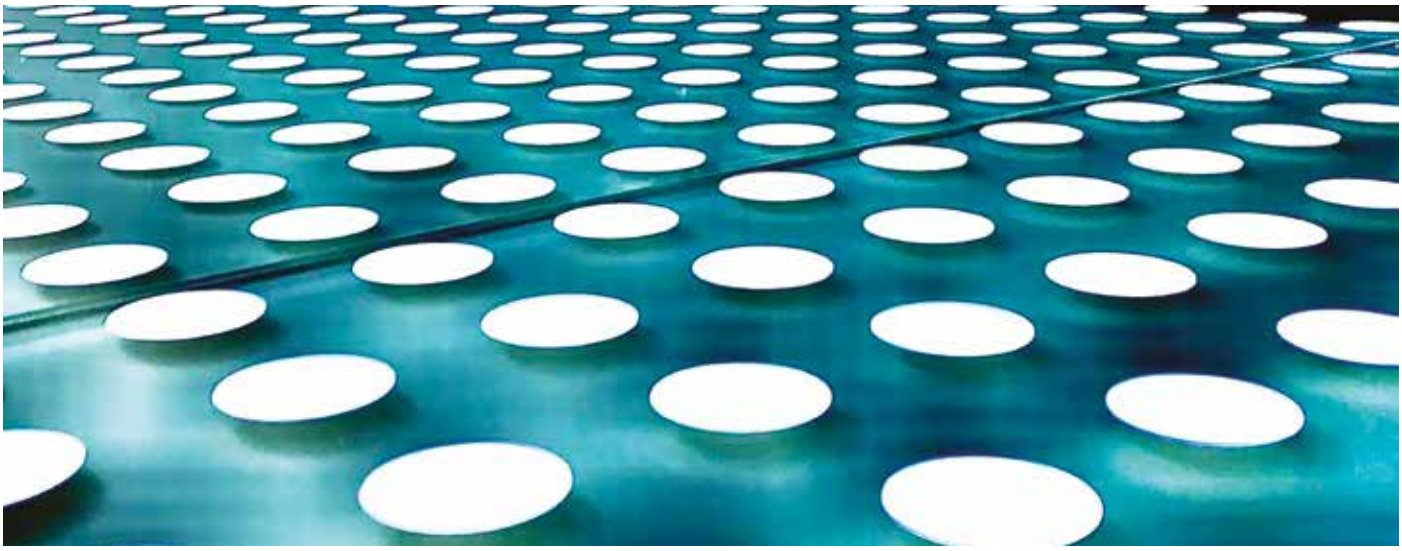
Un Club Abonnés

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

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.

Dastra SIMPLIFIE LE QUOTIDIEN DES OPÉRATIONNELS DE LA DONNÉE

Capitaliser sur les données est devenu l'une des priorités pour les organisations. Cela va sans dire que la sécurité est au cœur des stratégies d'autant que le travail à distance s'accélère. Retour sur le sujet avec Paul-Emmanuel Bidault, CEO de Dastra qui entend partager une vision responsable de la donnée !



Pourriez-vous nous présenter la société et évoquer l'idée de sa création ? Qu'est-ce qui vous différencie ?

Dastra (www.dastra.eu) est une nouvelle legaltech lancée pendant le confinement par quatre spécialistes complémentaires : consultant en gouvernance de la donnée, ancien juriste du service des sanctions de la CNIL, développeur full Stack et collaboration en mode SaaS.

Depuis mai 2018, nous avons discuté avec plus d'une centaine de Data Protection Officers de tout secteur et de toute taille, qui nous ont fait part de leurs difficultés à aborder l'angle IT du RGPD. Vu souvent comme une simple contrainte juridique par de nombreuses organisations, notre étude métier nous a confortés dans l'idée que des solutions techniques devaient être trouvées pour faire gagner du temps aux opérationnels, réduire les risques juridiques et sécuritaires, mais surtout apporter des solutions collaboratives techniques en API ouverte pour responsabiliser la communauté de la donnée dans les entreprises.

Plus de 60% des DPOs se sentent isolés dans leur entreprise.

Le temps de sécuriser nos situations respectives, nous avons lancé Dastra (pour Data - Stratégie) dès le début du confinement et en 6 mois, nous comptons déjà plusieurs DPOs clients motivés par l'envie de construire avec nous des outils qui apportent de réelles solutions aux opérationnels de la donnée dans les entreprises.

Vous constatez que les DPOs sont souvent isolés. Pourquoi ? Comment l'offre collaborative Dastra vise à simplifier la vie des opérationnels ?

Une étude du ministère du travail publiée en mai 2019 est sans appel : plus de 60% des DPOs se sentent isolés dans leur entreprise, et près de 42% d'entre eux estiment que leurs recommandations ne sont pas suivies par les métiers. Je pense que cela vient du fait que le DPO est aujourd'hui perçu comme un régulateur interne plutôt qu'un facilitateur au service d'une gestion fine des données dans l'entreprise. Or, c'est bien un rôle de chef d'orchestre qui lui incombe, avec comme objectif principal de responsabiliser et conseiller l'ensemble des opérationnels : SI RHs, achats, marketing, DSI, RSSI...

LES ASSISES

14.10.20 → → 17.10.20

/MONACO///

→ lesassisesdelacybersecurite.com

COMEXPOSIUM

DG CONSULTANTS

Paul-Emmanuel Bidault

Chez Dastra nous avons conçu des outils simples qui permettent d'une part au DPO de coordonner et piloter la conformité dans son quotidien, et d'autre part qui permettent aux opérationnels de la donnée de gagner du temps, de la conception de nouveaux produits jusqu'à la mise à jour des différents processus techniques et organisationnels.

Nous avons donc développé un logiciel RGPD en mode SaaS qui va aider les métiers à cartographier et automatiser certains processus techniques et organisationnels énergivores. Parce que chaque organisation est différente, il était nécessaire de construire un outil simple, collaboratif, Data-driven, en API Ouverte, mais aussi extrêmement flexible pour s'adapter aux différents modes d'organisation.

La solution entend donc gérer les risques RGPD : quelles sont les fonctionnalités clés à retenir ?

Gérer les risques est une chose, mais quand on sait que les risques sur les données personnelles dans les entreprises sont protéiformes et changent constamment, nous avons conçu plusieurs solutions pour :

- Cartographier visuellement les données des entreprises,
- Gérer et mettre à jour les registres facilement, avec la possibilité, par exemple, de s'inspirer des modèles de la CNIL, ou de construire des liens hiérarchiques entre les traitements - très utile lors d'un groupement de plusieurs entités juridiques par exemple,
- Gérer, piloter et valider le plan d'action de mise en conformité au RGPD,
- Gérer les exercices de droits, avec notamment la possibilité d'installer un widget sur le site de nos clients pour automatiser la validation de l'identité des demandeurs et centraliser la communication entre demandeurs et métiers,
- Gérer le registre des violations de données,
- Mais aussi gérer les consentements cookies avec un widget à intégrer sur le site internet de nos clients.

Nous avons développé un logiciel RGPD en mode SaaS qui va aider les métiers à cartographier et automatiser certains processus techniques et organisationnels énergivores.

Tout cela bien entendu en API Ouverte.

Des solutions techniques pour automatiser une partie du PIA mais aussi pour gérer la documentation juridique sont en préparation d'ici à la fin d'année et devraient bientôt enrichir notre palette d'outils à destination des opérationnels de la donnée. Ces nouveaux héros qui ne demandent qu'à trouver des solutions simples à des problèmes d'apparence complexes : le challenge est de taille mais nous avons des idées !

> Par Sabine Terrey

Téléphonie dans le cloud : vers la maturité des entreprises européennes !

Quelle est la perception de la téléphonie dans le cloud et les motivations des entreprises à migrer ? Plus de 1000 décideurs IT se sont exprimés dans la 3ème édition du baromètre Mitel.

L'adoption de la téléphonie dans le cloud augmente en Europe, le modèle as a Service a le vent en poupe. De plus, rester agiles et productives quelles que soient les circonstances, sont des éléments indispensables pour les entreprises européennes. D'ailleurs 44 % sont prêtes à migrer leur centre de contact dans le cloud, + 29 points par rapport à 2018.

Agilité & Innovation

La recherche d'agilité est le critère N° 1 de migration de la téléphonie dans le cloud, notamment pour les besoins opérationnels (35%).

Le critère de l'innovation arrive en position N° 2 avec 28 % (81 % en 2018).

En 2018, 84 % considéraient le coût de la migration comme le principal critère de calcul de ROI. Aujourd'hui, les décideurs IT se concentrent sur le coût des équipements nécessaires (intégration d'applications métiers, centre de contacts), la maintenance de l'architecture cloud ou le coût de gestion de la transition.

Liberté & Mobilité

D'un point de vue contractuel et opérationnel, le besoin de liberté arrive en première position : pouvoir changer de fournisseur si le contrat de service n'est pas respecté est une priorité (46%).

Le développement du cloud et des applications en mode SaaS pousse à vouloir bénéficier d'un modèle contractuel libre et ouvert. Pour 36% des décideurs IT, les usages en mobilité font croître la demande de l'UcaaS, tendance qui va se poursuivre avec la crise sanitaire, et la volonté de mise en place d'une workplace hybride.

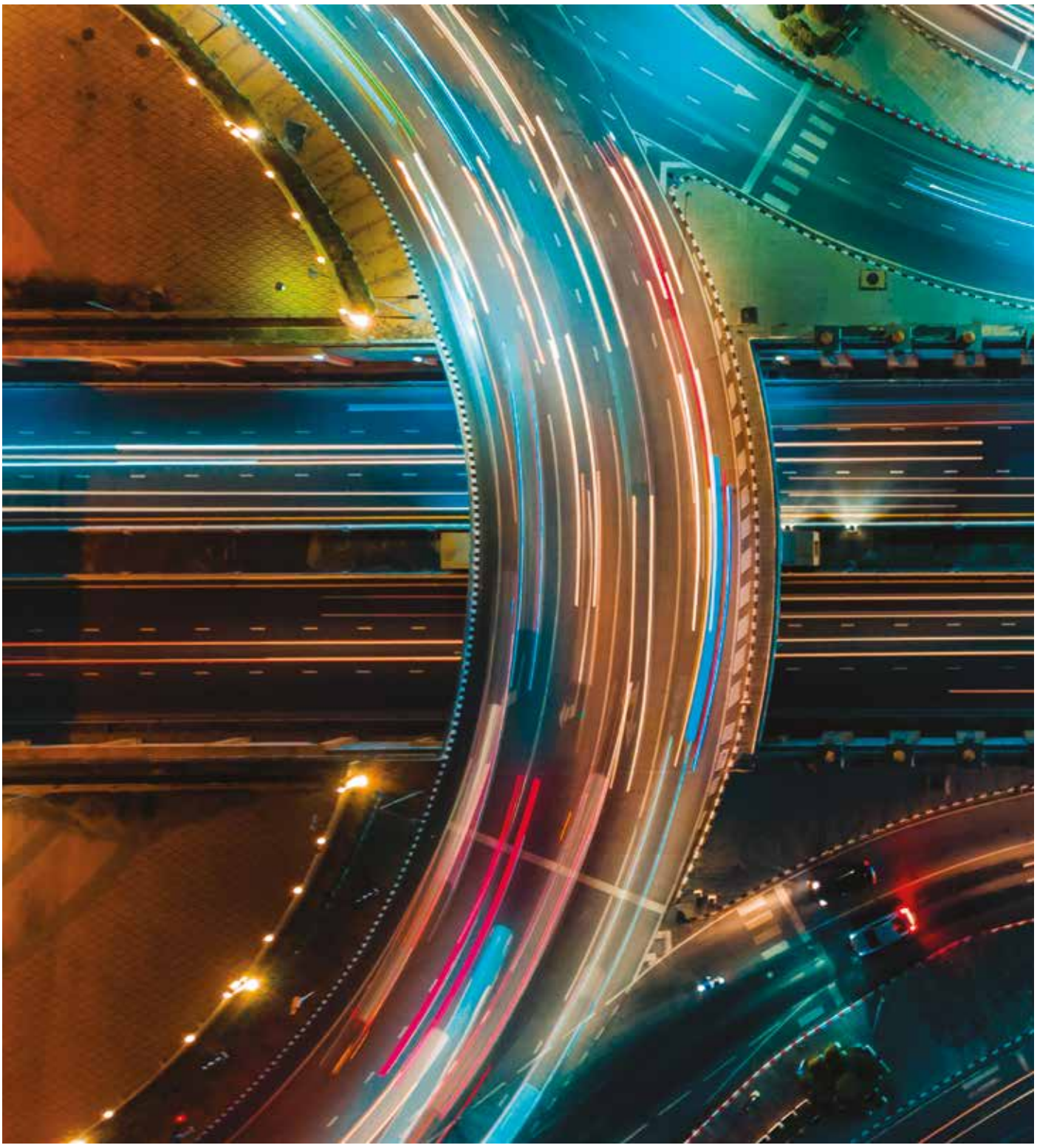
Les partenaires avant tout !

Si 24% des répondants songent à s'appuyer sur les ressources internes pour déployer la solution cloud, 29 % misent sur le binôme éditeur/ partenaire revendeur pour les accompagner dans cette migration. Selon Jean-Denis Garo, Directeur Marketing Intégré de Mitel, « Cette maturité technologique nouvelle est une opportunité et un défi pour les acteurs de la téléphonie, et notamment pour les partenaires revendeurs : en quête de liberté, les entreprises font le choix du cloud pour réaliser des économies et pour aussi s'affranchir des contraintes inhérentes à une solution on premise. »

Source Mitel & SpokingPolls - novembre 2019 / janvier 2020 - Allemagne, Espagne, France, Benelux, Royaume-Uni, Suède, Suisse - 1108 décideurs IT

Le Cloud
EST PERÇU COMME UNE PRIORITÉ AVEC LA CRISE DU COVID-19

Le temps est venu d'identifier et mesurer les défis informatiques posés dans les entreprises par la crise du Covid-19.



Plus de six mois après le début de la pandémie, les organisations s'efforcent d'optimiser leurs nouveaux modes de fonctionnement, basés en premier lieu sur le travail à distance. Il en ressort également que le Cloud, s'il était déjà ancré au cœur des stratégie d'entreprise, devient la priorité avec la crise sanitaire. Mais, la nécessité de contrôles accrus est primordiale.

Alors, quels sont les axes de réflexion menés par les dirigeants d'entreprise à retenir ?

- Le travail à distance s'est installé et va perdurer

La transformation digitale et les services gérés dans le cloud sont perçus comme une priorité. Le pourcentage des entreprises dont la majorité des employés travaillent à distance a plus que triplé : 21% avant la crise - 70% après. 40% des entreprises, soit deux fois plus qu'avant la crise, maintiennent une majorité des employés en télétravail.

- Les infrastructures informatiques et les contrôles de sécurité sont renforcés pour un travail à distance optimisé

La distribution d'équipements approuvés (35%), le renforcement de l'infrastructure réseau (35%) et la sécurisation du réseau (29%) sont les principaux défis informatiques liés à la transition vers le télétravail.

De meilleures technologies de détection et ou de réduction des menaces permettraient d'étendre le travail à distance dans l'organisation.

- La réduction des menaces et la visibilité du réseau restent les préoccupations de sécurité pour le travail à distance

De meilleures technologies de détection et ou de réduction des menaces permettraient d'étendre le travail à distance dans l'organisation (68%). Quant à la recherche d'une meilleure visibilité, elle se concentre plus spécifiquement sur les équipements connectés au réseau d'entreprise (65%), les applications cloud utilisées par les employés (61%) et les équipements infectés par des malwares (46%).

- La hausse des incidents de sécurité

Les entreprises constatent un nombre accru de cyber attaques – les plus fortes hausses étant signalées en Chine et en Australie – alors que seul un quart d'entre elles constatent une baisse.

- L'encouragement du travail collaboratif avec un changement des politiques et l'autorisation de l'utilisation d'applications personnelles

63% des entreprises autorisent les employés à communiquer entre eux via des applications telles que WhatsApp, Zoom, et Houseparty.

- L'utilisation d'outils de sécurité dans le cloud pour sécuriser le travail à distance

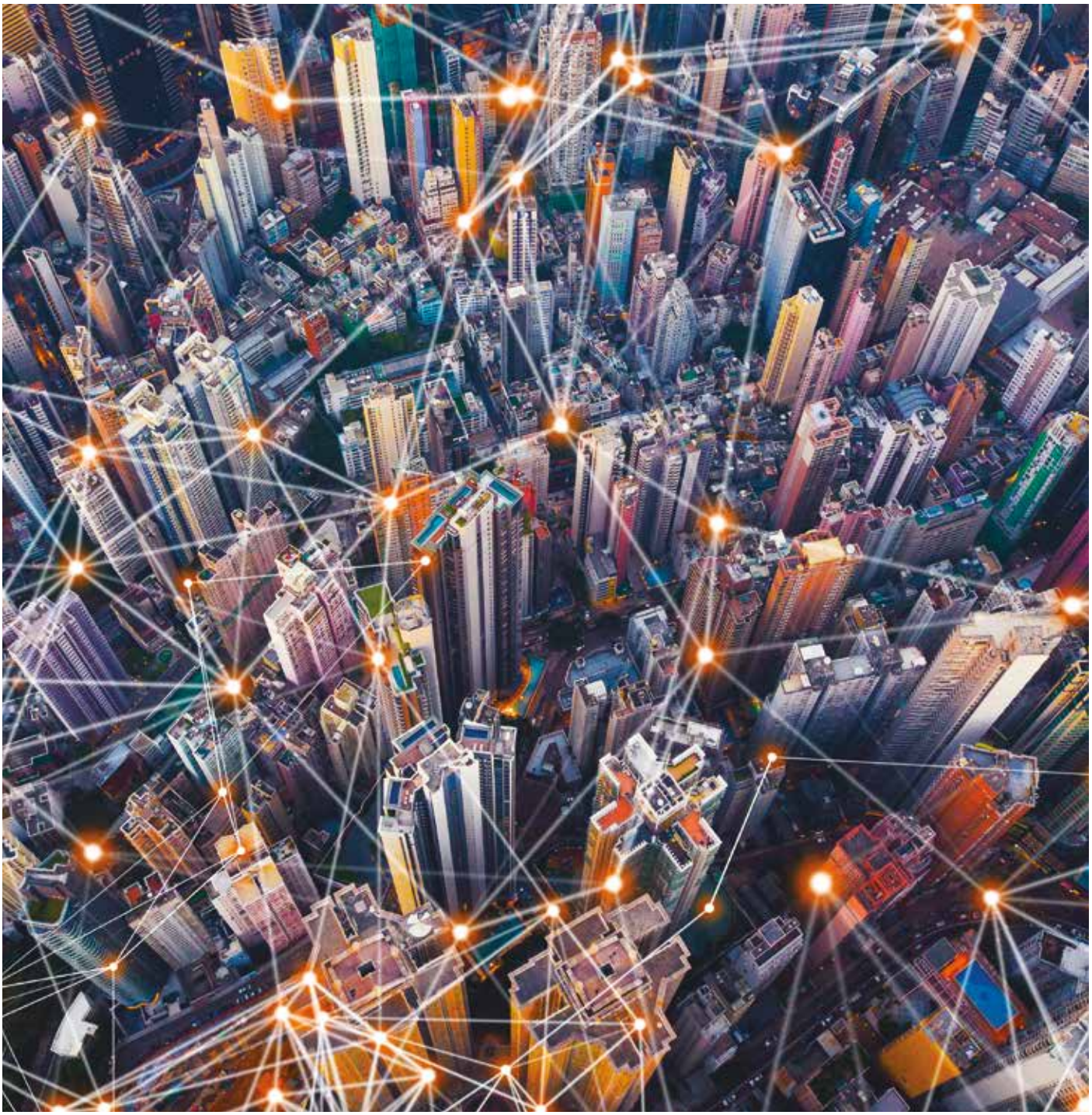
59% des entreprises prévoient des investissements supplémentaires dans les services DNS pour sécuriser leurs réseaux étendus.

> Par Sabine Terrey

Source Expertise Infoblox & Zogby Analytics

Cartographie des principaux métiers de la data POUR AIDER LES ENTREPRISES À APPRÉHENDER LES ENJEUX

Avec l'essor, de la data, les entreprises se posent un certain nombre de questions. Il est urgent d'y répondre. Pour cela, la commission Data de Syntec Conseil[1] vient de dévoiler un glossaire des principaux métiers de la Data. Un bon repère pour les acteurs de l'économie française !



Ce travail de classification et d'ordonnancement des métiers de la data matérialise la chaîne de la valeur de la donnée, puisqu'à chaque phase du traitement de la donnée intervient un métier spécifique.

« La constitution très rapide du secteur a eu comme principal effet pervers qu'un même métier soit compris et perçu de manière différente selon les entreprises, explique Arnold Haine, Chief Technical Officer du Groupe BVA et co-président de la commission Data de Syntec Conseil. L'exemple type est le métier de data scientist, qui pour certains est un statisticien, alors que pour d'autres, c'est un homme à tout faire de la data. Nous souhaitons donc aider les entreprises à mettre fin à cette confusion ».

Découvrez un partie de ce glossaire, fondamental à toute entreprise se transformant en une entreprise Data Centric.

Le Chief Data Officer

Le Chief Data Officer, CDO ou directeur des données, crée un environnement permettant aux différents responsables de l'entreprise d'accéder facilement - et en toute sécurité – aux informations dont ils ont besoin pour des prises de décisions stratégiques optimales. Il doit trouver les plateformes, systèmes logiciels de Data & Business Intelligence, et écosystème les plus appropriés pour que chacun puisse effectuer des analyses de manière autonome. Le CDO est au cœur de son organisation.

Le CDO est aussi responsable de la qualité et de la cohérence des données. Sa fonction croise donc celles d'autres métiers comme le contrôleur de gestion, le directeur informatique (DSI) ou le responsable des activités opérationnelles. Il officie en étroite collaboration avec tous les spécialistes des données au sein de son entreprise.

***Formation** : Bac+5 en Informatique, Management, Statistiques et/ou Marketing. Formations Big Data. 10 ans d'expérience*

Le CDO est aussi responsable de la qualité et de la cohérence des données. Sa fonction croise donc celles d'autres métiers.

Le Chief Analytics Officer

Il exploite des outils informatiques, techniques et utilise des méthodes statistiques (y compris data science) pour permettre d'organiser, synthétiser et traduire efficacement les données. Il repère, parmi toutes les informations à disposition de l'entreprise, quelles sont les plus importantes / pertinentes à extraire pour des prises de décisions optimales, en s'appuyant sur une méthodologie objective basée sur les statistiques. Il peut s'assurer que les informations recueillies en interne ou en externe sont fiables, cohérentes, et prêtes à être analysées. Il peut aussi piloter l'industrialisation du procédé pour les données les plus intéressantes. Il organise, synthétise et traduit les informations pour faciliter la prise de décision.

***Formation** : Bac+5 en Informatique, Statistiques. Cursus en Data Science ou en Econométrie. 10 ans d'expérience*

Le Data Protection Officer

Depuis l'entrée en application en mai 2018 du Règlement Général sur la Protection des Données, ce poste est obligatoire en Europe dans les entreprises et administrations qui traitent des données sensibles ou à grande échelle.

C'est un métier au carrefour du droit, de la sécurité informatique, de la conformité et de l'éthique.

Le Data Protection Officer (DPO) ou Délégué à la Protection des Données (DPD) a une mission d'information, de conseil et de contrôle de la gouvernance des données. Son défi est de se tenir au courant de tous les projets de l'entreprise lancés autour des données, pour pouvoir y apporter des préconisations suffisamment en amont dans des démarches privacy by design.

C'est un métier au carrefour du droit, de la sécurité informatique, de la conformité et de l'éthique.

Le DPO est chargé de veiller la conformité au règlement, de définir les rôles et responsabilités de chacun, d'établir une cartographie des traitements et flux de données, de tenir le registre des traitements et de piloter la gestion des incidents de sécurité (y compris avec les sous-traitants). En France, ce rôle prend souvent la suite de celui du Correspondant Informatique et Libertés (CIL).

***Formation** : Les DPO sont souvent des profils hybrides, qui peuvent mesurer les risques, piloter des projets IT, et intégrer la notion de « Privacy by design ».*

Le Data Architect

Il intervient en amont du traitement de la donnée pour organiser la récupération et la gestion des données brutes, plus ou moins structurées, en plus ou moins grande quantité et provenant de sources diverses (internes, externes). Après l'inventaire des données, il définit et optimise les infrastructures de collecte, de stockage, de manipulation et les

flux associés. Il propose des changements de modélisation pour répondre aux enjeux des métiers et faciliter le croisement des données en aval. Il peut être amené à travailler sur le dictionnaire des données, le design du MCD (Modèle Conceptuel des Données) ou l'état des lieux des référentiels en place. Le rôle devient de plus en plus clé dans un contexte d'architecture Cloud, ouverte, de temps réel et de contraintes de cyber sécurité et réglementaires.

***Formation** : Bac+5 en Informatique, Management, Statistiques, Formations Big Data, Ecole d'Ingénieur spécialisée, Maîtrise de la Business Intelligence et expérience nécessaire*

Le Data Steward est le référent dans un projet de gouvernance des données.

Le Data Engineer

Cet ingénieur data développe l'infrastructure définie par/avec le Data Architect. Il construit les solutions techniques robustes et fiables. Il en assure la maintenance et les évolutions conformément à l'état et des contraintes de sécurité. Il réalise l'intégration des données de diverses natures qui proviennent de ces sources multiples, les supervise et vérifie la qualité des données. En production, il assure le suivi et le monitoring des flux/interfaces de données. Il s'assure aussi que ses travaux sont suffisamment documentés.

***Formation** : Informaticien, il maîtrise un certain nombre de langages, technologies et méthodes : Python, SQL, ETL et ses versions "modernes" NoSQL (Hive, Impala, Spark SQL) et Hadoop pour la partie Big Data, le Cloud, les méthodes DevOps et CRISP. Bac+5 obligatoire. École d'Ingénieurs spécialisée*

Le Data Stewart

Ce contrôleur qualité et métiers de la donnée s'assure que les données sont bien pertinentes, présentes, conformes, cohérentes, comprises. Il traduit les règles métiers relatives à la qualité des données en requêtes (permettant leur vérification régulière), il définit les indicateurs de qualité et les seuils de tolérance correspondants. Le Data Steward est le référent dans un projet de gouvernance des données. Il joue un rôle clé dans sa réalisation, notamment parce qu'il détient la connaissance métier des données et de leurs métadonnées. Le Data Steward est une personne senior avec une autorité certaine dans l'organisation et qui a accepté d'être la personne responsable de la qualité d'un jeu de données défini comme, par exemple, le Directeur Financier pour les données financières.

Le Data Scientist

Il traite, analyse et valorise les données d'une entreprise afin de définir la meilleure stratégie de développement : stratégie marketing et commerciale, amélioration des performances et de la rentabilité, prospective... Cumulant la connaissance des outils mathématiques / statistiques et informatiques, il est capable de les coder (R, Python), de produire des méthodes (automatisées, autant que possible) de tri et d'analyse de données de masse et de sources plus ou moins complexes ou disjointes , et de construire des algorithmes "intelligents", afin d'en extraire des informations utiles. Les missions du Data Scientist sont différentes (souvent en lien avec le Data Engineer et le Data Architect) :

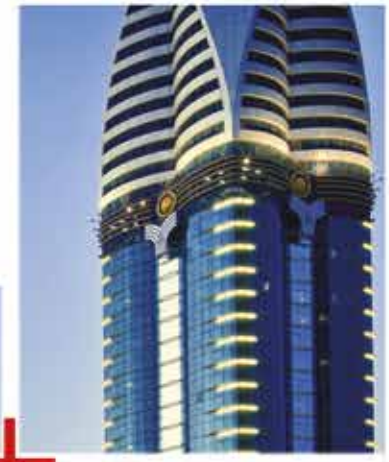
- Explorer de nouvelles sources de données pour élargir la capacité à identifier de manière plus précise et plus rapide des enjeux business et d'efficience opérationnelle
- Tirer profit des technologies de pointe pour obtenir une meilleure analyse des données et concevoir des modèles (prédictifs)
- Participer à l'industrialisation de ces modèles
- Combiner des méthodes d'analyse de données structurées et non structurées et de connaissances sur le domaine d'étude pour fournir aux métiers des modèles d'aide à la décision : Transformer les problématiques métiers en problèmes mathématiques. Appliquer les modèles statistiques pour expliquer un problème donné. Restituer aux métiers des présentations claires de l'analyse réalisée sur leurs problématiques, mettant en évidence les pistes d'évolutions possibles

***Formation** : Bac + 5, Informatique et Mathématiques avancées, Econométrie, Ecole d'ingénieurs spécialisée*

Le Data Consultant

Ce Data Analyst travaille en général sur un type spécifique de données issues d'une source unique et connue, qu'il analyse avec un regard « métier » afin d'orienter les prises de décisions stratégiques. Tour à tour en contact avec les Data Scientists et les experts métiers, il définit notamment des indicateurs clés de performance (KPI) pour vulgariser et restituer ses résultats aux décideurs sous un format exploitable. Il utilise les différents outils Data à sa disposition afin d'explorer, d'organiser, de synthétiser et de traduire les données brutes comme par exemple des tendances de consommation ou une évolution significative dans les profils d'acheteurs. Il peut être chargé plus largement de préciser à une organisation ce qu'elle peut attendre de ses données (y compris hors de ses domaines les plus courants) et d'apporter une réponse opérationnelle.

« COMPRENDRE LES ENJEUX, ÉVALUER LES PERSPECTIVES ET CONDUIRE LA TRANSFORMATION NUMÉRIQUE DE L'ENTREPRISE »



SMARTDSI

www.smart-dsi.fr

« Analyses, dossiers, chroniques pour conduire la transformation numérique de l'entreprise »

***Formation** : Bac + 5, Big Data et/ou Mathématiques et/ou Statistiques et/ ou Business Intelligence. École d'ingénieurs spécialisée*

Le Data Visualisation Consultant

Storyteller de l'entreprise, il est capable d'exploiter les données de l'entreprise, de les contextualiser et de proposer des visualisations simples pour en explorer le sens et les impacts. Grâce à un choix judicieux d'organisation spatiale, de liaisons entre les données, de couleurs, de formes, l'expert en data visualisation met en scène des données complexes, les rend intelligibles et accessibles dans le but de les présenter à des acteurs sans expertise technique. Ce profil a deux facettes : celui d'un expert d'outils de data visualisation faisant du reporting et du storytelling sur les données, ou celui d'un développeur qui crée des applications de data visualisation que ce soit en intranet, sur le web, sur des applications mobiles ou encore sur papier. Cet expert permet également aux équipes opérationnelles d'y voir plus clair dans leurs données en posant les bonnes questions, et d'identifier de nouvelles pistes d'analyse en explorant les données sous un nouveau jour. Il doit être capable de choisir les visualisations les plus pertinentes et susceptibles d'apporter le moins de biais.

***Formation** : Bac + 5, Mathématiques et/ou Statistiques + Business Intelligence (analyse de données et data visualisation). Ecole d'Ingénieurs spécialisée*

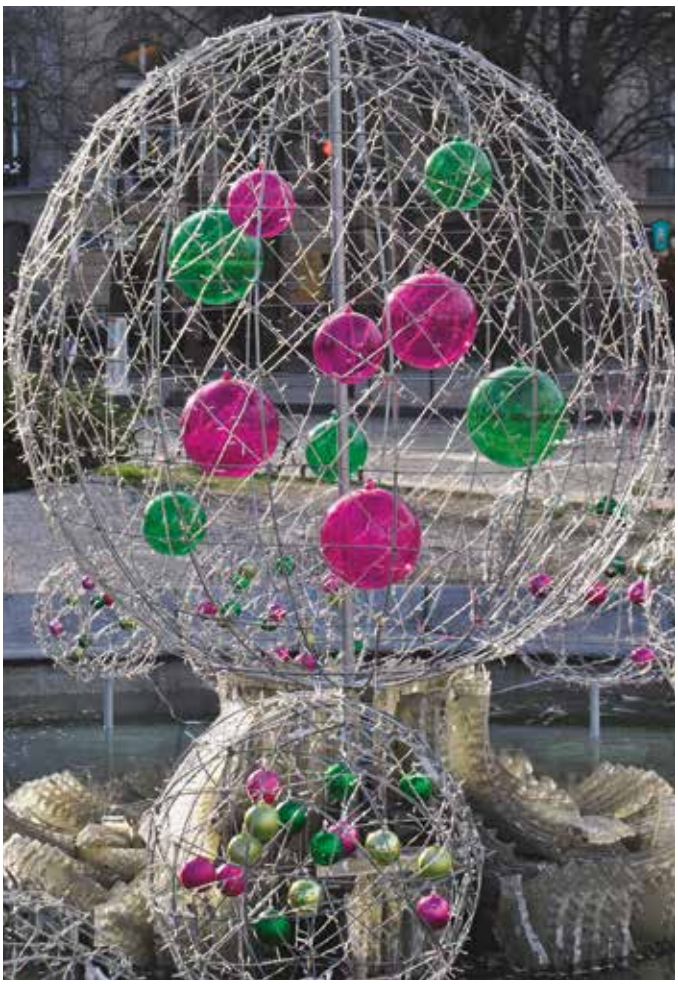
Le DataOps Engineer

Il orchestre le pipeline d'analyse de données en production, promeut les fonctionnalités de la production et automatise la qualité, toujours en lien avec le Data Engineer. Il s'assure aussi que les systèmes déjà en production sont disponibles et performants. Enfin, l'ingénieur DataOps évangélise les meilleures pratiques et les meilleurs outils parmi les équipes de science des données afin d'améliorer la productivité et d'éviter les erreurs courantes.

***Formation** : Bac+5, Informatique / Big Data. Ecole d'Ingénieurs spécialisée*

Enfin, l'ingénieur DataOps évangélise les meilleures pratiques et les meilleurs outils.

(1) Co-présidée par Jean-David Benassouli, Associé responsable de l'activité Data Analytics et Intelligence Artificielle au sein de PwC France et Arnold Haine, Chief Technical Officer du Groupe BVA, et composée de spécialistes de la data, de consultants spécialisés dans les ressources humaines et l'évolution professionnelle, la commission mène un important travail de classification et d'ordonnancement des métiers de la data.



La reconversion professionnelle après le déconfinement est-elle une réalité ?

Retour sur l'impact de la crise sanitaire pour les projets professionnels : des pratiques en matière de reconversion jusqu'aux motivations et facteurs de changement en passant par les freins !

La reconversion professionnelle plébiscitée

Le contexte sanitaire bouleverse les mentalités et n'en finit pas de questionner. En France, 1 actif sur 2 a envisagé, initié ou réalisé une reconversion professionnelle. Plus précisément, on remarque

- Une reconversion réalisée – 17%
- Une reconversion en cours – 5%
- Une phase de renseignements – 12%
- Une reconversion juste envisagée – 14%

Cette démarche est manifeste chez les actifs entre 25 et 44 ans et parmi ceux qui occupent le même poste depuis 4 ou 5 ans (63%).

1 actif sur 5 commence à se questionner sur la possibilité d'un changement pour donner du sens à son travail - 58%, et pour des contraintes personnelles – 31%.

La quête de sens avant tout !

La recherche d'un meilleur équilibre vie pro- vie perso et la quête de sens sont les moteurs du changement

Quels paramètres ont été déclencheurs ?

- L'ennui et le manque de sens dans leur poste actuel
- La pression subie dans leur emploi
- Les accidents de parcours : problèmes de santé (33%), contraintes familiales (20%), et licenciements/restructurations (26%)

Les actifs veulent se sentir utiles, redonner du sens aux actions, gagner en liberté ou en équilibre vie pro-vie perso et transposer leur passion en métier.

Les actifs, au stade de la réflexion, se partagent entre une meilleure rémunération et l'équilibre 'pro-perso'.

Service public, espaces verts & naturels, agriculture & pêche

Les actifs envisagent des reconversions en vue d'un changement de secteur d'activité notamment

- dans le service public
- les espaces verts et naturels,
- l'agriculture, la pêche
- les soins aux animaux

Quels sont les freins à la mise en œuvre des projets de reconversion ?

- La nécessité de préserver la sécurité financière (46%)
- Le manque de maturité du projet (32%)
- La crainte de l'échec (28%)

La formation à distance apparaît comme un levier concret de réussite à hauteur de 76%.

Source Enquête VISIPLUS academy & institut BVA- 19 au 25 juin 2020 – 1000 actifs : les projets de reconversion professionnelle des actifs français

ActiveViam FAIT TRAVAILLER LES DATA SCIENTISTS ET LES DÉCIDEURS MÉTIERS ENSEMBLE

Une plate-forme analytique pour prendre en main l'avenir de la société, c'est désormais un élément crucial. Qu'il s'agisse de détecter une anomalie, d'évaluer les risques ou bien encore de simuler différents scénarios, ActiveViam relève ces défis avec brio. Entretien avec Antoine Chambille, Directeur R&D chez ActiveViam. L'entreprise possède dorénavant cinq bureaux, New York, Paris, Toulouse, Londres et Singapour.

Pourriez-vous nous présenter ActiveViam et revenir sur un point de votre actualité ?

Depuis 2005, ActiveViam édite des solutions analytiques pour la prise de décision opérationnelle et la data science. La société compte plus de 60 clients internationaux, notamment des acteurs majeurs de la finance et de la grande distribution comme HSBC, la Société Générale, Intermarché ou encore Engie.

Nos produits sont construits en particulier autour de technologies d'agrégation in-memory et du Cloud pour permettre l'analyse en temps réel de grands volumes de données. Ils exploitent les langages Java, Python et Javascript pour offrir des capacités uniques sur le marché, comme de l'analyse multi-dimensionnelle entièrement libre et des simulations 'What-If' complètes à la volée.

Partis de l'analytique, nous nous sommes étendus vers la data science. En 2019 nous avons créé Data Lab pour accompagner nos clients et les aider à tirer toute la valeur de leurs données. En 2020, notre nouveau produit (gratuit) fait le pont entre le monde de la data science et celui de la prise de décision : atoti.

Il permet, d'un côté, aux data scientists d'explorer plus rapidement et avec plus de précision leurs données à petite ou grande échelle, et de l'autre, aux décideurs de consulter les résultats sous forme de dashboards interactifs.

Sur le plan commercial, nous avons lancé un projet de « pop-up offices », des bureaux éphémères que nous ouvrons un peu partout en France pendant deux ou trois jours pour aller à la rencontre de professionnels de la data. Les prochains se tiendront à Lille et à Lyon courant octobre.

« Sur iTPro.fr, nos experts vous accompagnent au quotidien pour vous aider à tirer le meilleur profit de vos environnements IT ... »

En ligne sur iTPro.fr, 9 chaînes d'information et de formation des experts en technologies informatiques d'entreprise, par les éditeurs de la revue SMART DSI.

Une bibliothèque de ressources éditoriales exclusive pour vous accompagner dans la gestion et l'optimisation de vos environnements IT Professionnels.

- Chaînes thématiques
- + 2800 Dossiers IT
- Guides exclusifs
- 7 Flux RSS
- Newsletters hebdos
- Videos &Webcasts
- Cloud
- Data
- Mobilité
- Sécurité
- IoT
- Enjeux IT
- Tech
- Boites à Outils
- Trucs & Astuces
- Hub éditoriaux
- Hors-Série
- Livres blancs...

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

Suivez-nous sur Twitter : www.twitter.com/itprofr

Partagez sur Facebook : www.facebook.com/www.itpro.fr

iTPro.fr

La bibliothèque éditoriale du site iTPro.fr est constituée de plus de 2800 dossiers technologiques signés par les meilleurs experts francophones et internationaux sur les thèmes de la définition, de la gestion et de l'optimisation des environnements IT Professionnels.

Pourquoi selon vous, est-ce un défi de faire travailler data scientists et décideurs métiers ?

Antoine Chambille

On pourrait dire qu'ils ne parlent pas le même langage, au sens propre comme au sens figuré. Les questions business posées par les décideurs métiers comme « Pourquoi mes ventes baissent ? Quel est le meilleur prix pour mes produits ? » doivent parfois être reformulées pour que les data scientists puissent trouver des réponses pertinentes et opérationnelles dans les données. A l'inverse, les réponses que trouvent les data scientists ne sont souvent pas immédiatement « consommables » par des non-experts qui ne sauront pas lire les résultats. Il faut les convertir en tableaux ou en graphes pour leur donner du sens.

Cela se retrouve aussi au niveau des outils. Pour un décideur métier, l'outil de prédilection, ce sont des outils de « business intelligence » comme Excel, Tableau ou Power BI. Pour un data scientist, cela varie selon les besoins et les habitudes mais aujourd'hui c'est Python qui est de loin le langage le plus répandu. Or, les deux univers ne communiquent pas ensemble, les data scientists recherchent en Python mais délivrent leurs résultats sous forme de dashboards dans d'autres applications. Dans les faits, cela veut dire pratiquement faire le travail deux fois, ce qui représente un temps important.

Dans ce cas, comment le data scientist peut-il travailler en collaboration avec les métiers ? quelle approche préconisez-vous ?

Chez ActiveViam, nous sommes des technologistes et notre réponse est donc technologique : c'est atoti.

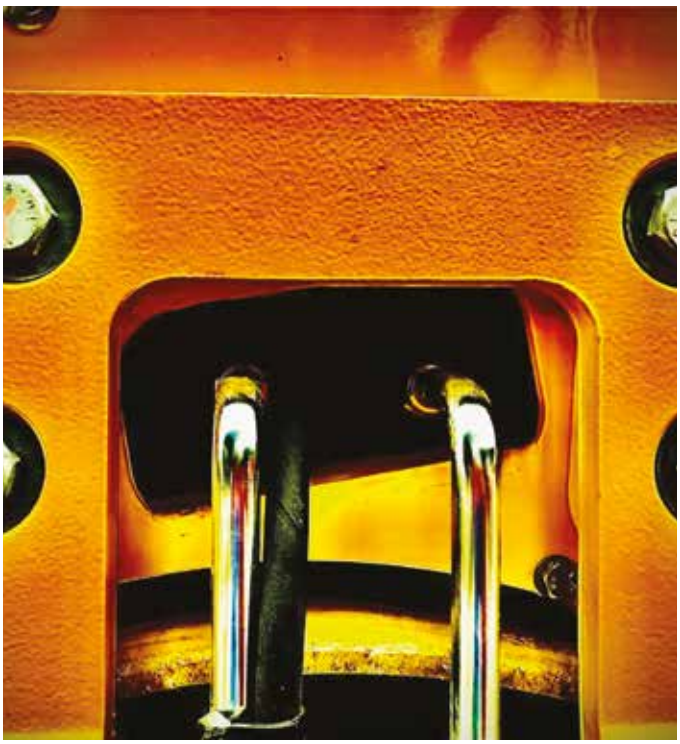
Cet outil est basé sur les technologies d'agrégation et de visualisation que nous avons développées depuis 15 ans et que nous avons intégrées avec les notebooks Python pour les rendre accessibles à 100% au public des data scientists.

atoti réunit la recherche et l'exploration des data en Python et la visualisation pour le business dans des tableaux de bord interactifs, le tout au sein d'un seul environnement dynamique et agile.

Cela permet une collaboration étroite entre les deux fonctions qui disposent d'une plateforme commune pour échanger et expliquer mutuellement leurs idées, valider de nouveaux modèles et co-construire des tableaux analytiques opérationnels.

Ce produit nous le mettons à disposition gratuitement de la communauté des utilisateurs et des data scientists sur atoti.io.

> Par Sabine Terrey



Cybersécurité : les 4 profils de collaborateurs

Plus aucun doute sur l'importance d'être sensibilisé à la sécurité informatique, mais les entreprises doivent prendre en compte la diversité des profils, les mentalités et les usages.

Top 10 des pays les plus consciencieux

Les salariés abordent différemment la cyber-sécurité ! Pour près des trois quarts (72% Monde et 77% France), ils se sentent plus investis dans la politique de cybersécurité de l'entreprise depuis le début du confinement.

Une grande majorité des Français fait confiance au service IT et est à l'écoute des conseils. La France est ainsi l'un des deux seuls pays européens à figurer dans le Top 10 des pays les plus consciencieux, avec la Norvège (76%).

Craintif, consciencieux, ignorant et téméraire

Pour adapter la stratégie de sécurité de l'entreprise au comportement des collaborateurs, il faut évaluer les 4 profils d'utilisateurs dressés par le Dr Linda Kaye, professeur en cyber-psychologie à l'université d'Edge Hill :

- les craintifs
- les consciencieux
- les ignorants
- les téméraires

Les valeurs, le niveau de responsabilité, la personnalité influent sur le comportement.

Le confinement : propice à la sensibilisation ?

Si le confinement fut une période propice pour les entreprises souhaitant sensibiliser leurs collaborateurs aux enjeux de cyber-sécurité, la formation est essentielle et les indicateurs à retenir s'orientent ainsi :

- La prise au sérieux des directives du service informatique (85% Monde - 79% France)
- La cyber-sécurité est en partie de leur responsabilité (81% Monde - 73% France)
- L'utilisation d'applications personnelles sur un appareil professionnel est un risque pour la sécurité informatique de l'entreprise (64% Monde - 62% France)

Les consignes sont-elles respectées ?

Les collaborateurs reconnaissent utiliser au moins une application personnelle sur leur outil de bureau, et ils ont déjà téléchargé des données de l'entreprise vers cette application.

Ils utilisent leur PC professionnel pour un usage personnel sur Internet (81% France) et seuls 34% en France se limitent dans les sites qu'ils visitent.

Ils accèdent régulièrement aux données à partir d'un appareil personnel et 7% (5% France) au dark web.

Source Etude Trend Micro 'Head in the Clouds' - 13 200 télétravailleurs répartis dans 27 pays

Invenis FAIT DE LA DONNÉE, UN ENJEU BUSINESS

A l'heure où il faut s'approprier la donnée et la positionner au cœur des enjeux quotidiens des métiers, Grégory Serrano, co-fondateur de Invenis, entreprise spécialisée dans l'analyse prédictive des données s'appuyant sur l'I.A et le Big Data, a accepté de répondre à quelques questions. La donnée n'est-elle pas un allié de choix pour défier les périodes incertaines ?

Invenis est une entreprise tournée vers la donnée, mais pourriez-vous nous en dire plus ?

Invenis, créée en 2015, a une ambition forte, qui consiste à démocratiser l'accès au Big Data et à l'Intelligence Artificielle à toutes les entreprises. En ce sens, Invenis permet aux entreprises de réaliser leur transformation digitale par la data en s'adaptant à leur maturité.

Nous les accompagnons vers l'autonomie dans leurs analyses de données en 3 étapes. Le **Conseil** (audit et recommandations sur leurs données et sur leur organisation data, suggestions de cas d'usage avec leurs données), l'**Accompagnement** (nos équipes de Data Analysts accompagnement nos clients dans la réalisation de leurs cas d'usage, qui sont accessibles 24/24 et 7/7 grâce à notre logiciel en SaaS) et l'**Autonomie** (les équipes de nos clients prennent en main notre logiciel en SaaS et réalisent tous leurs cas d'usage).

Nous permettons donc aux équipes métiers de s'approprier les technologies Big Data et Intelligence Artificielle et donc de diffuser la donnée au sein de toutes les équipes.

Pourriez-vous évoquer l'une des dernières actualités de la société ?

Invenis vient de lever 3 millions auprès de Crédit Mutuel Innovation afin d'accélérer son développement commercial et d'améliorer son logiciel.

Nous recrutons de nombreux profils pour atteindre nos objectifs : développeurs, sales et marketing, UX et UI designers, Data Consultants...

Face au contexte inédit de crise sanitaire, pensez-vous qu'il possible de rebondir grâce aux données ?

Pour prendre une bonne décision, il faut avoir en amont de bonnes informations.

Or dans l'analyse de données c'est justement l'accès à cette information qui fera la différence et qui permet de prendre des décisions éclairées.

La donnée représente ainsi une opportunité business importante dans un contexte de crise.

Elle permet de tirer les leçons du passé et de mieux se projeter dans l'avenir.

La data représente un allié de choix pour mieux appréhender des périodes incertaines et avoir la capacité à modéliser différents scénarios afin de s'adapter à ce contexte. Les entreprises qui exploitent leurs données ont cette capacité à penser autrement et à découvrir de nouveaux relais de croissance.

La donnée représente ainsi une opportunité business importante dans un contexte de crise.

Grégory Serrano

Encore faut-il savoir tirer toute la valeur de ces données.... Invenis permet à toutes les entreprises de tirer toute la valeur de leurs données, rapidement et simplement, grâce aux technologies modernes que sont le Big Data et l'Intelligence Artificielle.

Les cas d'usage sont nombreux : recommandation de produits ou de services basée sur le comportement d'achat, prévention du churn, maintenance prédictive, prévision des stocks.... Les données sont sources d'innovation et de croissance !

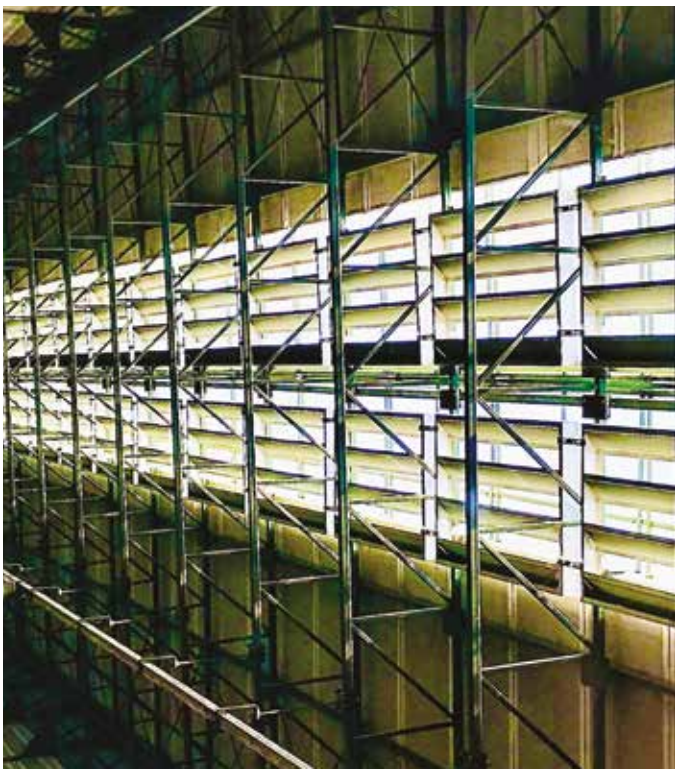
Comment aider les organisations à devenir data-driven ?

Pour devenir Data Driven, les entreprises doivent apprendre à désiloter l'accès à la donnée et faire de cette donnée un enjeu business et non plus un enjeu technique. Toutes les équipes d'une entreprise doivent avoir accès facilement à la donnée. Et doivent pouvoir la traiter et l'analyser grâce aux technologies les plus performantes du marché, sans avoir à faire appel à des techniciens, en toute autonomie.

En s'appropriant la donnée, les équipes opérationnelles (Opérations, Marketing & Sales, Logistique ...) peuvent ainsi placer la donnée au cœur de leurs enjeux quotidiens : augmenter les ventes, atteindre l'excellence opérationnelle, gérer mieux les stocks et les flux entre les espaces de stockage...

C'est pour cela qu'Invenis propose une révolution d'usage : permettre aux équipes métiers de mettre en place leurs analyses prédictives sur toutes leurs données, simplement, rapidement et en toute autonomie !

> Par Sabine Terrey



Les bénéfices de l'automatisation pour la transformation numérique

L'automatisation semble en bonne voie, l'adhésion est plus forte mais les défis de l'automatisation intelligente sont réels. Retour sur quelques indicateurs...

L'automatisation robotisée des processus résout les défis liés à la productivité selon 74% des décideurs français, et la RPA devient la réponse rapide à la demande des clients (84%).

Dirigeants & Métiers

78% des dirigeants et la moitié des spécialistes métiers veulent désormais découvrir les opportunités générées par l'automatisation Pourquoi souhaitent-ils tirer avantage de ce processus automatisé ? Plusieurs réponses sont évoquées à savoir :

- Le gain de temps
- La réduction des coûts
- La précision du travail
- L'agilité métier et la résilience

L'automatisation / RPA peut résoudre « les difficultés à répondre rapidement aux demandes clients » notamment pour assurer la permanence des activités.

Compétitivité & Productivité

L'automatisation bouleverse tous les niveaux de l'entreprise et permet de rester résilient et réactif. Ainsi ces technologies :

- Sont clés pour la compétitivité – 80% des décideurs
- Permettent d'affronter des projets complexes
- Augmentent les niveaux de productivité

Elles accroissent la capacité à développer l'activité (52 %), répondent aux besoins (83 %) et intègrent des processus de sécurité robustes (77 %).

Compétences & Formations

Acquérir de nouvelles compétences, bénéficier de formations, se requalifier sont des priorités. Ainsi 66 % des entreprises offrent des opportunités d'apprentissage de nouvelles compétences/ qualifications lors du déploiement des technologies.

68 % des spécialistes métiers souhaitent acquérir de nouvelles compétences pour assumer des fonctions différentes.

Autres sujets clés, créer précisément un lien de confiance entre les spécialistes métiers et la main-d'œuvre numérique (61% des métiers) et installer une sereine cohabitation entre collaborateurs humains et agents virtuels (77% des dirigeants).

Est-ce que la crise sanitaire actuelle n'accélérerait pas la tendance vers de nouvelles formes de travail, mêlant automatisation intelligente et main d'œuvre digitale, pour maintenir l'activité et la réactivité ?

Communication & Talents

Une communication en amont est nécessaire pour expliquer, répondre aux interrogations, atténuer les craintes et réussir l'implémentation. Qu'en est-il réellement ? 43 % des spécialistes métiers estiment que la communication n'est toutefois pas à la hauteur de l'enjeu.

Autre point non négligeable : l'automatisation attirera de nouveaux talents selon 82 % des dirigeants et améliorera la vie professionnelle selon 64 % des spécialistes métiers.

Source Etude Sapio Research & Blue Prism – Monde – Mars 2020


ARRÊTONS
LA CHASSE AUX JOURNALISTES
En 10 ans, plus de 900 journalistes ont été tués dans le monde.
FAITES UN DON SUR RSF.ORG
REPORTERS SANS FRONTIERES
POUR LA LIBERTE DE L'INFORMATION

Microsoft Teams Phone System
VS TÉLÉPHONIE D'ENTREPRISE

Le succès de Teams auprès des entreprises amène de plus en plus de sociétés à migrer leur environnement de téléphonie vers la solution collaborative. Mais l'offre Microsoft Phone System est-elle en capacité de répondre aux différentes contraintes de entreprises ?

Quels sont les points critiques qui pourraient s'opposer techniquement ou fonctionnellement à l'usage de Microsoft Teams Phone System en entreprise ?

L'offre Teams Phone System en quelques mots

L'offre Teams Phone System de Microsoft est articulée autour de deux infrastructures que sont les plans d'appel de Microsoft et la technologie Direct Sip Routing.

Les plans d'appels Microsoft

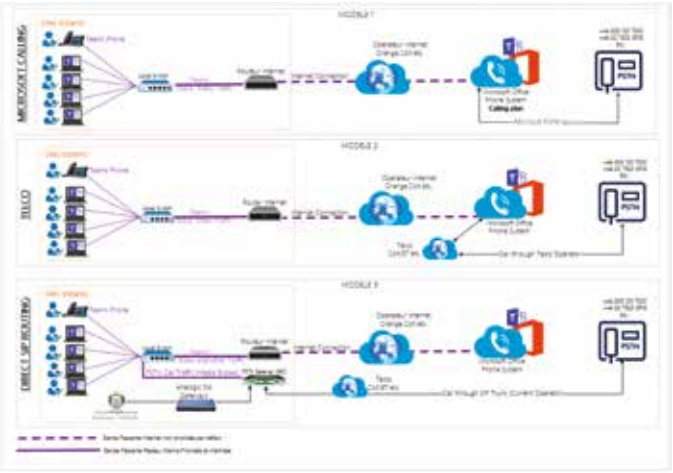
Les plans d'appel Microsoft disponibles dans une dizaine de pays seulement, permettent de fournir des minutes d'appel (Calling plan) à chaque collaborateur disposant soit d'une licence E3 + phone System soit d'une licence E5. La configuration du numéro de téléphone ainsi que la portabilité sont directement gérées à travers le portail d'administration Teams.

C'est simple, efficace, rapide mais attention tout de même à la tarification des appels à la minute. Sur les plans d'appel, l'éditeur de Redmond a de farouches compétiteurs qui occupent le marché depuis beaucoup plus longtemps que lui. Certains proposent des solutions peut être plus adaptées à vos usages comme un plan d'appel unique (pool) pour un ensemble de collaborateurs plutôt qu'un plan d'appel par personne. A vérifier donc !

Ces plans d'appel Microsoft correspondent bien aux besoins des petites entités, aux activités tertiaires mais vont vite montrer leurs limites dans le cadre d'entreprises plus importantes ayant des contraintes plus complexes. Patience nous allons y venir...

Le Direct Sip Routing

L'autre solution consiste à paramétrer l'environnement Teams pour que les appels sortants soient adressés à une passerelle SBC interfacée avec un fournisseur de téléphonie (Trunk Sip ou T1 E1). Ce SBC (Sonus -Ribbon, Audiocode) qu'il soit physique ou virtuel, réceptionnera les appels téléphoniques entrants et les acheminera vers l'environnement Teams. Ce SBC peut être soit positionné en interne, soit géré directement par votre opérateur. Le schéma suivant illustre ces configurations.



Téléphonie d'entreprise Vs Teams Phone System

Ces deux points étant précisés, je vous propose de rentrer dans le vif du sujet : la téléphonie d'entreprise. Malheureusement, cette dernière ne s'arrête pas aux seules fonctions d'émission et de réception d'appels téléphoniques.

Je vous propose donc de lister les points critiques que vous devrez prendre en compte si vous envisagez de migrer vers Teams Phone System.

• *Les dispositifs analogiques*

La plupart des entreprises disposent de périphériques analogiques directement connectés à l'environnement de téléphonie. C'est notamment le cas des interphones qui permettent d'appeler le standard de l'entreprise par l'appui d'un simple bouton. C'est aussi le cas des portails commandés par la composition d'un numéro de téléphone. Mais ce sont aussi des dispositifs d'alertes qui, pour fonctionner, n'ont pas besoin de connexion internet.

Si vous en disposez, leur raccordement vers des passerelles analogiques locales qui assureront la transformation en SIP constitue une excellente solution.

• *Les accueils ou standards d'entreprise*

Les accueils d'entreprise, les fameux standards téléphoniques, peuvent recevoir un nombre important d'appels téléphoniques qu'ils doivent aiguiller vers des postes internes, vers des mobiles ou vers des boites vocales. Les fonctions attendues dans ces cas d'usages sont, les transferts à l'aveugle, les transferts avec consultations, le parcage d'appel, la reprise d'appel etc.

Bien souvent, il vous sera demandé des statistiques d'appels avec une estimation moyenne des temps de décroché, du nombre d'appels par tranche d'heure etc.

Le client Teams classique se révèlera bien incapable de fournir ces fonctionnalités et vous devrez recourir à ce que l'on nomme des Teams Attendant Console (Console Opératrice). Solutions tierces parties dont certaines s'intègrent directement au sein du client Teams.

• *Les DECT*

Dans certaines entreprises ayant des entrepôts, les téléphones DECT sont légions. Beaucoup plus simples à gérer que des téléphones Wifi, ils sont massivement utilisés par les collaborateurs en raison de leur simplicité, de leur autonomie et de la couverture dont ils disposent.

Ces dispositifs sont généralement connectés à un concentrateur DECT, lui-même connecté soit en analogique à l'infrastructure de l'entreprise, soit en SIP. Si vous envisagez de conserver ces infrastructures et les interconnecter à Microsoft Teams Phone System, l'usage d'une passerelle de communication (SBC Sonus-Ribbon, Audiocode) locale est indispensable.

• *Les numéros internes*

La plupart des entreprises disposent de numéros internes basés bien souvent sur 4 ou 6 chiffres. Ces numéros internes sont difficilement portables vers Microsoft Teams dont le format de numérotation est basé sur la norme E164. Ces numéros courts constituent souvent un héritage d'un « ancien » monde, où les collaborateurs s'appelaient en interne en composant sur leur clavier de téléphone à neuf chiffres, ces fameux numéros courts. Technique beaucoup plus rapide que de chercher sur un écran Lcd monochrome de trois lignes, un nom dans l'annuaire de l'entreprise. Certains utilisateurs d'Alcatel se reconnaitront, j'en suis sûr.

Si ces numéros internes constituent un héritage, je vous engage à ne pas les reconduire. Dans l'environnement Microsoft Teams ils n'ont plus aucun intérêt.

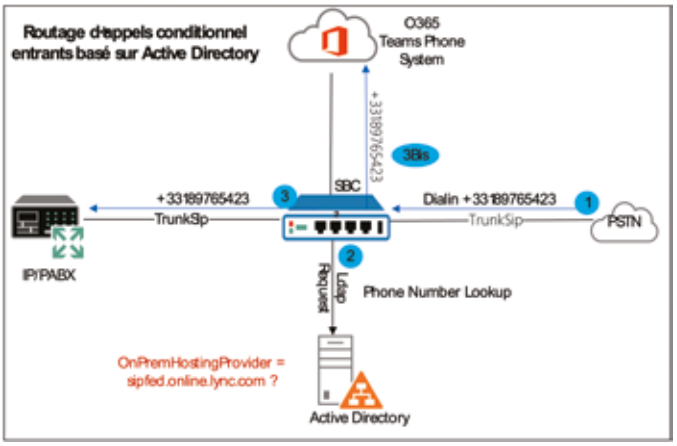
Attention tout de même aux utilisateurs DECT qui pourraient les avoir recensés dans leurs périphériques. Là aussi, la passerelle SBC locale pourra vous aider, à effectuer certaines transformations des numéros courts vers des numéros normalisés en E164.

• *Le routage conditionnel*

Selon vos scenarios de migration ou de cohabitation entre l'ancienne infrastructure de téléphonie et Microsoft Teams, vous aurez à gérer le routage conditionnel.

Lors de votre migration, vous allez vous retrouver à gérer des utilisateurs non migrés et des utilisateurs migrés sur Teams.

Dans le cas d'un appel entrant, une passerelle SBC locale interfacée à votre environnement Active Directory pourra prendre des décisions de routage en fonction de la valeur d'attributs spécifiques. Si la passerelle détecte une valeur spécifique dans un attribut particulier elle « routera » l'appel vers Teams et dans le cas contraire vers l'ancienne infrastructure de Téléphonie. La figure suivante illustre cette configuration.



• *Les Fax*

Quitte à parler d'héritage, parlons des fax. Dans la plupart des cas, ces dispositifs sont connectés en analogique soit sur une ligne analogique France Télécom, soit derrière votre PA/IPBX. Si vous bénéficiez d'une ligne analogique, un conseil, gardez-la et laissez vos fax en dehors de votre migration.

Dans le cas contraire l'usage d'une SBC, là aussi, vous permettra de gérer le fameux protocole T38. L'autre solution plus radicale, mais plus pérenne, consiste à migrer vers une solution FaxtoMail.

• *La dépendance à l'internet*

La migration de votre infrastructure de téléphonie vers Teams Phone System pose la question de la dépendance vis-à-vis d'internet. Si vous disposez d'un ancien environnement de téléphonie sur site et si vous perdez la connectivité Internet, vous pouvez toujours continuer à recevoir et émettre dans appels téléphoniques.

Avec Teams Phone System cela ne sera évidemment pas le cas. Pour cela, certains dispositifs Teams, comme les téléphones Yealink, possèdent un mode de basculement en SIP qui peut permettre au téléphone de se connecter directement sur une passerelle locale en cas de panne Internet. (cf https://workingtogether.fun/2019/12/02/yealink-ribbon-securisent-la-telephonie-teams/)

L'autre amélioration consiste à sécuriser vos liens via deux opérateurs différents ou un backup 4G.

• *Les centres d'appels*

Certaines entreprises disposent de centres d'appels connectés derrière l'infrastructure téléphonique. Certaines solutions peuvent évoluer vers un mode Teams compatible, d'autres devront être remplacées si vous envisagez d'arrêter totalement votre ancienne infrastructure.

Le SBC, couteau suisse de la téléphonie

L'usage d'un SBC local (Sonus-Ribbon, Audiocode) surtout positionné entre votre environnement de téléphonie et votre opérateur de téléphonie, mais aussi connecté à votre Active Directory, vous rendra de nombreux services.

Il vous permettra notamment de gérer sereinement la période de cohabitation des deux environnements de téléphonie, d'éviter un portage des numéros SDA et de manipuler aisément les numéros entrants et sortants. En cas de panne Internet, il accueillera des postes téléphoniques en mode Sip leur permettant de recevoir et émettre des appels via un mode dégradé.

Positionné directement chez l'opérateur qu'il soit physique ou virtuel, en cas de panne internet, il pourrait rediriger certains appels entrants critiques vers les numéros de mobiles des collaborateurs.

Comme vous pourrez le constater l'offre Microsoft Teams Phone System si elle s'adresse à une entreprise ayant un existant de téléphonie élaboré, seule, se révélera incapable de répondre à l'ensemble de ses contraintes. Accompagnée de solutions additionnelles et correctement paramétrées, Teams Phone System offrira un confort non négligeable à vos utilisateurs qui apprécieront le fait de pouvoir utiliser leur suite collaborative pour passer et recevoir leurs appels téléphoniques.

De quoi leur faire totalement oublier leurs clients Skype for Business ou leurs bons vieux téléphones physiques. Quant à savoir si le réseau téléphonique a encore un avenir... c'est un autre débat.

La migration de votre infrastructure de téléphonie vers Teams Phone System pose la question de la dépendance vis-à-vis d'internet.

Laurent Teruin | LTeruin@hotmail.com | https://workingtogether.fun

Oui, je profite de votre offre d'abonnement pour recevoir les 4 prochaines éditions du magazine SMART DSI au tarif de 120 € ttc*

Tarif d'abonnement pour la France métropolitaine, pour les abonnés hors de France métropolitaine, l'offre d'abonnement est au tarif de 140 € ht*

*Taux de TVA 2,1 %

** Taux de TVA du pays destinataire, surtaxe postale incluse soit 20 € par abonnement

Date + signature

VOS COORDONNEES

Société .....

Nom ..... Prénom .....

Adresse de livraison .....

.....

.....

Code postal ..... Ville .....

Pays .....

Tél. ..... Fax .....

email.....

Mode de règlement :

☐ A réception de facture* ☐ Par chèque joint

*réservé aux sociétés en France - Belgique - Luxembourg & Suisse.

Indiquez votre N° TVA Intracommunautaire :

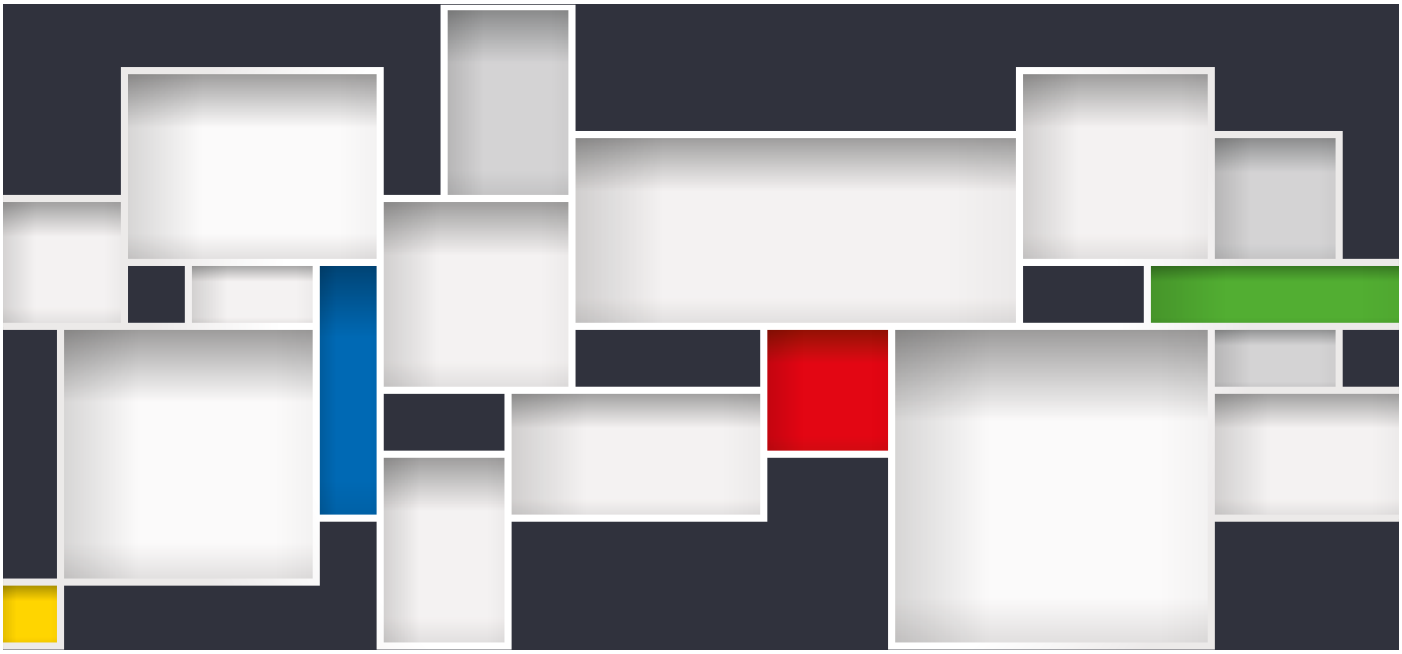
Renvoyez votre bulletin à notre service abonnements :

SMART DSI - TBS BLUE - Service des abonnements
11 rue Gustave Madiot - 91070 Bondoufle - France

Fax. +33 1 55 04 94 01 - e-mail : abonnement@smart-dsi.fr

Planifier SES COÛTS AZURE

Se lancer sur le Cloud Azure est une décision importante qui nécessite une bonne préparation. Elle est prise une fois qu'un grand nombre des questions (légitimes) que l'on se pose sont traitées.



Il est plutôt « facile » de répondre aux questions techniques de sécurité, de performance, d'accès ... etc. Il est également possible de répondre aux questions que l'on se pose en termes de sizing, de charge. Facile ne veut pas dire que cela se fasse rapidement et sans préparation. Mais plutôt que les données à exploiter pour arriver à obtenir les bons éléments de réflexion sont des données très concrètes et que l'on peut transposer de son informatique existante à son informatique portée sur le Cloud Azure.

Que l'on déplace son environnement existant dans un mode 1 pour 1 (Lift-and-shift) ou que l'on décide de redéployer en adaptant son environnement aux services Azure, une photo de l'existant et une vue de ce que l'on souhaite après migration sont les deux éléments nécessaires à la préparation.

Les données de départ nécessitent une bonne connaissance de son architecture complétées par l'utilisation des outils d'évaluation / inventaire. Par exemple, Azure Migrate qui est un outil gratuit de simplification à la migration. Si le choix est de redéployer, il faudra également se pencher sur les modèles de référence Azure pour porter ses applications et son infrastructure sur un modèle Cloud.

Voilà (très schématiquement) une façon classique d'aborder le sujet. Au final, toutes ces données sont très factuelles, elles sont mesurables puisqu'elles s'appuient souvent sur des métriques et on se retrouve rassuré par ces étapes de préparation.

Les services de départ sont clairement identifiés, les services équivalents ou complémentaires Cloud également, que reste–il à faire si ce n'est migrer ?

Il reste à chiffrer et à évaluer la dépense à venir.

Le « Combien cela va-t-il me coûter ? » est sans conteste la question pour laquelle il est plus difficile de répondre avec exactitude. Elle est pourtant et heureusement au cœur de la réflexion. Il existe quelques bonnes pratiques pour que cette estimation soit la plus précise possible.

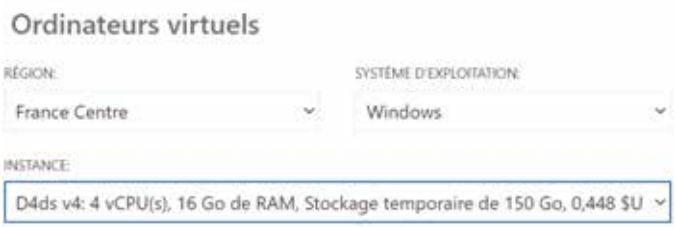
Quelles étapes pour affiner le besoin ?

Première étape, *certainement la plus importante après l'identification d'un service,* ***son niveau de performance / fonctionnalité****.*

- *Performance :* le niveau de performance de ma machine ou de ma base de données est à X, quel coût pour un même niveau de performance sur Azure. Ici, la calculatrice (https://azure.microsoft.com/fr-fr/pricing/calculator/) est l'outil indispensable pour cette évaluation. Calcul, mise en réseau, base de données, identité, tout est passé en revue.

Se faire plaisir peut avoir un surcoût non négligeable.

Par exemple, quel coût pour une machine 4 vCPU, 16 Go de ram sur système d'exploitation Windows



Calculatrice Azure pour une machine virtuelle.

- *Fonctionnalité :* L'exercice est un peu plus complet. Un service peut-être dispensé avec des fonctions simples dans son SKU (sa référence ou édition de niveau) la plus basique et offrir des fonctionnalités ou des performances complémentaires dans sa version la plus évoluée. Cette étude doit être menée en s'appuyant sur les tableaux comparatifs des SKU. Par exemple, le service IoT Hub n'autorise pas l'utilisation du calcul de périphérie Edge ou limite les débits dans les versions les moins coûteuses.

Édition de niveau	Débit soutenu	Vitesse de transmission soutenue
B1, S1	Jusqu'à 1 111 Ko/minute par unité (1,5 Go/jour/unité)	Moyenne de 278 messages/minute par unité (400 000 messages/jour par unité)
B2, S2	Jusqu'à 16 Mo/minute par unité (22,8 Go/jour/unité)	Moyenne de 4167 messages/minute par unité (6 millions de messages/jour par unité)
B3, S3	Jusqu'à 814 Mo/minute par unité (1144,4 Go/jour/unité)	Moyenne de 208 333 messages/minute par unité (300 millions de messages/jour par unité)

Accélération / limitation des débits selon le SKU.

La puissance et les modèles disponibles n'ont (presque) pas de limite, attention à ne pas tomber dans l'excès. Se faire plaisir peut avoir un surcoût non négligeable.

Dernière recommandation, certains modèles de base ne supportent pas d'évolution de niveau. Il sera, par exemple, impossible de choisir un niveau de fonctionnalité plus élevé. Ce qui oblige à détruire puis reconstruire. La lecture attentive des documentations SKU évitera ce genre de cas.

Le niveau choisi ne prend pas en charge la mise à niveau.

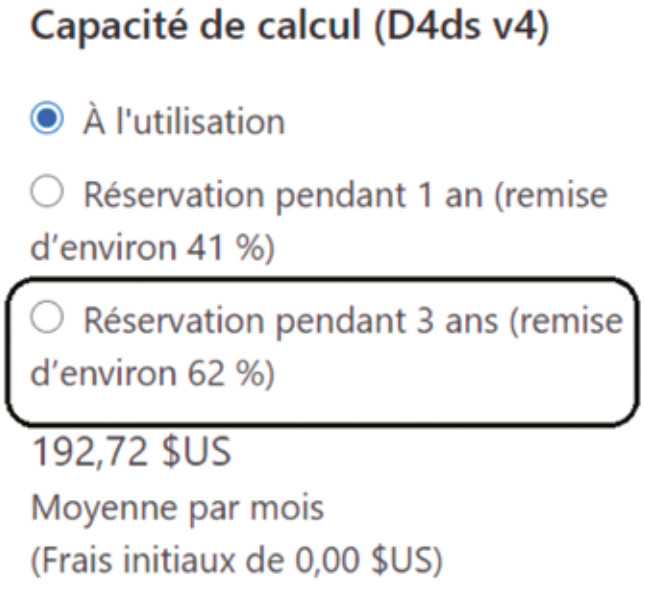
Seconde étape, son niveau d'élasticité. L'élasticité est la capacité à adapter sa charge de travail. A la hausse comme à la baisse, l'adaptation des ressources a un lien direct et extrêmement fort avec les coûts. Le mécanisme du paiement à l'utilisation propre aux solutions Cloud offre la possibilité de baisser les coûts sur des créneaux où le besoin de puissance est peu élevé, voire inexistant. Par exemple, une base de données peut disposer d'une puissance X en journée et d'une puissance X / 2 en cours de soirée ou de nuit. Mieux même, une machine virtuelle peut être stoppée hors heures de bureau.

Cette facilité de mise à l'échelle doit être intégrée lors du calcul des coûts. Cet exercice est à réaliser à la hausse comme à la baisse. On ne taille plus son environnement sur son besoin maximum, mais sur un besoin instantané. Ma machine est choisie pour un besoin qu'elle va couvrir 90 % du temps (ni plus, ni moins) et est adaptée pour les besoins exceptionnels. Par exemple, ma base utilise 16 cœurs 99 % du temps, mais 32 cœurs 2 jours dans l'année pour une consolidation. Passer du temps sur ces calculs est une garantie de facturation homogène avec son besoin.

Troisième étape, son niveau d'engagement. Le niveau d'engagement est la capacité à utiliser des machines éphémères ou des machines sur la durée. Que se passe-t-il pour une machine de test, machine éphémère par excellence ? Elle est utilisée quelques jours, semaines, puis attend un nouveau test pour être réutilisée. C'est une machine jetable.

Au contraire d'une machine qui héberge l'application majeure de l'entreprise et qui est amenée à durer. Cette notion d'engagement de durée a aussi un impact fort sur les coûts. Une machine jetable se paye à l'utilisation au prix fort. C'est à dire sans possibilité de réduction. Cloud oblige, elle n'est plus facturée dès qu'elle est détruite.

Une machine utilisée durablement dans le temps voit son prix réduit de façon très significative. Jusqu'à 70 % de réduction pour un engagement à trois ans. La machine D4dsV4 choisie plus haut affiche une réduction de 62 % sur la calculatrice Azure si la durée d'engagement est de trois ans.



Réduction importante pour des engagements de longue durée.

Là aussi, même si l'exercice demande du temps, il est indispensable ! C'est un peu la chasse au gaspillage et au rapport coût / performance adaptée aux besoins. Voilà de quoi voir beaucoup plus clair dans ses coûts pour ne pas partir à l'aventure.

Pourquoi il est important de « se faire la main » ?

Malgré toute cette préparation, il est possible et important de se faire la main. Les tests techniques sont indispensables et sont, je pense, systématiquement mis en place en entreprise.

Les tests de maitrise et compréhension des coûts le sont beaucoup moins (pas du tout ?). Pourtant, ce sont des éléments qui participent à la réussite d'une migration. Il y a beaucoup à apprendre !

Microsoft Azure offre une enveloppe de 170 € pour explorer Azure (https://azure.microsoft.com/fr-fr/free/).

Les tests techniques sont indispensables et sont mis en place en entreprise.

Que faire avec cette somme ? Déployer quelques ressources Azure (base de données, machines virtuelles ...etc.), les utiliser puis ... lancer le menu d'analyse des coûts.

Ici, à l'échelle d'un abonnement de test, quels sont les services qui me coûtent, sont-ils nécessaires ? Bien répartis ?

Répartition des coûts.

Que va-t-il se passer si je conserve ces ressources ? Quels coûts à venir ? Le déploiement d'un nouveau service génère un coût important et une projection des coûts à venir. Ce surcoût a-t-il été anticipé, est-il réellement nécessaire ? Le service doit-il être rendu à ce prix ?

Projection et courbes des dépenses J + 15.

Ces deux compteurs sont utilisés pour d'éventuelles actions de corrections.

Pour terminer, il faut utiliser Azure Advisor, outil intégré de recommandations. Il affichera les machines / services sous utilisées -és pour lesquels il est possible de réaliser des économies. Advisor s'appuiera sur les métriques constatés pour guider et aider à la mise en place d'actions correctives.

Au final, une belle liste d'outils de contrôle.

Pour résumer, un rappel des points importants :

1 / Il existe un grand nombre de ressources et d'outils pour piloter ses coûts Azure.

2 / Adapter son niveau de performance et de fonctionnalité au plus proche des besoins a un impact fort sur le montant de sa facturation.

3 / La projection des dépenses est utilisée pour piloter le montant des factures à venir

Advisor s'appuiera sur les métriques constatés pour guider et aider à la mise en place d'actions correctives.

Thierry Bollet, MVP Azure, travaille chez Capgemini. Auteur aux Editions ENI, il est passionné aussi de Powershell et d'automatisation

NOUVELLES DATES

17 > 19 NOVEMBRE 2020 MONACO

READY FOR IT!

LE RENDEZ-VOUS INCONTOURNABLE DES DÉCIDEURS DE L'IT

VENEZ CHALLENGER VOS STRATÉGIES

Networking **Contenu** **Business**

COMEXPOSIUM

#RFIT2020
@RFIT_event

ready-for-it.com

DG CONSULTANTS

METSYS

À l'aube d'un avenir meilleur