N°15 I SEPTEMBRE 2019

CONDUIRE LA TRANSFORMATION NUMÉRIQUE DE L'ENTREPRISE

SMART DSI®

DOSSIER
Cloud Computing
Défis & Solutions

INTERVIEW
Sécurité & Intelligence connectée : garder une vision 360 du SI

DECRYPTAGE
Valoriser les données produites en streaming ou temps réel : le nouvel eldorado du Big Data

L'ŒIL SECURITE
Quel avenir pour la cybersécurité ?

L'ETUDE A RETENIR
Un code de conduite pour réduire la fracture numérique

Club Abonnés sur www.iTPro.fr 119017

The new champion is here

Exakis Nelite
MagellanPartners

Au sein de Magellan Partners, le nouvel ensemble **Exakis Nelite devient le nouveau champion Microsoft en France** avec l'ambition de devenir le **1er partenaire Microsoft en Europe.**

Rejoignez-nous !

14 Agences

1er partenaire pure player Microsoft en France

500+ Collaborateurs

1 Centre de Service Unifié

13 Domaines de compétences Microsoft

1 Division « Customer Experience »

Elu par Microsoft

2018 Partenaire France Azure

2018 Vice-Champion du Monde Security & Compliance

2019 Partenaire France Grands Comptes

#ReadyToCreateTheFirstMicrosoftPartner

www.exakis-nelite.com

/company/exakis-nelite

@EXAKIS_NELITE

La cybersécurité est l'affaire de chacun !

L'amélioration de l'expérience client et la sécurité des données se hissent au rang des priorités des entreprises en 2019. De plus, pour proposer des expériences client de qualité, la collecte, la manipulation et le stockage des diverses données restent des éléments fondamentaux. Alors, à l'heure de budgets insuffisants et inadaptés, du manque de personnel qualifié, de l'absence de vision commune, d'une surface d'attaque étendue, du rôle clé des données au sein des organisations, comment préserver cette sécurité ?

Rien d'étonnant donc de voir toute l'énergie des équipes IT et Sécurité déployée sur le sujet. Les cadres informatiques semblent même plus préoccupés qu'il y a un an sur les risques encourus, puisque près de la moitié d'entre eux en font l'un des trois principaux enjeux extérieurs, les deux autres étant l'adaptation à l'évolution des attentes et des comportements des clients et les dysfonctionnements techniques avec l'indisponibilité des données et services. Cependant, les compétences techniques ne suffisent plus, il s'agit réellement aujourd'hui de développer des compétences relationnelles pour fédérer les différents services de l'entreprise autour d'une vraie stratégie sécurité. Toutes ces notions seront bien évidemment évoquées lors de la 19ème édition Assises de la Sécurité à Monaco !

Et le marché de la donnée, qu'en est-il ? Il n'attend pas et évolue sans cesse ! Les décideurs scrutent les opportunités business, et sont particulièrement sensibles à l'accélération des projets de traitement de la donnée et à l'automatisation des opérations de data management. De même, les questions liées aux data abondent : le rôle des données dans les innovations basées sur l'Intelligence Artificielle, le manque de collaboration entre les datascientists et les data engineers, l'arrivée massive de l'intelligence connectée... autant d'interrogations auxquelles les experts ont tenté de répondre au sein d'interviews exclusives dans ce numéro.

Alors, la révolution des données est en marche, intelligence artificielle d'une part, apprentissage automatique d'autre part, l'objectif n'est-il pas avant tout de recueillir rapidement des informations exploitables ? Les nombreuses réflexions et les analyses viennent renforcer l'intérêt et l'optimisation de telle ou telle technologie. Reste à faire les bons choix...

Très bonne lecture !

Sabine Terrey
Directrice de la Rédaction
sterrey@itpro.fr

1 - Tendances digitales 2019 : l'informatique à l'honneur – Adobe & Econsultancy

SMARTDSI

N°15 I SEPTEMBRE 2019

6 I DOSSIER
Cloud computing : des défis et des solutions multiples

12 I L'ETUDE A RETENIR
Les trois qualités du DSI moderne !

14 I SPECIAL REPORT
Le droit à la déconnexion : un enjeu RH

16 I INTERVIEW
ForePaaS accélère les projets data des entreprises

18 I PERSPECTIVES
Cybersécurité : techniques de cartographie Active Directory avec BloodHound

24 I L'ETUDE A RETENIR
Un code de conduite pour réduire la fracture numérique !

26 I L'ŒIL SECURITE
Quel avenir pour la cybersécurité ?

28 I DECRYPTAGE
Valoriser les données produites en streaming ou temps réel : le nouvel Eldorado data

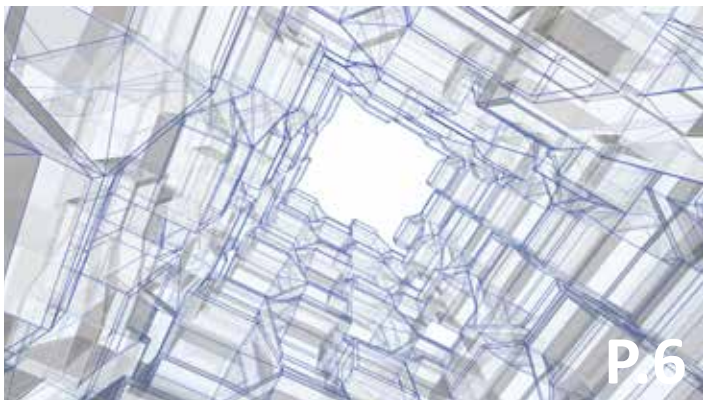
31 I BULLETIN D'ABONNEMENT

32 I INTERVIEW
Embarquez au cœur de l'archivage des données numériques avec CDC Arkhinéo

34 I DECRYPTAGE
Digital : le DSI à la tête des stratégies de changement

36 I RETOUR D'EXPERIENCE
Il y a une différence entre connaître le chemin et arpenter le chemin

39 I STRATEGIE
Leadership : 11 raisons d'échec des dirigeants



40 I L'ETUDE A RETENIR
Ne sous-estimez pas le potentiel de l'Edge Computing !

42 I INTERVIEW
Databricks accélère l'innovation sur les données

44 I EXPERT
Migration Office 365 : quelle stratégie de communication adopter ?

48 I INTERVIEW
Cybersécurité & intelligence connectée : Garder une vision 360 du système d'information

50 I L'ETUDE A RETENIR
Cyberattaques : 6 méthodes pour protéger les cadres dirigeants

SMART DSI

Rédaction
Pour joindre les membres de la rédaction
redaction@smart-dsi.fr
Comité de rédaction associé à cette édition

Didier Danse, Théodore-Michel Vrangos, Sabine Terrey, Sylvain Cortes, Laurent Teruin, Juvenal Chokogoue

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

© 2019 Copyright IT Procom
© Crédits Photos

Shutterstock : Sergey Mansurov - Paul Squid - AdobeStock - iStock - CDC Arkhineo

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

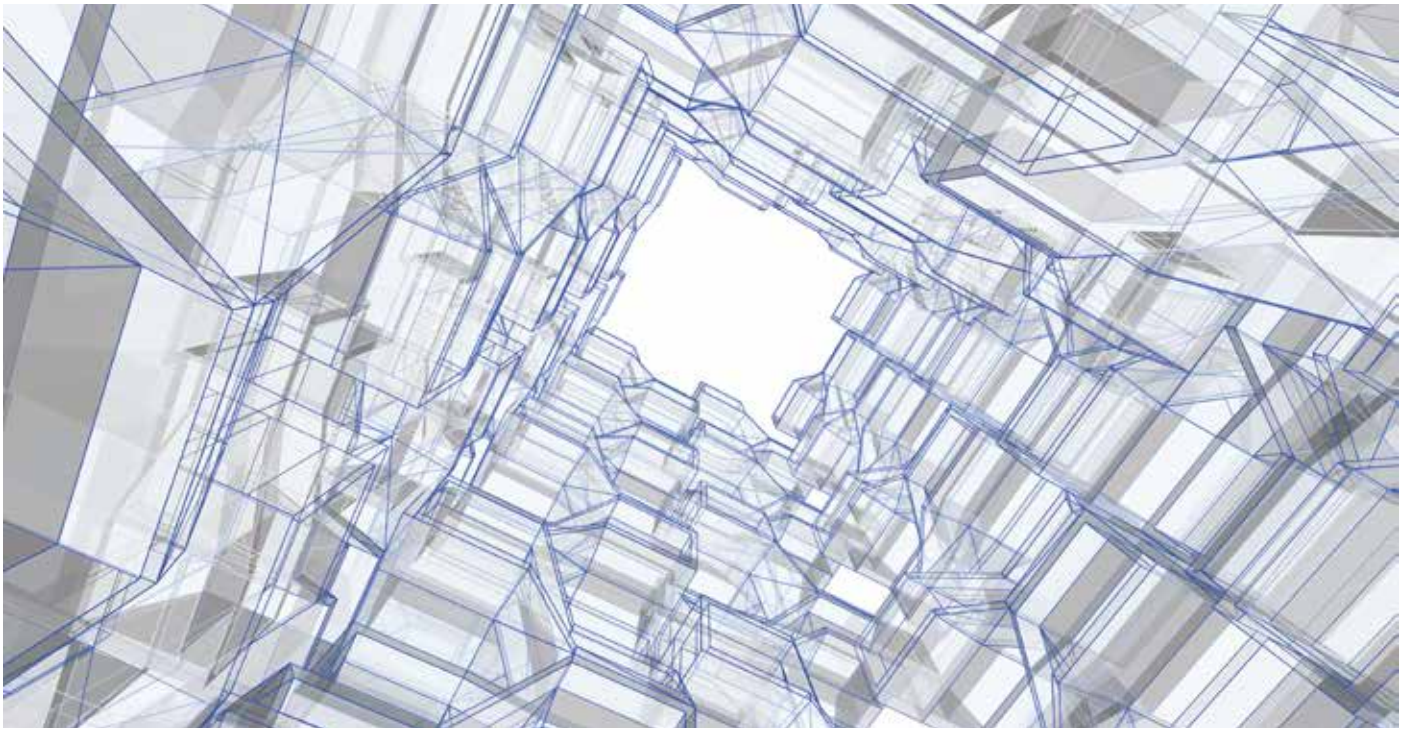
Toute reproduction, représentation, traduction ou adaptation, qu'elle soit intégrale ou partielle, quels qu'en soient le procédé, le support, le media, est strictement conditionnée à l'autorisation de l'Éditeur.
SMART DSI - IT PROCOM, tous droits réservés.
© 2019 IT PROCOM - Tous droits réservés

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

Cloud computing :
DES DÉFIS ET DES SOLUTIONS MULTIPLES

> Par Didier Danse



Le Cloud (computing) : des applicatifs accessibles à tous, sans les inconvénients d'un hébergement au sein de l'entreprise. Voilà la promesse entendue tant et tant, durant de nombreuses années. Le Cloud ouvre incontestablement de nouveaux horizons tant pour les gestionnaires de services que les utilisateurs de ces mêmes services. L'expérience acquise par le marché ces dernières années permet cependant de mettre en exergue de nombreux points d'attention. Une bonne compréhension des fondements du Cloud s'avère primordial dans un esprit de durabilité.

Pour beaucoup de lecteurs, cet article ne sera perçu que comme un rappel et c'est d'autant mieux. Un petit rappel est cependant toujours utile. Pour preuve, de nombreuses entreprises, pour qui cet article n'était qu'un rappel, font face à des pertes de contrôle de l'utilisation de leurs applications pouvant amener des fuites de données vers des tiers non habilités, de manière volontaire ou non, avec dans certains cas des conséquences majeures pour l'entreprise et ses clients.

Au travers de ces quelques pages, différentes questions seront posées et les fondations d'une solution durable seront présentées et ainsi limiter les pertes de contrôles.

Le Cloud computing, l'informatique abracadabrantesque ?

Le Cloud computing permet de stocker, accéder à des applications et manipuler de grands volumes de données sur l'Internet et ce, au travers de l'exploitation de différents composants groupés en services. Pour faire simple et pour ne citer que les principaux modèles, il s'agit de savoir ce que le fournisseur de services, qui deviendra un partenaire si il accompagne le client, déclare faire cette organisation : l'hébergement de serveurs (Infrastructure as a service), la mise à disposition d'un ensemble de composants à assembler (Platform as a service) ou encore un applicatif préconfiguré pour vous (Software as a service).

Assez similaire à ce qui pourrait être mis en place en entreprise, puisqu'il repose sur des technologies

similaires, le Cloud a comme intérêt de proposer nativement un hébergement adaptif permettant d'allouer des ressources en temps utiles, ressources qui sont partagées avec un plus grand nombre de clients, réduisant les frais de gestion à son minimum, ce coût étant partagé entre tous. La manière d'exposer ces ressources s'avère cependant bien différente de ce qui se fait en entreprise grâce à des architectures résilientes. Ainsi, le Cloud computing peut être vu comme l'abstraction d'un ensemble de ressources hébergées sur le matériel d'un tiers.

Le Cloud computing permet de stocker, accéder à des applications et manipuler de grands volumes de données sur l'Internet et ce, au travers de l'exploitation de différents composants groupés en services.

Comprendre les risques majeurs

L'indisponibilité des services

Les grands fournisseurs de services disposent de solutions de repli en cas de crash majeur de composants tant applicatifs logiques que les éléments d'infrastructure physiques, du simple routeur au datacenter dans son ensemble. Le risque 0 n'existe pas et la tolérance aux arrêts varie en fonction des utilisations faites par les exploitants des services.

Q : Quelles sont les mesures mises en place par le fournisseur de services ? Quel est l'impact pour vos équipes métier ? Quelles sont les solutions de contournement ? Où sont stockés les backups de données ? Qui en a possession ?

L'utilisation inadéquate des technologies

De plus en plus fréquemment, les solutions font appel à des approches mixtes, basées sur les différents modèles Cloud. Ce nouveau type d'architecture s'avère très intéressant pour autant que le service et les technologies sous-jacentes soient utilisés pour ce qu'ils sont conçus. Un passage du on-premises dans le Cloud, même en IaaS, nécessite divers ajustements pour fournir un niveau de performance mais aussi de sécurité suffisant pour limiter les risques.

Q : Les solutions déployées sont-elles pensées pour le Cloud ou est-ce englobé au dans un hébergement dit sécurisé ? L'ensemble des composants utilisés dans la solution est-il clairement identifié ? Où est stockée l'information ? La solution est-elle full cloud ou hybride ? Où le traitement de ces données s'effectue-t-il ? Par qui ?

La gestion des accès

Le Cloud est accessible de partout. C'était auparavant le message clé de l'Internet et c'est désormais une des plus grandes problématiques. En entreprise, il est généralement nécessaire d'être sur un réseau reconnu pour accéder à la donnée. Dans le cas du Cloud, il s'agit d'être en contrôle avec l'ensemble des accès et des dispositifs utilisés, leur configuration et leur niveau de sécurité proposé, notamment la double authentification, la possibilité de supprimer des données à distance.

Q : Quelles sont les méthodes d'authentification et d'autorisations ? Quelles sont les sécurités en place (multi-facteurs d'authentification) ? D'où, et depuis quels dispositifs, les applications et les données sont-elles accessibles ? Est-il possible d'empêcher l'enregistrement de certaines données sur des dispositifs donnés ? Est-il possible de supprimer cette donnée à distance en cas de perte ou de vol de ce dispositif ?

L'absence de ressources compétentes

Souvent perçu comme une transition naturelle, le passage du On-premises vers le Cloud requiert pourtant de comprendre ce dernier et les services qui sont utilisables. Il ne s'agit pas uniquement de « mettre dans le Cloud », mais de transformer la solution existante vers une solution Cloud ou hybride. Ainsi, il est fréquent de voir ces nouveaux paradigmes oubliés lors des phases de conception, pour autant que ces phases aient réellement lieu.

Q : L'ensemble des intervenants est-il Cloud-oriented ? Sont-ils formés à cette approche Cloud ?

La gouvernance et le contrôle

Ce point est crucial. Chaque perte de contrôle a pour impact d'augmenter les risques associés à la solution et peut mettre en péril la solution et les données qui y sont stockées. L'absence de points de contrôle favorise l'apparition de failles de sécurité, des problématiques de performances mais aussi des impacts en cas d'incident majeur, tel que l'arrêt d'un service. Par la présence de droits anormalement élevés pour certains utilisateurs, de l'IT mais aussi du métier, il est fréquent de voir des points de contrôle contournés.

Q : Qui dispose des droits d'administrations ? Comment sont effectués les points de contrôle ? Comment sont définies les règles générales de bonne gouvernance ? Quel est le processus de mise à disposition d'une solution ?

La gestion des coûts

Avoir un système à géométrie variable en fonction de l'utilisation de celui-ci amène avec lui des problématiques autres : les coûts augmentent de manière significative et inexpliquée. Cette situation empêche une refacturation des services agrégés aux clients. Ces coûts doivent être absorbés et deviennent ainsi des coûts structurels, augmentant ainsi le prix du service de base sans pour autant en augmenter la valeur.

Q : Les services sont-ils facturés à la consommation ou forfaitairement ? Comment les coûts sont-ils agrégés et refacturés ? Les coûts tiers tels que ceux liés aux ressources sont-ils comptabilisés ?

La conformité

De plus en plus d'applicatifs se targuent d'être respectueux du RGPD. L'applicatif lui-même l'est en effet. Qu'en est-il de l'utilisation qui en fait ? Les données se trouvent souvent à différents endroits et bien souvent sur des appareils qui sont hors de contrôle, stockées par des utilisateurs qui possèdent ainsi de nombreuses informations privées. Il en va de même pour les administrateurs qui accèdent à l'information directement à la source.

Q : Comment sont accédées les données ? Par quels composants ces données transitent-elles ? Les données sont-elles encryptées à tout moment, lors du transfert de celles-ci mais aussi au repos ? Qui accède à ces composants ? Quelles sont les procédures en cas de départ d'un employé ? Comment sont-elles exécutées automatiquement ?

La performance

Avec des serveurs distants, la performance peut être fortement impactée, notamment lorsque l'on souhaite mettre en place des composants en charge de la sécurité sans pour autant avoir conçu une architecture adéquate. Un service informatique qui répond lentement réduit le niveau d'adoption de ce service et entraine des conséquences sur le métier lui-même. Dans ces cas, le service agonise lentement, jusqu'à ce qu'il soit remplacé par quelque chose d'autre. Très souvent cette nouvelle solution est choisie au plus vite, sans faire de choix stratégiques et sans tenir des bonnes règles de conception de services.

Q : Quels sont les composants par lesquels les données transitent ? Que prévoient les différents niveaux de services des composants ? Quels sont les impacts pour les utilisateurs ?

L'adoption

Au même titre que des performances faibles, ne pas comprendre comment un système fonctionne entraine un rejet par ses utilisateurs cibles. Lorsque l'utilisateur n'a d'autre choix que d'utiliser un service qu'il ne souhaite pas, il ne fait guère attention à comment les données à leur disposition sont utilisées, ne les mettent pas à jour voire même produisent des informations fausses, ou tout du moins incorrectes, et qui peuvent également avoir des conséquences importantes.

Q : Qu'est-il prévu pour augmenter le niveau d'adoption par les utilisateurs ? A quel moment sont-ils inclus ? Dès les phases de conception ?

Ne pas comprendre comment un système fonctionne entraine un rejet par ses utilisateurs cibles.

Minimiser les risques

Maîtriser les RTO, RPO and backups plans

La solution se base sur un ensemble de composants, certains sont critiques, d'autres non. Ainsi, il est important de comprendre ce qui est défini pour chacun d'entre eux. En effet, chaque service propose un niveau de service différent et par niveau de service, on entend évidemment la disponibilité et la performance mais aussi le modèle de support et les compensations. Les techniques de mesure sont également importantes à comprendre puisqu'elles définissent comment l'ensemble des niveaux de service est vérifié.

Ces aspects sont souvent omis et pourtant il s'agit de concevoir le service fourni de manière adéquate, en tenant compte de l'ensemble des composants utilisés. Dans certaines situations, il s'agit de définir des procédures manuelles tandis que dans d'autres, l'application a été conçue pour supporter cet arrêt temporaire et redémarrer par la suite. Pensez à mettre ces procédures en lieu sûr et accessible, idéalement hébergé chez un autre fournisseur de services.

Comprendre les rôles et responsabilités

La suscription à un service permet de bénéficier du service pour un coût donné. Il y a quelques rôles explicites qui doivent être joués par le preneur et très souvent des rôles implicites qui sont omis des contrats, puisque le contrat porte sur la fourniture du service et non son utilisation. Ainsi, au-delà des niveaux de service, la maitrise des rôles et responsabilités adhérents à ce service est nécessaire.

S'associer aux personnes de métier... hors IT

Eh oui ! Aussi surprenant que cela puisse paraitre, on parle de fourniture de services. De plus en plus, la souscription se base sur un « quoi » et non plus un « comment ». Le quoi c'est ce que l'on peut attendre, dans quel délai, avec quel niveau de qualité. De ce fait, juristes et gestionnaires de conformité, pour ne citer qu'eux, ont un rôle prédominant dans la souscription à des services Cloud.

Concevoir des applications Cloud-first

Même en IaaS ou en « serverless », c'est-à-dire qu'il n'est pas nécessaire de se préoccuper des serveurs qui supportent les services et ses interfaces, il s'agit de penser les solutions pour le Cloud et non hébergées dans le Cloud. Concevoir des applications Cloud c'est avant tout architecturer un ensemble de services ensemble, un peu comme pour une application qui embarque de nombreux composants tiers mais en tenant compte de la localisation des services, de la disponibilité de ceux-ci et des capacités de gestion des allocations de service.

Se baser sur différents fournisseurs de services Cloud

Lorsque l'ensemble des éléments ci-dessous est bien géré, il est possible de partir sur une approche multi-cloud soit en incluant ces différents fournisseurs dans une même solution soit selon un modèle actif/passif, notamment en cas de crash. Lorsque l'ensemble est géré efficacement, l'ensemble propose alors un risque moindre tandis qu'une solution hybride non maitrisée multipliera le risque associé.

Allouer des ressources en fonction du besoin

Disposer de ressources physiques et logiques au moment opportun, à savoir lorsqu'elles sont consommées est un véritable atout du Cloud. Il faudra cependant veiller à paramétrer au mieux l'ajustement automatique pour éviter des changements intempestifs qui pourront entraîner davantage de problèmes de performance. L'automatisation du démarrage, de l'arrêt et des allocations de ressources prend tout son sens dans ce contexte.

Augmenter la disponibilité et les performances des services en les déployant dans diverses régions

Le multi-régions devient un standard auprès des plus grands fournisseurs de services Cloud. Celui-ci permet de déployer des services Cloud dans différentes parties du monde, tout en gardant une gestion centralisée et unifiée. Ainsi, certains services peuvent être utilisés de différentes manières : les données sont physiquement stockées dans une seule région donnée ou encore automatiquement dédoublées dans les différentes régions, et ce de manière transparente pour l'utilisateur.

Bien maitrisé, le multi-régions peut permettre la mise en place d'une solution simple et en phase avec les règlementations des différentes régions.

Ce nouveau type d'architecture permet ainsi d'augmenter drastiquement les performances des solutions en rapprochant les composants au plus proche des utilisateurs. Un autre avantage certain est l'augmentation de la disponibilité des services. Ainsi lorsqu'une région est touchée par un incident, les utilisateurs sont automatiquement redirigés vers une autre instance du service, dans une autre région.

Utiliser des connexions directes vers le fournisseur

La connexion entre un poste client et le fournisseur de services nécessite de faire transiter des données par de nombreux routeurs. Evidemment, les routes empruntées sont optimisées pour satisfaire le plus grand nombre. Des connexions directes entre les zones de travail et les fournisseurs de services réduisent le temps de latence et augmentent ainsi la performance. A nouveau, cela doit être réfléchi car ces connexions engendrent des coûts et ne sont utilisables que depuis un point donné.

Former l'ensemble des intervenants, y compris les utilisateurs

Le degré de formation et la méthode divergent en fonction du public cible. Les concepteurs et les administrateurs sont formés aux différentes techniques et surtout aux fondements que ces techniques supportent. Les utilisateurs seront eux accompagnés dans leurs démarches, au travers de messages de l'applicatif lui-même.

Documenter, documenter, documenter

« Oui, mais nous sommes agiles, il n'y a plus de documentation ». Un conseil, oubliez cette maxime, à part si l'objectif est d'augmenter le risque tant en termes de sécurité que de gestion au quotidien. D'ailleurs avec des points de contrôles adéquats, la documentation doit être fournie, au risque de se voir refuser tout déploiement de solution.

La documentation se veut la représentation d'une situation attendue. Ainsi, les changements doivent être répercutés dans la documentation. Ces changements, pour des raisons de traçabilité et de timeline, sont répertoriés dans un catalogue de changements, quelle qu'en soit la forme.

Le degré de formation et la méthode divergent en fonction du public cible.

Inclure les notions de sécurité dès la conception

Durant de nombreuses années, il s'agissait de sécuriser les applications en évitant que celles-ci ne soient accessibles sans autorisation préalable. On pourrait ainsi dire qu'il s'agissait de sécuriser l'hébergement de l'applicatif. Pourtant, il n'y a pas un seul composant en charge de la sécurité. La sécurité s'applique à chaque composant, chaque flux, chaque rôle, chaque client. En résumé, à chaque utilisation.

La sécurité doit se faire en tenant compte de l'ensemble des composants. Bien que cela s'avérait d'ores et déjà préconisé, la sécurité fait partie prenante de l'applicatif et se doit d'être incluse dans la phase de conception. D'ailleurs, dans un monde où DevOps est le terme à la mode, peut-être serait-il nécessaire de parler de DevSecOps. La perception serait cependant limitée par rapport aux concepts même du DevOps.

Encrypter les données autant que possible

Une architecture limitant la duplication de données a un objectif d'avoir une vérité vraie. Au-delà de cet aspect, il s'agit également d'être en contrôle sur les différents composants qui disposent de cette donnée et de comment il est possible d'y accéder.

Quelle que soit l'architecture, des données résideront toujours dans une zone de stockage, temporaire ou long-terme. Par ailleurs, les données transitent d'un composant à l'autre. L'ensemble de ces données peuvent être accédées à tout moment, par les différents fournisseurs, par les administrateurs ou les utilisateurs eux-mêmes.

Enfin, certaines données peuvent être hébergées en dehors de la zone de contrôle. Dans ce cas, il faut qu'une autorisation explicite soit octroyée, rendant alors celui qui a donné cette autorisation responsable de ce qui est fait de la donnée.

Utiliser plusieurs facteurs d'authentification

Pour faire simple, la combinaison de facteurs d'authentification permet de vérifier que la personne connectée est bel et bien celle qu'elle prétend être. Pour cela, elle doit fournir à minima 2 éléments parmi des choses que l'on a, des choses que l'on est et des choses que l'on sait. Ainsi, un accès sécurisé se fera depuis un appareil enregistré ou encore un jeton ou une carte d'authentification, en utilisant la reconnaissance facile ou digitale et l'utilisateur devra depuis fournir un code PIN.

Auditer les permissions, les accès, ...

L'audit des solutions doit se faire dès les phases en amont. Certains appelleront cela de la validation.

Quoiqu'il en soit, une revue préalable permet de réduire drastiquement le risque de mettre en place des solutions non viables ou qui introduisent du risque.

Dans le même esprit, en période opérationnelle, l'utilisation de composants tiers mais aussi les permissions doivent être audités de manière régulière afin de confronter ce qui est attendu avec le réel afin de réajuster ou de ré-évaluer le risque associé à une déviation.

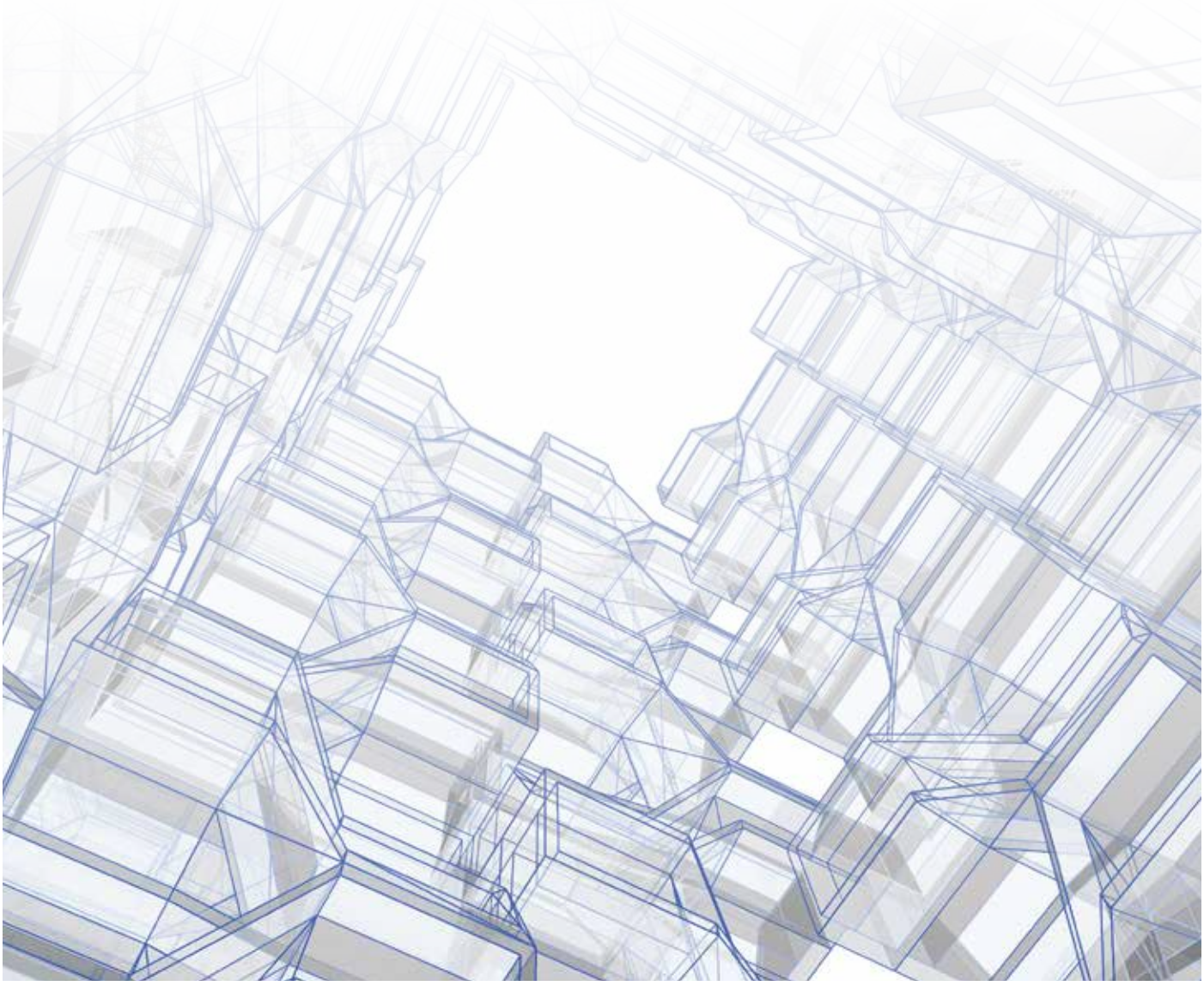
Et maintenant ?

Que les applications se trouvent d'ores et déjà dans le Cloud ou non, il s'agit de comprendre au mieux les flux de données et des différents intervenants dans ce flux. La documentation peut se faire de manière préventive, lors des phases de conception et même de la définition de la stratégie ou lorsque la solution est d'ores et déjà opérationnelle.

« Oui, mais nous sommes en SaaS, pourquoi devrais-je m'en soucier ? ». Rappelez-vous que les applicatifs, tout du moins ceux de qualité, sont pensés dans le but de donner les fondations nécessaires, tout comme les routes empruntées quotidiennement par des millions de personnes sont conçues. Dans les deux cas, des incidents peuvent survenir, avec des conséquences bénignes le plus souvent. Parfois pas.

La maîtrise de l'architecture du système d'informations au travers d'une conception et d'une transition contrôlées, une documentation au plus juste et des audits réguliers contribue largement à la fiabilité des solutions et services fournis aux clients.

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



Les trois qualités du DSI moderne !

Quelles sont les clés de réussite et de performance du DSI moderne ? Influence auprès de la direction générale, orientation clients et maturité de la transformation numérique...

Les objectifs d'entreprise, les attentes des clients et collaborateurs et les besoins métiers se hissent au rang des priorités, bien avant l'approche technologique de la fonction.

Des DSI visionnaires et leaders

Les compétences managériales et les qualités de leader stratégique remportent la palme pour 63%. Les DSI visionnaires ont le vent en poupe et mettent en avant 3 qualités :

- Être avancé dans la digitalisation des process
- Avoir construit des relations de confiance avec la direction générale et avoir de l'influence auprès d'elle
- Se concentrer sur la réalisation des objectifs clients

20% estiment posséder ces qualités !

Stratégiques et innovateurs

Les DSI entendent aligner les objectifs de l'IT sur ceux de l'entreprise, afficher de hauts niveaux de productivité, d'innovation et de satisfaction client, et entretenir des relations étroites avec la direction.

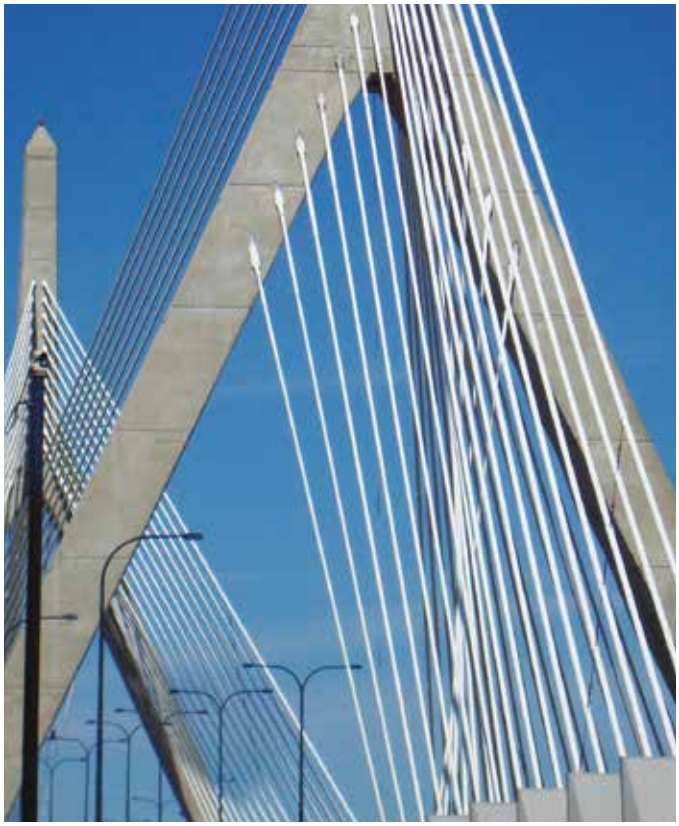
La mise en place de partenariats et projets transversaux passe par

- La sensibilisation des autres membres de la direction aux technologies numériques – 64%
- La collaboration avec la Direction Générale et la mise en place de feuilles de route - 69%
- La coopération avec les services RH pour recruter et retenir les talents – 77%

Les DSI prônent aussi l'automatisation et l'intégration des processus de travail et l'instauration de workflows numériques pour

- les gains d'efficacité (80 %)
- la performance financière (78 %)
- la productivité (78 %)
- la performance des employés (76 %)
- l'innovation (75 %).

Source Etude internationale ServiceNow - 516 DSI



GRANDE
ÉCOLE DU
NUMÉRIQUE

Ils recrutent des apprenants de la GEN, pourquoi pas vous ?

«Son aisance en public en fait une consultante hors pair.»

Jean-Noël Karamian,

Manager d'Imane,
Software Engineer formée dans l'une des **750 formations labellisées GEN.**

En plus des compétences acquises à la GEN, les savoir-être des apprenants en font des profils polyvalents.
Grâce à son école de théâtre, Imane excelle chez Capgemini.

www.grandeecolenumerique.fr

Le droit à la déconnexion : UN ENJEU RH

Smartphones, nouveaux outils de communication, messageries professionnelles hébergées dans le Cloud, autant de technologies qui permettent aux salariés de se connecter à leur environnement de travail à tout heure du jour et de la nuit. Génératrices de stress, et contre productives, les connexions addictives deviennent des préoccupations majeures pour les entreprises.

Promodag, éditeur français propose un outil leur permettant d'encadrer et de prévenir ces comportements. Un moyen d'être en conformité avec le droit à la déconnexion.

Teint halé, détendus, reposés... les français de retour de congés ont-ils pour autant pleinement profité de leurs vacances estivales ? Ont-ils réussi à se déconnecter ? Selon une étude menée, début juillet 2019, par la société d'intérim Qapa, 71 % des femmes et 62 % des hommes éprouvent des difficultés à se déconnecter du travail alors qu'ils n'étaient respectivement que 35% et 66% en 2017.

Plusieurs raisons à ce phénomène. L'essor du télétravail et du travail à distance, la multiplication des smartphones, les nouveaux outils de communication (visioconférence, chat....) et les messageries professionnelles de plus en plus hébergées dans le Cloud.

93% des français interrogés en 2019 attribuent, d'ailleurs, la responsabilité de cette dépendance excessive aux smartphones contre 28,5% en 2017. Et si pour certains leurs responsabilités, charges de travail ou la peur de perdre leur emploi sont les raisons de cette connexion, d'autres ont développé un comportement addictif.

Déconnexion : chaque entreprise doit formaliser ses règles

Pourtant, le droit à la déconnexion existe en France et figure même parmi les obligations légales des entreprises depuis la loi Travail El Khomri en 2016. Mais bien que ce droit soit notifié dans l'article L2242 8, rien n'en définit le cadre. Charge aux entreprises d'en définir les modalités et de les formaliser dans leurs règlements intérieurs.

Or en 2018, une étude d'OpinonWay révèle que seules 23 % des entreprises ont rédigé des chartes de bonnes pratiques. Un faible taux au regard de l'augmentation de ces comportements et des conséquences pouvant en découler : stress, fatigue, burn out.

Le droit à la déconnexion existe en France et figure même parmi les obligations légales des entreprises depuis la loi Travail El Khomri en 2016.

Aussi, pour inciter les salariés et notamment les cadres à profiter de leurs congés, leurs RTT ou leurs week-ends, de plus en plus d'entreprises souhaitent se doter de moyens pour repérer les excès de zèle et sensibiliser les addicts à l'importance de se préserver du temps hors connexion pour concilier vie personnelle et vie professionnelle.

Des outils au service de la déconnexion

Dans ce contexte, des outils, permettant de vérifier l'application des conditions du règlement intérieur, peuvent être mis en place. Promodag, éditeur de logiciels français créé il y a vingt cinq ans, propose une gamme complète d'outils permettant d'analyser le trafic de la messagerie Exchange (serveurs internes ou Office 365) et d'automatiser la gestion de son utilisation.

Grâce aux 80 rapports prêts à l'emploi proposé par le logiciel, les entreprises et notamment les Ressources Humaines disposent d'une vision globale des usages des messageries que ce soit par collaborateur, par service, région, ville ou pays. Elles peuvent également extraire des courbes de ventilation des messages envoyés en fonction des jours de la semaine et des heures.

Promodag Reports est à la fois un outil d'alerte, de sensibilisation et de prévention.

Interfacé à l'annuaire et au SIRH de l'entreprise, l'outil intègre la gestion des horaires selon le profil de chaque collaborateur afin de prendre en compte son planning, ses congés et ses RTT. Promodag Reports est, aussi, en mesure d'extraire des listes nominatives ou anonymes de collaborateurs utilisant la messagerie en dehors des heures ouvrables. L'outil gère également l'envoi de courriers mails aux salariés qui outrepassent le règlement afin de les sensibiliser aux bonnes pratiques de l'entreprise.

Enfin, grâce à un historique des connexions mails, les Ressources Humaines peuvent suivre leur évolution des connexions et ainsi mieux identifier les éléments à l'origine de ce type de comportements. Promodag Reports est à la fois un outil d'alerte, de sensibilisation et de prévention. Il permet aux entreprises d'être en conformité avec l'article L2242 8 du Code du travail et de s'assurer de ne pas entraver le droit à la déconnexion, tout manquement à ce droit pouvant se régler devant les tribunaux.

Promodag

www.promodag.fr

ForePaaS ACCÉLÈRE LES PROJETS DATA DES ENTREPRISES

Comment accélérer les projets de traitement de la donnée et automatiser les opérations de data management ? Des défis que la startup ForePaaS, basée à Paris et à San Francisco, relève aisément avec sa plate-forme data tout en un ! L'entreprise co-fondée en 2005 par Paul Sinaï, Vincent Michel et François Vaillant, édite une plate-forme Big Data Analytics multi Cloud qui permet de créer, déployer et gérer les applications rapidement. Entretien avec Paul Sinaï, CEO & CTO ForePaaS.

« Le marché de la data n'attend pas, il évolue et affiche une forte croissance chaque année, il y a énormément de demandes ». Si la data est un enjeu géo stratégique, les startups accélèrent indéniablement la performance des entreprises.

Une plate-forme analytique de bout en bout

ForePaaS « c'est une plate-forme as a Service end to end pour l'analytique ». L'ensemble des outils permet de traiter les données, de l'extraction, la transformation au stockage, et mise en production d'algorithmes jusqu'à la création d'applications. L'intégralité de la chaîne est disponible et ce, sur n'importe quel Cloud (Amazon, Azure, Google, OVH, Outscale, cloud privés, Openstack, VMware...) « afin de garder une grande flexibilité sur l'endroit où les applications des entreprises sont hébergées et bénéficier de toute la rapidité et l'agilité qu'offrent les plates-formes de développement as a Service ». Les fonctionnalités, gestion des données, tableaux

de bord, API, Machine Learning, viennent fluidifier et simplifier les projets basés sur l'analyse des données.

Si la donnée est essentielle dans la décision de l'entreprise, elle est livrée aujourd'hui de façon exponentielle.

« Nous ne faisons pas de technologie as a Service mais notre environnement entièrement automatisé dispose de ses propres technologies pour réaliser chacune des étapes de traitement et s'adresse aux datascientists, dataanalysts, business analysts afin d'accélérer les projets data de façon très significative ».

La valeur ajoutée des projets data !

Quand on voit que plus de 50% des projets d'Intelligence Artificielle et 70% des projets analytiques Big Data ne partent pas en production, « notre écosystème de partenaires nous permet d'aider les clients à gagner en maturité sur les projets data afin de ne pas passer à côté des projets à valeur ajoutée pour le marketing, la finance, la supply chain… ».

Face au nombre de projets data en entreprise devant être étudiés, les décideurs IT ou métiers scrutent toutes les opportunités business et ne doivent pas ignorer des solutions permettant de tester et déployer rapidement et facilement des projets qui répondent aux besoins métiers.

Si la donnée est essentielle dans la décision de l'entreprise, elle est livrée aujourd'hui de façon exponentielle (Internet des Objets, industrie 4.O…), ce qui accélère encore plus la quantité, la vélocité et la diversité des informations qui permettent d'agir en temps réel.

« C'est pourquoi pour gagner du temps, il faut traiter en parallèle le maximum de projets grâce à des plateformes qui ont déjà fait des choix technologiques, comme ForePaaS, sans besoin de construire sa propre plate-forme ».

Une sécurité à plusieurs niveaux

Au niveau de la stratégie. En Europe, si le sujet de l'indépendance vis à vis des fournisseurs Cloud est une question délicate, le multi-cloud est considéré comme une des grandes avancées technologiques « avoir de vraies réflexions multi cloud dès maintenant est essentiel pour les entreprises européennes pour garder sous contrôle la propriété intellectuelle. Demain nous pensons que les organisations iront chercher la puissance de calcul au meilleur offrant selon les types d'applications, et mettront en concurrence les différents cloud providers ».

Avoir une politique sur un seul cloud provider est très risqué notamment en raison de la dépendance et lors de la construction d'applications stratégiques autour des données.

La valeur business est un enjeu crucial, il faut donc des solutions business oriented. ForePaaS relève les défis du Big Data et de l'IA et permet d'accéder à une sécurité et un vrai contrôle .

Au niveau de l'accès. Dans des environnements automatisés, il est plus simple d'avoir une traçabilité des données de A à Z sur toute la chaîne (de la collecte à la consommation).

Au niveau de la protection. Les Cloud providers investissent massivement dans des équipements de sécurité (pare-feu…) et « en déployant nos plateformes sur ces Clouds, nous permettons à nos clients de bénéficier de la puissance de leur réseau de protection ».

> Par Sabine Terrey

Paul Sinaï

Cybersécurité :
TECHNIQUES DE CARTOGRAPHIE ACTIVE DIRECTORY AVEC BLOODHOUND

L'objectif de cet article est de vous donner les pistes nécessaires afin que vous puissiez comprendre, évaluer et enfin utiliser le fantastique outil qu'est BloodHound. BloodHound est un outil OpenSource et gratuit, régulièrement utilisé lors des attaques sur Active Directory.

L'objectif de BloodHound n'est pas la réalisation de l'attaque elle-même mais de fournir à l'attaquant ou à la RedTeam l'ensemble des informations nécessaires sur l'environnement Active Directory visé, et ce de façon extrêmement détaillée.

Les différentes étapes d'une attaque sur Active Directory

Il existe plusieurs modèles pour décrire les séquences d'attaque, nous utiliserons ici une méthode parmi tant d'autres afin de décrire l'enchainement des étapes pour réaliser une attaque complète sur un environnement Active Directory :

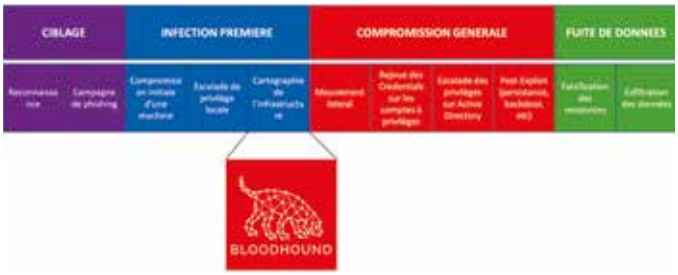


Fig 1. Les étapes classiques d'une attaque visant Active Directory

BloodHound est un outil de cartographie, il va permettre à l'attaquant de cibler de manière diablement efficace les cibles internes à privilégier et les chemins les plus simples à exploiter pour arriver au Graal que représente le compte Administrateur du domaine.

Cette étape est tout à fait primordiale pour un attaquant, car elle lui permettra de sélectionner les ressources ou objets à compromettre pour rapidement arriver à ses fins. Dans un Active

Directory de plusieurs milliers d'objets, il est nécessaire de pouvoir aller vite en visant les objets principaux qui possèdent des « faiblesses ». Ces faiblesses peuvent être d'ordre structurel ou comportemental, mais l'idée est d'aller directement au but en ayant au préalable parfaitement cartographié l'environnement, ceci permettant de cibler l'attaque pour la rendre efficace.

Le mot anglais 'BloodHound' se traduit en français par 'Limier'. Le limier est une race de chien possédant un excellent nez, il est selon les spécialistes le meilleur chien pour suivre une piste, quelle que soit la distance - aux Etats-Unis, les Limiers sont utilisés par la police pour retrouver des personnes disparues, dans l'environnement IT, notre limier-BloodHound nous servira à pister le meilleur chemin vers la compromission Active Directory !

Téléchargement et installation de BloodHound

Téléchargement de BloodHound

Le projet BloodHound est disponible sur GitHub à cette adresse : https://github.com/BloodHoundAD/BloodHound - mais vous devez en fait télécharger deux éléments :

1) La version compilée pour votre environnement sur https://github.com/BloodHoundAD/BloodHound/releases - par exemple pour Windows, vous devez télécharger le fichier ***BloodHound-win32-x64.zip*** :

Fig 2. Téléchargement de la version compilée de BloodHound

Notre limier-BloodHound nous servira à pister le meilleur chemin vers la compromission Active Directory.

2) La version non compilée en clônant le projet sur GitHub depuis l'adresse https://github.com/BloodHoundAD/BloodHound :

Fig 3. Téléchargement de la version non compilée de BloodHound

Installation et dépendances de BloodHound

Afin de pouvoir installer et utiliser BloodHound, vous devez avoir au préalable installé trois composants :

- Les packages Java pour votre environnement
- .NET Framework 3.5
- La version communautaire du serveur Neo4j

Pour ceux qui ne connaissent pas Neo4j, il s'agit d'une solution permettant de manipuler des données extrêmement complexes sous forme de graphe, permettant alors une exploration des données collectées et leur exploitation simplifiée. Neo4j est utilisée dans de nombreux projets communautaires ou applications professionnelles et possède une communauté croissante d'utilisateurs.

Vous devrez être Administrateur local de la machine sur laquelle vous installerez BloodHound, mais vous n'avez pas besoin d'être Administrateur du domaine pour utiliser l'outil ! C'est d'ailleurs logique, puisque l'outil vous servira justement à explorer et sélectionner les meilleures pistes afin de devenir Administrateur du domaine ou de la forêt ! Il suffira d'utiliser un compte utilisateur classique, permettant la lecture des objets Active Directory via le protocole LDAP, ce qui est un droit par défaut de tous les utilisateurs créés dans Active Directory.

Rappelez-vous notre schéma d'introduction sur les étapes d'une attaque, BloodHound s'utilise entre 'l'Escalade de privilèges locale' et le 'Mouvement latéral' et cible l'action de Cartographie.

Première étape : Collecte des données Active Directory et injection dans BloodHound

BloodHound possède dans les dernières versions un outil dédié à la collecte des données Active Directory, cet outil est localisé dans le répertoire ***Ingestors*** de BloodHound et s'appelle ***SharpHound***. Il suffit d'ouvrir une fenêtre de commande, de se rendre dans le répertoire ***Ingestors*** et de lancer la commande suivante : ***SharpHound.exe***

--CollectionMethod All

A la fin de la commande, un fichier ZIP est automatiquement généré dans le même répertoire, ce fichier compressé contient plusieurs fichiers JSON qui contiennent les données collectées. Ce fichier ZIP sera ensuite injecté dans la base de données Neo4j via l'interface de BloodHound.

Il faut maintenant se connecter à l'interface de BloodHound en exécutant ***BloodHound.exe*** puis s'authentifier :

Fig 4. Interface d'authentification de BloodHound

Vous arriverez alors à une page d'accueil par défaut, qui ne contient aucune données. Il faut alors sélectionner le bouton ***Upload Data*** et choisir le fichier ZIP à importer. A la fin de l'import vous devez obtenir un premier graph sur l'interface :

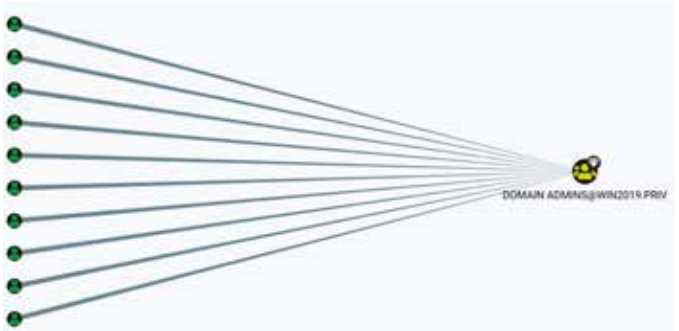


Fig 5. Votre premier graph

Nous y sommes, tout est prêt pour commencer l'exploration des données Active Directory.

Deuxième étape : Utiliser BloodHound pour explorer les données Active Directory et identifier les cibles

BloodHound s'appuie donc sur la notion de graph, vous permettant une navigation facilitée dans les données complexes collectées. La notion de graph peut être résumée en trois éléments :

- Les **Nodes** : Les Nodes sont globalement des objets - Dans le cadre d'Active Directory, cela peut donc être un utilisateur, une machine, un groupe, un domaine, etc.
- Les **Edges** : Les Edges sont les relations entre les objets, ils sont définis par deux éléments principaux : (1) le sens de la relation (2) la nature de la relation – Dans le cadre d'Active Directory, cela peut définir l'appartenance à un groupe, le fait d'être administrateur d'un objet, etc.
- Les **Paths** : Le Path est un en ensemble de Nodes connectés par des Edges – Un Path est un chemin logique en partant d'un objet pour arriver à un autre, dans le cadre d'Active Directory cela permet de définir un chemin d'attaque.

Voici un résumé de ces trois éléments en prenant un exemple simpliste basé sur les goûts culinaires et la relation entre différentes personnes :

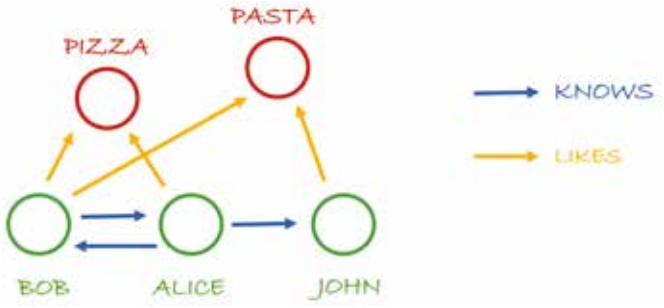


Fig 6. Exemple d'objets, de relations et de chemins basés sur la notion de graph

BloodHound possède une interface de recherche très bien pensée, comportant trois boutons principaux : **Database Info, Node Info** et **Queries**.

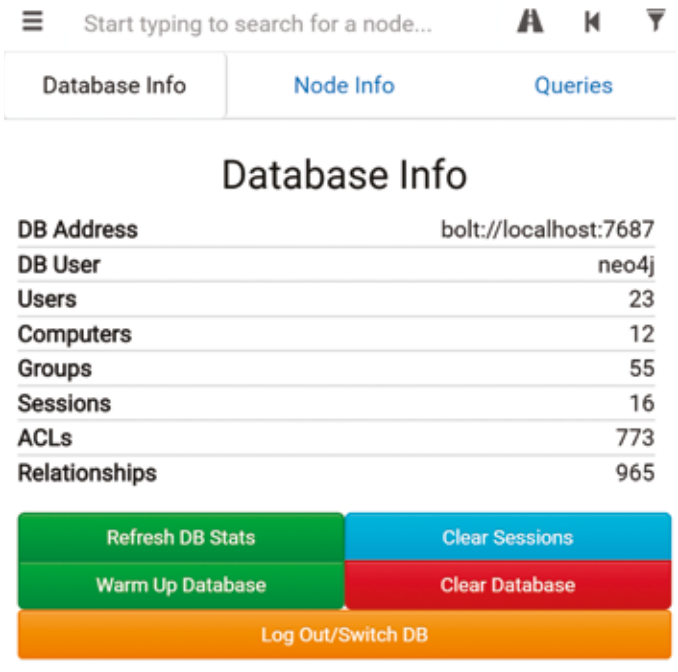


Fig 7. Interface de recherche et moteur de requêtes

Le bouton **Database Info** vous permet de visualiser les statistiques des données injectées depuis Active Directory.

Le bouton **Node Info** s'active automatiquement dès lors que vous sélectionnez un nœud, c'est à dire globalement un objet sur votre graph, par exemple ici une partie des caractéristiques d'un nœud utilisateur se nommant Yoda :

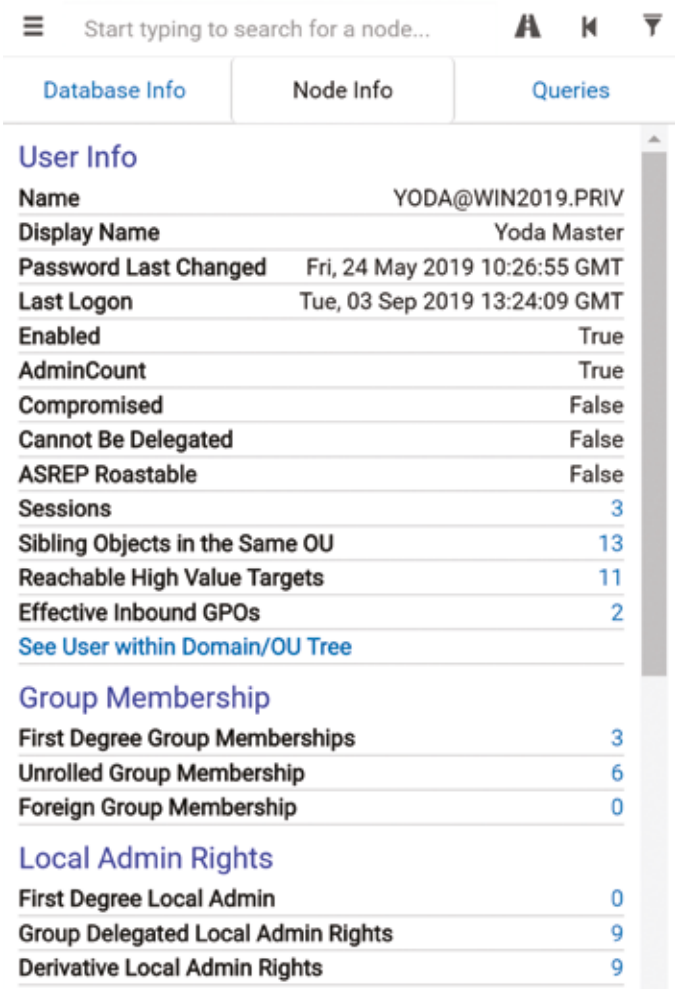


Fig 8. Exemple d'informations sur un nœud utilisateur

La plupart des informations sont cliquables, c'est-à-dire que l'on peut explorer petit à petit les objets en relation les uns avec les autres, il suffira ici de cliquer sur la valeur indiquée pour ***First Degree Group memberships*** afin d'obtenir la liste des groupes d'appartenance et ainsi de suite.

La plupart des informations sont cliquables, c'est-à-dire que l'on peut explorer petit à petit les objets en relation les uns avec les autres.

Le bouton Node Info s'active automatiquement dès lors que vous sélectionnez un nœud.

Le bouton ***Queries*** présente des requêtes toutes prêtes à l'utilisation et permet de lancer les premières recherches simples mais aussi de produire ses propres requêtes personnalisées :

Fig 9. Le bouton Queries donne accès aux requêtes préformatées

Une des meilleures requêtes préformatées pour commencer l'exploration et viser de devenir Administrateur de domaine est la requête ***Shortest Paths to High Value Targets***, voici un exemple de résultat :

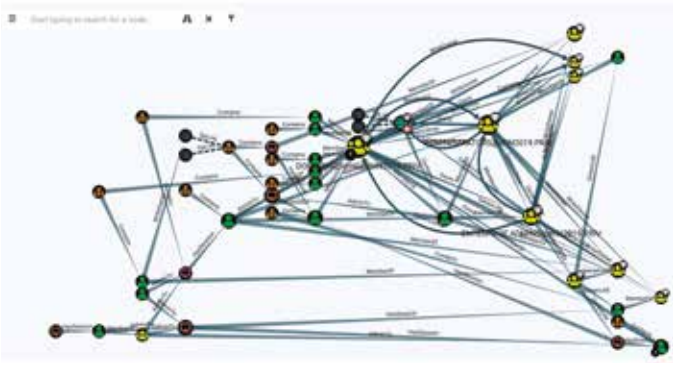


Fig 10. Exemple de graph résultant de la la requête ***Shortest Paths to High Value Targets***

Le graph vous présentera ainsi les relations entre les différents objets du domaine, avec notamment les informations suivantes :

- Les comptes à pouvoir et leurs groupes
- Sur quelles machines les comptes à pouvoir ont ouvert des sessions
- Quel groupe est capable d'administrer quel objet
- Les liens des GPOs importantes
- Etc.

Grace aux graphs, il est possible de définir un chemin d'attaque, par exemple, considérons que l'attaquant a réussi à compromettre le compte DARK, l'idée est de demander aux graphs, en partant de DARK, quel est le meilleur moyen (c'est-à-dire le meilleur chemin) pour devenir Administrateur du domaine :

Fig 11. Exemple de requête ciblée

Le résultat est parlant :

Fig 12. Exemple de chemin d'attaque

Nous savons maintenant grâce aux graphs que :

- DARK a les droits d'administration sur la machine WIN2016US02
- Le compte ROOT a déjà ouvert une session sur la machine WIN2016US02
- ROOT est membre du groupe Domain Admins

BloodHound et les graphs deviennent des outils classiques pour le Pentest Active Directory et sont importants à maitriser si vous travaillez dans le domaine de la cybersécurité.

Il suffira donc maintenant d'utiliser un outil tel que mimikatz sur ce serveur pour espérer jouer une attaque de type pass-the-hash en visant le compte ROOT.

Pour aller plus loin

Maintenant que vous connaissez les bases de BloodHound, vous voudrez peut-être aller plus loin. Je vous recommande de parcourir les forums de discussions liées à BloodHound et de vous documenter sur la notion de graphs.

En effet, BloodHound et les graphs deviennent des outils classiques pour le Pentest Active Directory et sont importants à maitriser si vous travaillez dans le domaine de la cybersécurité.

> Par Sylvain Cortes – Microsoft MVP Security Evangelist - @sylvaincortes

« 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.

Un code de conduite pour réduire la fracture numérique !

Comment pallier les fossés trop importants : 40 % des salariés français redoutent d'être mis à l'écart par ceux férus de nouvelles technologies… Il y a nécessité à mieux accompagner les collaborateurs dans l'intégration et l'utilisation des nouveaux outils.

Chat, collaboration ou projets…

Les technologies peuvent créer une fracture sur le lieu de travail : les employés moins enclins à utiliser les outils numériques peuvent être mis à l'écart s'ils n'adoptent pas les dernières applications, et notamment les outils de communication numériques :

- 52 % (plus de 65 ans)
- 46 % (18-34 ans)

Outils numériques = critère de promotion

Slack, WhatsApp ou Yammer s'implantent rapidement et prônent la flexibilité du travail :

- Ceux qui utilisent régulièrement ces technologies pour communiquer et collaborer ont plus de chances de bénéficier d'une promotion (41% - France / 65% - Monde))

L'adoption d'outils de communications numériques est un critère de promotion décisif selon 47% (18 à 34 ans) contre 33 % (plus de 65 ans).

Une dégradation des relations

La technologie établit des relations avec d'autres employés dispersés aux quatre coins du monde.

Cependant, l'utilisation du courrier électronique et d'applications de messagerie instantanée aboutirait à la création de clans et de sous-groupes (19%)

Les collaborateurs se cachent derrière les communications électroniques au lieu d'échanger ou utiliser leur téléphone (46%).

Un code de conduite

Elaborer un code de conduite pour les employés est préconisé, encore faut-il se poser les bonnes questions

- de quelle technologie l'entreprise a besoin et pour quoi faire ?
- comment avec ces outils séduire les plus jeunes sans exclure les plus âgés ?
- comment respecter des valeurs lorsque les collaborateurs utilisent ces outils à titre professionnel ?

Source Avast Business 3 558 personnes aux États-Unis, Royaume-Uni, Allemagne, France et Brésil

GOODMEETING

OPTIMISEZ LA GESTION DE VOS SALLES DE RÉUNION

www.goodmeeting.fr

Quel avenir pour la cybersécurité ?

A la veille de la 19ème édition des Assises de la Sécurité à Monaco, événement mythique de cette toute jeune profession d'une petite vingtaine d'années, il est, dans un sens, surprenant de constater à quel point l'avenir de ce monde est trouble. Va-t-on réussir à garder protégées nos vies de plus en plus en plus numérisées ? Ou allons-nous assister à de graves crises de type black-out de tel ou tel service numérique quotidien, sécurité sociale, banques, transports, infrastructures IT d'hôpitaux, etc. ?

Pourquoi ces questions ? Pourquoi ces interrogations venant d'un professionnel de la cybersécurité, plutôt optimiste et croyant fortement en l'utilité de son métier ?

La vague de solutions des éditeurs

Plusieurs phénomes, plusieurs événements ou tendances profondes touchent la cybersécurité. Commençons par celui qui est positif : la vague de solutions des éditeurs. Prolifique et constante, elle vient essentiellement de start-ups américaines, proposant de nombreuses solutions pour sécuriser telle ou telle facette de l'IT : messagerie, bases de données, lutte contre le phishing, protection des informations personnelles, scan pour détecter des failles, assainissement et remédiation d'un système après une attaque ou des incidents, suivi et filtration des données dans le cloud, etc., etc.

Profitant d'une abondance sans limite d'argent et de financements, des VCs et fonds d'investissements, des IPOs stratosphériques sans aucun lien avec une certaine réalité économique, les start-ups de la Silicon Valley ou d'ailleurs, mais rarement européennes, arrivent en masse avec des solutions prometteuses mais presque inutiles sans une intégration fine, une ingénierie adaptée à chaque contexte, sans une adaptation aux environnements IT spécifiques des entreprises clientes. Cette adaptation, ces ingénieries cousues-main sont l'une des clés de la bonne protection d'une entreprise.

La pénurie d'ingénieurs

Et c'est là un deuxième phénome, négatif celui-là : la pénurie d'ingénieurs capables de ''soulever le capot'', comprendre les solutions, les intégrer et les adapter aux environnements spécifiques des entreprises, puis exploiter leurs compétences pour le bien des entreprises clientes. Aucune chance d'espérer à un moment, une diminution de ce manque d'ingénieurs. Au contraire même. Le métier d'ingénieriste en cybersécurité étant complexe et compliqué, stressant et éprouvant, et les demandes des éditeurs étant fortes, le segment souffrira de plus en plus de ce manque d'expertises.

Les services managés de sécurité

Mais, cette deuxième tendance de fond en a fait émerger une troisième, positive et encourageante : le développement des services managés de sécurité, les MSSP. Mutualisés, externes, véritables pôles de compétences engagés (ah, l'engagement de projet d'intégration, qu'il est difficile à obtenir mais comme il est important), ils apportent des services de surveillance, de remédiation, d'analyse, de lutte contre la fraude, de support en SSI, etc.

Est-ce suffisant ? Non pas vraiment, car ces prestataires MSSP et intégrateurs sont peu nombreux et interviennent d'abord auprès des très grands comptes, les fameux ''CAC40'' ou Fortune 500. Pour les millions d'autres entreprises - souvent des sous-traitants ou des clients des grandes - les failles et les attaques restent fréquemment non détectées, jusqu'à la demande de rançon....

On le constate tous les jours. Hier, par exemple, les chaînes de production de la PME alimentaire Fleury Michon ont été touchées. L'industriel Fleury Michon a suspendu sa production pendant cinq jours en raison d'une attaque de phishing-ramsomware. Un incident dont les coûts devaient être couverts par son assurance.

Aujourd'hui, on apprend qu'Eurofins a été victime d'une cyberattaque qui a plombé le bénéfice semestriel du groupe de services d'analyses pour la pharmacie, l'agroalimentaire et l'environnement, à 58,9 millions d'euros au premier semestre, principalement en raison des perturbations et des frais liés à cette attaque au "rançongiciel" subie en juin. Le groupe estime pour l'heure que l'attaque a affecté son chiffre d'affaires de 62 millions d'euros pour le semestre (sur un total de 2,17 milliards) et que sa rentabilité a également été entamée. Et, il se retourne vers ses assureurs, autre nouvelle tendance de la cybersécurité. Là aussi, nous allons avoir des surprises, car les assureurs ne sont pas naïfs. Vont-ils payer à chaque fois ou vont-ils plutôt conditionner leurs polices aux efforts réels de protection de leurs clients ?

Les attaques des éditeurs et constructeurs

Mais, ce n'est pas tout. Une autre tendance de fond, inquiétante celle-là, est liée aux attaques des éditeurs et autres constructeurs de cybersécurité. Les policiers se font tirer dessus et cela malheureusement réussit. Ainsi, un des leaders mondiaux de la protection des sites et bases de données, classées par les fameux cadrans Gartner parmi les meilleures technologies WAF et DAM, Imperva, a annoncé en août qu'une violation de données divulguée par une « tierce partie » avait révélé les adresses électroniques, les mots de passe hachés, les clés d'API et les certificats SSL de certains utilisateurs de WAF (Web Application Firewall).

Enfin, et pour rester dans le monde des éditeurs, nous assistons aussi à la course à la consolidation. Les ''anciens'' tels que Symantec, McAfee, VMware, Cisco, etc. procèdent à des acquisitions multi-milliards de technologies nouvelles comme par exemple pour la sécurisation du cloud, Skyhigh et les technologies de CASB ou pour le très concurrentiel segment de l'EDR (Endpoint Detection and Response) l'exemple de Carbon Black récemment repris par l'éditeur VMware.

Avant toute chose, sensibiliser et former au sein des entreprises des utilisateurs de toutes professions, l'awarness comme disent les anglo-saxons.

L'awareness ...

Un monde de la cybersécurité toujours en forte croissance (125 Md en 2019 selon Gartner), avec de plus en plus d'incidents touchant toutes les entreprises, des éditeurs de solutions qui prolifèrent mais manquent d'intégrateurs, des services managés en forte croissance et surtout une pénurie de bonnes compétences humaines.

Que faut-il faire dans ce contexte ? Avant toute chose, sensibiliser et former au sein des entreprises des utilisateurs de toutes professions, l'awarness comme disent les anglo-saxons. Le MOOC de l'ANSSI est un excellent outil ! 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, des chercheurs aux marketeurs et commerciaux.

Cela permettra de gagner du temps, de stabiliser un peu les risques, malgré la crainte des grands incidents à venir.

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

Valoriser les données produites en streaming ou temps réel :

LE NOUVEL ELDORADO DU BIG DATA

Après 5 ans, le Big Data est maintenant bien établi ! Il a atteint son paroxysme ces dernières années avec les objets connectés, l'intégration des capteurs dans les objets de la vie courante (voiture, réfrigérateur, télévision, etc.). Ces derniers captent en temps réel le comportement de l'objet dans lequel ils sont implantés et transfèrent les données captées à une application qui les traite soit pour prédire le comportement de l'objet ou de l'utilisateur de l'objet, soit pour déclencher une action au niveau de l'objet, ou prescrire des recommandations d'action à l'utilisateur de l'objet.

Ces objets produisent des données en continu, ou en streaming. Il n'y a pas que les capteurs qui produisent des données en streaming. De plus en plus de cas d'usage et de modèles économiques s'appuient sur des données générées en streaming. Il peut s'agir de la publicité en ligne avec la facturation par clic, l'analyse du parcours client, la recommandation en temps réel, la détection de fraude, la cyber-sécurité (spécialement avec l'utilisation des SIEM), le tracking des achats, ou encore l'analyse omni canal.

Réussir à valoriser ces données représente donc la nouvelle frontière du Big Data. Malheureusement, les cas d'usage généralisés qui s'appuient sur les données streaming ou temps réel sont encore nouveaux dans la plupart et très peu de DSI savent comment les opérationnaliser.

Dans cette chronique, nous vous montrerons les approches conceptuelle, stratégique et technologique adaptées pour tirer profit de vos données streaming.

Réussir à valoriser ces données représente donc la nouvelle frontière du Big Data.

1- Limites de l'approche classique pour le « Big Data Streaming »

L'approche classique utilisée jusqu'à présent par la majorité des DSI pour stocker les données consiste à les considérer comme des faits et à les historiser dans une base de données centrale qui est elle-même gérée par un SGBDR. Cette approche est appelée Data *Warehouse* ou Data Warehousing (entrepôt de données). Au niveau du traitement, l'approche classique consiste à appliquer des calculs batch sur les données hébergées dans la base de données centrale ou dans le Data Warehouse.

La collecte traditionnelle est faite à l'aide d'un ETL, *Extract Transform & Load*, qui extrait les données des sources opérationnelles, les transforme de sorte qu'elles soient conformes aux règles d'homogénéisation définies par le métier et les charge dans le Data Warehouse.

Malheureusement, dans le cadre des cas d'usage des données générées en streaming (ou au fil de l'eau), cette approche "*collecte ETL + Stockage Data Warehouse + Traitement Batch sur des données historisées*" n'est pas appropriée, car au-delà de leur débit et de la vitesse avec laquelle elles sont produites, **les données streaming se caractérisent principalement par un délai de péremption très rapide** : il est estimé qu'elles perdent en moyenne 60% de leur valeur métier dans les instants qui suivent leur création. En d'autres termes, les données streaming perdent leur valeur métier quelques instants seulement après avoir été générées.

Pensez-y un moment : lorsque les capteurs implantés dans un véhicule connecté génère des données concernant les conditions du trafic l'environnant par exemple, ces données ne sont valables que dans le contexte des conditions de ce trafic. En d'autres termes, ces informations ne sont actionnables que dans les instants où le trafic est dans les conditions capturées par les données. A cause de leur rapide péremption, les données streaming doivent donc être exploitées à l'immédiat (ou en temps réel) dans les secondes qui suivent leur création, sinon elles perdent leur valeur métier et n'ont plus aucun intérêt à être historisées. A cause de leur rapide péremption, On ne peut pas les collecter ENSUITE les ingérer et ENFIN les traitées. Toutes ces 3 actions doivent se passer au même moment.

Le problème que pose le Data Warehouse en streaming est celui-ci : l'ère dans laquelle nous fonctionnons actuellement se caractérise par la croissance des différents types de données stockées. Les données stockées ne sont plus juste des données structurées d'ERP, ou des fichiers csv d'Excel, mais ce sont des données aussi diverses que les logs d'activité des serveurs Web, les logs d'un centre appel, les données des réseaux sociaux qui combinent contenus textuels, images, audio et vidéos, les vidéos de centre de surveillance, les données de capteurs etc...

Pour résoudre les challenges liés au stockage et à l'exploitation de cette grande variété d'actifs de données, l'approche appropriée ne consiste plus à centraliser leur stockage dans une base de données, mais à distribuer le stockage des données et à paralléliser leurs traitements dans un cluster Hadoop. **Les technologies utilisées pour implémenter le Data Warehouse ne permettent ni le stockage distribué, ni le parallélisme des requêtes des utilisateurs.** Par conséquent, le Data Warehouse ne peut pas être utilisé pour les cas d'usage de streaming.

Le problème avec l'ETL est que c'est un processus Batch qui charge les données périodiquement, il ne peut pas être utilisé pour charger les données qui arrivent en flux continu. Dans son principe même, l'ETL est composé d'un ensemble de routines (fonctions et procédures) qui transforment les données, gèrent leur qualité et appliquent une série de normalisations aux données avant de les charger par lots dans le Data Warehouse.

Pour traiter les données à l'immédiat ou en temps réel, la meilleure approche consiste à considérer la data non plus comme un fait, mais plutôt comme un événement.

2- Approche appropriée pour valoriser les « Big Data Streaming »

Pour tenir compte de la diversité des données à stocker en streaming, la meilleure approche consiste à s'appuyer sur un Data Lake construit sur un système de fichiers distribué tel que le HDFS. Pour réussir à collecter les données en flux continu et les délivrer efficacement, il faut s'appuyer sur 2 éléments :

- une structure de stockage particulière appelée le Log ou bus d'événements
- un système de messagerie Publish/Subscribe

Apache Kafka est l'une des technologies qui implémente ces deux éléments.

Pour traiter les données à l'immédiat ou en temps réel, la meilleure approche consiste à considérer la data non plus comme un fait, mais plutôt comme un événement. Traditionnellement, un traitement de données se fait sur un historique persisté du fichier de données. Par exemple, un fichier client stocké sur le disque dur, une table de base de données, etc.

valoriser les données produites en streaming demande un changement de paradigme, aussi bien stratégique que technologique.

Ce fichier, dans certains cas, est chargé en mémoire et le traitement y est exécuté en one-shot. Malheureusement, en streaming, cette approche n'est pas applicable car les données arrivent au fil de l'eau. Un traitement streaming ne s'exécute ni sur un historique persisté sur le disque dur, ni sur une image statique des données.

L'approche la plus appropriée pour traiter les données au fil de l'eau consiste à découper les données streaming en *fenêtres* (Windows) et à appliquer un *traitement micro-batch* sur ces fenêtres. Cette approche est communément appelée approche par fenêtrage. Spark Streaming est un exemple de technologie qui implémente très bien cette approche.

Comme vous pouvez le voir, valoriser les données produites en streaming demande un changement de paradigme, aussi bien stratégique que technologique.

Ce changement de paradigme fait entrer en scène de nouveaux concepts indispensables pour aborder avec aisance la gestion des données streaming : la sémantique de livraison des messages (Exactement-Une Fois, Au-Moins-Une-Fois, Au-Plus-Une-Fois), la sémantique de traitement, le domaine temporel, l'idempotence, la persistance anticipée de messages (Write Ahead Logging), la sémantique de résultat, les bus d'événements, les systèmes de messageries Publish/Subscribe, le fenêtrage, le micro-batch, les états, les modèles de collecte de données streaming, la cohérence streaming, la diffusion atomique, les architectures lambda, les architectures kappa, les architectures hybrides, etc.

Pour vous aider à aller plus loin, nous avons rédigé l'ouvrage « *Big Data Streaming : le traitement streaming et temps réel des données en Big Data* ». Vous pouvez vous procurer un extrait en cliquant sur le lien suivant : https://www.data-transitionnumerique.com/extrait-livre-big-data-streaming/

> Juvénal Chokogoue, auteur des ouvrages « Maîtrisez l'utilisation des technologies Hadoop » paru chez les éditions Eyrolles et « Hadoop – Devenez opérationnel dans le monde du Big Data » paru chez les éditions ENI

ABONNEZ-VOUS MAINTENANT !

SMARTDSI

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

Embarquez au cœur DE L'ARCHIVAGE DES DONNÉES NUMÉRIQUES AVEC CDC ARKHINÉO

Créée en mars 2001, cette filiale de la Caisse des Dépôts et Tiers de Confiance Archiveur, est la première société française d'archivage à valeur probante des données numériques, avec deux sites en région parisienne (actif) et un site à Bordeaux (backup). Entretien avec Charles du Boullay, président de CDC Arkhinéo.

Pour faire face à ce métier très réglementé et normé, l'entreprise ne dépend pas de prestataires externes mais s'appuie sur sa propre technologie, ce qui renforce son engagement et son action vis-à-vis de ses clients (différents secteurs d'activité publics et privés sont représentés : banque, assurance, distribution, électronique, audiovisuel, aéronautique, automobile...).

Les « électrochocs démat » !

Jusqu'en 2006, la vague de la dématérialisation prend petit à petit son envol. Cependant, Charles du Boullay met en exergue deux évènements qui ont servi de déclic à la dématérialisation en France. En 2007, Carrefour prend la décision de voir 70% de ses échanges avec les fournisseurs réalisés sous forme numérique, en 2 ans. Puis l'arrivée des smartphones

et tablettes vient enfoncer le clou et accélère le développement de la mobilité. Côté chiffres pour CDC Arkhinéo, c'est 25 millions d'archives en 2008, 1 milliard en 2016, et 2 600 000 en 2019.

En tant que Tiers de Confiance Archiveur, le métier de l'entreprise est la conservation des données, « aussi, nous nous engageons sur l'intégrité de la donnée, la durée de la conservation et la disponibilité de la donnée en ligne jusqu'à sa restitution en fin de contrat ».

« En France, premiers à nous positionner sur ce marché, nous gérons directement avec les Prestataires de services de confiance (opérateurs de dématérialisation de factures, de bulletins de salaires, de process de notes de frais, de contractualisation en ligne...). 85% de notre activité passe au travers de ces prestataires, ce qui nous permet de toucher un panel plus large de clientèle et d'avoir cette position de leader » complète Charles du Boullay.

Longtemps, l'archivage n'a tout simplement pas été la préoccupation des entreprises jusqu'à l'arrivée des premiers litiges aves la restitution des archives numériques.

Archivage & Transformation numérique

Deux manières de percevoir la transformation numérique selon le président de CDC Arkhinéo. Un flux papier peut être substitué par un process numérique (bulletins de salaire par exemple), « on part d'un existant qu'on transforme ». Mais il est possible de créer quelque chose inexistant auparavant (objets connectés & flux numériques), « on part d'un usage nouveau ».

L'archivage se retrouve ainsi en bout de chaîne, « longtemps, l'archivage n'a tout simplement pas été la préoccupation des entreprises jusqu'à l'arrivée des premiers litiges aves la restitution des archives numériques... ». Cette prise de conscience de la conformité et du respect de la réglementation a pris le pas, « de notre côté, nous nous sommes toujours attachés à permettre à nos clients en même temps qu'ils consultent leurs archives de leur fournir les éléments de preuve pour faire valoir leurs droits ».

Au fur et à mesure que les volumes ont augmenté, les entreprises ont voulu savoir si elles étaient conformes à la législation et aujourd'hui, elles se préoccupent réellement de l'archivage, dès le début de leur transformation numérique, « car c'est une obligation de restituer ses données de manière intègre et durable ».

Charles du Boullay

Une solution doublement certifiée !

La solution en mode SaaS de CDC Arkhinéo est notamment certifiée Afnor NF 461 (Z 42013), ISO 27001, agréée par le SIAF et le Ministère de la Santé (qualification d'hébergeur des données de santé) et qualifiée eIDAS (qualification européenne) pour la validation et la préservation des signatures électroniques.

Un petit mot du côté RGPD (Règlement Général de la Protection des Données). « Nous n'avons pas eu de changement majeur puisque le RGPD concerne les données personnelles et le traitement qu'on en fait, or nous n'opérons aucun traitement sur les données confiées par nos clients ».

CDC Arkhinéo est perçu comme un facilitateur par les clients car « nous les obligeons à mettre un durée de conservation associée à une archive ».

Alors sujet juridique ou sujet technique ? Les clients, de manière générale, sont plus attentifs « sur le plan juridique quant aux engagements RGPD, mais le RGPD est avant tout un sujet d'organisation : comment et pourquoi archiver ? Quels documents archiver ? etc... ».

Fin 2020, nous serons arrivés vraisemblablement à 5 milliards d'archives.

> Par Sabine Terrey

Digital : LE DSI À LA TÊTE DES STRATÉGIES DE CHANGEMENT

L'évolution de l'informatique et la transformation numérique bouleversent la dynamique au sein des équipes dirigeantes et font du DSI le responsable de la conduite du changement.

Pour 72% des dirigeants d'entreprise français, la transformation digitale accentue les différences stratégiques entre les services informatique et financier, et accroît la confiance dans le service informatique.

La stratégie

56 % des entreprises qui entament leur transformation digitale adoptent une approche stratégique agile, souple et évolutive. Les leaders technologiques changeront de modèle économique au cours des trois prochaines années, dans une recherche d'équilibre entre le besoin de croissance et la nécessité d'exploiter les systèmes informatiques existants.

L'équipe dirigeante

La transformation digitale renforce la collaboration au sein de l'équipe dirigeante lors du développement de nouveaux produits et services (68%), mais brouille les lignes hiérarchiques.

Les cadres dirigeants ne sont pas toujours en phase avec les priorités de l'activité ou la stratégie technologique. Les DSI et les DAF sont perçus comme ceux qui le sont le moins.

Le pouvoir de persuasion

Les DSI sont investis de la mission de conduire le changement : cette tendance est marquée aux États-Unis où 28 % des dirigeants jugent leur DSI plus efficace. Pour 81% (France), le département informatique a besoin d'être plus influent au sein de l'entreprise pour mener les changements.

Les décisions

Le cloud est crucial, mais les problématiques de gouvernance compliquent l'adoption et la migration : 30 % des dirigeants font confiance à la capacité du service informatique à gouverner le cloud. L'agilité offre les conditions d'une adoption accélérée des technologies nouvelles et de la transformation digitale, mais 16 % ont défini un cadre pour en planifier le succès. La mise en place d'un plan d'investissement clair en matière d'investissement informatique est une priorité dans les trois prochaines années à venir (32% France contre 24%)

Les données

Les données en temps réel confèrent aux directions IT le pouvoir d'évaluer les investissements dans les nouvelles technologies : selon 51 % des dirigeants, les DSI ont une approche plus proactive que les autres dirigeants en matière de responsabilité des données.

> Par Sabine Terrey
Source rapport du cabinet d'étude Focus, commissionné par Apptio - 555 cadres dirigeants d'entreprise de niveau mondial de niveau C et C-1(PDG, DAF, DSI, CDO et COO) dans 12 pays et 9 secteurs

Il y a une différence entre

CONNAÎTRE LE CHEMIN ET ARPENTER LE CHEMIN

Ce récit n'est que le reflet de mon interprétation d'évènements passés, il est donc subjectif.

Il y a un an, j'ai voulu réaliser un de mes deux rêves, travailler chez Microsoft. Tous les signaux semblaient au vert : j'avais une bonne compréhension de l'écosystème de la firme de Redmond, j'étais passionné par une technologie fortement portée par l'éditeur et j'étais reconnu par les internes de la société comme une personne compétente.
Et pourtant, rien ne se passa comme prévu...

"Ils ne savaient pas que c'était impossible, alors ils l'ont fait" a dit Mark Twain

Revenons une vingtaine d'années en arrière : durant mes études, après le Bac, j'ai été orienté, un peu malgré moi, vers une filière électronique. Or, j'étais passionné par l'informatique. Je m'ennuyais à souder, réparer des composants, et mes notes en étaient le reflet.

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

Au bout de 3 mois, j'ai demandé un entretien avec le responsable du département Informatique, et croyez-moi, à l'époque, c'était très mal vu. Cet homme, Mr Andréani, a changé ma vie. Après un entretien de quelques minutes, en me regardant droit dans les yeux, il m'a dit : "Je vois quelque chose en toi, mais je ne sais pas quoi. Je te laisse une chance, mais ne me fait pas regretter mon choix". Parfois, convaincre une personne peut changer votre vie. Par la suite, j'ai suivi ce nouveau cursus avec succès et ai donné des cours d'informatique en tant que professeur vacataire durant 10 ans. Je ne l'ai plus recroisé, mais en écrivant cet article, je l'ai appelé. A 79 ans, très touché, il enseigne encore l'informatique. En contribuant à m'apprendre le métier d'informaticien, ce professeur m'a permis de m'épanouir dans ce domaine.

J'ai toujours osé demander. Et cela a été bien souvent payant, car j'étais le seul. Dans notre société, il me semble que nous n'osons pas provoquer les situations car nous avons trop peur d'être jugés et de faire des erreurs.

Nous sommes d'ailleurs fortement encouragés à ne pas en faire, très tôt, via le processus de notation. Pourtant les erreurs permettent justement d'apprendre...

***"Votre temps est limité, ne le gâchez pas en menant une existence qui n'est pas la vôtre."* Steve Jobs**

Cela fait plus de 15 ans que je considère ne pas travailler, car je vis de ma passion, l'informatique. Et objectivement, je me débrouille plutôt bien. Avez-vous remarqué que les gens passionnés par leur job étaient particulièrement compétents dans celui-ci ?

Soyez curieux, soyez affamés ! Et transmettez. Vous récolterez bien plus que vous ne donnerez.

***"Beaucoup de chemins mènent à la réussite, mais un seul mène immanquablement à l'échec, celui qui consiste à tenter de plaire à tout le monde".* Benjamin Franklin**

Malheureusement, ces initiatives créent un ressentiment auprès de ceux qui n'osent pas. Et justement, dans la dernière société que j'ai traversé, des tensions sont vite apparues avec mon manager, qui a tout fait pour m'isoler et me faire virer, alors que je facturais 3 fois plus que mes homologues. Suite à une réorganisation où j'avais négligé l'aspect "politique", j'ai été placardisé. Sur le moment, j'ai vécu cela comme une injustice, ne comprenant pas comment une société pouvait promouvoir des comportements à la limite de la pathologie, qui desservaient ses propres intérêts. Peu importe l'investissement dont vous faites preuve dans votre travail, si vous ne soignez pas votre réseau, votre évolution sera difficile.

Les gens aiment travailler avec ceux qui leur ressemblent.

J'ai appris, dans la douleur, que le faire savoir était tout aussi important que le savoir-faire. Peu importe vos titres, certifications, publications et conférences, le travail acharné dont vous faites preuve, à la fin, votre réseau comptera aussi.

Soyez curieux, soyez affamés ! Et transmettez. Vous récolterez bien plus que vous ne donnerez.

J'ai fini par démissionner, prenant un risque lié à tout changement : celui que le futur soit moins bien que le présent. Mais avec le recul, ce choix très difficile fut un des meilleurs que j'ai pu faire, car je me suis concentré sur un objectif, mon embauche chez Microsoft. Et je m'en suis donné les moyens.

Revenons de nos jours, au processus de recrutement, difficile, propre à Microsoft : pour postuler à une ouverture de poste précise, il est nécessaire de le faire sur le site https://careers.microsoft.com/us/en. Puis vient le temps des entretiens, en général au nombre de 4. Physiquement et à distance, ce processus peut prendre plusieurs mois. L'un avec la personne en charge du recrutement, l'autre orienté technique, un autre avec votre futur manager, et un dernier avec un manager qui ne travaillera pas avec vous (et qui aura donc un avis plus objectif sur ce que vous pouvez apporter à la société). Tout cela généralement en anglais. J'ai échoué 3 fois. J'ai eu des périodes de doute, refusant d'apprendre de ces multiples échecs, me trouvant des excuses...

Mais un matin, j'ai décidé de plus laisser l'échec me définir, mais de m'en servir comme indicateur des faiblesses à améliorer. J'ai travaillé tous les jours mon anglais, progressé dans différents domaines, parfois éloignés de l'informatique, comme la survie et... j'ai de nouveau postulé, envoyant à la personne en charge du recrutement une dizaine de recommandations de salariés Microsoft.

Ai-je été retenu ? Est-ce vraiment le plus important ? Vous me croiserez sans doute au détour d'une conférence... sur les technologies Microsoft !

Si vous osez demander et accepter qu'une personne change votre vie, si vous acceptez que quelque chose de négatif produise un changement positif et que vos erreurs ne sont que des indicateurs des faiblesses à corriger, alors la réussite sera au bout du chemin...

Leadership :
11 RAISONS D'ÉCHEC DES DIRIGEANTS

Être promu à un poste de manager est la première partie d'un parcours difficile. La deuxième consiste à constituer et à maintenir une équipe efficace. Voici 11 caractéristiques pouvant aboutir à un déraillement de carrière !

L'échec du management est souvent lié à la compétence interpersonnelle (1). Et comme la personnalité est au cœur de la compétence interpersonnelle, les évaluations de la personnalité sont utiles pour identifier les 11 traits de la personnalité qui font échouer les dirigeants.

• Versatile

Ayant beaucoup d'énergie et d'enthousiasme pour de nouveaux projets, ils se désintéressent rapidement lorsque les projets ne se déroulent pas comme envisagé. Avec ce climat de travail instable, les collaborateurs ont peur de les contrarier ou décevoir.

• Sceptique

Le dirigeant reste vigilant dans des situations à risque, mais est finalement incapable de gagner la confiance de qui que ce soit. Les décisions sont prises dans des réunions secrètes et sans discours ouvert.

• Précautionneux

Craignant de commettre une erreur, ils croient que l'on ne peut jamais être certain de quoi que ce soit. Ils hésitent à essayer des nouvelles approches. Les membres de leur équipe les contournent souvent.

• Réservé

Ils croient que le travail se fait mieux lorsque les gens peuvent se concentrer en toute solitude. Ils réduisent au minimum le temps de contact et ont moins de compassion pour les problèmes des autres. Ils sont perçus comme froids, insensibles et peu constructifs.

• Nonchalant

Polis et socialement compétents, ils sont souvent respectés au sein de leur organisation. Face à des obstacles, ils ne sont pas très productifs et réagiront en trouvant des moyens de détourner leurs responsabilités.

• Sûr de soi

Inspirants, courageux et confiants, il est difficile de travailler avec eux car ils refusent d'assumer la responsabilité de leurs erreurs. Ces leaders s'attribuent le mérite des belles réussites et sont incapables de récompenser le travail de leur équipe.

• Malicieux

Ils aiment le frisson et l'excitation et prospèrent dans des situations explosives. Ils sont prêts à prendre des risques et passeront à l'action en période de stress. Ces dirigeants manquent de considération à l'égard des membres de leur équipe.

• Théâtral

Aimant être le centre d'attention, ils s'épanouissent dans les situations de stress Ils apprécient la notoriété et l'attention que ces projets apportent. Les salariés trouvent souvent la collaboration avec ces dirigeants chaotique et erratique.

• Imaginatif

Très créatives, ces personnes participent à des séances de brainstorming, considèrent que les problèmes les plus simples sont complexes et nécessitent des solutions très innovantes. Les collaborateurs les considèrent comme déconcentrés et irréalistes.

• Exigeant

Perfectionnistes, ils délèguent difficilement, et ont tendance à accomplir la plupart des tâches eux-mêmes. Ils ralentissent la productivité et gèrent de trop près leur personnel.

• Dévoué

Manquant d'initiative et d'ingéniosité, ils comptent trop sur les membres de leur équipe, espérant qu'ils mèneront le projet à terme sans avoir à prendre ni de réelles responsabilités ni des décisions risquées.

1)Travaux de recherche de V. Jon Bentz – VP des ressources humaines chez Sears - 1970
Source Hogan Assessments - Le Hogan Development Survey : évaluation de personnalité identifiant les raisons critiques qui aboutissent à un déraillement de carrière.

Ne sous-estimez pas le potentiel de l'Edge Computing !

Pour bénéficier du potentiel de l'Edge Computing, les entreprises doivent changer leur approche de la technologie, opérer des changements structurels et stratégiques, et opter pour des modèles économiques plus dynamiques !

Les technologies d'Edge Computing sont conçues pour traiter et analyser les données des utilisateurs à l'endroit où ils se connectent au réseau. Elles transforment l'expérience clients et employés, et produisent des modèles économiques bien plus réactifs et personnalisés. L'Edge Computing crée de nouveaux débouchés commerciaux permettant aux entreprises d'utiliser les données pour mieux comprendre les clients (par exemple, les détaillants proposeront des vêtements sur mesure, ajustés à un hologramme en 3D...)

La personnalisation de masse

D'ici 2025, un tiers des entreprises vont créer des personnalisations de masse reposant sur l'Edge Computing et 30 % des entreprises se serviront de l'Edge Computing au cours des cinq prochaines années pour créer des « personnalisations de masse » (67%).

Parmi les avantages, retenons :

- L'adaptation des produits, services et tarifs au marché local – 52%
- Une meilleure vision en temps réel du marché – 50%
- Une satisfaction accrue des clients et des utilisateurs – 48%
- Des innovations plus rapides de produits et de services – 47%

3 actions à mener !

Résumons les axes amélioration pour saisir les opportunités...

- Une évolution de l'état d'esprit

Ce changement est nécessaire pour intégrer le concept des stratégies Edge : acceptation de l'autonomie décisionnelle des périphériques Edge, soutien et encadrement de la direction pour des expériences plus intelligentes, et volonté d'expérimenter des modèles économiques et de conception de solutions adaptés aux applications Edge

- Une définition précise des avantages pour les clients

50 % veulent une définition plus claire, une allocation appropriée des investissements, une formation à l'identification et à la spécification des applications Edge potentielles (45 %)

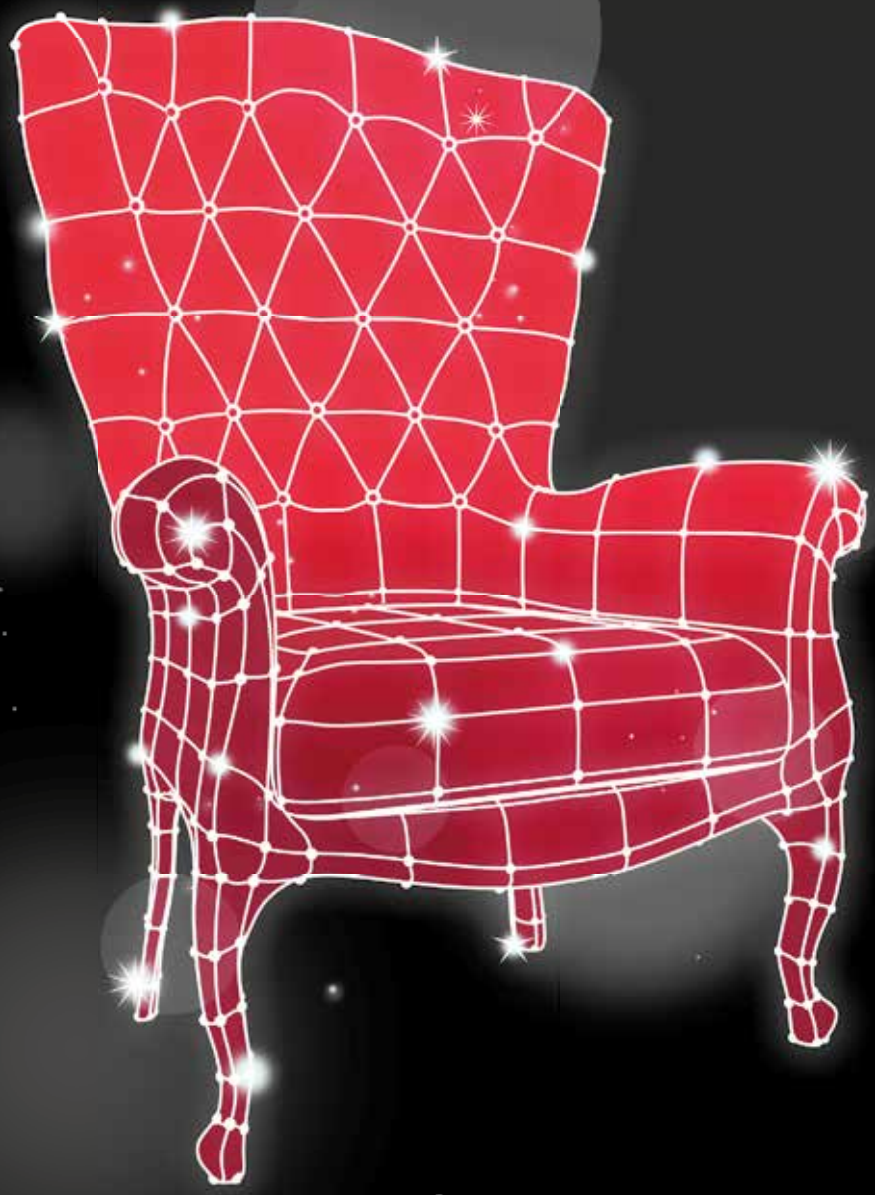
- Une réponse aux préoccupations cybersécurité

Il faut relever les défis liés à la sécurité des réseaux (périphériques connectés) et notamment la création de points d'exposition aux risques sur le réseau (82 %), l'absence de certitude quant à la compromission ou non d'un périphérique (67 %), le piratage des dispositifs de sécurité vocaux ou biométriques et la sécurité intrinsèque des capteurs et des appareils IoT.

Source Opportunity at the Edge: Change, Challenge, and Transformation on the Path to 2025- Aruba & Fast Future

les assises

de la sécurité et des systèmes d'information



AU CŒUR DE LA COMMUNAUTÉ CYBER

9 › 12 OCTOBRE 2019 MONACO

COMEXPOSIUM

lesassisesdelasecurite.com @Les_Assises #AssisesSI

DG consultants

Databricks
ACCÉLÈRE L'INNOVATION SUR LES DONNÉES

Quel est le rôle des données dans les innovations basées sur l'IA ? Comment concilier data science, data engineering et business ? L'objectif des organisations est bien de gagner en compétitivité, améliorer l'expérience client et réduire les coûts d'automatisation. Entretien avec Nick Peart, VP Marketing EMEA de Databricks.

Qui est Databricks ?

Créée en 2013, Databricks a pour mission d'aider les équipes travaillant sur les données à résoudre les plus grands défis du monde d'aujourd'hui. Ses fondateurs ont fait trois " gros paris " : Cloud, Open Source et Machine Learning.

Cette combinaison a permis à Databricks de fournir à plus de 5 000 entreprises dans le monde une plate-forme unifiée pour accélérer l'innovation axée sur les données dans les domaines du data engineering, de la data science, et de l'analytique.

En 2017, la société a installé son siège social EMEA à Londres, ainsi que son European Development Centre à Amsterdam au service de l'avant-vente, des ventes, des partenaires et des clients. Aujourd'hui, l'équipe EMEA est basée à Londres, Munich, Paris, Amsterdam et Tel Aviv. En 2019, Databricks a annoncé un tour de table de série E qui a porté la valorisation de l'entreprise à 2,75 milliards de dollars.

Les entreprises vont devoir composer avec l'IA désormais, c'est un constat. Qu'en pensez-vous ?

La promesse de l'IA est énorme avec le potentiel d'être à l'origine d'innovations remarquables qui touchent la plupart des organisations de la planète. Elle permet désormais de générer un avantage concurrentiel, d'améliorer l'expérience client et de réduire les coûts grâce à l'automatisation.

90% des organisations investissent dans l'IA, mais très peu y parviennent.

Cependant, malgré son attrait, la plupart des entreprises luttent pour réussir avec l'IA. Une enquête menée par Databricks a montré que 90% des organisations investissent dans l'IA, mais que très peu y parviennent. Leurs problématiques sont

liées aux données et concernent les silos et les ensembles de données incohérents, ainsi que des frictions organisationnelles importantes, telles que le manque de collaboration entre les data scientists et les data engineers.

Les responsables informatiques considèrent l'analytique unifiée comme une solution à ces défis. Ils prennent conscience que l'approche consistant à unifier la data science et la data engineering tout au long du cycle de vie du machine learning permet de surmonter le dilemme de l'IA.

Nick Peart

Un mot sur votre offre ?

Les cofondateurs de Databricks sont les créateurs à l'origine de projets open source populaires autour des données et du machine learning, dont Apache Spark, MLflow et Delta Lake. Ces projets ont un impact direct sur la capacité des organisations internationales à traiter les données à l'échelle, à accéder et à construire des modèles basés des données fiables, et à gérer le cycle de vie de bout en bout du machine learning.

Pour mener ses innovations portées par les communautés open source, Databricks propose un modèle de service cloud managé pour une offre logicielle open source.

La plate-forme Unified Analytics de Databricks permet aux entreprises d'accélérer l'innovation en unifiant les données et les technologies d'IA. Conçu pour les data engineers et les datas scientists, Databricks accélère l'exploration et la préparation d'énormes ensembles de données pour des applications basées sur l'IA les meilleures de leur catégorie, l'entrainement continu et le déploiement de modèles d'IA d'avant-garde basés sur les big data, tout en optimisant la collaboration entre les équipes tout au long du cycle de vie de l'IA.

Les entreprises doivent accélérer l'automatisation des tâches de la data science. Qu'en pensez-vous ?

Les données d'entreprise sont elles-mêmes cloisonnées dans des centaines de systèmes tels que les entrepôts de données, les data lakes, les bases de données et les systèmes de fichiers qui ne sont pas compatibles avec l'IA.

Cela signifie qu'énormément de temps est consacré à combiner les données, les nettoyer et les vérifier, les enrichir et les mettre en valeur pour qu'elles soient prêtes pour le modèle.

La préparation des données pour l'IA est un goulot d'étranglement majeur. Lorsque les données ont atteint le stade des modèles prédictifs, les data scientists découvrent souvent que les résultats ne sont pas assez bons et doivent retourner à la case départ.

Étant donné la nature hautement itérative du développement de l'IA, les entreprises doivent parcourir rapidement le cycle de vie de la préparation des données, d'entraînement des modèles et du déploiement en production.

Lorsque les entreprises unifient et automatisent les tâches des équipes en charge des données, il en résulte des cas d'utilisation basés sur l'IA remarquables, tels que dans la biotechnologie avec qui l'analyse des données génomiques pour la médecine de précision, dans la vente de détail pour améliorer les moteurs de recommandations et la finance pour la détection de fraudes liées aux cartes de crédit.

Lorsqu'elle est bien conçue, l'IA peut avoir un impact considérable sur la façon dont nous vivons notre vie quotidienne. Aujourd'hui, les entreprises qui unifient les équipes travaillant sur les données font la différence.

Aujourd'hui, les entreprises qui unifient les équipes travaillant sur les données font la différence.

> Par Sabine Terrey

Migration Office 365 : QUELLE STRATÉGIE DE COMMUNICATION ADOPTER ?

La mise en place d'une solution Office 365, outre les aspects techniques et les problématiques de gouvernance qu'elle soulève, devrait en toute légitimité déboucher sur une stratégie de communication adaptée.

Comment présenter les nouveaux services aux utilisateurs, comment communiquer sur les usages et sur les risques de sécurité liés aux solutions Cloud ? Le volet communication dans le cadre d'un projet Office 365 est une des composantes majeures de la bonne mise en œuvre de votre projet, à ne surtout pas négliger donc !

La stratégie de déploiement des services...

L'ouverture des services Office 365 peut, selon l'environnement source, constituer une révolution pour les utilisateurs. L'apport fonctionnel des différentes applications présentes dans la suite Office 365 est très important et se recoupe parfois entre applications. Une ouverture de ces services sans communication et sans accompagnement risque d'être mal perçue par les utilisateurs et les métiers. Devant le nombre important de services proposés, dont l'usage aurait été mal cadré, les utilisateurs risquent bien de s'y perdre. La première étape est donc de définir la stratégie de déploiement des services qui va préciser l'agenda de l'ouverture des applications et plus précisément, à l'intérieur de chaque service, les fonctionnalités retenues en regard des fonctionnalités désactivées. Un exemple parmi tant d'autres consisterait à déployer les services Exchange Online (sans la fonctionnalité de boîtes aux lettres d'archive), couplés au déploiement du client Teams, mais uniquement avec la messagerie instantanée dans un premier temps.

Dans la réalité, peu de sociétés décident d'ouvrir l'ensemble les services. La plupart d'entre elles activent progressivement les briques applicatives en appliquant des limites qu'elles jugent adaptées à leur contexte. Est-il bien nécessaire par exemple de laisser la possibilité à vos utilisateurs de pouvoir s'envoyer des messages électroniques de 150 Mo alors que ces derniers n'ont que très peu de chances d'être reçus sur Internet et que OneDrive existe ? Le choix de paramétrage des applications Office 365 aura des impacts importants sur ce que pourront ou ne pourront pas faire les utilisateurs. Ces choix de paramétrage, d'activation voire de restrictions, temporaires ou

définitives, doivent donc être consignés dans un document de Description des Services, et doit guider les étapes de votre communication. Il vous évitera, par exemple, d'annoncer aux usagers des fonctionnalités certes natives aux produits mais désactivées par les administrateurs.

La prise en compte de la stratégie de déploiement des services (SDS) est, vous l'aurez compris, indispensable pour bâtir une stratégie de communication des services 0365 (SCS) adaptée. Cette stratégie de déploiement des services sera influencée par un certain nombre de contraintes techniques ou même légales mais également par des décisions portant sur les fonctions que l'on souhaite activer ou restreindre en fonction des métiers. Ces décisions et contraintes, comme la « capacité à réaliser » de vos équipes ou l'usage des liens de communication vers 0ffice 365 par exemple, peuvent également avoir une influence directe sur l'agenda du projet.

Se posent ensuite les questions éternelles du fond et de la forme :

- Que devez-vous annoncer et comment ?
- Quelle organisation pouvez-vous mettre en place pour permettre une adoption rapide des nouveaux services ?

Le fond

La première préoccupation « préprojet » que vous devez avoir est de personnaliser ce projet Office 365 en lui donnant un nom. Le terme « Office 365 » est inconnu des utilisateurs et il est fort à parier que cela ne leur évoquera pas grand-chose.
Incarner le projet en le nommant doit amener vos équipes à définir les objectifs du projet et ses apports fonctionnels vis-à-vis de chaque métier de l'entreprise. Pourquoi migrons-nous vers le Cloud ? Quels sont les avantages personnels au quotidien ? Quels bénéfices pour le travail en équipe ? Quels changements concrets dans les usages pour les utilisateurs ?

Le fait d'apporter des réponses à ces questions et de communiquer sur l'objectif de cette mutation permettra non seulement de justifier le choix de l'entreprise mais surtout de faciliter l'adoption des nouveaux usages par chaque utilisateur cible. Et j'ai la naïveté de penser que l'on ne migre pas dans le Cloud par effet de mode mais pour des raisons valables, autres que purement financières. Expliquer ses choix, présenter les avantages et ses conséquences, c'est bien le rôle de toute équipe projet, afin de permettre aux utilisateurs de comprendre et accepter plus facilement les étapes de migrations.

La seconde préoccupation « préprojet » doit être de définir la communication adaptée aux plannings de l'ouverture des différents services. Ces éléments communication préciseront ainsi ce qui va changer radicalement du point de vue utilisateur. La migration vers Office 365 occasionne bien souvent un remplacement des services locaux aux fonctionnalités limitées vers des outils plus modernes, ouverts et accessibles depuis n'importe quel périphérique connecté. Ces nouveaux services sont bien souvent accompagnés d'une nouvelle gouvernance des données, adossée à des politiques d'accès renforcées. Ces informations doivent accompagner votre communication pour une meilleure acceptation du projet.

La phase de tests auprès d'utilisateurs pilotes mettra en lumière un certain nombre de questions, point de départ de la rédaction d'une FAQ.

La tâche la plus ardue reste bien de communiquer justement. Trop de communication tue la communication, ce n'est pas une nouveauté. Je vous invite d'ailleurs à tester la vôtre sur un groupe pilote afin de valider sa pertinence et éventuellement l'ajuster a posteriori avant sa diffusion étendue. Il existe parfois des distorsions importantes entre le sens présumé d'une communication et sa perception par les destinataires. La phase de tests auprès d'utilisateurs pilotes mettra en lumière un certain nombre de questions, point de départ de la rédaction d'une FAQ.

Abordons maintenant le volet sécurité. Migrer vers les applications d'Office 365 inclut nécessairement un volet sécurité important, avec une stratégie propre. L'ouverture des services et les fonctionnalités de mobilité et de synchronisation des données devraient normalement occasionner un renforcement de la sécurité d'accès et des périphériques qu'il vous faudra expliquer avec pédagogie.
L'ouverture de certains services (Teams, Yammer) vers d'éventuels partenaires doit faire partie d'une information assez soutenue auprès de vos utilisateurs afin qu'ils assimilent le nouveau contexte de travail et son ouverture vers le monde extérieur.

Le volet transition enfin. Ouvrir le service n'est pas synonyme de transition vers le service. Ouvrir le service Exchange Online ne signifie pas obligatoirement que vous allez migrer du jour au lendemain, l'ensemble de vos boîtes aux lettres depuis vos infrastructures locales vers les services cloud de Microsoft.
Le projet inclura obligatoirement une période de transformation qui, de facto, va générer un certain inconfort. Passer d'une messagerie Lotus Notes vers Exchange Online en quelques semaines en est un bon exemple.

Pour communiquer, il faut comprendre. Vos équipes de communication devront nécessairement assimiler les différentes phases de coexistence, comprendre les impacts sur les utilisateurs, sur leurs métiers, et surtout les différences de modus operandi entre l'ancien monde et le nouveau. Elles devront expliquer ces différences de façon simple et limpide puis, comme communiquer n'est pas accompagner, elles devront orienter les utilisateurs vers des ressources d'accompagnement au changement que vous aurez prévues pour faciliter l'adoption.

Un « sponsorship » actif et visible est le premier facteur de réussite du changement.

La forme

La forme la plus traditionnelle reste l'envoi de messages électroniques mais il est temps d'arrêter de considérer qu'une simple diffusion de messages revient à informer suffisamment les utilisateurs. L'efficacité de ce mode de communication est à l'évidence limitée devant la quantité de messages que nous recevons tous chaque jour.
L'envoi de messages d'information sur le projet Office 365 reste donc nécessaire mais s'avère incontestablement insuffisant. La plupart du temps, on aura recours aux canaux d'information traditionnels de l'entreprise comme la newsletter ou l'Intranet, pouvant supporter de courtes vidéos d'information. Les formats les plus courts sont bien sûr à privilégier.

Plus innovant, un chatbot, des campagnes d'affichage dans les divers locaux de l'entreprise, la tenue d'un stand d'informations aux emplacements stratégiques comme par exemple le restaurant d'entreprise ou encore la tenue des plusieurs journées projets dédiées à l'information. La réalisation d'un portail spécifique au projet où les utilisateurs pourront retrouver toutes les informations utiles comme l'agenda, les Faq, ou des liens vers des ressources de formations. La tenue d'une ou plusieurs sessions de lancement officiel du projet, expliquant dans les grandes lignes les enjeux de la transformation, les risques de ne pas évoluer et toute communication qui favorisera l'appropriation des changements par chaque utilisateur.

Cette campagne d'information devrait être sous la responsabilité d'un sponsor identifié. C'est ce dernier qui portera la communication du projet. Un « sponsorship » actif et visible est le premier facteur de réussite du changement.
Les possibilités sont donc multiples et dépendront de l'énergie et des ressources dont vous disposerez.

Depuis que nous réalisons des projets d'intégration 0ffice 365 (depuis Microsoft BPOS pour les plus anciens), la communication a pris une part de plus en plus importante dans ces transformations. Et c'est bien la richesse fonctionnelle de l'offre 0ffice 365 acquise au fil des années qui explique cette évolution. D'une simple migration Exchange vers le nuage Microsoft, nous sommes passés au déploiement de plusieurs centaines de fonctionnalités complémentaires pour les utilisateurs désormais.

D'un simple projet technique, nous sommes passés pour certains clients à une révolution des usages. Plus que jamais, vos équipes projets auront ainsi besoin d'informer via des canaux de communication efficaces aux contenus ciblés sur vos différentes populations d'utilisateur. La personnalisation est ici une des **clés du succès**.

> Laurent Teruin
https://unifiedit.wordpress.com/
Remerciement à Cecile Coste pour ses conseils rédactionnels

« 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.

Cybersécurité & intelligence connectée : GARDER UNE VISION 360 DU SYSTÈME D'INFORMATION

Gérer l'explosion des données est un défi quotidien pour toutes les entreprises notamment pour bénéficier de réponses aux requêtes en temps réel. Retour sur les cas d'usage, les bonnes pratiques, l'intelligence connectée et les notions de fiabilité et de performances avec Bahaaldine Azarmi, Responsable Architecture Solutions chez Elastic.

Pourriez-vous revenir sur l'actualité de la société ?

En octobre 2018, Elastic a fait une entrée remarquée à Wall Street en doublant sa valorisation (+94%), soit près de 5 milliards de dollars, à l'issue du premier jour de cotation.

Début juin 2019, Elastic annonce le rachat d'Endgame pour un montant de 234 M$. Ce dernier fait partie des jeunes acteurs combinant protection du poste de travail (EPP) et détection/remédiation (EDR). Dans la foulée, Elastic annonce Elastic SIEM. Ce lancement s'appuie sur la dynamique et le succès que connaît déjà la Suite Elastic dans le monde de l'analyse de la sécurité. Elastic SIEM introduit un nouvel ensemble d'intégrations de données conçu pour la sécurité, ainsi qu'une nouvelle application dédiée dans Kibana, son interface de visualisation. Celle-ci permet aux spécialistes de la sécurité d'examiner et de catégoriser de façon plus rationnelle les workflows de sécurité réseau et de sécurité de l'hôte.

Cybersécurité & intelligence connectée : auriez-vous quelques conseils à partager avec les RSSI et DSI ?

Je sous-entends ici que l'*intelligence connectée* fait référence à l'IoT.

Avec l'arrivée, puis l'adoption massive de l'intelligence connectée, les RSSI voient leur challenge augmenter de façon significative, sachant que sécuriser le SI de l'entreprise est déjà une manœuvre qui s'avère très complexe, un effort continu, et oblige d'imposer en interne une discipline et des règles strictes. Il n'est pas simple de mettre toutes ces politiques en place, surtout lorsque l'on manque de solutions adéquates et encore moins évident lorsque l'on dispose d'outils qui ne permettent pas d'obtenir la visibilité totale sur l'ensemble des évènements qui traversent le SI de l'entreprise.

La tâche parait impossible, lorsqu'on ajoute à tout cela, des sources externes déployées massivement

telles que l'IoT, exposées sur Internet, et générant des Terabytes de données quotidiennement.

Tous les secteurs d'activité sont concernés, les télécoms avec l'avènement des offres d'alarmes connectées, les assurances avec l'arrivée des boîtiers embarqués dans les voitures, l'industrie automobile avec les voitures connectées.

Personne n'est épargné, si bien que de plus en plus de DSI & RSSI ont fait le choix de moderniser leur architecture de sécurité et notamment l'architecture de *threat hunting*. Elle est souvent caractérisée par une solution SIEM (Security Information and Event Management) traditionnelle, qui ne permet pas de gérer des flux de données quantifiés en Terabytes et de donner des réponses en temps réel à des questions critiques telles que : "Où est mon adversaire?".

En s'inscrivant dans cette démarche de transformation, en s'intégrant à des solutions de pointe comme l'EDR (Endpoint Detection & Response) & l'EPP (Endpoint Protection Platform), de TI (Threat Intelligence), d'UEBA (User and Entity Behavior Analytics), Elastic permet d'indexer tous les évènements transitant dans le SI et de les corréler aux données de ces systèmes. Ce qui permet aux équipes de sécurité de garder une vision à 360° du SI et d'être capable de détecter les menaces, de chasser les adversaires et de prendre des mesures adéquates dans un temps très court

Comment ingérer des téraoctets de données et bénéficier de réponses aux requêtes en temps réel ?

Stocker des Téraoctets de données n'est pas vraiment un défi, beaucoup de datastores, de systèmes de fichiers, de bases de données étant capables de le faire. Le plus compliqué est plutôt d'accéder à la donnée une fois stockée, puisque l'accès signifie souvent de requêter les données, de les corréler, et d'obtenir une réponse le plus rapidement possible, de préférence en temps réel. Beaucoup de systèmes offrent une interface de requêtage. Leurs limites sont néanmoins rapidement atteintes lorsqu'il s'agit de rapidité de temps de réponse, ou de quantité requêtable de données.

En matière de cybersécurité, il est important pour certains secteurs comme la finance, de garder les données 6 mois, 1 an, voire plus longtemps. Dans de tels cas, il n'est plus acceptable pour un CSIRT (Computer Security Incident Response Team) d'attendre des heures à chaque requête au cours d'investigations. La réponse d'Elastic pour construire des architectures de ce type, consiste à offrir à ses utilisateurs une solution répondant au besoin de bout en bout à savoir :

- La collecte et la transformation des données avec les solutions Beats et Logstash, accompagnées de fonctionnalités de monitoring et de gouvernance, puisqu'il s'agit en général de déployer plusieurs dizaines de milliers de Beats près des sources.
- Elasticsearch, moteur de recherche et d'analyse, qui par nature est distribué et scalable. Peu importe le volume de données, les clients peuvent augmenter ou réduire la capacité de leurs déploiements, et avoir la promesse d'accéder à leur données en temps réel.
- Kibana, la couche de visualisation d'Elastic mettant à la disposition des analystes les outils d'investigation d'incidents de sécurité, tel qu'Elastic SIEM.

Bahaaldine Azarmi

Selon vous, quelles seraient les bonnes pratiques pour déployer le cas d'usage de détection de menaces ?

Notre recommandation est de centraliser la totalité des données dans une plateforme globale, telle qu'Elastic, pour profiter de tous les bénéfices d'accès temps réel à la donnée, mais notamment des règles de détection d'anomalies, packagées et basées sur des jobs de machine learning, que l'utilisateur peut activer, et même personnaliser.

La réussite de ces projets est de toute évidence basée sur la capacité de l'architecture à détecter une anomalie, mais surtout une fois détectée, d'être en mesure de prendre des actions appropriées. D'où l'importance de cette couche de détection d'anomalie à mettre en place puisqu'elle sera la source des alertes pro-actives permettant aux analystes d'agir et d'appliquer les procédures.

> Par Sabine Terrey

Cyberattaques : 6 méthodes pour protéger les cadres dirigeants

Comment aider les responsables à mieux se protéger des cyberattaques et notamment des attaques d'ingénierie sociale ?

Les équipes de management ayant accès aux informations très sensibles, sont visées par les cybercriminels et bénéficient parfois de règles de sécurité aménagées pour faciliter leur connexion. Voici 6 conseils à suivre pour mieux se prémunir :

- Être très attentif dans la gestion des comptes de réseaux sociaux

Prévoir une stratégie en matière de médias sociaux et une gestion attentive de chaque compte. Les données disponibles sur les plateformes sociales sont utilisées à des fins d'hameçonnage (phishing), pour récupérer des données personnelles ou commerciales. Conseil : mieux vaut partager le moins d'informations personnelles possibles, empêcher l'étiquetage (tagging) d'images et ne pas publier de photos d'ordre privé.

- Éviter de se connecter à des réseaux publics

Les pirates informatiques utilisent les réseaux des gares, aéroports, hôtels, cafés créer de faux points d'accès et accéder aux appareils mobiles d'utilisateurs. Conseil : mieux vaut ne pas utiliser les réseaux publics et ne pas donner d'information sensible par téléphone dans un espace public.

- Sécuriser son réseau domestique

Mettre en place les mêmes mesures de sécurité chez soi que celles appliquées au réseau des entreprises.

- Sensibiliser aux faux appels

Les faux appels reçus de prétendus employés du service d'assistance pour récupérer des informations (mots de passe...) se multiplient : les dangers de l'ingénierie sociale doivent être expliqués à l'ensemble du personnel.

- Restreindre l'ouverture des e-mails

Certaines attaques ciblées imitent les e-mails d'amis ou de collaborateurs : il ne faut en aucun cas ouvrir un fichier ou cliquer sur un lien sans avoir vérifié que sa source a bien été validée.

- Utiliser un gestionnaire de mots de passe

Il est recommandé d'utiliser un gestionnaire de mots de passe : outil qui permet de créer des mots de passe complexes et différents pour chaque identifiant de connexion. De plus, l'espionnage physique reste une méthode très pratiquée : s'assurer, en saisissant un mot de passe, que personne ne se tient à côté ou derrière, en train d'observer.

Source Expertise NTT Security

GRANDE
ÉCOLE DU
NUMÉRIQUE

Ils recrutent des apprenants de la GEN, pourquoi pas vous ?

“Il est toujours le premier arrivé et le dernier parti”

Amaël Le Lan,

Manager de Tony,
Développeur full stack, formé dans l’une des **750 formations labellisées GEN.**

Les apprenants de la GEN tirent leurs forces de leur parcours. Tony, ancien du BTP, est aujourd’hui à la tête d’un projet de pointe chez Expertime.

www.grandeecolenumerique.fr

METSYS

Laissez-vous guider !

Pour en savoir plus, scannez ce QR code

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