N°26 I JUIN 2022

CONDUIRE LA TRANSFORMATION NUMÉRIQUE DE L'ENTREPRISE

SMART DSI®

DOSSIER
L'informatique responsable

INTERVIEW
Trois conseils pour assurer la sécurité des comptes et des données

L'ETUDE A RETENIR
Se réunir moins souvent mais faire plus !

STRATEGIE
Gestion de la surface d'attaque : les nouvelles pratiques autour des méta-connecteurs et des puits de données adaptifs

PERSPECTIVES
Les 7 clés pour réussir sa modernisation et répondre à la pénurie de talents

INTERVIEW
Des tests d'intrusion à 360° grâce à l'IA pour lutter contre les failles de sécurité

CLOUD IN ONE

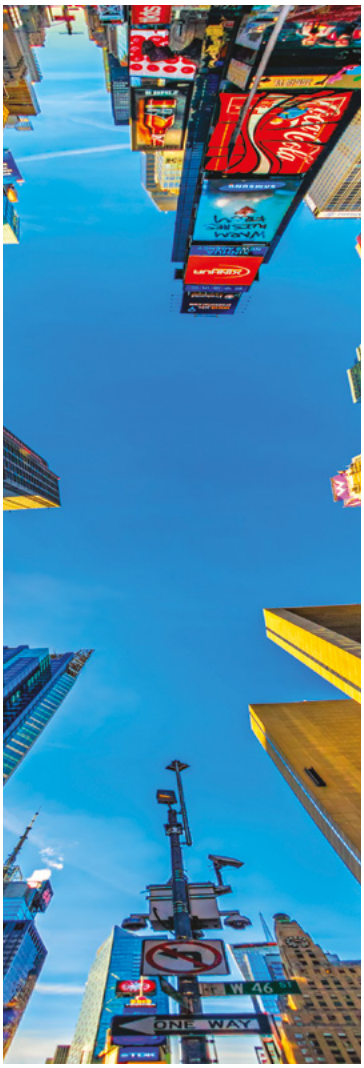
www.cloud-in-one.fr

Accélérez votre transition vers le Cloud avec les experts DIB France

Simples à appréhender, évolutives et sécurisées, les Solutions Cloud In One de DIB France permettent aux Directions IT et Métiers de s'affranchir des contraintes IT pour gagner en réactivité, souplesse et sécurité.

Desktop-as-a-Service • Infrastructure-as-a-Service • Sécurité des données

Testez dès à présent les Solutions Cloud in One de DIB France sur **www.cloud-in-one.fr**



Des défis à la hauteur de la complexité des environnements !

Quelques mots posent d'emblée la situation, « les dirigeants exercent leurs responsabilités dans l'un des environnements les plus complexes qui soient : guerre, inflation, pénurie de talents et crise sanitaire liée à la pandémie de COVID-19 » commente Alex Bauer, Directeur Général, IBM Consulting France.

Face à ce constat et au contexte incertain, les dirigeants entendent mener à bien et avec détermination les nombreux chantiers qui s'ouvrent devant eux. Il en est un pour lequel ils ne lâchent rien, le développement durable, perçu comme un impératif commercial et moteur de croissance, et qui fait désormais partie de leur Top 3 derrière la réglementation et le cyber-risque. Ainsi, 73 % reconnaissent qu'ils doivent assumer la responsabilité de l'impact des activités de leur entreprise sur l'environnement(1), même s'ils identifient aussi des obstacles technologiques à la mise en œuvre du développement durable dans leur organisation.

Autre chantier et non des moindres, la pénurie des talents, notamment dans la cybersécurité. En effet, 8 entreprises sur 10 auraient subi au moins un incident attribué à un déficit de compétences ou de sensibilisation(2). En ce sens, le sujet est fondamental parmi les dirigeants car les conseils d'administration se focalisent spécifiquement sur la cybersécurité et 76 % recommandent précisément d'étoffer les effectifs en informatique et en cybersécurité.

Enfin, pour compléter le futur de la cybersécurité, on ne peut passer sous silence la crainte des cyberattaques au cœur des tensions géopolitiques, avec notamment 59% des PME-ETI qui pressentent une recrudescence des cybermenaces, ce qui oblige la quasi-totalité des entreprises à réfléchir à l'origine de leurs solutions informatiques(3). De plus, si la guerre en Ukraine révèle la nécessité d'avoir un meilleur équilibre entre les solutions de cybersécurité étrangères et les solutions nationales, cet électrochoc pousse in fine les équipes à durcir ou transformer leurs dispositifs de sécurité.

Ainsi, entre responsabilité et attentes, entre tendances et défis, entre opportunités et engagement, les organisations redessinent et affinent leurs réflexions, ambitions stratégiques et vision de l'avenir.

Bonne lecture !

Sabine Terrey
Directrice de la Rédaction
sterrey@itpro.fr

(1) Source IBM - « CEO Study » Own your impact: Practical pathways to transformational sustainability

(2) Source Fortinet – 2022 Cybersecurity Skills Gap

(3) Source CESIN & Opinionway – Rapport Guerre en Ukraine

SMARTDSI

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

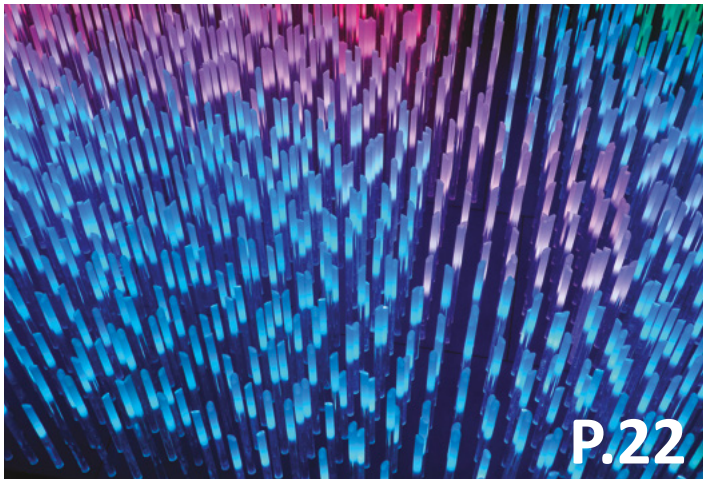
« SMARTDSI est la 1ère revue d'informatique professionnelle trimestrielle dédiée aux décideurs informatiques, aux décideurs métiers et aux professionnels des nouvelles technologies de l'information et de la communication (NTIC). La revue SMART DSI, au travers de chroniques, dossiers, études et analyses,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

SMART DSI

N°26 I JUIN 2022

SMART DSI est un revue trimestrielle éditée par IT PROCOM
Directeur de la Publication : Sabine Terrey
Strategy Center - BP 40002 - 78104 St Germain en Laye, France.

N° ISSN : 2494-9701 - N° CPPAP : 0518 T 93059
www.smart-dsi.fr



SMARTDSI

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

Thierry Bollet, Sylvain Cortes, Didier Danse, Gautam Khanna, Sabine Terrey, Laurent Teruin, Théodore-Michel Vrangos.

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

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

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

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

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

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

Site officiel : www.smart-dsi.fr

Le numérique RESPONSABLE

> Par Didier Danse

Avec des chiffres en constante augmentation (+9% en moyenne par an), une émission des gaz à effet de serre d'ores et déjà plus élevée que l'aviation civile et représentant 5% du total des émissions mondiales, l'aspect écologique du numérique est devenu l'affaire de tous. A ces émissions de gaz s'ajoute l'utilisation de ressources naturelles dont l'extraction augmente l'impact tant en termes énergétiques, écologiques mais aussi sociaux. Pourtant censé faciliter les actions de chacun, le numérique a également renforcé les écarts sociaux pour les personnes déjà en proie à des difficultés.

Le numérique est un vecteur de transformation pour des générations futures et bien qu'il n'y ait actuellement aucune contrainte légale – notamment dû au fait que la mesure de la situation initiale et du progrès est compliquée - la réappropriation du numérique est en marche et tous les acteurs ont leur rôle dans cette démarche, quel que soit leur positionnement sur la chaine de valeur.

Les entreprises disposent désormais d'une « licence sociale » bien plus puissante que l'ensemble des licences administratives puisque les consommateurs peuvent aisément se détourner des produits ou se rendre à la concurrence.

Qu'est-ce que le numérique responsable ?

Le numérique responsable est un terme que l'on entend régulièrement ces dernières années, notamment depuis l'apparition du Cloud grand public et l'augmentation de la visibilité d'acteurs du marché tels que Netflix ou Amazon. On retrouve pourtant les fondements du numérique responsable dans les textes initiaux sur le développement durable.

Par le fait qu'on ne parlait du durable que pour les activités dans la forêt Amazonienne, le durable a souvent été confondu avec l'unique écologie malgré

son aspect bien plus large. Pourtant, le durable visait déjà à atteindre la rentabilité financière tout en favorisant la réduction des inégalités sociales et de la pression sur l'environnement. Ainsi le durable cherche à réduire l'impact, au sens le plus large, de l'exploitation. Par la suite, la notion de durable s'est vue étendue pour devenir la responsabilité sociale – ou sociétale - des entreprises qui en est son extension au sein de l'entreprise.

Aujourd'hui, on tend non plus à minimiser l'impact négatif mais à proposer un impact positif en tenant compte des risques écologiques, économiques, humains, sociétaux, politiques et individuels tout autant que les opportunités que le numérique amène. C'est ainsi que l'on parle de *numérique responsable* qui représente « l'ensemble des technologies de l'information et de la communication (TIC) dont l'empreinte économique, écologique, sociale et sociétale a été volontairement réduite (sobriété numérique) et/ou qui aident l'humanité à atteindre les objectifs du développement durable » et qui s'applique sur toute la chaine de valeur.

La notion de durable s'est vue étendue pour devenir la responsabilité sociale – ou sociétale.

On y trouve 3 grandes catégories d'activités ayant des finalités différentes et complémentaires :

1. Respecter l'environnement en proposant un usage raisonné des TIC, que l'on nomme généralement *Green IT*.
2. Faciliter l'optimisation des opérations via des outils numériques, notamment les outils de mesure permettant de mieux comprendre comment fonctionnent certaines activités.
3. Créer des opportunités grâce au numérique. C'est ainsi que l'on parle souvent de *IT for Green* lorsque l'on se penche principalement sur les aspects écologiques mais cette catégorie d'activités numériques permet d'aller plus loin et de faciliter la transition écologique et circulaire au travers d'applications mobiles, éclairage intelligent, ou encore l'Internet of Things avec ses capteurs divers. Ces activités visent également l'amélioration des conditions de travail à toutes les étapes ou encore l'accès à l'ensemble des personnes, y compris les personnes en situation de handicap, ayant une éducation moindre ou encore n'ayant pas accès à la technologie pour des raisons telles que l'âge ou le niveau de richesse.

Il existe de nombreuses initiatives, menées par le public voire le privé comme le *pacte vert pour l'Europe*, ou encore le *Green Deal* à l'horizon 2030 mais aussi IT for Good et Fair IT, visant la neutralité carbone, la résilience et l'inclusivité y compris au sein même de l'entreprise.

L'aspect écologique

LA CONSOMMATION ÉNERGÉTIQUE

La consommation d'énergie provient principalement du CPU, GPU et de la RAM. Evidemment, le temps de marche des appareils s'avère un multiplicateur important dans ce contexte. De même la multiplication du matériel utilisé, notamment due à la parallélisation, influe fortement sur l'énergie consommée. En plus des composants directement utilisés, de nombreux autres composants annexes tels que les écrans et le réseau, sont eux aussi source de consommation d'énergie. Au-delà de l'énergie utilisée directement, il est aussi nécessaire de tenir compte de l'énergie nécessaire pour compenser la création de chaleur par l'ensemble de ces composants.

LES FACTEURS À PRENDRE EN COMPTE

L'efficacité des composants et leur taux d'utilisation sont évidemment primordiaux dans les discussions et dépendent de différents facteurs :

- Le matériel utilisé, tant les ordinateurs que les autres appareils
- La taille des données (volume et quantité)
- La rétention de données
- L'architecture du réseau et des services
- Le type de tâche à accomplir

LA MESURE DE LA CONSOMMATION

De nombreux éléments peuvent être mesurés : les gaz à effet de serre directement émis, ceux émis à cause de l'énergie ou encore les autres émissions indirectes - on parle des scopes 1 à 3 des émissions – mais aussi la consommation énergétique dont la mesure peut se faire en amont de l'utilisation des appareils et présentés au travers de grilles d'efficacité fournies par différents labels tels que l'*afnor, NF environnement, TCO, Eco-Label, Energy Star, FSC, PEFC, PC Green Label* et bien d'autres. Il est également possible de faire des estimations sur base de sa propre utilisation au travers d'outils, parfois en ligne, tels que *ML CO2* Impact ou *Green Algorithms*. Certains vont encore plus loin en mesurant leur consommation en temps réel grâce à des trackers à intégrer dans les applications : *Experiment impact tracker, Carbon tracker, CodeCarbon*.

En tenant compte des éléments ci-dessus, il est alors possible de définir des indicateurs tels que le *Power Usage Effectiveness* en lien avec l'efficacité énergétique du datacenter ou encore le WUE (*Water Usage Effectiveness*) et le CUE (*Carbon Usage Effectiveness*).

Le facteur humain

Bien que ce paragraphe soit assez court, l'humain, dans l'entreprise et dans la société, est un facteur important à prendre en compte dans une démarche responsable. L'humain, c'est-à-dire nous, doit être au centre des préoccupations afin de promouvoir la santé et le bien-être.

Être responsable démarre en permettant aux employés de travailler avec des technologies récentes, d'accéder aux formations auxquelles ils ont droit ou encore de respecter leurs conditions de travail.

Les finances

Malgré sa mauvaise image liée aux abus, le profit financier a du bon. C'est celui-ci qui permet de financer la recherche et le développement mais aussi la formation ou encore l'accompagnement des employés à diverses étapes de leur vie. C'est également sur cette base que des entreprises sont en mesure de proposer, de manière volontaire, des jours de congé supplémentaires. Enfin, l'impôt issu du profit sert quant à lui à financer les infrastructures nécessaires au bon fonctionnement des transports, tant de personnes que des biens. Ce même impôt sert de plus à financer l'éducation des plus jeunes, les pensions et autres.

Payer ses impôts là où l'activité se passe est une manière concrète de financer les projets locaux et ainsi d'avoir un impact positif sur la société.

La technologie responsable

LES BLOCKCHAINS

Les blockchains sont des technologies combinant du stockage et de la transmission d'informations afin de former des registres répliqués et distribués, sans organe central de contrôle et sécurisés grâce à la cryptographie, et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers grâce à un consensus partagé entre tous, rendant la falsification complexe.

Le consensus est le mécanisme permettant de valider qu'un nœud est fiable et il existe de nombreux protocoles de consensus. Ces protocoles sont la source principale de consommation d'énergie bien que la réplication au travers des réseaux pairs à pairs multiplie d'autant les ressources nécessaires pour le stockage et le transfert des données et que le chiffrement des données a une part importante dans l'équation. Le niveau de difficulté pour l'encryption est un facteur déterminant dans la consommation d'énergie. Certaines blockchains publiques consomment 4 à 6 fois moins que le Bitcoin et d'autres blockchains sont très peu énergivores en comparaison avec les enjeux.

Le choix du protocole dépend ainsi du modèle de rémunération pour les participants. Bitcoin favorise la compétition et la création de nouveaux Bitcoins nécessitant un processus de minage important qui requiert la consommation électrique équivalente à la Belgique pour y parvenir. Les prévisions montrent également une augmentation inquiétante de 200 à 300%, tout cela sans compter la consommation liée à la construction des machines. De manière générale, les blockchains publiques nécessitent clairement bien plus de sécurité et requièrent un grand nombre de participants au réseau alors que les blockchains de consortium ou privées sont bien moins énergivores.

L'INTELLIGENCE ARTIFICIELLE

L'intelligence artificielle fait peur à certains et pourtant elle est partout : la reconnaissance vocale, les véhicules autonomes, l'aide à la rédaction et la lecture de textes afin de générer de la connaissance ou encore l'aide à la décision. L'intelligence artificielle a d'ailleurs fortement été utilisée durant la période Covid notamment pour simuler l'évolution de la pandémie mais aussi pour agréger l'ensemble de la littérature en quelque chose de digeste. Elle a aussi permis l'accélération de la préparation des vaccins.

L'intelligence artificielle repose principalement sur une approche statistique et pour cela, il est nécessaire de collecter de l'information. L'apprentissage, tel qu'on le nomme, requiert de l'acquisition permanente d'informations nécessitant une grande taille de données, en transit ou stockées, mais aussi des ressources matérielles importantes notamment dans le cas du *Deep Learning*.

Mais au-delà de l'aspect énergétique, la manière d'exploiter les technologies peut influer sur le développement humain. On distingue en général deux types d'IA : l'IA forte – souvent appelée *générale* (IAG) – et l'IA faible, c'est à dire avec un périmètre défini tel que la traduction automatique ou la lecture de plaques d'immatriculation.

L'IAG, qui ne sont jamais que des algorithmes, n'a ni émotion, conscience ou encore intention et peut ne pas tenir compte de facteurs importants dans les résultats générés. Par ailleurs, il est important de former et contrôler l'IA efficacement afin d'éviter des biais cognitifs, mais aussi des détournements des technologies – tels que le *deep fake* - et des utilisations par l'humain et qui vont contre d'autres humains.

Notons l'exemple de la Chine qui exploite la reconnaissance faciale et la collecte officielle et massive d'informations dans le but de mettre en place le crédit social, limitant fortement la liberté des personnes qui postent des articles contre le gouvernement notamment.

INTERNET OF THINGS

L'Internet of Things, c'est cet ensemble de capteurs et d'appareils connectés ensemble pour interagir à des évènements donnés. C'est ainsi que la détection de l'augmentation de la température en temps réel permet d'effectuer des ajustements de différentes manières, selon le contexte, tant dans le privé que l'industriel.

Bien que les protocoles en place et les technologies permettent une réduction importante de la consommation énergétique, il n'en demeure pas moins que la multiplication des appareils peut avoir un impact important. L'architecture des services et l'utilisation du *Edge computing*, permettant de traiter de l'information au plus proche des appareils sans les envoyer dans le Cloud, diminue la quantité d'informations en transit.

Evidemment, les capteurs doivent être réglés pour ne se déclencher qu'en cas de besoin. Toujours dans le même contexte, il est important de s'assurer du bienfondé de l'utilisation des technologies afin qu'elles soient utiles à l'humain et non uniquement à l'aspect financier.

L'Internet of Things, c'est cet ensemble de capteurs et d'appareils connectés ensemble pour interagir à des évènements donnés.

Les premiers pas dans l'informatique responsable

Bien qu'il existe de nombreuses solutions, nous ne pouvons toutes les aborder dans un seul article. Voyons dès lors les plus directes.

REVOIR L'UTILISATION

Le plus efficace est d'éviter la consommation de biens et services. Evidemment, cela est plus facile à dire qu'à faire. Mais de manière générale et dans la mesure du possible,

- Privilégiez le Wi-Fi aux technologies 4G, 3x plus consommatrices du point de vue énergétique
- Evitez la 5G pour des services qui ne requièrent pas d'être « en temps réel »
- Lorsque cela est envisageable, téléchargez en amont au lieu d'exploiter le streaming, qu'il soit audio ou vidéo
- Adaptez la qualité en adéquation avec l'usage. De nombreuses vidéos ne requièrent aucunement la HD, comme les vidéos YouTube dans le but d'écouter la musique
- N'envoyez des courriels qu'à ceux qui en ont besoin, évitez les mails tels que « Merci » qui sont envoyés à de nombreuses personnes et ce avec l'historique de la conversation

- Utilisez des appareils moins consommateurs (attention que le remplacement des anciens par des neufs est parfois plus « coûteux » que l'exploitation d'une technologie existante). Dans tous les cas, dès que possible, envisagez la mise en veille ou coupez le courant automatiquement
- Utilisez de l'énergie renouvelable (photovoltaïque « local »)
- Mutualisez et louez
- Utilisez des nouvelles approches de travail pour diminuer globalement l'impact
- Rassemblez dans un endroit unique un certain nombre d'appareils ou externalisez la gestion de ces appareils, idéalement dans un centre de données efficace
- Enfin, revoyez les approches de travail permettant la réduction du transport, l'utilisation de lumière non utile dans les bâtiments.

L'ensemble de ces actions permettent évidemment de réduire l'impact énergétique mais elles ont également des impacts positifs sur les personnes et les finances.

ADOPTER DES CYCLES DE VIE ET DES ARCHITECTURES DE SOLUTIONS TENANT COMPTE DE L'EFFICIENCE

Pour pouvoir faire évoluer sa propre consommation énergétique mais aussi pour comprendre le milieu dans lequel un système fonctionne, il est important d'analyser et de comprendre son propre environnement, y compris le facteur humain.

Concrètement, le logiciel a un impact important du fait de son architecture et est bien souvent le moteur de l'obsolescence du matériel comme l'incompatibilité de Windows 11 avec de nombreuses machines. Pour autant que ces incompatibilités soient maitrisées et que l'architecture respecte les éléments fondateurs, la modernité des applications propose de nombreux avantages : la capacité d'utiliser plus efficacement les composants en fonction des besoins logiciels, qui peuvent varier dans le temps. Dans tous les cas, l'objectif sera d'augmenter le taux d'occupation et d'utilisation pour éviter les serveurs dormants, puisque l'énergie consommée lors de la production n'est jamais exploitée. A l'inverse, lorsque l'application requiert 100% d'utilisation, le serveur « à l'ancienne », mais dans un environnement maitrisé, est alors plus efficace.

Au niveau logiciel, l'architecture doit garantir de minimiser les transferts et le stockage d'information au strict minimum tandis que la qualité du code est primordiale pour réduire l'empreinte énergétique. De plus, le cycle de vie des services et des appareils doit permettre la réutilisation interne ou externe voire le recyclage des appareils.

Du point de vue de l'humain, l'utilisation d'architectures et de technologies modernes permet de maintenir ses concepteurs à jour, en phase avec un marché en permanente évolution.

OPTIMISER LES FINANCES

L'argent en transit doit être utilisé à bon escient. Ainsi payer pour des services ou des technologies non exploitées entièrement est source de réduction du bénéfice financier. Dans un précédent article, nous avons abordé comme axe d'optimisation la gestion de portefeuilles pour créer de la valeur, dont de la valeur financière. La réutilisation d'appareils déjà utilisés – provenant tant de l'interne que de l'externe – est également une manière de réduire les coûts. De la même manière, il existe des plateformes de revente de licences – c'est bel et bien légal – tels que *SoftCorner*.

Il est bon d'inclure les risques fournisseurs dans la gestion des risques.

PROCÉDER À DES ACHATS RESPONSABLES

L'entreprise commanditaire est partie prenante des agissements de ses fournisseurs et partage donc la responsabilité. La coresponsabilité client/fournisseur requiert de revoir les critères de sélection et y inclure la notion de durabilité. En plus des attentes par rapport aux fournisseurs, il s'agit de réduire la pression financière sur ceux-ci, cette pression pouvant en effet mener à une baisse de qualité, la perte de compétences rares ou encore simplement la faillite.

De plus, l'appel à des ressources partagées s'avère efficace économiquement et en termes d'efficacité. Il en va de même pour l'externalisation qui permet de réduire les risques techniques et environnementaux. La responsabilité étant partagée, il est important de s'assurer de l'impact des prestations externalisées pour l'entreprise mais aussi de la rentabilité des projets pour les différents acteurs.

Pour évaluer l'impact de l'externalisation, il peut être intéressant d'intégrer le personnel dans les décisions pour assurer la pérennité sociale et a minima refuser les pratiques non éthiques tout autant que de suivre l'exécution au travers d'indicateurs sur les aspects sociaux, économiques et environnementaux. De manière générale, il est bon d'inclure les risques fournisseurs dans la gestion des risques.

Enfin, il peut être utile de clarifier les indicateurs clés, transparents et lisibles afin d'évaluer les services numériques et vérifier leur adéquation avec les réels besoins tout en étudiant le bilan carbone de ces mêmes fournisseurs.

Didier Danse - IT Manager | IT Architect | Agilist

Accompagner la transformation digitale avec One Call, Cloud Care et les Services Managés

Découvrez comment les offres de support, d'accompagnement et de services managés d'Insight vous guident sur la route de l'agilité, la sécurité et la résilience de vos environnements Cloud.

Pour en savoir plus et contacter nos experts, rendez-vous sur : **fr.insight.com**

+33 (0)1 30 67 25 00 | info.fr@insight.com
https://fr.insight.com

Special Report

METSYS

Microsoft

Metsys invite les entreprises à découvrir et adopter une sécurité moderne « Zero Trust »

Une démarche Zero Trust ne s'improvise pas. Elle se construit en adoptant une nouvelle culture de la sécurité et une multitude de briques de sécurité. C'est ce que Metsys a expliqué et démontré par la pratique un peu partout en France d'ateliers gratuits dédiés aux approches modernes de la cybersécurité et de la cyber-résilience des entreprises, au sein des Microsoft Labs.

L'approche Zero Trust, cette sécurité « sans confiance » au cœur des discussions actuelles sur la cybersécurité, ne se construit pas en un jour. Cette façon d'aborder la sécurité numérique des entreprises se construit progressivement, brique par brique, et présuppose la maîtrise d'un certain nombre de principes qui lui servent de fondation.

Comme le rappelle l'ANSSI dans son rapport sur « le modèle Zero Trust », « *cette approche demeure ardue, faute de maturité* ». D'autant qu'elle va exactement à l'inverse du principe de « *confiance implicite* » qui rythmait le modèle ancestral de défense périmétrique auquel trop d'entreprises restent encore attachées, alors qu'il n'a plus aucun sens dans un monde de travail hybride avec des collaborateurs travaillant à domicile et des données délocalisées dans le Cloud.

Le Zero Trust n'est pas une technologie. C'est un concept qui consiste à réduire la confiance accordée aux utilisateurs, aux administrateurs et aux appareils qu'ils utilisent en focalisant les efforts de sécurité sur les identités, le réseau, les accès, les applications, les données avec des contrôles permanents, granulaires et dynamiques.

Afin d'aider les entreprises à progresser sur le chemin du « Zero Trust », Metsys a animé avec Microsoft, des « Labs » dédiés à la cybersécurité moderne (format présentiel et en ligne, et disponibles également en replay). Au cours de ces « Labs 100% Cybersécurité », les interlocuteurs sont revenus sur les piliers d'une sécurité Zero Trust et sur les démarches et outils proposés par Microsoft pour adopter une posture « Zero Trust » complète, globale et pérenne.

Connaître son niveau de maturité

La démarche prônée par Metsys et Microsoft démarre par une compréhension du niveau de la maturité Cyber de chaque entreprise. « *Zero Trust is a journey* » (le Zero Trust est un voyage) » rappelle **Paul Dominjon**, directeur des solutions Cybersécurité chez Microsoft. « *Comme dans toute démarche, il est important de savoir d'où on part pour savoir quelles sont les étapes à suivre dans cette trajectoire qui vous mènera au Zero Trust. Applications des basiques de l'ANSSI, utilisation systématique du MFA, taux d'usage des applications cloud… Il est essentiel d'évaluer le niveau de maturité en matière de cybersécurité* ».

Microsoft a ainsi élaboré un questionnaire de maturité Zero Trust qui permet d'évaluer le degré d'avancement d'une entreprise sur la sécurisation des 6 piliers de la cybersécurité Zero Trust : les identités, le réseau, les accès, les applications, les données et l'infrastructure élargie au cloud.

Celui-ci en main, chaque entreprise peut mesurer les efforts à faire pour progresser sur ces 6 piliers avant d'adopter une posture « Zero Trust » à proprement parler. Des efforts qui doivent s'accompagner d'un changement de culture.

Un changement de culture…

Zero Trust est un changement de modèle de sécurité pour s'adapter aux menaces actuelles et répondre aux nouveaux besoins d'ouverture. « *C'est un changement d'état d'esprit* » explique **Paul Dominjon**. « *Le passage en travail à distance imposé par la crise pandémique a fait exploser les dernières velléités de concevoir le SI comme un château fort* ».

Les confinements successifs et l'adoption du travail hybride qui en découle aujourd'hui ont encouragé bien des entreprises à réfléchir sur la notion de confiance, « à qui » elles pouvaient faire confiance et, au final, à prendre conscience qu'il est plus simple et plus logique de choisir par défaut de ne faire confiance à personne.

Par ailleurs, avec des besoins intensifiés par la crise de prendre le contrôle à distance des infrastructures privées mais également les besoins engendrés par une adoption massive des infrastructures dans le Cloud (IaaS), « *les entreprises ont cherché des moyens de mieux contrôler l'attribution des privilèges et de gérer avec une attention accrue les comptes administrateurs en s'assurant que les privilèges nécessaires à ces accès soient fréquemment remis à jour* » ajoute **Paul Dominjon**.

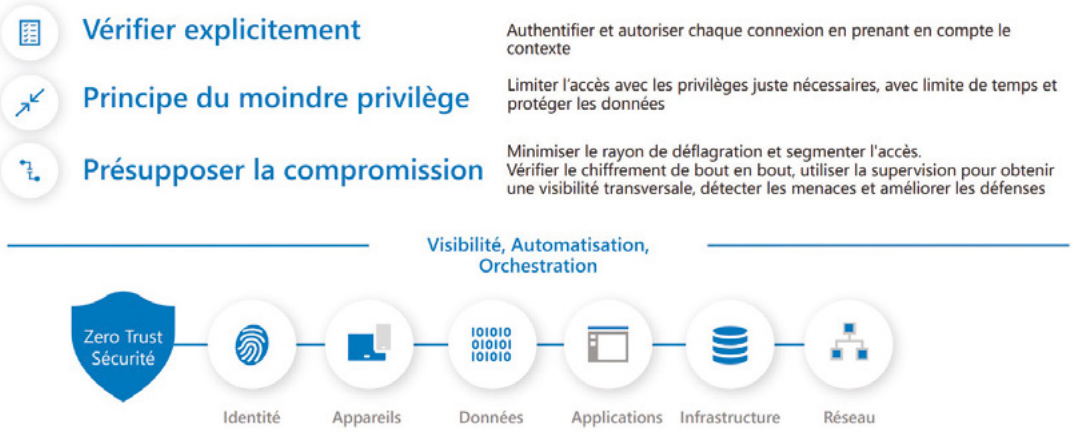
Enfin, la démarche Zero Trust est aussi marquée par un autre changement de mentalité fondamental comme l'explique **Hervé Thibault**, Chief Strategy Officer de Metsys : « *il est essentiel de présupposer que l'on est attaqué. Cela impose de savoir se projeter, de faire de la détection & réponse, et d'agir comme si le réseau était compromis* ».

… Qui nécessite un accompagnement

« *Face à un tel changement d'état d'esprit, qui demande à être expliqué, vulgarisé, assimilé, les entreprises ont besoin d'un accompagnement* » constate **Hervé Thilbault**. « *Et bien évidemment une telle approche a aussi un impact sur les outils et technologies à mettre en œuvre* ».

Microsoft propose ainsi de multiples briques permettant de couvrir l'ensemble des piliers d'une architecture Zero Trust. Ils permettent une approche progressive, éclairée par la compétence des experts cybersécurité de Metsys. « *Faire de Microsoft une fondation de sa sécurité peut encore surprendre certains responsables informatiques* » note **Hervé Thibault**. Pourtant, la division cybersécurité de l'éditeur comporte plus de 8.500 experts et réalise un chiffre d'affaires de 15 milliards de dollars, ce qui fait aujourd'hui de Microsoft l'un des tous premiers acteurs du marché de la cybersécurité.

Zero Trust est un changement de modèle de sécurité pour s'adapter aux menaces actuelles et répondre aux nouveaux besoins d'ouverture.



L'approche Zero Trust repose sur 3 principes fondamentaux et 6 piliers sur lesquels se focalisent les efforts

Construit au fil du temps, ce portfolio de solutions est l'un des plus complets et des plus matures du marché. « *Aujourd'hui, les entreprises ne s'interrogent plus sur la performance des outils ou la pertinence de Microsoft en matière de sécurité. Nous sommes désormais bien plus interrogés sur l'articulation des multiples solutions qui forment la plateforme Microsoft* » confirme ainsi **Laurent Cayatte**, Président de Metsys.

Une offre qui couvre l'intégralité des besoins

L'offre Microsoft couvre aujourd'hui les 6 piliers de la sécurité Zero Trust :

* **L'identité** avec des concepts comme le MFA, le passwordless, l'accès conditionnel, la gestion dynamique des comptes à privilèges tous pris en charge par Azure AD et renforcé par son bouclier « Microsoft Defender for Identity ».
* **Le réseau** avec cette idée qu'Internet devient le réseau de l'entreprise et qu'il faut diminuer la surface d'attaque en pratiquant une segmentation (avec Azure Networking) et en s'appuyant sur Azure Firewall, Azure WAF, Azure Security, Microsoft Sentinel et Microsoft Defender XDR.
* **Les appareils et points d'accès** avec notamment la mise en œuvre de l'accès conditionnel Azure AD, mais aussi la sécurité des appareils avec Microsoft Defender for Endpoint et Microsoft Endpoint Manager mais aussi Microsoft Defender for IoT afin de protéger les appareils dans toute leur diversité.
* **Les applications** avec la solution CASB et Microsoft Defender for Cloud Apps,
* **Les données** avec une surveillance accrue des accès mais aussi le chiffrement et le classement automatique via Microsoft Information Protection.
* **L'infrastructure élargie au Cloud** avec Azure Security et Microsoft Defender for Cloud qui s'étend au-delà du Cloud Microsoft dans une véritable approche multicloud.

> Une telle démarche réclame un accompagnement de proximité avec des experts dotés d'une véritable expérience de terrain

Progresser sur ces piliers et assembler ce puzzle en un tout cohérent à même de soutenir une démarche Zero Trust est devenu une priorité pour bien des entreprises.

« *Ce qu'on a voulu montrer au travers des 4 ateliers, c'est toute la pertinence de l'approche Microsoft et la complétude de l'offre,* explique ainsi **Laurent Cayatte**, *mais aussi l'importance pour l'entreprise de se faire accompagner face à ce qui peut sembler un énorme défi à relever.* »

Special Report

En route vers le Zero Trust

Pour les DSI, les RSSI, les responsables d'entreprises, l'approche Zero Trust a quelque chose de très marketing. Derrière, se cachent des méthodes de travail nouvelles, des modes de fonctionnement nouveaux, et de nouveaux composants défensifs. Tout ceci ne se décide pas d'un claquement de doigts, ne s'implémente pas d'un clic et ne se maîtrise pas en un jour.

« *Les outils de sécurité ne sont pas là pour combler l'absence de stratégie et de bonnes pratiques* » explique **Laurent Cayatte**. « *À l'inverse, ils sont là pour implémenter les stratégies et la posture de sécurité élaborées conjointement par les responsables de l'entreprise, les responsables métiers, la DSI et le RSSI* ».

Une telle démarche réclame un accompagnement de proximité avec des experts dotés d'une véritable expérience de terrain, habitués à insuffler les bonnes pratiques et à mettre en œuvre les outils pour servir les besoins réels des entreprises. Des experts aussi capables de soutenir au plus près les clients lorsqu'ils sont attaqués.

« *Notre métier est d'avoir désormais une approche globale dans la construction de la sécurité d'infrastructure hybride, cloud et multicloud, dans la sécurisation des applications, dans la protection des données, dans la sécurisation des identités et jusqu'à la sécurisation de tous les appareils, du PC aux smartphones en passant par les équipements connectés (imprimantes, enceintes, etc.)* » conclut **Laurent Cayatte**.

Pour aller plus loin

Cybersécurité Metsys
https://www.metsys.fr/offres/cybersecurity/

Les ateliers gratuits proposés
https://www.metsys.fr/offres/cybersecurity/nos-offres-cybersecurite#programmes-financements-ms

Le maturity model Microsoft
https://www.microsoft.com/fr-FR/security/business/zero-trust/maturity-model-assessment-tool

METSYS
www.metsys.fr

Conception éditoriale & réalisation : Agence COM4MÉDIAS www.com4medias.com - crédit photos : Shutterstock

Sensibilisation, formation, supervision permanente,
LES BASES DE LA CYBERSÉCURITÉ !

Le bilan 2021 de la CNIL s'est une nouvelle fois concentré sur l'état de la cybersécurité. De la veille à la protection des données personnelles aux cyberattaques le pas est direct. Et les chiffres aussi : 5037 notifications de violation de données en 2021, une hausse de 80% par rapport à 2020.

Augmentation de la digitalisation

Certes, RGPD oblige les entreprises à notifier la CNIL lorsqu'elles constatent l'atteinte aux données personnelles dont elles sont responsables. Il y a bien sûr les pertes, les fuites involontaires, mais ce que la CNIL souligne pour 2021, ce sont les causes liées aux attaques informatiques qui sont en très forte hausse. Seule faible circonstance atténuante face à cette croissance, la très forte augmentation de la digitalisation des processus des entreprises, transformation profonde qui créé des nouvelles failles et axes d'attaques cyber.

Personnellement, j'ai confiance dans les chiffres et les constats de la CNIL. Quand on écoute quotidiennement les discours marketing des éditeurs de cybersécurité, l'état des lieux donné par la CNIL dans un sens rassure et donne bonne conscience à nos actions de tous les jours.

La clarté des chiffres donnés par la CNIL impressionne : 6 notifications sur 10 étaient liées directement à une attaque cyber! Et la plupart de ces attaques étaient liées à des ransomware (rançongiciels).

Accélérateur de votre transformation numérique

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

Digital Workplace

Infrastructures & Réseau

Sécurité & Stockage

Services Cloud Managés

www.dib-france.fr

Tél : 01 34 57 90 00

Multiplication des attaques aux rançons

Durant l'année 2021, la CNIL a enregistré 2200 attaques ransomware !

La face visible de la cybersécurité tourne actuellement majoritairement autour des attaques de phishing porteuses des ransomwares. C'est un sujet critique, les attaques aux rançons se multiplient et causent des graves sinistres aux entreprises de tout segment économique. Ces incidents ont d'ailleurs fait émerger une nouvelle génération d'antivirus, les EDR (Endpoint Detection and Response).

On ne peut pas citer ce fléau, sans souligner la triple peine subie par les utilisateurs victimes de ces attaques : premièrement, ils sont bloqués, perdent leurs données et leur activité, deuxièmement, ils payent les rançons, mais souvent, ils n'arrivent pas à récupérer les données voire ils sont obligés de changer de matériel.

Sensibilisation et formation des utilisateurs

Revenons au bilan annuel de la CNIL, qui estime être bien en deçà de la réalité.... Et de synthétiser le faible niveau de protection informatique des entreprises : techniques de chiffrement dépassées, mots de passe faibles, pas de RSSI au sein des entreprises, pas de budget ou budget insuffisant (on dit souvent qu'un budget entre 15 % à 20 % du budget global IT doit être alloué à la cybersécurité).

Tout cela nous ramène aux bases de la cybersécurité d'une entreprise, qui au-delà d'un socle d'outils SSI à mettre en œuvre et des processus de surveillance et d'exploitation de ces outils, doit reposer sur la sensibilisation continue et la formation des utilisateurs.

Il faut éduquer les utilisateurs, tous et dans toutes les entreprises et indifféremment des secteurs économiques, aux dangers de l'utilisation du Web, de la messagerie, de l'importance des processus d'authentification forte et de contrôle des identités, etc.

La face visible de la cybersécurité tourne actuellement majoritairement autour des attaques de phishing porteuses des ransomwares.

Un plan global, cohérent et adapté à chaque entreprise

Les entreprises doivent se doter des logiciels de sensibilisation et tests anti-phishing adaptés aux métiers de chacun au sein de l'entreprise, on va ainsi mieux tester et in fine mieux former un comptable en utilisant ses propres mots clés liés à son métier et son quotidien. De même, il faudra débriefer avec ceux qui sont tombés dans le piège, pas pour les pénaliser, mais pour leur expliquer les fautes à ne plus commettre et les habitudes à prendre (par exemple de vérifier l'adresse source des mails entrants, ou de l'importance des mots de passe robustes), l'attention à porter constamment et les former pour qu'ils puissent maîtriser les vraies attaques. Car la vraie attaque viendra certainement ; dans le monde de la cybersécurité, on dit qu'il y a deux types d'entreprises : celles qui ont subi une attaque cyber et celles qui ne le savent pas encore.

Sensibiliser, tester, former, re-tester, etc. c'est la clé pour que l'entreprise rester à l'abri des attaques et incidents cyber. Bien sûr, il faut un ''peu'' investir en outils et en personnels, mais cela sera de toute manière bien inférieure aux dommages et aux pertes financières d'une vraie attaque.

Cela implique un plan global, cohérent et adapté à la taille, l'empreinte digitale de l'entreprise et la criticité de ses données, un plan qui s'articule entre la partie sensibilisation-test-formation et la partie supervision permanente des infrastructures IT de l'entreprise par des ingénieurs et cyber-analystes.

Sensibiliser, tester, former, re-tester, etc. c'est la clé pour que l'entreprise rester à l'abri des attaques et incidents cyber.

> Par Théodore-Michel Vrangos, cofondateur et CEO de I-TRACING Group

Promodag

Promodag Reports pour Office 365 & Exchange

Promodag Reports est un outil puissant conçu pour l'analyse, le contrôle et le reporting complet des systèmes de messageries Microsoft Office 365 & Microsoft Exchange

Mise en conformité avec les règles de l'entreprise

Planification simplifiée des processus de gestion

Interopérabilité avec les Systèmes RH

Optimisation des performances de la messagerie

Audit & planification de l'utilisation des e-mails

Rapports d'analyse de trafic, suivi des messages

Droit à la déconnexion et RGPD

« OPTIMISEZ VOS USAGES COLLABORATIFS & RÉGLEMENTAIRES À L'HEURE DE LA **DIGITAL WORKPLACE GÉNÉRALISÉE** »

Rendez-vous sur **www.promodag.fr** pour télécharger gratuitement une version entièrement fonctionnelle ou contactez nous pour bénéficiez d'une démonstration complète avec l'un de nos experts.

www.promodag.fr • info@promodag.com

codein.

Hébergement traditionnel ou cloud, quelle solution choisir ?

Avec la popularité croissante du cloud, les entreprises de toutes tailles s'intéressent au cloud. Vous hésitez à migrer votre infrastructure sur le cloud ? Même en tenant compte des avantages du cloud, est-ce la solution qui vous convient le mieux ?

LA REVOLUTION DU CLOUD

Le cloud computing est la mise à disposition de ressources informatiques facturées de manière précise (à la seconde, minute, heure…) dont les fonctionnalités permettent d'automatiser la création de l'infrastructure.

Les ressources "infinies"

Aujourd'hui, dans le modèle du cloud, il suffit de passer commande et un serveur virtuel est accessible en quelques secondes. Tout est prévu pour être automatisable via API. Votre serveur est disponible quasi instantanément et utilisable en quelques minutes.

De son point de vue, le consommateur a accès à une infinité de ressources, que ce soit en terme horizontal (nombre de serveurs) ou vertical (caractéristique cpu/ram/disque d'un serveur). Les serveurs physiques sont toujours là, mais le problème est déporté : c'est le fournisseur de cloud qui gère ses stocks, son approvisionnement et les problématiques liées à cela.

La scalabilité et les gains financiers

La rapidité avec laquelle il est possible de créer et de détruire un serveur dans un contexte cloud permet de moduler continuellement le nombre de serveurs pour son application en fonction de la charge.

L'élasticité et l'auto scaling

En fonction de métrique qu'il faut préciser (charge des serveurs, trafic du site…), une infrastructure peut automatiquement "grossir" et s'adapter continuellement à la réalité des besoins.
Il est par exemple difficile de prévoir à l'avance le trafic d'un site de "news". Son succès est tributaire de l'actualité. Lors d'un évènement important, le trafic va augmenter brutalement et l'infrastructure doit alors s'adapter automatiquement. C'est le concept "d'Auto Scaling" qu'on retrouve chez plusieurs cloud publics.

LE CLOUD N'EST PAS MAGIQUE !

Les plaquettes commerciales des cloud public donnent l'impression que tout est magique : votre application va "scaler" en toute autonomie, votre site sera disponible quel que soit le trafic. Il est en effet possible d'atteindre cet objectif avec les outils proposés, néanmoins, pour y arriver, il faut parfois passer beaucoup de temps à tout configurer, que ce soit au niveau de l'application ou du cloud en lui-même.

Toute application peut être placée «dans le cloud»

Il ne s'agit que d'un serveur virtualisé accessible depuis une adresse IP. Toutefois, il faut que l'application soit adaptée pour réellement bénéficier de l'intérêt du cloud.

Plusieurs problématiques se posent alors, par exemple :

- l'application peut-elle être dupliquée sans problème d'accès à des fichiers partagés, de partage de sessions ?
- si l'on augmente le nombre de frontaux, quid d'une base de données qui pourrait devenir le point de contention ?
- comment se déploie l'application au sein d'un serveur fraîchement créé ?
- …

Besoin de conseils concernant votre infrastructure web ?
hosting@codein.fr - 09 72 42 26 03 - codein.fr

Des réponses techniques complexes nécessitant du temps et de l'argent !

Il faut rapidement se demander si le jeu en vaut la chandelle. Dans certains cas, il n'est pas nécessaire de migrer dans le cloud une application classique qui fonctionne très bien et répond à tous ses objectifs de charge sur l'année.

La difficulté d'anticipation des coûts et les mauvaises surprises

- Certains fournisseurs peuvent avoir une facturation très complexe.
- facturation du trafic (entrant/sortant/interne)
- gestion des entrées/sorties des volumes réseau qui peuvent être "garanties" ou "optimisées"
- ...

Cette complexité est telle qu'un nouveau métier a émergé : le "FinOps", chargé d'optimiser les factures en traquant les services peu, mal ou pas utilisés, les ressources surdimensionnées...

La maîtrise de la performance

Il est parfois difficile de maîtriser l'environnement sur lequel s'exécute nos serveurs.
Il est possible par exemple de choisir une instance à 4 "vCPU", 16GO de RAM et 100GO d'espace disque "SSD" mais connaître les caractéristiques précises du matériel sous-jacent est rarement possible.

L'over-commit

De la même façon, il est compliqué de savoir dans quelle mesure le fournisseur de cloud pratique «l'over-commit». Cette pratique consiste à allouer plus de ressources aux serveurs virtuels que ce que propose réellement le serveur physique.

La question de la localisation des données : le Cloud Act

Le Cloud Act est une loi de 2018 qui permet au gouvernement américain d'accéder aux données où qu'elles soient dans le monde du moment que le fournisseur de cloud est américain.

LE CLOUD N'EST NI LA SOLUTION À TOUS LES PROBLÈMES NI UNE SOLUTION À ÉVITER !

Pour **les sites e-commerces**, **les sites de news,** etc., le cloud public peut être une bonne solution, car ce sont des sites à fort changement de trafic qui nécessitent des infrastructures modulables au cours du temps.

Pour les **sites éditorialistes,** dont le trafic est très stable, cela se discute et un hébergement classique peut être plus performant.

L'important avant de souscrire à une offre d'hébergement est de donc définir clairement quels sont vos besoins.

*Par **Mathieu Blanc** - Responsable Hosting*
Agence Codéin

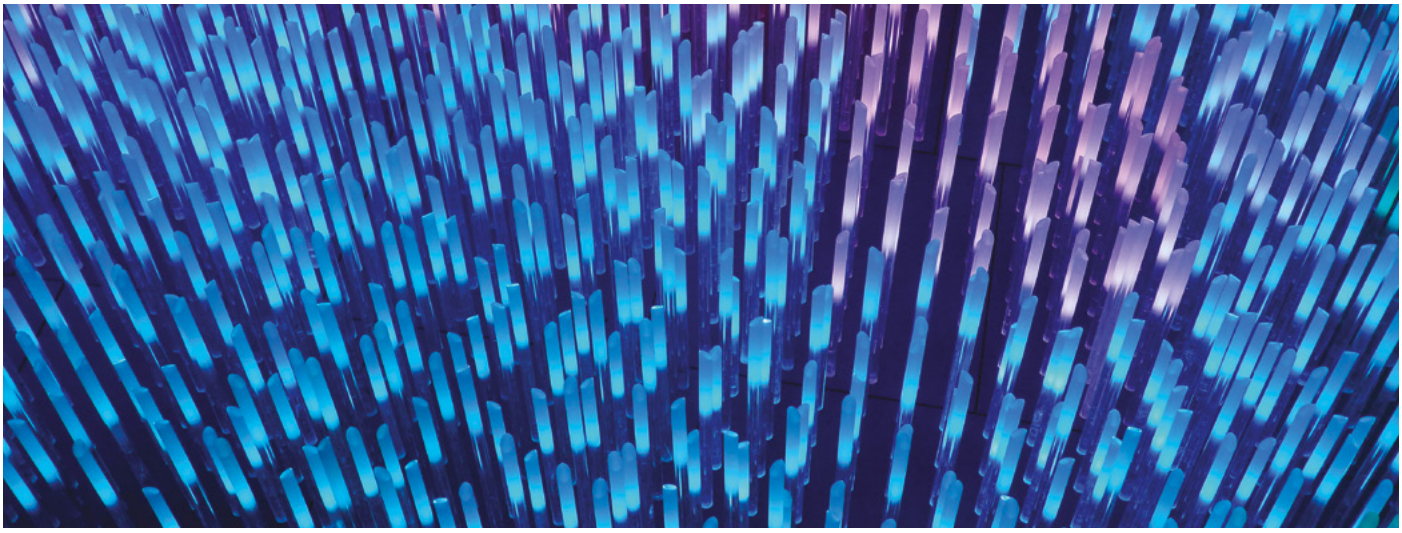
***Codéin** vous accompagne dans le cadrage de votre projet, le design de votre architecture et le monitoring de votre infrastructure.*
Nous vous garantissons une solution sur mesure, sécurisée et performante et des Ingénieurs Système, force de conseils disponibles et joignables (vraiment !)

hosting@codein.fr - 09 72 42 26 03 - codein.fr

Les 7 clés pour réussir sa modernisation

ET RÉPONDRE À LA PÉNURIE DE TALENTS

La modernisation de l'informatique est devenue un impératif stratégique. Cependant, un grand nombre d'entreprises rencontrent encore des complexités pour mener à bien leurs projets de modernisation. En cause : une feuille de route du numérique quelque peu opaque et une main-d'œuvre qui ne dispose pas des compétences techniques nécessaires pour obtenir les résultats souhaités. Or, cette pénurie de talents et de compétences se fait lourdement ressentir au sein des entreprises et des intégrateurs de systèmes.



Gautam Khanna, VP and Global Head, Modernization Practice, Infosys présente 7 clés pour réussir sa modernisation.

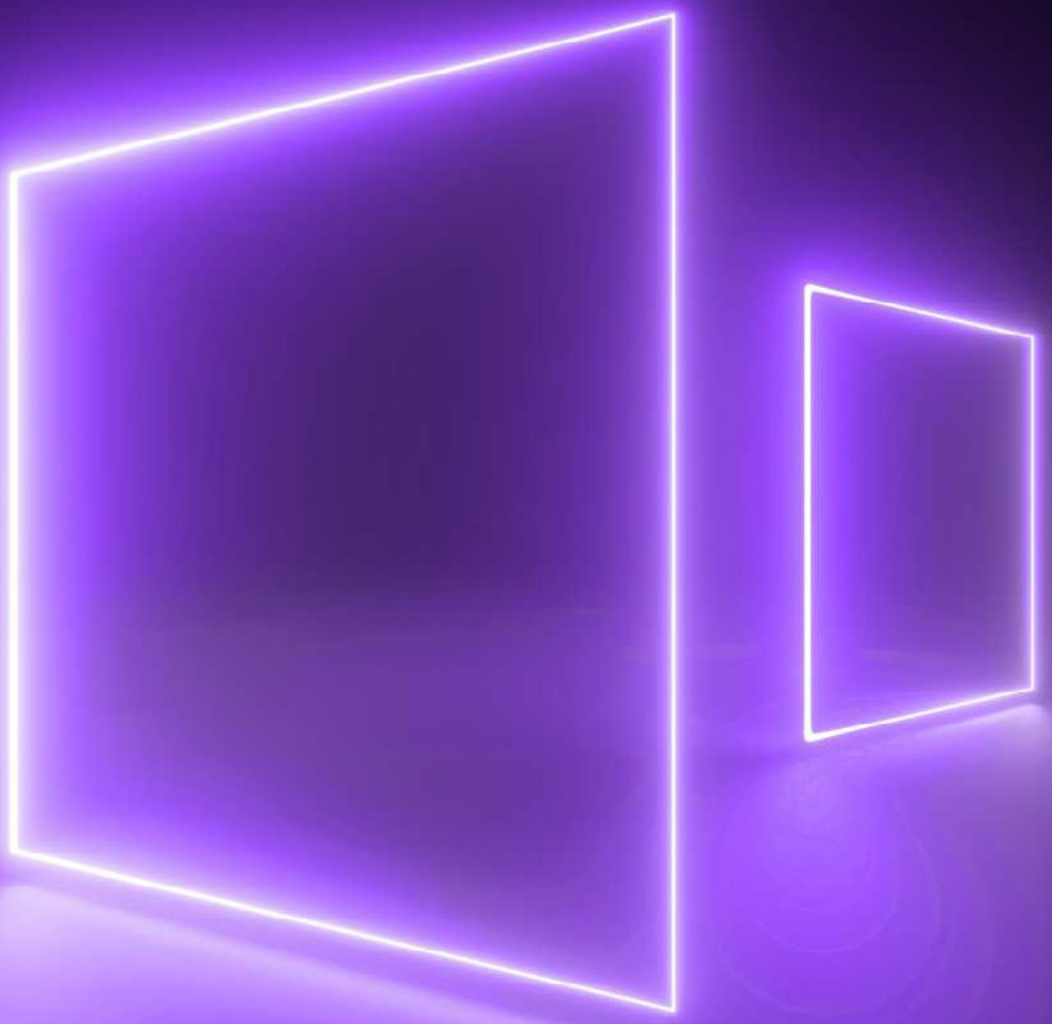
Le risque de perturbation de l'activité et le coût étaient les principaux facteurs de dissuasion des programmes de modernisation. Néanmoins, le manque de talents est devenu une priorité bien plus importante pour les dirigeants, selon les résultats d'une récente étude. Les budgets des programmes de modernisation peuvent atteindre des sommes à sept chiffres et prendre parfois plus de trois ans à être mis en place, or il s'agit ici d'un point critique où est déterminé le succès ou l'échec du programme. Une bonne partie de ce budget de modernisation doit être consacrée à l'amélioration des compétences, à l'établissement de partenariats et à l'utilisation de l'automatisation basée sur des plateformes. Pour réussir ces programmes de transformation, il est primordial de s'appuyer sur les architectes de solutions. La transformation numérique et, avec elle, l'innovation commerciale, tireront ainsi parti de la nouvelle ère numérique.

Il existe une série de sept interventions à implémenter pour assurer le succès des initiatives de modernisation. Ces mesures leur permettront de respecter les délais et la qualité, même si leur base de talents accuse un certain nombre de changements.

1. **Utiliser les services 'cloud-managed'.** Les plateformes modernes de cloud computing offrent une gamme de composants technologiques dans le cadre d'un modèle "as-a-service". La plupart des strates de la pile d'applications peuvent désormais être exploitées sans qu'il soit nécessaire de recourir à un personnel dédié pour gérer leurs opérations. Les organisations devraient maximiser l'utilisation de ces composants "as-a-service" au sein de leurs architectures afin que le fournisseur de services en cloud soit responsable des compétences spécialisées nécessaires pour les configurer et les gérer.

CARBONITE® + WEBROOT®

opentext™ companies



Microsoft 365 ne sauvegarde pas tous vos fichiers.

Nous, oui

Pour en savoir plus :
https://www.carbonite.com/cp/intl/fr/microsoft-365-backup
Ou contactez-nous au +33 (0)1 47 96 55 41
ou par email france-smbc@opentext.com

Les Agile PODs sont de petites équipes autonomes qui peuvent exécuter toutes les phases du cycle de vie nécessaires à la construction d'un module.

2. Mettre à profit les plateformes Low-code/No-code. Ces dernières années, nous avons assisté à l'essor de plusieurs plates-formes qui prennent en charge la création d'applications complètes, à l'aide de modules préconstruits avec des fonctions glisser-déposer. Les entreprises sont ainsi en mesure de créer rapidement des applications dotées de caractéristiques telles que la compatibilité avec les mobiles, une interface utilisateur standardisée et des intégrations solides. Ce modèle est idéal pour créer des applications de petite et moyenne taille, qui prennent en charge les fonctions non différenciées d'une entreprise sans nécessiter d'un personnel informatique expert pour les développer et les maintenir.

3. Une automatisation basée sur plateforme. Une approche de la modernisation des applications basée sur une plateforme offre une automatisation des tâches routinières du programme et ce, de manière standardisée et reproductible. Elle permet aux architectes experts de déterminer dès le départ les composants et les cadres à utiliser dans le programme, mais aussi à faciliter les tâches subséquentes. Cela accélère le développement tout en garantissant la mise en place des meilleures solutions.

4. S'appuyer sur des architectes de la modernisation. Les architectes de la modernisation comprennent les compromis complexes, nécessaires d'un point de vue technique et commercial. Ils disposent d'une vision globale du cycle de vie d'un système et adoptent une approche axée sur l'architecture pour déterminer les composants technologiques les mieux adaptés. Cela peut réduire le nombre de cycles consacrés à l'expérimentation de différents composants de niche qui nécessiteraient autrement des talents et des compétences spécialisés.

5. Tirer parti des partenariats avec les fournisseurs indépendants de logiciels (ISV). Les entreprises doivent travailler avec des intégrateurs de systèmes globaux (GSI), qui peuvent réunir plusieurs ISV et leurs compétences techniques pour résoudre des problèmes complexes. Les entreprises informatiques peuvent tirer parti de l'expertise des produits et des meilleures pratiques offertes par les ISV pour élaborer des solutions solides.

GAUTAM KHANNA

6. Faire appel à des « Agiles PODs ». Les Agile PODs sont de petites équipes autonomes qui peuvent exécuter toutes les phases du cycle de vie nécessaires à la construction d'un module. Alors que les analystes d'affaires préparent les exigences et les testeurs valident leur bonne construction, la structure Agile Pod garantit qu'une fois qu'un travail est entrepris, il sera achevé de manière Agile. Les organisations peuvent augmenter ou diminuer le nombre de pods en fonction de la disponibilité des compétences et des talents, modulant ainsi la vitesse de livraison en fonction de la capacité existante.

7. Expérimenter avec l'IA. L'Intelligence Artificielle progresse rapidement dans des domaines tels que la traduction des langues. Cela peut s'avérer être un levier précieux lors de la modernisation des systèmes existants. Bien qu'elles ne soient pas encore tout à fait au point, les expériences basées sur l'IA comme le langage GPT-J devraient être expérimentées afin que les organisations soient prêtes à les utiliser lorsqu'elles deviendront matures.

La modernisation est en cours. Et elle est rapide. Alors que des milliards de dollars sont aujourd'hui consacrés à la modernisation, il est primordial de s'assurer que les talents soient efficaces, efficients et prêts à s'engager sur le long terme. Ce n'est plus un luxe, mais un élément essentiel de toute transformation d'entreprise.

La modernisation est en cours. Et elle est rapide.

« Observatoire DSI 2022 » : quels services pour les métiers ?

De l'ITSM à l'Enterprise Service Management : une évolution transparait depuis la dernière étude menée en 2019 selon Micro Focus.

Un marché de l'ITSM mature

Côté équipement d'outils ITSM, les indicateurs suivants sont remontés :

- 79,3% sont équipés d'un outil
- 55% depuis plus de 3 ans
- 24,3% plus récemment

Si les outils sont gérés majoritairement sur site, le Cloud et le Saas augmentent, avec 59,2% on premise, 32,8% en mode hébergé et 8% en infogérance

75% connaissent l'ESM mais 6,5% sont experts

« Les évolutions portent surtout sur un développement du mode SaaS, même si cette croissance n'est pas aussi importante que supposée, mais également par plus d'externalisation. Quant à l'approche ESM, si celle-ci est plus importante, peu de projets sont en production. On constate d'ailleurs que si une grande majorité des répondants connaissent le concept peu sont experts » commente Isabelle Roth, International ESM Practice Lead Micro Focus.

Ouverture aux métiers administratifs

Les outils ITSM sont ouverts aux métiers et services suivants, avec par ordre :

- Administratif et Financier – 58,1%
- Ressources Humaines – 51,4%
- Services Généraux – 51,4%
- Services clients / Réclamations – 40,5%

Mais seulement 31% des métiers sont satisfaits de la solution proposée.

Si 60% des métiers s'équipent sans passer par la DSI, 13,6% ont déjà une démarche ESM mais 43,2% l'envisagent.

Les principaux freins et gains de la démarche ESM

A la question quels sont principaux freins d'une démarche ESM ? Le classement des réponses s'oriente ainsi :

- N°1 - les budgets informatiques - 44,8%
- N°2 - le manque de ressources et compétences - 43,2%
- N°3 - la difficulté à travailler en collaboration avec les métiers- 39,2%

Les gains d'une démarche ESM sont la satisfaction utilisateurs (67,2%), la diminution du temps de l'équipe support et le gain de réactivité au changement.

Source Micro Focus – Enquête janvier et février 2022 - plus de 176 décideurs IT en France et en Belgique (75% des directeurs, 75% du secteur privé et dont la taille d'entreprise est à 63,2% de plus de 1000 salariés)

Specops : TROIS CONSEILS POUR ASSURER LA SÉCURITÉ DES COMPTES ET DES DONNÉES

L'entreprise fondée en 2001, avec son siège social situé à Stockholm, en Suède, dispose de bureaux aux États-Unis, au Canada, au Royaume-Uni et en Allemagne. Entretien avec Darren James, Head of Internal IT chez Specops Software.

Un mot sur Specops ?

Specops Software, une société d'OutPost24, est le leader des solutions de gestion des mots de passe et d'authentification, et protège les données de l'entreprise en bloquant les mots de passe faibles et en sécurisant l'authentification des utilisateurs. Avec un portefeuille complet de solutions intégrées nativement à Active Directory, Specops garantit que les données sensibles sont stockées sur site et sous contrôle de l'entreprise.

Des organisations font appel à Specops Software pour protéger les données essentielles à leur activité.

Pour Specops, que signifie le renforcement de la sécurité informatique ?

Chez Specops, nous pensons que le renforcement de la sécurité informatique commence par l'amélioration de son maillon le plus faible : les mots de passe.

En tant que partenaire Gold de Windows, nous aidons des clients dans plus de 120 pays à se protéger contre les éventuelles cyberattaques en créant des politiques de mots de passe et des pratiques d'authentification des utilisateurs plus robustes.

Quelles sont les dernières actualités de l'entreprise ?

Specops Software a récemment publié la dernière édition de son rapport sur les mots de passe faibles (février 2022), qui s'est penché à la fois sur le côté humain et le côté technique des raisons pour lesquelles les mots de passe sont le point faible du réseau d'une organisation. On peut retenir ces points forts:

- Même les mots de passe les plus complexes sont susceptibles de faire l'objet de violations. En effet, **41 % des mots de passe utilisés dans les cyberattaques comportent 12 caractères ou plus,** souvent des lettres, des chiffres et des caractères spéciaux.
- 54 % des organisations ne disposent pas d'une solution pour gérer les mots de passe des salariés
- 48% des organisations n'ont pas mis en place de vérification de l'utilisateur final pour les appels au service d'assistance informatique.

Les recherches présentées dans ce rapport ont été compilées grâce à des enquêtes exclusives et à l'analyse des données de 800 millions de mots de passe compromis, un sous-ensemble des plus de 2 milliards de mots de passe compromis figurant dans la liste de Specops Breached Password Protection.

Le rapport a également mis en évidence les mots les plus couramment utilisés dans les mots de passe compromis.

Quelles sont les recommandations à suivre pour prévenir une entreprise d'une cyberattaque ?

Si nous lisons de plus en plus de choses sur les cyberattaques subies par des entreprises de premier plan (comme Nvidia), les pirates peuvent aussi s'en prendre à des PME ou à des entreprises de secteurs non stratégiques. Par conséquent, toutes les entreprises et organisations doivent aller au-delà des traditionnelles bonnes pratiques du "mot de passe fort" et assurer la sécurité des comptes et des données. Et elles doivent s'attaquer au problème dès aujourd'hui, car la prévention est moins coûteuse que la récupération des attaques.

54 % des organisations ne disposent pas d'une solution pour gérer les mots de passe des salariés

DARREN JAMES

Si on devait retenir quelques conseils clés, voici trois conseils à suivre dès maintenant :

1. Bloquez les mots de passe faibles et compromis

Selon une étude, environ 1 million de mots de passe sont volés chaque semaine. De plus, une enquête menée par PCMag en 2021 a révélé que 70 % des personnes interrogées admettaient utiliser le même mot de passe à plusieurs reprises, ce qui rend chaque utilisation vulnérable à une violation.

En effet, avons déjà constaté que les pirates font des dégâts considérables avec des mots de passe déjà compromis, comme l'a montré l'attaque de Colonial Pipeline l'année dernière. Les entreprises doivent donc mettre en place un outil qui bloque systématiquement non seulement les mots de passe faibles qui ne répondent pas aux exigences de longueur et de complexité, mais aussi les mots de passe compromis connus.

2. Ajouter des strates supplémentaires à l'authentification multifacteurs

Les entreprises peuvent ajouter d'autres couches de leur authentification multifacteurs (AMF) existante aux processus de sécurité, comme la biométrie, des jetons/codes d'authentification, des questions secrètes et des applications d'authentification. Chaque méthode d'authentification multifacteurs a ses forces et ses faiblesses, et n'est pas entièrement à l'abri des cyberattaques.

Toutefois, les dirigeants d'entreprises tech ont indiqué que l'utilisation de l'AMF pourrait prévenir 80 à 90 % des cyberattaques. Les plates-formes MFA qui prévoient des facteurs de sauvegarde en cas de panne de service d'authentification ou en cas de suspicion de compromission sont un moyen crucial pour les services informatiques d'éviter les perturbations dans le paysage actuel de l'authentification.

3. Appliquer la vérification des utilisateurs par le service d'assistance informatique

En juin 2021, des pirates ont infiltré un canal de discussion Slack chez EA et ont manipulé un employé du support informatique afin qu'il leur donne un jeton MFA pour accéder au réseau social de l'entreprise.

Cette arnaque d'ingénierie sociale a finalement abouti au vol de 780 Go de données. De nombreuses organisations sont exposées à ce type d'attaques, car 48 % d'entre elles n'ont pas mis en place de politique de vérification des utilisateurs pour les appels entrants vers le service informatique.

La vérification de l'utilisateur par le service d'assistance IT permet de reconnaître les escroqueries et d'établir une interface sécurisée avec les employés, ce qui renforce la sécurité de l'entreprise. L'AMF renforcée est un excellent moyen d'y parvenir.

Si une entreprise est victime d'une cyberattaque, quelles actions doit-elle mener ?

Si une entreprise est malheureusement victime d'une cyberattaque, voici ce qu'elle doit faire :

- **Exécutez une réinitialisation du mot de passe à l'échelle de l'entreprise**

Pour se remettre d'une cyberattaque, il est essentiel de procéder à une réinitialisation des mots de passe à l'échelle de l'entreprise afin que les hackers qui ont récupéré les mots de passe de votre entreprise ne puissent pas les réutiliser pour une nouvelle attaque.

La vérification de l'utilisateur par le service d'assistance IT permet de reconnaître les escroqueries.

Il est préférable d'encourager vos utilisateurs finaux à réinitialiser ou à modifier eux-mêmes leurs mots de passe avant de les y contraindre.

De nombreuses solutions telles que Specops uReset peuvent aider les entreprises à soulager leur service d'assistance. Depuis Microsoft Active Directory, il est possible de faire expirer tous les mots de passe et forcer une réinitialisation à la prochaine connexion pour tous les utilisateurs qui n'ont pas encore changé leur mot de passe. Cela peut également contribuer à soulager une partie de la charge de travail du service informatique.

- **Révisez et renforcez votre politique de mot de passe existante**

Vous devrez revoir et renforcer votre politique de mot de passe existante et, idéalement, mettre en œuvre les trois conseils susmentionnés. Microsoft Active Directory dispose d'outils pour vous aider à définir une politique de mot de passe suffisamment solide. Toutefois, il lui manque plusieurs fonctionnalités essentielles pour protéger les entreprises contre des cyberattaques de plus en plus sophistiquées.

Par exemple, il ne permet pas de créer un dictionnaire personnalisé pour interdire les mots-clés liés à l'entreprise, ni de bloquer l'utilisation de mots de passe compromis connus. Les mots-clés liés à l'entreprise sont faciles à deviner pour les pirates et autoriser l'utilisation de mots de passe susceptibles d'être compromis met votre entreprise en danger.

Vous pouvez envisager de mettre en œuvre un outil tiers si vous souhaitez simplifier les tâches, mais vous devez vous assurer que la solution que vous choisirez dispose d'un système permettant de bloquer tous les mots de passe faibles et compromis.

Autoriser l'utilisation de mots de passe susceptibles d'être compromis met votre entreprise en danger.

> Par Sabine Terrey

LE DROIT À LA DÉCONNEXION : UN ENJEU RH

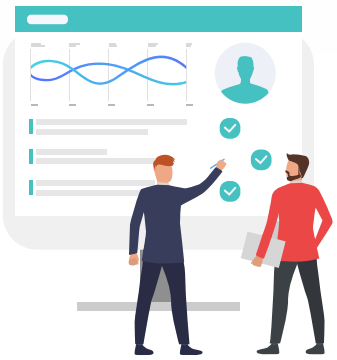
DANS UN MONDE RÉGI PAR L'IMMÉDIATETÉ,
LA DÉCONNEXION N'EST PLUS UNE OPTION, MAIS UN DROIT.

PROMODAG REPORTS PERMET LA CONFORMITÉ AVEC LE DROIT À LA DÉCONNEXION

GÉRER LA DÉPENDANCE EXCESSIVE AUX TECHNOLOGIES

LE DROIT À LA DÉCONNEXION EST UNE OBLIGATION LÉGALE

DES CHARTES DE BONNES PRATIQUES POUR LE CONFORT DES SALARIÉS



UN OUTIL AU SERVICE DES RESSOURCES HUMAINES

UNE SOLUTION DE SENSIBILISATION, D'ALERTE ET DE PRÉVENTION

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

Découvrez la solution Promodag Reports

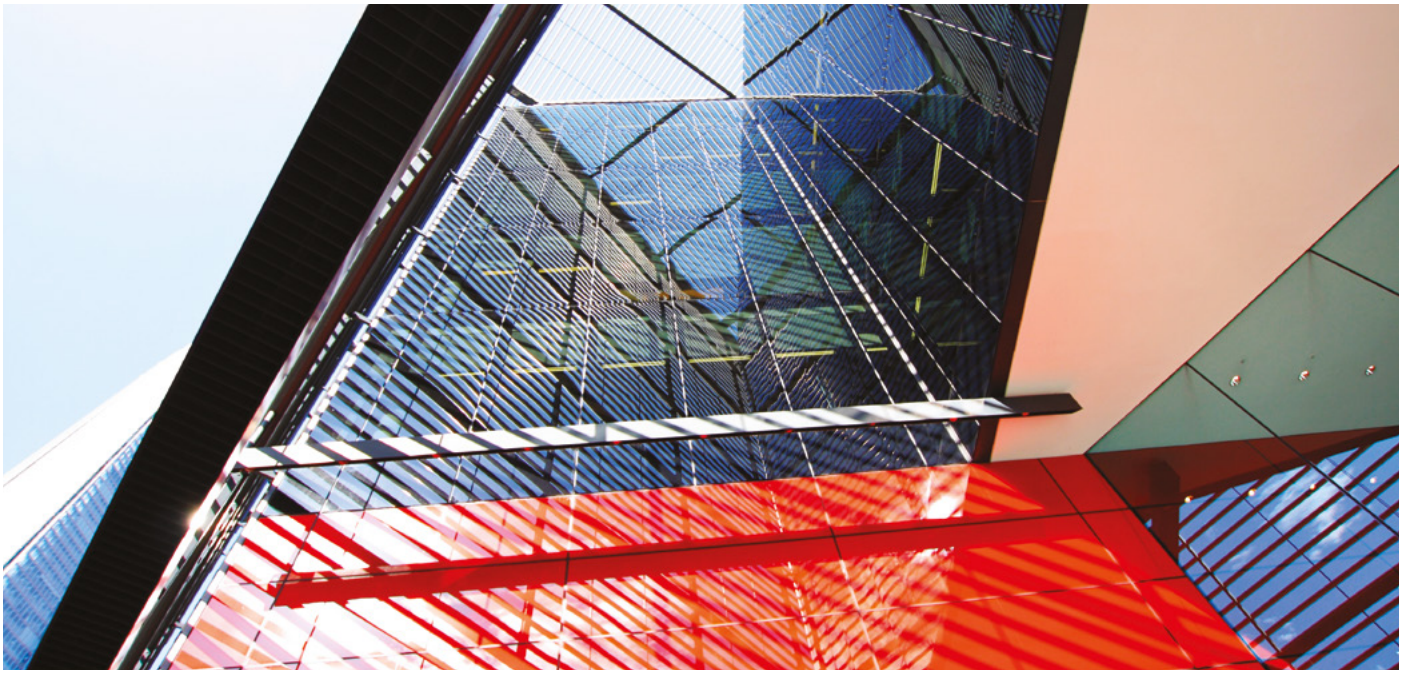
Promodag

www.promodag.fr

Gestion de la surface d'attaque :
LES NOUVELLES PRATIQUES AUTOUR DES MÉTA-CONNECTEURS ET DES PUITS DE DONNÉES ADAPTIFS

> Par Sylvain Cortes

Faites donc un test, interrogez un RSSI relativement proche de ses équipes, et demandez-lui quels sont ses pires « cauchemars », il vous répondra irrémédiablement avec les éléments suivants :
• La lutte contre les ransomwares
• La sécurité d'Active Directory
• La gestion des patchs sur les différents systèmes
Bien sûr, l'ordre des réponses nous importe peu.



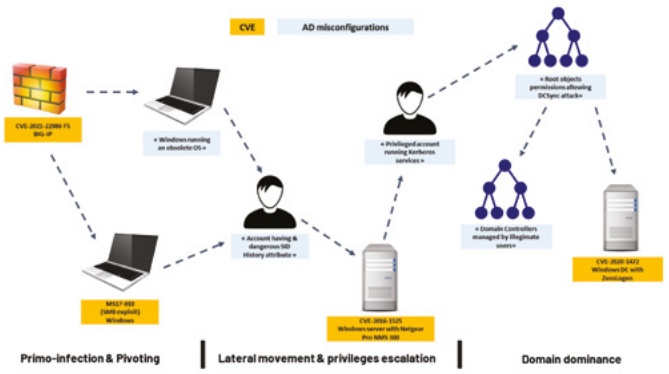
Globalement, la gestion de ce que l'on appelle la surface d'attaque est un défi quotidien pour les équipes du RSSI – mais que les choses soient claires, ne vous laissez pas abuser par le terme « surface », nous l'employons ici car il s'agit du terme consacré. Bien évidemment, votre exposition générale intègre également vos applications dans le Cloud public, vos sites web, votre code hébergé dans GitHub, etc. Le terme de « surface d'attaque » englobe donc l'ensemble de votre exposition aux risques cyber, quelle que soit sa « localisation ». De plus, cette notion ne se limite pas aux systèmes en surface mais prend bien en compte les réseaux locaux profonds ou n'importe quelle « machine » gérée par l'IT.

Lorsque l'on tente de plonger dans les détails de l'utilisation de la surface d'attaque par un acteur malveillant, on réalise rapidement que la partie offensive utilise ce que l'on désigne habituellement comme étant un « chemin d'attaque » - pour le novice, un chemin d'attaque représente le parcours emprunté par un attaquant pour passer d'un point A à un point B, par exemple l'attaquant commence par compromettre un de vos firewalls et terminera administrateur de votre domaine Active Directory.

Le chemin d'attaque n'exploite finalement que deux éléments :

- Une mauvaise configuration d'un système
- Une CVE non patchée sur un système

Ensuite, la logique du chemin se mettra en place pour sauter d'actif en actif et compromettre globalement l'organisation :



Principe du chemin d'attaque

Comme vous pouvez le constater sur le schéma précédent, la gestion des CVEs représente un élément extrêmement important dans le périmètre des équipes de sécurité. L'objectif de cet article est de donner un coup de balai dans le monde poussiéreux de la gestion des vulnérabilités et de vous exposer les nouvelles pratiques qui vous permettront de gagner en efficacité et globalement augmenter votre niveau de résilience.

Les deux pratiques historiques liées aux vulnérabilités : Vulnerability Management & Patching

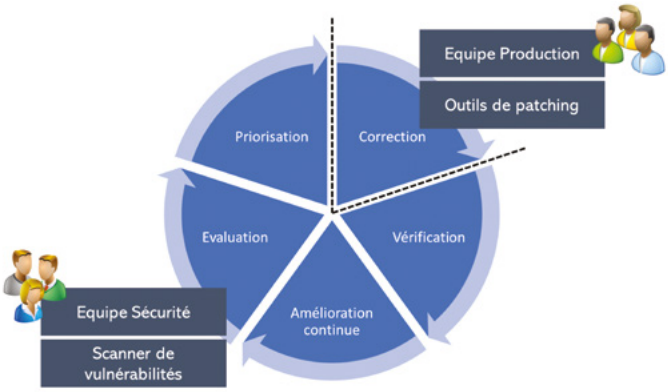
LE CYCLE DE GESTION DES VULNÉRABILITÉS

Traditionnellement, le cycle de gestion des vulnérabilités s'organise autour de 5 grandes étapes :

- **Evaluation** - cette étape initiale consiste principalement à découvrir ses actifs et les étudier pour lister les vulnérabilités présentes :
  - Identification des actifs
  - Scan des actifs
  - Rapport sur les vulnérabilités liées aux actifs

Le terme de « surface d'attaque » englobe donc l'ensemble de votre exposition aux risques cyber, quelle que soit sa « localisation ».

- **Priorisation** – en se basant sur l'étape d'évaluation, il s'agit ici de définir une priorisation des actions, car il n'est généralement pas possible de patcher l'ensemble des vulnérabilités au sein d'un même cycle :
  - Enrichir le contexte de l'actif - assigner une valeur à l'actif
  - Comprendre le score CVSS
  - Décider du plan de correction
- **Correction** – cette étape représente globalement le fait d'appliquer les correctifs/patchs fournis par les éditeurs afin de corriger les CVEs présentes sur les systèmes :
  - Action de remédiation
  - Documentation des actifs non patchés et atténuation des risques
- **Vérification** – suite à l'étape de patching, il s'agit maintenant de vérifier que les actifs sont effectivement patchés afin de s'assurer du niveau de sécurité réel :
  - Re-scan des actifs
  - Validation des hypothèses
- **Amélioration continue** – comme tout cycle vertueux, le cycle de gestion des vulnérabilités devra s'améliorer lors de l'exécution de chaque itération :
  - Evaluer les mesures
  - Evolution des procédures et traitement des problèmes rencontrés



Cycle de gestion des vulnérabilités

DES OUTILS ET DES ÉQUIPES DIFFÉRENTES

Comme vous pouvez le constater sur le schéma précédent, l'implémentation du cycle nécessite à minima l'usage de deux types d'outils différents :

- Les scanners de vulnérabilités
- Les outils de patching

Historiquement, l'équipe sécurité est en charge de découvrir quels sont les actifs vulnérables et d'évaluer le risque lié à chaque actif, de plus c'est généralement l'équipe sécurité qui se chargera de définir quels sont les actifs à patcher en priorité. Ces informations sont ensuite transmises à l'équipe de production, garante du maintien opérationnel, qui devra appliquer les correctifs aux différents systèmes listés par l'équipe sécurité.

Cette séparation des responsabilités et des outillages est extrêmement complexe à gérer et produit irrémédiablement des difficultés opérationnelles et organisationnelles majeures. Il est donc primordial que le responsable de production et le RSSI puissent travailler de façon concertée et dans la plus grande transparence, car les enjeux liés au bon déroulé des opérations sont majeurs pour maintenir le niveau de résilience de l'organisation.

Les challenges actuels dans le domaine de la gestion des vulnérabilités

UN NOMBRE TOUJOURS PLUS IMPORTANT DE CVES

Premièrement, si vous désirez comprendre comment les scores de CVE sont attribués, je vous conseille fortement la lecture de cet article sur le site web cve.org : https://www.cve.org/ResourcesSupport/AllResources/CNARules

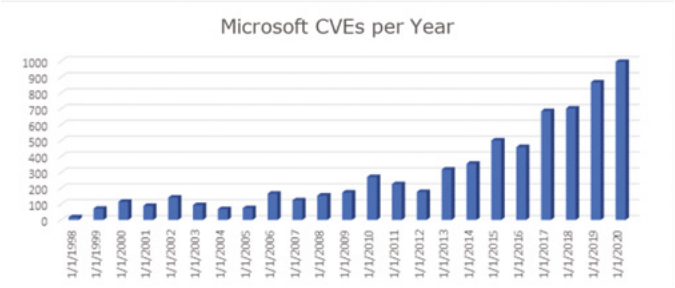
De plus, si vous désirez consulter la liste de toutes les CVEs connues, vous pourrez télécharger différents fichiers depuis le site du MITRE : https://cve.mitre.org/data/downloads/index.html

Lorsque l'on consulte les différents référentiels de CVEs, on constate instantanément deux choses :

- Le nombre de CVEs ne fait que grandir, car il s'agit d'un nombre cumulé au fil des années – bien sûr les CVEs de l'année 2022 ne remplacent pas les CVEs de l'année 2021, donc le nombre global de CVEs à gérer ne peut que grandir au fil du temps
- Le nombre de CVEs découvertes chaque année (et non en cumulé maintenant) grossit lui aussi !

Le cycle de gestion des vulnérabilités nécessite l'intervention d'équipes différentes ainsi que d'outils divers et variés.

Pour illustrer le deuxième point, le schéma suivant représente le nombre de CVEs identifiées sur les environnements Microsoft, année par année :



Nombre de CVEs découvertes chaque année en environnement Microsoft - Source : https://bit.ly/3lvLVux

En conclusion, non seulement le nombre de CVEs à gérer augmente au fil du temps, car il s'agit d'un nombre cumulé, ensuite, il y a statistiquement de plus en plus de CVEs découvertes chaque année !

UN MANQUE D'AUTOMATISATION ET D'ALIGNEMENT ENTRE LES OUTILS ET LES DONNÉES

Comme indiqué au début de cet article, le cycle de gestion des vulnérabilités nécessite l'intervention d'équipes différentes ainsi que d'outils divers et variés. Cet état de fait contribue à augmenter l'entropie autour de cette activité. De plus, des facteurs « aggravants » doivent être pris en compte :

- Manque de communication entre les équipes de production et les équipes sécurité
- Des référentiels de données disparates et peu d'alignement entre les bases de vulnérabilités, les outils de scan et les outils de patching
- Une confiance relativement faible des équipes sécurité envers la qualité des données résidant en CMDB, voire, une pratique de sécurité qui ignore les données de gestion des actifs et qui se concentre uniquement sur le scan de vulnérabilité
- Peu ou pas de connexion et d'échanges de données entre les différents référentiels, il en résulte des ressaisies manuelles occasionnant de nombreuses erreurs, des capacités de reporting centralisé très médiocres et une difficulté grandissante à aligner les exigences de sécurité avec les enjeux du business

En conclusion, il apparait que les données et les processus manquent cruellement de liant.

LE CAUCHEMAR DE LA PRIORISATION

La priorisation demeure actuellement l'enjeu majeur de la gestion des vulnérabilités. En effet, l'organisation doit être en capacité de définir quels sont les actifs critiques, quels sont les risques associés et définir un plan de remédiation cohérent se basant sur une priorisation des actions à mener.

FIC

Forum International de la Cybersécurité

“Shaping Europe’s digital future”

7, 8 et 9 juin 2022

Lille Grand Palais

Organisé par

Gendarmerie nationale

avisa partners

Avec le soutien de

Région Hauts-de-France

forum-fic.com

La priorisation demeure actuellement l'enjeu majeur de la gestion des vulnérabilités.

En effet, comme nous l'avons vu précédemment, le nombre de CVEs augmentant sans cesse, et de façon exponentielle, il n'est plus possible de patcher l'ensemble des CVEs présentes sur le parc informatique, et ce sur des cycles de plus en plus courts. De plus, de nombreuses vulnérabilités critiques étant découvertes chaque jour, les équipes de production sont soumises à une pression quotidienne pour corriger en urgence la dernière faille critique découverte la veille...

Pour rappel, les CVEs sont « notées » selon un degré de criticité allant de 0 à 10, il s'agit du score CVSS. Si vous désirez comprendre comment est calculé ce score CVSS, je vous invite à consulte cette page du NIST : https://nvd.nist.gov/vuln-metrics/cvss

Il faut accepter l'idée qu'actuellement le score CVSS seul ne permet plus de définir une priorisation efficace liée à la remédiation des risques.

Des évolutions nécessaires prévues par les analystes

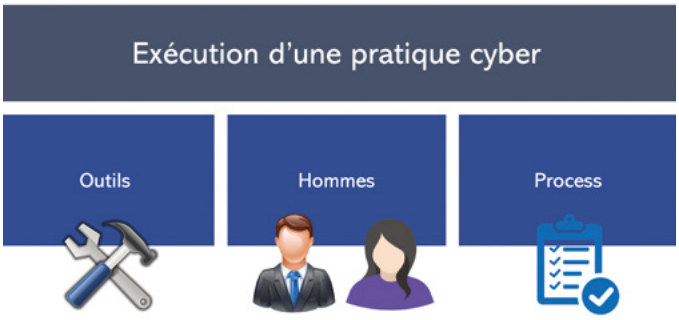
La plupart des analystes recommandent une évolution majeure des pratiques liées au cycle de gestion des vulnérabilités afin d'assurer un niveau de sécurité minimal dans les organisations. En effet, la situation actuelle ne permet plus d'assurer un équilibre sain entre charge de travail et sécurité opérationnelle.

La pratique dite d'« Attack Surface Management » devra être mise en œuvre dans l'ensemble des organisations, soit comme pratique interne, soit sous la forme d'un service managé. Cette pratique s'appuie sur 3 piliers :

- **« Cyber Asset Attack Surface Management » :** C'est certainement l'élément le plus important, nous l'évoquerons dans le chapitre suivant, car il mérite un éclaircissement dédié – globalement il s'agit ici de casser les silos et d'unifier les données puis de permettre la collaboration des équipes via des outils dédiés
- **« External Attack Surface Management » :** Ce pilier réalise un focus sur la découverte des actifs rattachées à l'organisation mais qui sont exposés directement sur Internet – le niveau de risque lié à ces actifs externes sera donc lui aussi évalué
- **« Digital Risk Protection Services » :** Globalement, cette pratique consiste à enrichir son puits de données « interne » avec des informations provenant de référentiels externes, tel que par exemple l'étude des données disponibles sur le Deep Web ou le Dark Web

« Pratique Attack Surface Management »

Par expérience, toute pratique Cyber s'appuie sur les trois piliers principaux que sont les outils, les hommes et les process. Les outils jouent un rôle fondamental dans l'exécution de la mission car ils permettent d'assurer une cohérence générale et assurent de guider l'organisation dans l'implémentation de sa pratique.



Mise en exécution d'une pratique Cyber

Les organisations doivent donc s'équiper d'une nouvelle génération d'outillage, apportant un cadre structurant à la pratique, les solutions logicielles permettant d'exécuter le « Cyber Asset Attack Surface Management » jouent un rôle tout particulier dans cet ensemble cohérent.

Un nouveau monde, les solutions de Cyber Asset Attack Surface Management (CAASM)

Les solutions de type CAASM permettent généralement d'exécuter les missions suivantes :

- Consolidation des données et priorisation du traitement des vulnérabilités
- Vue holistique des actifs et des risques présents au sein de l'organisation
- Alignement des pratiques de cybersécurité au sein des différents silos organisationnels et techniques
- Pilotage de la remédiation des risques majeurs
- Contrôle des écarts entre les mesures réalisées et la réalité de la production

Par expérience, toute pratique Cyber s'appuie sur les trois piliers principaux que sont les outils, les hommes et les process.

Ces solutions possèdent une architecture particulière, hautement adaptive, permettant globalement de prendre en compte n'importe quel type de données. Ils proposent des fonctions permettant d'alimenter sans cesse le référentiel et d'adapter le schéma structuré des informations consolidées afin de pouvoir gérer les besoins présents et futurs. Elles s'appuient sur un certain nombre de briques fonctionnelles majeures que nous listons ci-après.

CAASM – LES META-CONNECTEURS

Une solution de type CAASM possède des connecteurs permettant d'absorber ou d'envoyer des informations depuis ou vers les outils déjà déployés dans l'organisation. Ces connecteurs permettent de maximiser les investissements existants, en effet, il ne s'agit pas ici de rajouter un énième outil de sécurité mais bel et bien de magnifier le potentiel des investissements déjà réalisés. On peut catégoriser les différentes familles de connecteurs :

- *Les scanners de vulnérabilités :* le connecteur permettra de rapatrier toutes les informations liées aux scanners de vulnérabilités présents dans l'organisation, ils peuvent être de type open-source ou commerciaux – généralement l'organisation possède plusieurs scanners de vulnérabilités, en fonction des actifs étudiés : scanner des système IT, scanner du code, scanner des actifs web, etc.
- *Les CMDBs (Configuration Management DataBase) :* ce connecteur n'est généralement pas vu comme un élément de sécurité informatique, pourtant comment gérer les vulnérabilités des systèmes si l'on ne possède pas une vue holistique de ces actifs ? Les connecteurs CMDBs permettent finalement de réconcilier la vue « Actif » avec la vue « Vulnérabilité »
- *Les outils de Pentest et de BugBounty :* le connecteur permettra d'enrichir les informations collectées en amont par des apports contextualisés et liés à un test d'intrusion ou à un test d'exploitation de vulnérabilité
- *Les Orchestrateurs de Sécurité :* Il s'agira ici d'envoyer des informations vers les Orchestrateurs de Sécurité afin qu'ils puissent consolider leur vision des états et enfin appliquer les meilleurs scénarios de remédiation possible
- *Les outils ITSM (Information Technology Service Management) et Helpdesk :* ces connecteurs permettront d'interagir avec les outils de gestion de service IT existants et assureront une intégration en profondeur dans les processus de l'organisation

De nombreux autres types de connecteurs existent généralement dans les solutions CAASM : lien vers les outils de gestion des risques, connexion aux SIEMs, intégration avec les bases de CVEs officielles, etc.

Une solution de type CAASM possède des connecteurs permettant d'absorber ou d'envoyer des informations depuis ou vers les outils déjà déployés.

CAASM – LE PUITS DE DONNÉES ADAPTIF

Le puits de données contenant l'ensemble des données collectées est hautement adaptif, cela signifie qu'il n'est pas limité à un type de données spécifique et que son schéma est adaptable aux besoins actuels et futurs. Ce point est très important car il assure la pérennité du modèle et permettra demain de rajouter des connecteurs pour des usages encore inconnus actuellement !

De plus, l'outil CAASM doit permettre la déduplication des données et assurer leur unicité – par exemple si l'organisation utilise plusieurs scanners de vulnérabilités et que les dits scanners remontent 95% de vulnérabilités communes, il faut nécessairement que l'outil CAASM soit en mesure de repérer ses informations doublonnées et n'affiche qu'une seule fois les vulnérabilités associées à chaque actif.

Enfin, un modèle de corrélation doit permettre d'associer les différents objets et attributs collectés via les connecteurs – par exemple, il faut pouvoir associer automatiquement les actifs gérés au sein de la CMDB avec les vulnérabilités repérées sur ces mêmes actifs via les scanners de vulnérabilités.

Il faut donc comprendre que le puits de données est un élément critique d'une solution CAASM et doit permettre l'adaptation à n'importe quel usage actuel ou futur. De plus, la conservation des données selon un modèle unifié permettra à l'organisation de changer facilement les outils s'exécutant derrière les connecteurs – Par exemple, comme les données sont standardisées, il sera aisé de changer de fournisseur pour le scanner de vulnérabilité sans que l'historique ne soit affecté.

CAASM – LE PORTAIL DE GESTION

Une fois les données récoltées, dédupliquées et corrélées, un portail de gestion permettra de naviguer dans le puits de données. Les interfaces varient en fonction des fournisseurs, mais l'un des plus grands challenges sera de fournir une vision claire des informations, permettant alors de prioriser les actions à réaliser en fonction de l'étude du jeu de données.

Il est donc primordial que l'interface utilisateur soit la plus claire possible et que les dashboards associés soient facilement personnalisables - dans cette optique, l'interface du Français Hackuity est particulièrement remarquable.

Exemple de dashboard CAASM chez l'éditeur Français Hackuity

Le portail doit permettre un usage différencié au travers des différentes équipes, il devra gérer un modèle RBAC afin de constituer des interfaces adaptées en fonction de l'utilisateur. Le portail CAASM devient l'outil unique pour le pilotage des vulnérabilités au sein de l'organisation et permettra de s'affranchir des nombreuses interfaces disparates associées aux différents outils s'exécutant derrière les connecteurs.

Les éditeurs de solutions associés à la pratique CAASM investissent massivement pour le futur de leur plateforme.

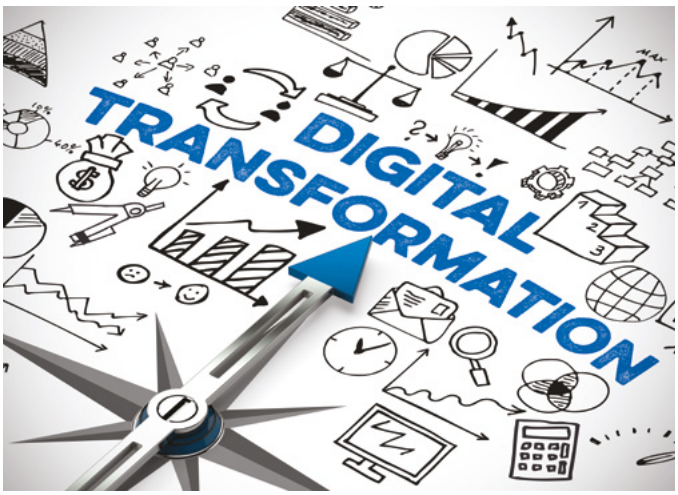
Les futurs enjeux

Les éditeurs de solutions associés à la pratique CAASM investissent massivement pour le futur de leur plateforme, il s'agit, en effet, d'un des domaines les plus innovants dans le monde de la cybersécurité. Nous pouvons considérer que l'adoption à venir du Machine Learning permettra d'enrichir considérablement les scénarios d'usage de ce type de plateforme. Grace au volume des données collectées, nous pourrons repérer certains modèles répétitifs dans l'objectif de créer des règles automatiques d'aide à la décision et d'aide à la priorisation.

Les solutions CAASM permettent de surmonter de nombreux challenges de sécurité liés à la gestion des vulnérabilités, n'hésitez pas à vous renseigner pour comprendre comment cette pratique pourrait aider votre propre organisation.

Merci d'avoir consacré du temps à la lecture de cet article.

> *Sylvain Cortes- Security Evangelist & Microsoft MVP*



Les 4 tendances qui vont bouleverser le business des entreprises

Les réalités physiques et virtuelles remodèlent les expériences humaines et secouent les stratégies et le business des entreprises

Le Continuum du métavers va redéfinir la façon dont le monde interagit. En ce sens, la réalité étendue, la blockchain, les jumeaux numériques et le edge computing, convergent et remodèlent les expériences humaines. Si selon 71 % des dirigeants, le métavers aura un impact positif sur leur organisation, selon 42 %, il s'agira d'une percée ou d'une transformation.

LES 4 TENDANCES À SUIVRE !

Selon le rapport 2022 d'Accenture, voici les 4 tendances technologiques à surveiller de près.

• Le Moi connecté

Les stratégies d'entreprise sont conçues pour l'Internet d'aujourd'hui, monde numérique où les plateformes manquent d'interopérabilité et de portabilité des données. Le métavers et le Web3 von remodeler l'internet : le métavers conduira à un environnement 3D persistant dans lequel se déplacer d'un "endroit" à un autre sera aussi simple que de marcher d'une pièce à une autre.
Selon 95 % des dirigeants, les futures plateformes numériques devront offrir des expériences unifiées, permettant l'interopérabilité des données des clients sur différentes plateformes et espaces.

• Un monde programmable

La 5G, l'informatique ambiante, la réalité augmentée et les matériaux intelligents progressent, et les environnements numériques seront de plus en plus intégrés au monde physique. Ces environnements remodèleront la façon dont les gens s'engagent dans ces deux mondes, physique et virtuel, et redéfiniront tout ce qui y est construit, la façon dont les gens ressentent et interagissent, le contrôle qu'ils exercent sur ces mondes.
Selon 92 % des cadres, les grandes entreprises repousseront les limites du monde virtuel pour le rendre plus réel, ce qui accroît le besoin de continuité et de navigation transparente entre les mondes numérique et physique.

• Au-delà du réel

Les entreprises et les environnements sont de plus en plus soutenus par des données générées par l'Intelligence Artificielle qui reflètent le monde physique. L'IA est au cœur des préoccupations des entreprises, car les entreprises et les consommateurs cessent de considérer ce qui est vrai ou faux pour se concentrer sur ce qui est authentique, non seulement en termes de contenu et d'algorithmes, mais aussi de marque. Le monde virtuel étant sur le point de devenir réalité, il est temps pour les dirigeants de préparer leurs entreprises.
Selon 96 % des dirigeants, leur entreprise s'est engagée à authentifier l'origine de ses données et l'utilisation authentique de l'IA.

• L'Informatique amplifiée

L'émergence d'une nouvelle catégorie de machines permet aux organisations de tous les secteurs de repousser les limites de ce que les ordinateurs peuvent résoudre. L'informatique quantique et l'informatique inspirée par la biologie permettent aux entreprises de résoudre des problèmes qui seraient trop coûteux, inefficaces ou impossibles à résoudre par l'informatique traditionnelle. Les "grands défis" deviennent des opérations banales, et la manière dont les entreprises se concurrencent, apporte de la valeur.
Selon 94 % des cadres, le succès à long terme dépendra de l'exploitation de l'informatique de nouvelle génération pour résoudre des problèmes apparemment insolubles.

Rapport 2022 Accenture- 4 600 dirigeants d'entreprises et experts en technologies dans 23 secteurs et 35 pays

Azure Backup, EXEMPLE D'ARCHITECTURE

Les sauvegardes sont toujours dans le TOP 3 des sujets opérationnels. Pour le Cloud Azure, il existe plusieurs solutions différentes et complémentaires pour réaliser ces opérations. Sous la forme de services PaaS. Voire d'un service « SaaS» pour les bases de données managées. Ce sont des services natifs, disponibles directement dans le portail, qui bénéficient également d'une console de gestion centrale appelée *Backup Center*, élément indispensable pour faire le lien entre tous les sujets de la sauvegarde.

Ces services ont été améliorés ces dernières semaines et proposent maintenant plus d'options avec par exemple, pour le service *Coffre Recovery Service*, la possibilité de planifier plusieurs sauvegardes dans la même journée.

Comme souvent, la solution peut être complétée par des services périphériques Azure pour simplifier et améliorer l'expérience.

Ces 3 services sont *Azure Policy*, des diagnostics avancés pour *Log Analytics* ainsi que l'*Explorateur Azure Resource*. Ils seront présentés dans cet article pour montrer comment ils viennent épauler et donner plus de valeur aux services de sauvegarde.

Présentation

Il y a plusieurs types de sauvegardes sur Azure. Ce qui est abordé dans ce sujet concerne la sauvegarde des ressources. Et plus spécifiquement celle des machines virtuelles. Le sujet est trop vaste pour pouvoir en quelques pages faire une présentation même succincte de tout ce qu'il existe en termes de possibilités pour l'ensemble des autres ressources.

C'est du côté des PaaS que l'on trouve les deux services distincts pour les machines virtuelles. Ces PaaS couvrent plus que les machines virtuelles, voici la liste exhaustive des possibilités.

- Coffre Recovery Services, pour les VM, mais aussi les partages de fichiers, SQL Server dans une VM et SAP Hana dans une VM.
- Coffres de sauvegarde, pour les disques Azure (et par extension, les VM) mais aussi les Blobs et les serveurs Azure Database pour PostGreSQL.

S'il y a pas mal de choses qui rentrent en compte avant de déployer ces PaaS, voici quelques informations qui doivent être connues pour mieux décider de son architecture. Les éléments de base constituants la sauvegarde sont la redondance et les stratégies (fréquence et durée de conservation).

EXPOSITION - TABLES RONDES
ATELIERS - RENDEZ-VOUS BUSINESS

SYMPOSIUM • CONFERENCES • WORKSHOPS •
USE CASES • RENCONTRES ONE TO ONE

IoT+MtoM Embedded

CLOUD DATA CENTER +INFRA

#MtoM / IIoT #Embedded
#Objets connectés
#Réseaux (pan, Lan, LPWAN, 5G, ...)
#Plateformes
#DATA (Edge Computing, Big Data, IA...)
#Cybersécurité

www.salon-iot-mtom.com

#Cloud Hybride
#Open Source
#Cybersecurity
#Plateformes
#Supervision
#Stockage Cloud
#Green IT

www.datacenter-cloud.com

29 et 30 juin 2022

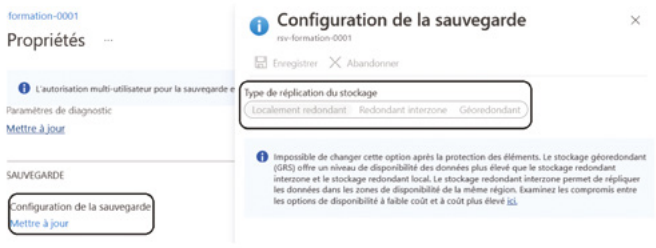
PARIS EXPO- PORTE DE VERSAILLES

@IoTWorldParis1 @salonMtoM

Groupe Cloud et Datacenter Management

Comme pour toutes les études d'architecture, il doit y avoir à ce stade de la réflexion, une volonté d'optimisation des coûts. S'il est évident que fréquence et durée de conservation auront un impact sur le coût (puisqu'elles vont directement impacter le volume de stockage dont dépend en grande partie de la facturation), la redondance qui se « cache » derrière les coffres n'est pas toujours bien connue.

Car le stockage des données est possible selon 3 niveaux de redondance allant de la redondance locale LRS à faible coût, à une redondance géographique, GRS, avec un coût plus important. Cette option n'apparait pas à la création. Elle doit impérativement être revue avant la sauvegarde des premières ressources. Il n'y aura, ensuite, d'autres solutions que de détruire le coffre pour le recréer si la redondance choisie par défaut (GRS) ne convient pas.



Type de réplication de stockage.

Type de réplication de stockage.

Une fois assimilés ces points essentiels et structurants, il est plus facile de décider. Pour en terminer avec la partie théorique, depuis quelques semaines, *Coffre Recovery Service* a été enrichi par un type de stratégies (Stratégie améliorée) en préversion. C'est une belle amélioration avec notamment une fréquence de sauvegarde beaucoup plus élevée. Celles et ceux qui utilisent déjà la sauvegarde Azure trouveront là une belle opportunité. Avant cette nouveauté, la solution pour de multiples backups / jour pour les VM n'était pas très élégante. Puisqu'il fallait utiliser le second service PaaS, *Coffres de sauvegarde*, pour sauvegarder les disques de VM indépendamment de la machine.

Version améliorée de la stratégie.

Version améliorée de la stratégie.

Il y a de fortes chances pour que cet ajout vienne modifier l'architecture de la solution de sauvegarde chez les clients Azure.

Centre de sauvegarde

A ce niveau de la présentation, il manque un maillon essentiel pour une gestion centralisée. C'est ce que propose la console *Centre de sauvegarde*, avec :

- De la gestion d'instances (de ressources), de stratégies, de coffres.
- De la supervision, avec des alertes, de la mesure ou du rapport.
- De la stratégie de conformité.

Il faut faire une parenthèse ici pour préciser ce que sont les deux types de stratégies dont il est question.

- La stratégie de sauvegarde, où sont paramétrées les différentes règles (durée de la rétention, heure de la sauvegarde... etc.).
- La stratégie (*Policy*) Azure qui est un élément de gouvernance. Il va être question de cet important sujet dans la partie mise en œuvre de cet article. Afin de clarifier la présentation, le terme *Policy* est conservé pour la suite.

La console Centre de sauvegarde

La console Centre de sauvegarde

Il est grandement recommandé d'utiliser cette console qui permet toutes les actions sur les fonctionnalités de sauvegarde, et de creuser l'utilisation du menu *Rapports de sauvegarde* qui va rendre de nombreux services ! Comme la détection des anomalies fréquentes ou l'affichage du volume de stockage par VM. Une mine d'or !

Comme pour toutes les études d'architecture, il doit y avoir à ce stade de la réflexion, une volonté d'optimisation des coûts.

Mise en œuvre

Si la mise en œuvre unitaire est une opération assez simple, la solution de sauvegarde doit être pensée dans son ensemble. Les différentes possibilités ainsi que les services périphériques dont il a été question plus haut offrent tellement d'avantages qu'il serait dommage de s'en passer. Pour illustrer ce propos, un exemple d'architecture de sauvegarde pour des machines virtuelles est présenté ci-dessous. Il intègre plusieurs notions.

Avant de rentrer dans le détail, le cas d'usage auquel il va répondre est le suivant :

- Une gestion automatique des sauvegardes pour les ressources existantes.
- Une gestion automatique des sauvegardes pour les nouvelles ressources.
- Des rapports de diagnostics avancés (en plus des rapports de base).
- Une optimisation des coûts avec une sauvegarde différente pour une machine hors production et une machine de production.

Si la mise en œuvre unitaire est une opération assez simple, la solution de sauvegarde doit être pensée dans son ensemble.

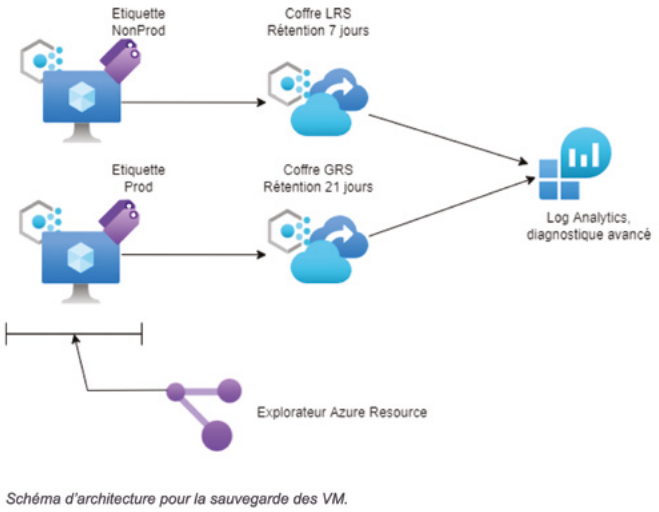


Schéma d'architecture pour la sauvegarde des VM.

Schéma d'architecture pour la sauvegarde des VM.

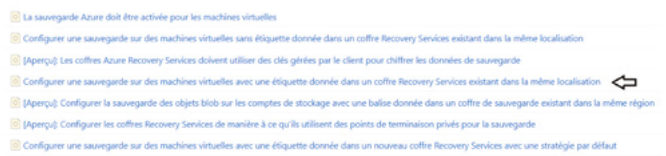
Comme toujours lorsqu'il est question de gouvernance, Azure Policy et les étiquettes (ou tags) sont au centre du sujet. Pour que le schéma d'architecture soit respecté, il faut que les machines virtuelles soient clairement identifiées par une étiquette. Ici, tout est possible.

Soit avec un couple nom valeur Sauvegarde/Prod ou Sauvegarde/NonProd par exemple. Ou par l'utilisation d'une convention pour le nommage du groupe de ressource qui héberge la VM. Peu importe la méthode. Ce qu'il faut retenir, c'est qu'Azure Policy va utiliser ces données et faire les actions automatiquement.

Reste à enrichir le Centre de sauvegarde par le déploiement des paramètres de diagnostic avancé pour le Coffre.

Bien utilisé, il peut ajouter / corriger les valeurs manquantes pour l'existant / le futur mais il peut aussi imposer certaines valeurs. Résultat, chaque VM est correctement identifiée comme Prod ou NonProd.

Pour la suite, c'est toujours du côté d'Azure Policy qu'il faut se tourner. Puisqu'il y a dans les Policy BuiltIn la possibilité d'attacher automatiquement une VM à un *Coffre Recovery Service* existant en se basant sur une étiquette.



Configurer une sauvegarde sur des machines virtuelles avec une étiquette donnée dans un coffre Recovery Services existant dans la même localisation

Comme tout va se faire automatiquement, autant que cela se fasse avec bon sens.

- Une machine étiquetée NonProd se verra attachée à un Coffre localement redondant, avec une rétention de sauvegarde à 7 jours. Ici, c'est un bon compromis entre la sécurité des données et un coût modéré.
- Une machine étiquetée Prod se verra attachée à un Coffre géo redondant, avec une rétention de sauvegarde à 21 jours. Ici, c'est une élévation de sécurité des données et un coût plus important. Mais justifié par le fait que c'est une machine de production.

Reste à enrichir le *Centre de sauvegarde* par le déploiement des paramètres de diagnostic avancé pour le Coffre. Cette opération va ajouter plus de 10 points de diagnostic supplémentaires dans le rapport. De quelle façon ?... toujours et encore par Policy.

Déployez les paramètres de diagnostic du coffre Recovery Services

La promesse de cette architecture est tenue ! Une fois déployée, les machines sont automatiquement sauvegardées, la console de gestion centrale expose des paramètres de diagnostics avancés et l'optimisation financière est au rendez-vous.

Cerise sur le gâteau, l'utilisation de l'outil de requêtes l'*Explorateur Azure Resource* va traiter le sujet des éventuelles ressources en anomalies. Avec un exemple de requête qui retourne toutes les machines qui n'auraient pas le tag (en Anglais dans la requête) nommé Backup.

```
Resources
| where type =~ 'Microsoft.Compute/virtualMachines'
| where isempty(tags.Backup)
| project name
```

Une piste pour affiner encore et encore le sujet.

En résumé, ce qu'il faut retenir : un bon point de départ en 3 étapes

1 / Les sauvegardes Azure sont traitées par plusieurs services PaaS ou SaaS.

2 / Azure Policy permet une automatisation complète des sauvegardes et la garantie d'un service optimal.

3 / Les leviers pour optimiser la facturation sont nombreux, le coût de stockage représente une bonne partie de cette optimisation.

L'utilisation de l'outil de requêtes l'Explorateur Azure Resource va traiter le sujet des éventuelles ressources en anomalies.

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

FRANSEC

SECURING FRANCE FROM CYBER THREATS

13 - 14 Septembre 2022

Paris, France

Pass Gratuit Avec Le Code: ITPRO

Rejoignez-Nous À La Conférence FranSec Les 13 et 14 Septembre !

La 3ème **conférence annuelle FranSec** rassemble plus de **100 leaders de la sécurité informatique** issus des secteurs de la **vente au détail, des produits de grande consommation, de la banque et de la finance, de l'automobile, des services publics, de l'alimentation**, pour deux jours d'échanges d'idées et d'expertises les **13 et 14 Septembre** prochains. Rejoignez-nous à **Paris**, afin d'affiner vos compétences dans les domaines suivants :

- Transformation Digitale et Cyber-résilience
- Le Cyber-environnement Actuel et Comment Améliorer vos Capacités de Sécurité
- Travailler Avec des Tiers pour Améliorer votre Situation en Matière de Cybersécurité
- Réagir à une Surface d'Attaque Croissante
- Mise en œuvre de Stratégies de Sécurité Basées sur les Risques
- Le Facteur Humain dans la Cybersécurité Organisationnelle

CPD CERTIFIED
The CPD Certification Service

Parmi les **intervenants** figurent des RSSI, vice-présidents, responsables de la sécurité informatique chez : **La Banque Postale, Airbus, AXA, Interpol, Total, Suez** et plus encore...

Saisissez cette occasion unique de vous réunir avec des leaders de la cybersécurité de toute la France et de protéger au mieux vos organisations. Consultez le programme et **réservez votre place GRATUITEMENT** en utilisant le code "**ITPRO**" à : **france.cyberseries.io/register/**. Des conditions générales de vente s'appliquent.

Colibris RÉVOLUTIONNE LA RSE !

Comment mesurer, analyser et agir pour une innovation responsable ? Tel est l'objectif de Colibris. Développé par Leasetic, société toulousaine spécialisée dans les solutions digitales éthiques et responsables, Colibris entend donner une nouvelle dimension à la politique RSE des entreprises, notamment leur impact environnemental. Retour sur le sujet avec Emmanuel Rousseau, fondateur de Colibris.

Dédiée à la mesure de la performance économique et environnementale des actifs alloués aux collaborateurs, l'application automatise l'analyse des usages et répond aux objectifs de diminution de l'empreinte environnementale. En outre, Colibris se distingue des autres solutions disponibles par la transversalité de ses modules, qui fournissent une mesure continue.

Colibris se distingue des autres solutions disponibles par la transversalité de ses modules, qui fournissent une mesure continue.

Pourriez-vous présenter l'entreprise Colibris et son actualité ?

Colibris est une application SaaS qui permet de mesurer la performance économique et environnementale des contrats facturés à l'usage, comme la location de PC et Smartphones, les licences logicielles, les imprimantes, les services Cloud et les locations de parc automobile. Elle permet de fournir à chaque collaborateur un rapport individuel, lui permettant d'influer sur son usage et d'agir directement sur son impact environnemental.

EMMANUEL ROUSSEAU

Dans le cadre de notre développement nous venons de signer un accord de partenariat commercial avec la filiale du groupe SPIE, SPIE ICS. Ce partenariat a pour but d'accélérer la mise en place de notre solution conjointe de Numérique Responsable.

Quelle est la mission de Colibris, qu'est ce qui la différencie ?

La mission de Colibris est de proposer une solution indépendante des fournisseurs qui offre à l'entreprise et à chacun de ses collaborateurs les moyens d'être acteur pour atteindre ses objectifs économiques et environnementaux. Les outils existants fournissent des analyses ponctuelles aux Directions des Entreprises.

Colibris fournit à ses clients des analyses continues sur l'ensemble des moyens mis à disposition des collaborateurs pour réaliser leur mission, leur permettant ainsi d'agir continuellement sur leur impact environnemental.

Il est indiqué « qu'avec Colibris les entreprises peuvent mesurer l'empreinte environnementale de leurs outils digitaux », il y a urgence certes, mais comment cela se passe concrètement ?

L'urgence est là, les réglementations se mettent en place mais on demande aux entreprises et à leurs collaborateurs des résultats sans vraiment mettre à disposition les outils dont ils ont besoin pour les atteindre.

Pour nous, le seul moyen de réaliser les objectifs ambitieux de baisse de notre empreinte carbone, est d'associer le collaborateur de l'entreprise et de lui montrer sa capacité à avoir un impact direct.

Le seul moyen de réaliser les objectifs ambitieux de baisse de notre empreinte carbone, est d'associer le collaborateur de l'entreprise.

Avec Colibris, chaque collaborateur pourra choisir entre des matériels neufs ou reconditionnés, adapter l'usage de ses licences à ses besoins réels, partager les meilleures pratiques d'usages et avoir une mesure objective de ses décisions.

> Par Sabine Terrey

Les politiques de retour au bureau dégradent l'expérience collaborateur

Quels sont les réels impacts des politiques de retour au bureau sans flexibilité dans les horaires...

Si 34 % des salariés travaillent aujourd'hui en présentiel 5 jours par semaine, le stress et l'anxiété liés au travail ont atteint un très haut niveau. Ces salariés mécontents du manque de flexibilité sont susceptibles de chercher un nouvel emploi au cours de l'année à venir.

Clivages entre les cadres et non-cadres

Les employés non-cadres sont deux fois plus susceptibles que les cadres de travailler au bureau cinq jours par semaine. « Les dirigeants doivent cesser d'imposer des journées de travail avec des horaires rigides de 9 h à 17 h, et plutôt œuvrer à rassembler leurs équipes autour d'un objectif commun et donner l'exemple. Vous obtiendrez de meilleurs résultats et vos salariés seront plus épanouis si vous leur offrez la possibilité de travailler où et quand cela leur convient le mieux. » commente Brian Elliott Directeur exécutif, Future Forum.

Chute des indicateurs de l'expérience collaborateur

Les indicateurs de l'expérience collaborateur ont baissé pour l'ensemble des salariés. Ainsi pour les salariés en présentiel à temps plein, on relève :

• *Equilibre vie professionnelle et vie privée*

Baisse deux fois plus importante de l'équilibre entre vie professionnelle et vie privée par rapport aux salariés flexibles

• *Environnement de travail*

Baisse 1,6 fois plus importante de la satisfaction globale à l'égard de leur environnement de travail par rapport aux salariés flexibles

• *Stress et Anxiété*

Augmentation 1,5 fois plus importante du stress et de l'anxiété liés au travail par rapport aux salariés en télétravail

• *Femmes et mères actives*

De nombreuses femmes et mères actives souhaitent bénéficier de flexibilité quant à leur lieu de travail : 58% (travailler de manière flexible 3 jours par semaine) et 82% (flexibilité du lieu de travail)

• *Projets d'entreprise flous*

Les salariés sont irrités face aux indications floues et tardives des dirigeants sur l'avenir du travail dans l'entreprise et n'apprécient pas l'employeur non « transparent sur ses projets d'entreprise ».

Flexibilité & Bien-être & Fidélisation

Les discussions sur le retour au travail oublient l'importance de la flexibilité des horaires et du lieu. Aujourd'hui,

- 94% veulent bénéficier d'horaires de travail flexibles
- 79% de flexibilité quant à leur lieu de travail

La rigidité d'emploi du temps nuit à l'expérience collaborateur : stress, anxiété, équilibre vie privée/professionnelle, surmenage.

Il faut prendre en compte la flexibilité des horaires et penser à réduire le nombre de réunions, encourager les équipes à limiter le temps consacré à la collaboration pure chaque jour, et expérimenter rapidement d'autres stratégies.

Source Slack - Future Forum Pulse - 10 818 salariés aux États-Unis, en Australie, en France, en Allemagne, au Japon et au Royaume-Uni - 27 janvier et le 21 février 2022. Enquête menée par Qualtrics

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 :

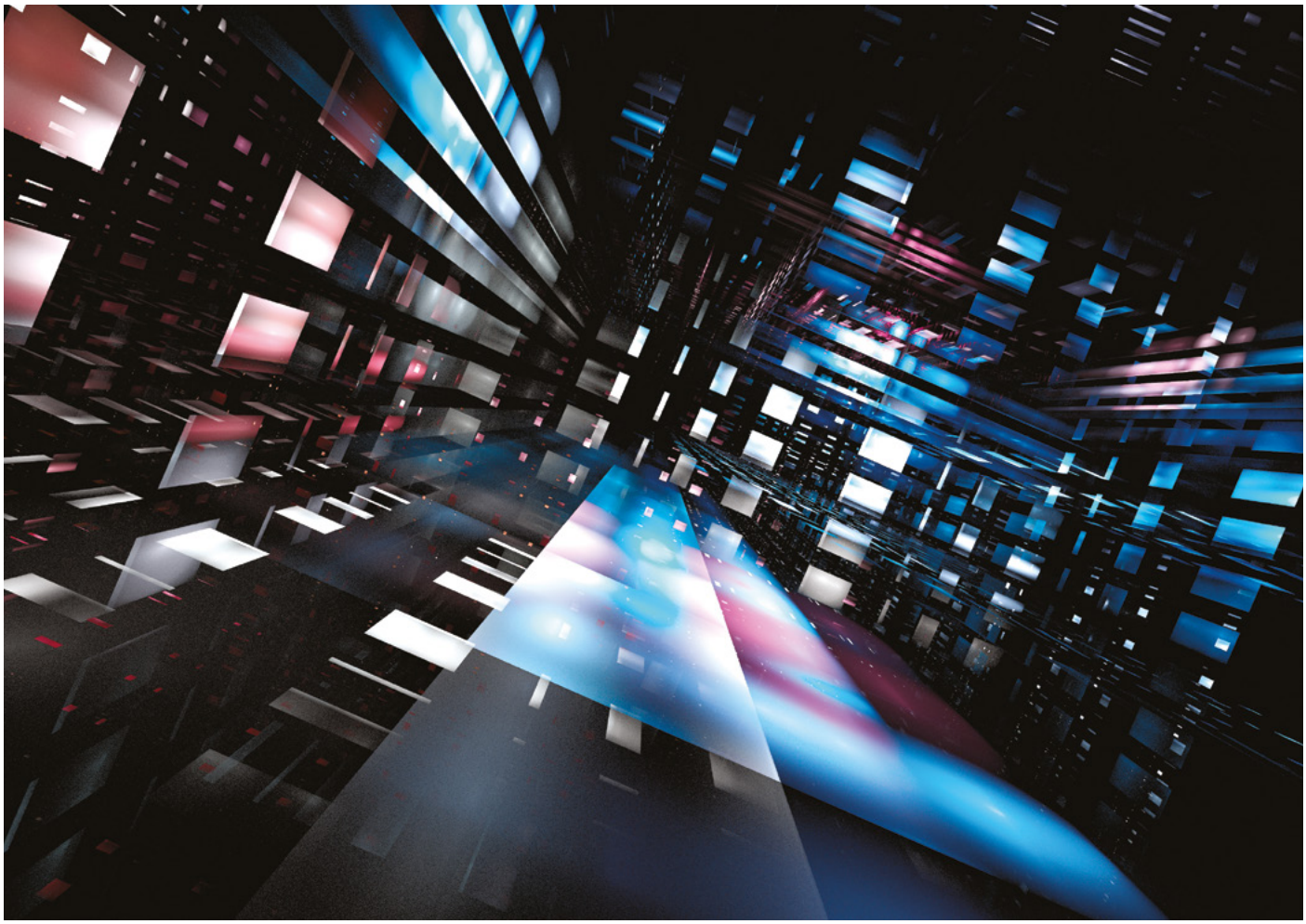
Renvoyez votre bulletin à notre service abonnements :

SMART DSI - ABOSIRIS - Service des abonnements
BP 53 - 91540 Mennecy - France

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

ASKLÉPIAN : DES TESTS D'INTRUSION À 360° GRÂCE À L'IA POUR LUTTER CONTRE LES FAILLES DE SÉCURITÉ

En 2019, l'entreprise Asklépian, référence en matière de sécurité IT et des réseaux, est fondée par Fabien Fernandez. En 2022, face aux cyberattaques de plus en plus perfectionnées, Asklépian engage des moyens pour le développement d'une nouvelle direction opérationnelle en cybersécurité préventive. Les compétences de Délégué à la protection des données (DPO) sont d'ailleurs certifiées par l'AFNOR selon l'agrément CNIL. Décryptage avec Fabien Fernandez.



Numérique, dématérialisation des processus ou documents, interconnexion des réseaux ... tout est fait pour répondre aux enjeux du télétravail et de la mobilité, mais que se passe-t-il du côté de la sécurité, des risques de vol, de modification ou de destruction de données ?

L'audit technique ou du test d'intrusion est une solution qui permet d'éprouver et valider le niveau de sécurité du SI, d'identifier des axes d'amélioration, énonce des recommandations et contribue à l'élévation du niveau de sécurité, dans une démarche constructive et d'amélioration continue.

Ainsi, grâce à l'Intelligence Artificielle, Asklépian propose une série de tests d'intrusions ou audits techniques "nouvelles générations". Cette prestation automatise la réalisation de l'audit et chaque entreprise peut maîtriser ses systèmes d'information à 360°.

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

SMARTDSI

www.smart-dsi.fr

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

Pourquoi la création d'Asklépian en 2019 ?

Pour Fabien Fernandez, il s'agit « d'aider les organisations à mieux s'organiser, définir leur stratégie pour atteindre leurs objectifs, de se servir de la RGPD pour minimiser, optimiser les process tout en sécurisant les données, et de ne pas subir un texte de loi mais en faire une force au service de la rentabilité. »

Et plus précisément, qu'offre Asklépian ?

Nous offrons un accompagnement clé en main à 360°. Ainsi nous accompagnons les organisations (entreprise, association ou collectivité) sur tous les enjeux et volets suivants : juridiques, organisationnels, technologiques, physiques, logiques et documentaires. Notre solution est totalement clé en main ! La technologie que nous utilisons, développée en France, contient l'intégralité des écrans & périphériques nécessaires à l'audit. Nous proposons une solution d'automatisation d'audit.

Asklépian s'engage aussi à une totale transparence : devis, lettre de mission, conditions générales de vente, convention d'audit et contrat, programmation des rendez-vous, réunion formelle de lancement, conseils de sauvegarde... Enfin, Asklépian garantit le respect d'une Charte d'éthique exigeante, les prestations sont réalisées avec loyauté, discrétion et impartialité

Revenons sur le rôle de l'Intelligence Artificielle au service des audits ?

En s'appuyant sur une technologie basée sur l'IA, Asklépian produits tests et rapports en quelques jours. Les entreprises bénéficient d'une connaissance détaillée de l'état de sécurité d'un périmètre défini.

La simulation des attaques informatiques par cette technologie en conditions réelles s'effectue dans le respect des standards (PASSI - Prestataires d'Audit de la Sécurité des Systèmes d'Information - et ISO27001).

Quels sont les différents types de fuites de données ?

On pourrait résumer les 7 types différents de fuites de données : exposition accidentelle sur Internet, accès non autorisé, données en déplacement (transmission en clair via HTTP ou d'autres protocoles non sécurisés), erreur/négligence/problème de mise au rebut ou perte par un travailleur, hacking/intrusion, vol interne et vol physique : les données sont extraites à partir d'ordinateurs, de smartphones ou de tablettes volés.

Un mot sur les différents tests d'intrusion réalisés ?

Parmi les tests réalisés, on peut mentionner les tests d'intrusion externes, internes, Wifi, fuites de données, Média, l'audit empreinte numérique.

FABIEN FERNANDEZ

Enfin, pour effectuer les correctifs et supprimer les failles révélées par l'audit, Asklépian propose des outils de sécurisation pour protéger les populations mobiles et renforcer la sécurité du réseau sur l'ensemble des périphériques & objets connectés.

En résumé, si on devait retenir 5 points clés, quels seraient-ils ?

Les 5 points que l'on peut retenir sont les suivants,

- *Un tarif attractif* permettant à toutes les tailles d'organisation de s'offrir la maitrise et l'anticipation en matière de sécurité informatique, cela permet de réaliser 2 à 3 fois plus de tests par an pour le même prix
- *Notre capacité à intervenir sur tous les volets* complémentaires : juridiques, techniques et organisationnels, documentaires, physiques...

En s'appuyant sur une technologie basée sur l'IA, Asklépian produits tests et rapports en quelques jours.

- *Notre proximité avec le client*
- *Notre volonté de se baser sur l'existant* pour optimiser la conduite du changement en tenant compte des investissements déjà effectués
- Il s'agit d'une valise d'audit *à la pointe de la technologie, made in France*, extrêmement puissante !

Quelles perspectives en 2022 ?

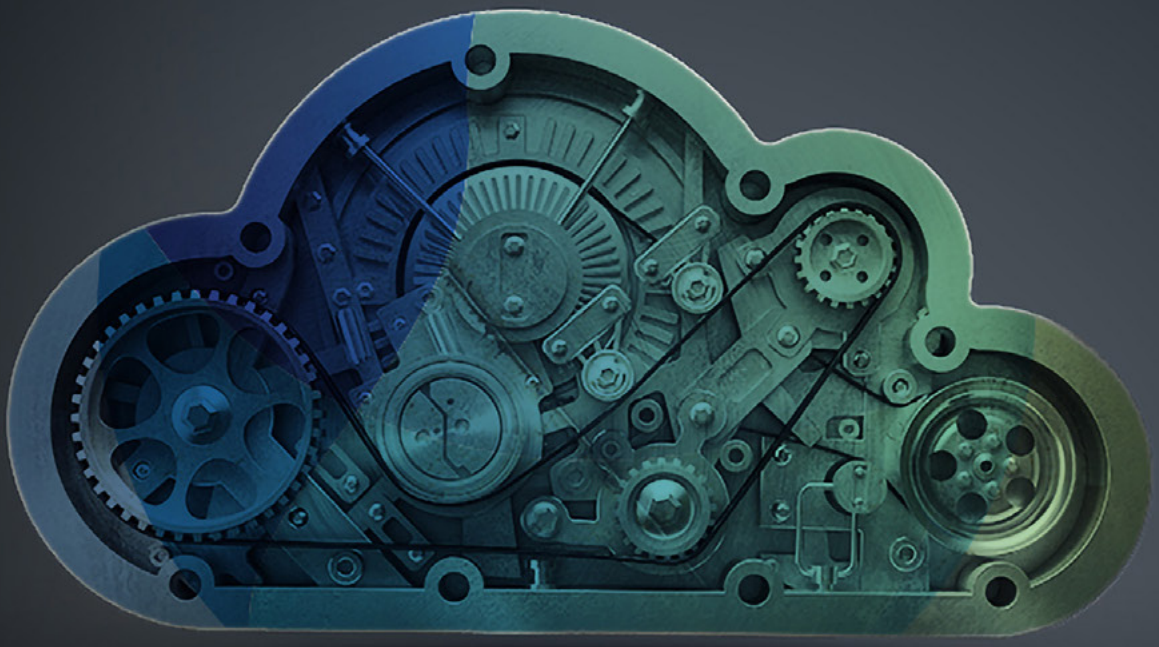
Nous souhaitons poursuivre dans le développement de tests d'intrusion basés sur l'IA, permettre de réduire les coûts et d'obtenir les résultats rapidement et proposer un plan de sécurisation et mise en conformité adéquat et cohérent.

> Par Sabine Terrey

CLOUD EXPO EUROPE PARIS 16 & 17 NOVEMBRE 2022, PARIS PORTE DE VERSAILLES.

PRÉ-INSCRIVEZ VOUS SUR : www.cloudexpoeurope.fr

Repensez les rouages de votre stratégie IT et trouvez les technologies adaptées à vos besoins et à votre organisation.



Cloud, DevOps, Cybersécurity Big Data, IA... toutes ces technologies s'imbriquent et se complètent ! Venir au salon c'est l'occasion unique de retrouver les experts de ces domaines sous un seul et même toit.

Un rendez-vous incontournable avec au programme des tables rondes passionnantes, des conférences spécialisées et des études de cas. Les meilleurs spécialistes et les leaders de l'industrie seront à vos côtés pour vous guider et vous inspirer dans cet univers toujours en mouvement.

Que vous soyez déjà spécialiste du cloud ou en pleine transformation digitale, manager d'une start up ou cadre d'une grande entreprise, le salon est l'allié de choix qui vous permettra d'affiner votre mécanique numérique !

Votre entrée gratuite vous donnera accès aux événements co-organisés : DevOps Live, Cloud & Cyber Security Expo, Big Data & AI World et Data Centre World.

CLOUD EXPO EUROPE

16-17 novembre 2022 Paris Porte de Versailles
www.cloudexpoeurope.fr

CO-ORGANISÉ AVEC

DEVOPS LIVE
CLOUD & CYBER SECURITY EXPO
BIG DATA & AI WORLD
DATA CENTRE WORLD

ORGANISÉ PAR

CloserStill

Traduire le risque IT en risque financier, UN IMPÉRATIF POUR BIEN COMMUNIQUER AVEC LE CONSEIL D'ADMINISTRATION

Il ne passe plus une semaine sans que la presse ne relaie l'actualité d'une entreprise victime d'une cyberattaque et de pertes financières. Dans ce contexte, être en capacité de communiquer avec le board devient un impératif pour le RSSI. En effet, il doit être capable de traduire, c'est-à-dire d'expliquer l'impact potentiel du risque IT sur les résultats financiers de l'entreprise. Un effort de langage nécessaire quand il s'agit de se faire entendre du conseil d'administration. En quoi est-ce essentiel ? Et surtout, comment faire ? Décryptage avec Damien Bénazet, Directeur Technical Account Management chez Tanium.

DAMIEN BÉNAZET

Pour le RSSI, communiquer avec le board s'apparente à de la communication externe

Le conseil d'administration a un pied à la fois dans et hors de l'entreprise : il ne dispose généralement pas des compétences particulières en cybersécurité. C'est pour cela que le RSSI doit adapter son discours comme s'il s'agissait d'une communication externe. Car communiquer en tant que RSSI auprès du board, c'est également rendre compte aux actionnaires. Cet effort de traduction est nécessaire car il permet au RSSI d'asseoir sa crédibilité et d'établir un lien de confiance auprès des membres du conseil d'administration. C'est de cette manière qu'il pourra justifier les investissements qu'il souhaite réaliser, qu'il s'agisse de l'achat d'un outil, ou bien du recrutement de moyens humains.

L'enjeu, pour le RSSI, est donc de réussir à traduire le risque cyber en impact opérationnel et financier, compréhensible par le conseil d'administration et par les actionnaires.

Pour ce faire, le RSSI doit s'appuyer sur des données fiables, obtenues en temps réel et mesurables sur la totalité de son système d'information. Il faut également qu'il puisse disposer d'éléments de contextualisation par rapport au secteur économique de l'entreprise. En effet, un indicateur de risque n'aura pas la même importance d'un secteur d'activité à un autre. Par exemple, certaines entreprises du monde industriel sous-estiment le risque sur leur système d'information car elles mettent la priorité sur leur chaîne de production, alors qu'une entreprise du tertiaire y consacrera toute son attention. Toutefois, lorsque le RSSI évoque le risque auprès du board, il doit pouvoir s'appuyer sur des indicateurs business compréhensibles de tous.

Traduire le risque IT en impact financier

Les membres d'un board ont une approche globale du risque mais ne se soucient pas des implications précises comme un patch manquant sur un poste de travail ou un serveur. L'enjeu, pour le RSSI, est donc de réussir à traduire le risque cyber en impact opérationnel et financier, compréhensible par le conseil d'administration et par les actionnaires.

Les RSSI ont conscience de l'importance de la disponibilité des systèmes, à savoir la capacité à délivrer ou produire de la valeur quotidiennement. Assurer la disponibilité des systèmes est l'un des enjeux majeurs de la sécurité informatique, car ils permettent à l'entreprise d'accomplir le métier pour lequel elle existe. C'est sur cet axe qu'il faut communiquer : primordiale pour l'organisation, la disponibilité est compréhensible par toutes les équipes et encore plus au sein du conseil d'administration.

Pour être en état de communiquer efficacement avec le board, le RSSI doit également travailler avec les équipes métier, avec sa direction des risques internes, pour être capable de chiffrer et de traduire ce risque cyber en valeur monétaire. En informant le board sur le niveau de risque, en s'appuyant notamment sur cette notion de disponibilité, le RSSI doit continuer à guider les membres afin que les décisions visant à remédier à ces risques soient faciles à prendre. Aussi, il doit être capable de leur donner une bonne visibilité sur le niveau de risque. Le tout avec des données fiables, tangibles et un langage compréhensible.

Par exemple, quel serait le coût pour l'entreprise si une chaîne de production s'arrête pendant X heures car ses endpoints sont hors service suite à une vulnérabilité issue d'un patch manquant ? Cet effort de traduction est essentiel car seul l'impact sur le business importe pour les membres du conseil d'administration. Pour tout RSSI, parler dans un langage simple, contextualisé par rapport à son secteur est plus que jamais nécessaire. Sans cela, les entreprises continueront à subir des pertes financières qui auraient pu être évitées.

Lorsque le RSSI évoque le risque auprès du board, il doit pouvoir s'appuyer sur des indicateurs business compréhensibles de tous.

0365
SÉCURISER VOTRE TENANT FACILEMENT

La mise en place d'un environnement 0365 est bien souvent guidée par l'activation des couches applicatives telles que la messagerie, les outils de collaborations, mais, dans une moindre mesure par les aspects de sécurisation, qu'il s'agisse des identités ou des données. Un peu comme si certaines entreprises considéraient que le fait d'utiliser nativement les services de Cloud de Microsoft se révélait être un gage d'inviolabilité.

Adapter un telle posture c'est en réalité s'exposer à un nombre important de risques qui devraient être pris en compte dès l'ouverture des services. Mais comment connaitre les innombrables paramétrages sans finalement contraindre les usages ou sans être sûr de ne rien oublier ? Et si la sécurisation d'un tenant 0365 n'était pas finalement une activité régulière ? plutôt qu'une addition de paramétrages à un instant précis ?

UN DÉFI POSÉ AUX ENTREPRISES

Nous le savons tous, exposer ses services sur Internet c'est augmenter les risques liés au piratage mais c'est aussi pouvoir bénéficier des services de protection et de sécurité que votre propre entreprise ne pourrait jamais acquérir.

C'est bénéficier, sans pour autant en avoir l'expertise, des connaissances des services de sécurité Microsoft. Avouez qu'il serait dommage de ne pas en profiter. Or, la plupart des consultants sécurité que j'ai croisés sont la plupart du temps, extrêmement pertinents dès lors qu'il s'agit de parler d'intrusion, de faille de sécurité logicielle, de règles de pare-feu etc. mais le sont beaucoup moins sur la partie applicative (Exchange Online, Teams, Sharepoint, One drive etc.). Or là aussi, les risques de pertes de données et d'usurpation d'identité existent bel et bien.

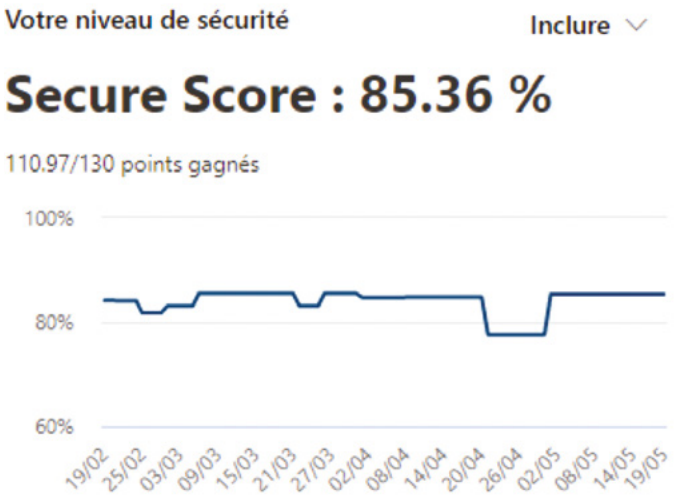
Le défi est donc le suivant : comment, sans nécessairement faire appel à des spécialistes applicatifs, sécuriser de façon pérenne, son environnement 0365 mais surtout comment expliquer tout cela dans un article de quelques pages

Les 4 principes de base que vous devez adopter sans hésiter, et qui ne concernent que l'accès à vos services sont les suivants :

1. *Recourir systématiquement à la mise en place d'un second facteur d'authentification* pour tous les utilisateurs et plus particulièrement pour les comptes ayant des rôles d'administration dans le tenant. https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks
2. *Mettre en place des règles d'accès conditionnel* pour empêcher des connexions intempestives depuis des emplacements géographiques non souhaités. https://docs.microsoft.com/fr-fr/azure/active-directory/conditional-access/overview
3. *Contrôler l'accès à vos services Cloud* par des périphériques que vous maitrisez. https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-register
4. *Mettre en place des comptes de services de secours* notamment si vous utilisez des domaines fédérés (https://docs.microsoft.com/fr-fr/azure/active-directory/roles/security-emergency-access)

Malheureusement, ces quatre mesures ne suffiront pas car même si vous avez renforcé l'accès à vos services, certains paramétrages applicatifs pourraient vous exposer à une fuite importante de données. Microsoft met en place un certain nombre de règles par défaut qui ont pour vocation de sécuriser dirons-nous « moyennement » vos services. Reste à votre charge de revisiter ces applications et de renforcer leur protection. Mais comment faire si vos équipes ne sont pas expertes sur Exchange, Sharepoint Online, Onedrive, PowerBI, etc...

La solution que propose Microsoft est de vous présenter un score de sécurité (https://security.microsoft.com/securescore?viewid=overview) portant à la fois sur la sécurité des identités et celle des données. Ce tableau de référence vous permettra de vérifier régulièrement la posture de sécurité de votre tenant en vous affichant un score comme l'illustre la figure suivante.

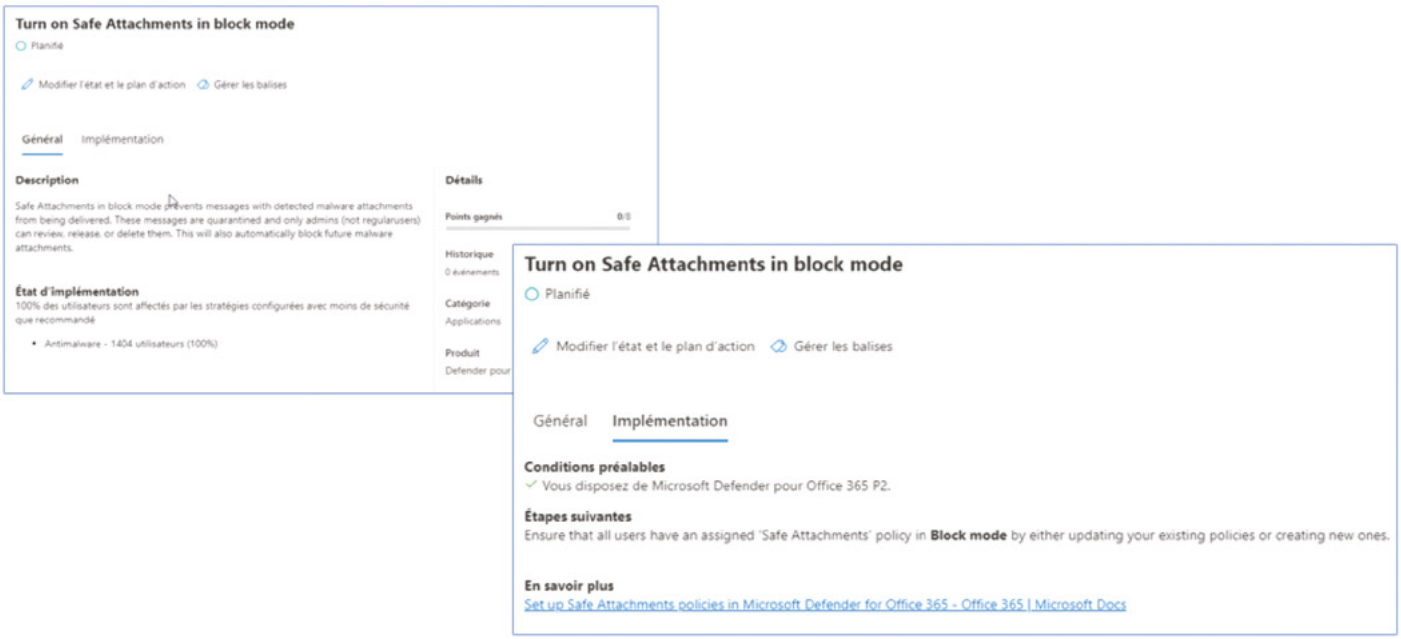


Comme vous pouvez le constater, ce score peut donc varier au fil du temps. C'est le cas si vous ouvrez de nouveaux services ou si de nouvelles règles de sécurité sont à mettre en place . Son affaiblissement par exemple peut être lié à l'ajout de nouveaux utilisateurs pour lesquels un second facteur d'authentification n'a pas été encore activé. Le Secure Score est donc d'une analyse « vivante » de votre tenant que vous devez regarder régulièrement et que vous devez tenter d'améliorer.

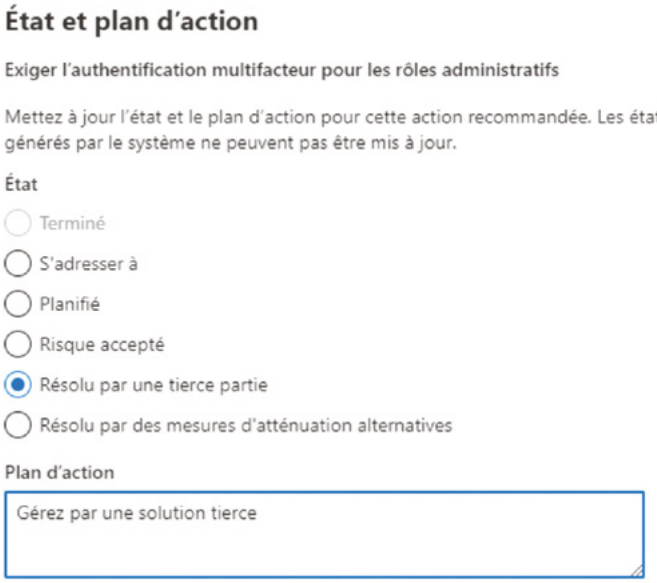
Comme nous l'avons précisé, sécuriser une application que l'on ne maitrise pas forcement n'est pas chose facile. Mais sur ce point précis, l'application Secure Score s'en tire plutôt bien.

Le principe se base sur un système de points et sur des recommandations à mettre en place. Pour rapidement sécuriser votre tenant, je vous engage donc à mettre place les recommandations qui vous feront « gagner » le plus de points. Dans celles-ci, vous trouverez notamment comme recommandé dans les 4 mesures précédemment citées, la mise en place systématique du MFA.

L'outil est plutôt bien conçu car pour chaque mise en place d'une recommandation, l'interface vous indiquera en quoi consiste la recommandation, mais également comment la mettre en place. L'interface vous informera également sur le niveau de licence dont vous devez disposer pour activer cette fonctionnalité.



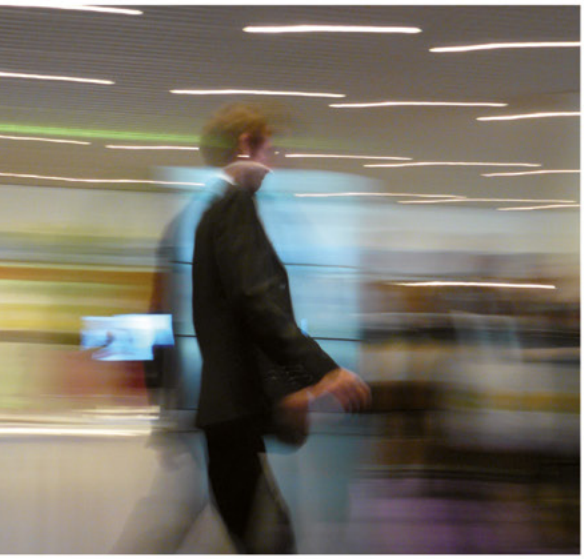
Dans certains cas, l'activation de certaines fonctionnalités n'est pas possible ou peut être gérée par des solutions tierces comme par exemple l'authentification Multi-Facteurs. Dans ce cas, il est possible d'indiquer dans l'interface que le risque est géré par une tierce partie comme le montre la figure suivante .

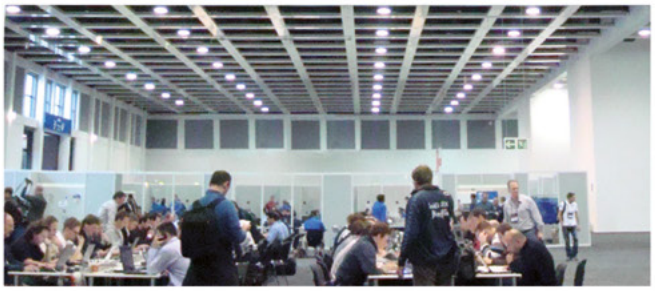


Les statut possibles pour chaque recommandation que le Secure Score vous proposera sont les suivants :

- **À traiter** - Vous reconnaissez que l'action d'amélioration est nécessaire et prévoyez de la traiter à un moment donné dans le futur. Cet état s'applique également aux actions qui sont détectées comme partiellement, mais pas complètement achevées.
- **Planifié** - Des plans concrets sont en place pour réaliser l'action d'amélioration.
- **Risque accepté** - La sécurité doit toujours être mise en balance avec la convivialité, et toutes les recommandations ne fonctionneront pas dans votre environnement. Si tel est le cas, vous pouvez choisir d'accepter le risque, ou le risque restant, et ne pas mettre en œuvre l'action d'amélioration. Vous ne recevrez pas de points, mais l'action ne sera plus visible dans la liste des actions d'amélioration. Vous pouvez consulter cette action dans l'historique ou l'annuler à tout moment.

Le principe se base sur un système de points et sur des recommandations à mettre en place.





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

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

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

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

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

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

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

iTPro.fr

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

- **Résolu par une tierce partie et Résolu par une autre mesure d'atténuation** - L'action d'amélioration a déjà été traitée par une application ou un logiciel tiers, ou par un outil interne. **Vous gagnez les points que vaut l'action**, de sorte que votre score reflète mieux votre posture de sécurité globale. Si un outil tiers ou interne ne couvre plus le contrôle, vous pouvez choisir un autre statut. Gardez à l'esprit que Microsoft n'aura aucune visibilité sur l'exhaustivité de la mise en œuvre si l'action d'amélioration est marquée comme l'un de ces statuts.

POURQUOI LE SECURE SCORE EST-IL PERTINENT ?

L'utilisation du Secure Score est pertinent là aussi pour 4 raisons majeures.

1. **La première raison** est qu'il peut adresser les petites et moyennes entreprises qui ne disposent ni d'expert applicatif, ni d'expert en sécurité. Grâce à son interface guidée, il permettra aux PME PMI de renforcer rapidement leur sécurité sans pour cela faire appel à des sociétés spécialisées.
2. **La seconde raison** tient dans le fait que les équipes en charge de la sécurité au sein des entreprise peuvent rapidement obtenir un statut des recommandations en place et notamment, celles qui restent à déployer. Elles peuvent contrôler le niveau de sécurisation des applications sans en connaitre les moindres détails et demander aux équipes en charge des applications pour quelles raisons certaines mesures de sécurité n'ont pas été déployées.
3. **La troisième raison** est que l'outil permet une analyse constante de la situation et qu'en fonction de l'activité du Tenant (ouverture de nouveaux services, création de nouveaux utilisateurs, activation de nouvelle fonctionnalité etc.) sa situation sera réévaluée.
4. **La quatrième raison** est que les recommandations proposées sont issues du département de sécurité de Microsoft qui, pour le coup est le mieux placé pour définir des recommandations de sécurité pour Office 365.

Le Secure Score est donc un outil fort utile pour quiconque doit surveiller le niveau de sécurisation de son tenant de façon ponctuelle mais aussi régulièrement.

Je ne saurais trop vous conseiller de vous y intéresser de plus près.

Peut-être allez-vous y découvrir des mesures urgentes à prendre en compte.

Le Secure Score est donc un outil fort utile pour quiconque doit surveiller le niveau de sécurisation de son tenant.

Laurent TERUIN / http://Workingtogether.fun

CONGRÈS & CONFÉRENCES

CENTRE DE CONGRÈS RIVE MONTPARNASSE

Plus d'informations sur **www.metadays.fr**

METADAYS

SAVE THE DATE

LE PREMIER RENDEZ-VOUS B2B CONTENU & BUSINESS

DU MÉTAVERS EN FRANCE

29 30 NOVEMBRE 2022

500 PARTICIPANTS **80** SPEAKERS **40** PARTENAIRES **2** JOURS DE CONGRÈS

PADOK : « FAIRE DU CLOUD ET DE L'INFRASTRUCTURE, UN VÉRITABLE ACCÉLÉRATEUR BUSINESS »

Spécialiste des enjeux d'infrastructure, de Cloud et de cybersécurité, Padok se positionne comme acteur majeur du Cloud en France, 4 ans après sa création par Aurore Malherbes et Clément David, les cofondateurs. Interview d'Aurore Malherbes, CTO et co-fondatrice de Padok.

Pourriez-vous nous présenter l'entreprise Padok ?

Créée fin 2018, Padok est une startup spécialisée dans le Cloud apportant une réponse technique et technologique aux enjeux d'infrastructure et de cybersécurité des grandes entreprises, PME et startups.

Ses cofondateurs, Aurore Malherbes, Clément David, CEO, et les 80 padokiens qui composent l'équipe se donnent pour mission de faire du Cloud et de l'infrastructure un véritable accélérateur business.

Padok a des contrats de partenariat avec tous les principaux Cloud providers : Amazon, Google, Microsoft, OVH et Scaleway. Les experts DevOps, Cloud et cybersécurité de Padok définissent, construisent et améliorent les infrastructures de leurs clients. Les missions vont de l'audit à l'infogérance en passant par la migration, la construction et la sécurisation des infrastructures cloud. Ils utilisent des technologies de pointe telles que Kubernetes, ArgoCD, GitlabCI, etc. Padok a notamment construit les infrastructures Cloud du Prêt Garanti par l'État (PGE) et compte parmi ses clients ManoMano, Ornikar, Botify mais aussi Thalès, la BNP et Total.

Qu'est-ce qui vous différencie ?

Les clients viennent chercher chez Padok deux choses principalement :

- L'excellence technique : nous avons une forte expertise sur les technologies modernes telles que Terraform et Kubernetes. Et nous sommes partenaires de tous les plus gros cloud providers pour garantir une vraie neutralité : AWS, GCP, Azure, OVHcloud et Scaleway.
- Le respect des délais : notre méthodologie et culture nous permettent de délivrer très rapidement et efficacement et ainsi garantir le respect des délais.

Nous travaillons en étroite collaboration avec les équipes internes pour transmettre ce que l'on sait, fait et former les salariés à l'utiliser.

Et dès le début de la collaboration, ils découvrent et apprécient deux autres points différenciants de l'offre Padok:

- DevX : nous construisons ou améliorons des infrastructures en collaboration avec les développeurs du client pour nous assurer qu'elles soient conçues pour leur faire gagner le plus de temps possible.
- L'accompagnement humain et sur mesure : nous travaillons en étroite collaboration avec les équipes internes pour transmettre ce que l'on sait, fait et former les salariés à l'utiliser.

Vous venez d'obtenir la certification HDS, qu'est-ce que cela implique désormais ? qu'est-ce que cela va changer ?

La santé est pour nous synonyme de projets qui ont du sens et un fort impact. C'est une certification difficile à obtenir, ce qui fait qu'il y a peu d'acteurs sur le marché. Nous pensons que notre capacité à faire de l'agile avec un point d'attention tout particulier sur le respect des délais va aider les entreprises du secteur médical à évoluer plus rapidement. Les hôpitaux, groupes pharmaceutiques, laboratoires sont, pour la plupart, en retard par rapport au reste des entreprises sur les sujets de transformation numérique du fait de leurs contraintes techniques et réglementaires (sécurité, maîtrise des données...).

AURORE MALHERBES

Notre expertise technique du cloud va considérablement les aider à migrer sans risque, à accélérer leur transformation numérique. Nous sommes également ravis de pouvoir créer une vraie synergie avec Hokla, autre entreprise du groupe Theodo, spécialisée dans la MedTech.

Votre stratégie pour 2022 ? Perspectives ?

Nous visons d'être 100 padokiens d'ici la fin de l'année 2022 avec un chiffre d'affaires de 9 millions d'euros. Nous allons continuer de développer notre activité cybersécurité car c'est un enjeu essentiel pour nous, nos clients et leur migration cloud. Et après la santé, nous allons nous positionner sur d'autres domaines de compétences.

Chaque marché a besoin d'avoir des interlocuteurs qui comprennent leurs spécificités et contraintes sur le cloud.

Chaque marché a besoin d'avoir des interlocuteurs qui comprennent leurs spécificités et contraintes sur le cloud. Nous allons donc nous spécialiser de plus en plus pour y répondre au mieux : nos priorités seront le secteur public, les banques et services financiers, ainsi que l'e-commerce, etc.

> Par Sabine Terrey

Se réunir moins souvent mais faire plus !

N'est-il pas temps de changer quelques mauvaises habitudes liées aux réunions, pour se concentrer sur l'essentiel et accomplir davantage ?

Les entreprises doivent repenser les opérations, méthodes de travail et tirer parti des leçons pour innover. Modifier la manière dont sont menées les réunions impactera la productivité.

Des actions simples pour faire la différence

Si le passage à un modèle de travail hybride est perçu comme une opportunité, outre les changements à grande échelle, ce sont les actions simples qui font la différence. Quelques recommandations :

Adopter des pratiques simples et efficaces pour améliorer les réunions

- Planifier des réunions de 25 ou 50 minutes en prenant en compte un retard de 5 à 10 minutes par rapport à l'heure du début de la réunion
- Indiquer clairement l'objectif et le programme de la réunion sur l'invitation
- Reconsidérer la nécessité des réunions régulières et récurrentes

Identifier et remettre en cause la nécessité des réunions pouvant être remplacées par des modes de travail asynchrones

l'e-mail, le chat, le partage de documents ou la révision de ceux-ci hors ligne.

Pratiques expérimentales

Pour suivre l'efficacité des changements apportés aux réunions, Verizon Business a analysé les habitudes de réunion d'une équipe d'environ 150 employés pendant un mois. Des enquêtes quotidiennes et hebdomadaires ont été envoyées aux participants pour un feedback continu.

Les résultats démontrent l'impact des petits changements :

- Les nouvelles méthodes de gestion des réunions ont amélioré l'efficacité générale de ces réunions - 90%
- Un sentiment d'être plus à l'aise pour travailler via la méthode de travail asynchrone (e-mail, outils de collaboration et partage de documents) - 83%
- Moins de perte de temps à assister à des réunions où la participation en direct n'est pas requise.

Les 4 étapes pour modifier la façon dont le travail est effectué

Voici 4 axes pour identifier, mettre en œuvre et prendre en charge des actions simples

- **Joindre le geste à la parole**
Garantir un soutien par un leader respecté, dès le départ.

- **Concevoir de l'intérieur**
Comprendre les difficultés et arriver à de meilleures méthodes au sein des équipes ciblées pour un changement.

- **Faciliter les choses**
Créer et recréer des outils de support pour gérer la mise en œuvre et mesurer l'efficacité.

- **Réitérer en cours de route**
Créer des cycles de feedback réguliers et fréquents pour soutenir l'adaptation continue des modes de réunion et des outils de support.

L'étape suivante est la mise à l'échelle.

Source Livre blanc Verizon Business & Boston Consulting Group


STORMSHIELD
Le choix européen de la cybersécurité
Partenaire de confiance
pour
sécuriser vos
infrastructures
opérationnelles
IT
OT
www.stormshield.com

METSYS

Libérez-vous de la gestion de votre cybersécurité et de vos environnements cloud !

Centre Opérationnel de Cybersécurité

Optez pour un dispositif organisationnel et technique afin d'assurer la supervision de la sécurité informatique de votre entreprise et de garantir une intervention rapide en cas d'incident ou d'attaque.

Services Managés Cloud

Externalisez vos services d'infrastructure, d'infogérance et de support. Bénéficiez d'une écoute 24/7/365 et d'une garantie de transparence sur les prestations tout en maîtrisant votre budget.

Faites appel à nos experts

contact@metsys.fr

www.metsys.fr

Paris - Rennes- Nantes - Tours- Bordeaux - Toulouse - Aix-en-Provence - Lyon - Strasbourg - Lille