# RAPPORT

## 7ème Edition du séminaire de sensibilisation à la Cybersécurité

ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

# Externalisation des Systèmes d'information et enjeux de cybersécurité

12 NOVEMBRE 2019

# Table des matières

# Note de Présentation

L'externalisation ou l'outsourcing, consiste pour une organisation à confier à des partenaires extérieurs, la réalisation de tout ou partie des activités qu'elle réalisait préalablement en interne. Quand il s'agit d'activités liées aux systèmes d'information, cette pratique porte notamment des noms comme infogérance, Tierce Maintenance Applicative ou cloud computing (informatique en nuage). Il s'agit de démarches pratiques largement tolérées, voire même souvent inscrites dans les stratégies de développement des entreprises privées et de certains organismes publics et Infrastructures d'Importance Vitale.

L'infogérance peut être globale et concerner l'intégralité des composantes du système d'information, ou partielle et se limiter à certaines activités comme le développement, l'exploitation ou la maintenance d'applications, ou encore l'hébergement, la fourniture de matériel et logiciels ou la supervision du système d'information.

Le Cloud Computing peut être considéré comme une extension naturelle de l'offre d'infogérance. Il est associé à la virtualisation et aux solutions IaaS (Infrastructure as a Service), PaaS (Platform as a Service) et SaaS (Software as a Service). On peut différencier quatre types d'implémentation partant du cloud privé au cloud public en passant par les cloud hybride et communautaire. Chacune de ces implémentations désigne un degré plus ou moins élevé en termes d'externalisation et de dépendance vis-à-vis du prestataire.

Le recours à l'externalisation est généralement entrepris dans l'objectif de :

***Réduire les coûts d'investissement et de fonctionnement des systèmes d'information :***

Les économies d'échelle réalisées grâce aux sociétés d'infogérance permettent aux organisations de tirer profit de la mutualisation des moyens et ainsi de baisser leurs coûts informatiques. A travers un contrat d'infogérance adapté à ses besoins, une organisation pourra dépenser ce qu'elle consomme réellement et donc pourra éviter les dépenses imprévues et mieux planifier son budget. De ce fait, les coûts fixes liés à l'informatique sont évités et ne restent que les coûts variables. De plus les risques inhérents au surinvestissement et sous-investissement sont transférés vers le prestataire.

***Se consacrer à son cœur de métier :***

Dans un environnement hyper connecté, les organisations sont constamment à la recherche de performance et d'optimisation. Le rythme toujours plus élevé des échanges et des mutations économiques impose des

structures plus spécialisées et très réactives. Dans ce cadre, les fonctions qui demandent des qualifications particulières qui sortent du cœur du métier de l'organisation ou qui sont moins stratégiques, sont confiés à des prestataires externes. A ce titre l'infogérance permet d'une part, de profiter de compétences et de spécialistes dans les métiers des technologies de l'information aptes à mettre en œuvre et maintenir des solutions technologiques en phase avec les besoins de l'organisation. Et d'autres part, de gagner en termes, de temps et de souplesse en se focalisant sur le métier de base de l'organisation.

***Faire évoluer le système de manière agile:***

Pour obtenir un système d'information agile, il y'a lieu d'équilibrer au mieux la balance entre les besoins liés au développement de la valeur de l'entreprise ou de l'organisation et la consommation de ressources pour y arriver. Dans le cadre d'une politique d'externalisation, le prestataire sera en mesure de proposer une offre adaptée qui pourra évoluer à la hausse ou à la baisse en fonction des besoins ponctuels permettant à l'organisation de réagir rapidement et d'une manière efficiente à de nouveaux besoins métier

***Bénéficier de l'expérience du prestataire :***

En matière d'infogérance, le prestataire est en position de maitriser son métier grâce à son expertise, il est en mesure de proposer des solutions à jour, fiables et performantes. Les organisations désireuses d'augmenter la qualité de service et optimiser les coûts, peuvent ainsi se tourner vers l'infogérance plutôt que d'investir pour améliorer la qualité des services informatiques en interne.

Il ressort des objectifs du recours à l'externalisation que les motivations derrière cette décision sont d'ordre technique, à travers la maitrise de la complexité et le recours à des experts dans leurs domaines, mais également économiques dans la mesure où l'externalisation permettrait une meilleure maitrise des coûts. Toutefois, il ne faudrait pas négliger l'importance de la prise en compte des risques face à des bénéfices immédiats. Il s'agit de risques opérationnels, réglementaires et surtout de sécurité.

***Risques et précautions à prendre :***

Les risques opérationnels sont étroitement liés à la perte du savoir-faire en interne et à la perte du contrôle de l'activité. Ainsi, une situation de dépendance peut se créer entre le sous-traitant et le donneur d'ordre.

Les aspects réglementaires et juridiques constituent un point important qu'il convient de considérer avant de confier tout ou partie de son système d'information à un partenaire externe. Il faut d'abord pouvoir s'assurer que ce dernier se conforme rigoureusement aux

lois et aux réglementations applicables. Ensuite, même en ayant intégré ces aspects dans la réflexion préparatoire à toute externalisation, il reste néanmoins la question du contrôle de l'activité lorsque le prestataire est localisé dans un pays tiers où l'on ne dispose d'aucun pouvoir contraignant.

Enfin, les risques qui semblent aujourd'hui les mieux compris sont ceux liés à la sécurité des systèmes d'information. En effet, des sous-traitants peuvent avoir accès à des informations à caractère sensible (commerciales, techniques, financières, etc.) dont la divulgation consciemment ou inconsciemment à des tiers, peut avoir des conséquences néfastes pour l'organisme concerné. Aussi, les risques liés à la disponibilité ou même à l'intégrité des données traitées dans les systèmes externalisés peuvent s'avérer difficilement maitrisables chez un prestataire externe.

Dans la même optique, l'infogérance d'un système d'information peut nécessiter des accès à distance à l'ensemble ou partie du SI ce qui peut être à l'origine d'intrusions et de vol de données confidentielles. De plus, la mutualisation des données ou des applications avec d'autres clients représente un risque important si le prestataire ne met pas en place les cloisonnements nécessaires entre les environnements de chaque client.

Dans un passé relativement récent, l'externalisation était un privilège réservé aux grandes entreprises jouissant de moyens et infrastructures importantes. Aujourd'hui en revanche, avec les progrès technologiques et la réduction des coûts du matériel et des infrastructures de télécommunication, il est désormais possible, voire avantageux, de pouvoir profiter de cette solution, même au sein des structures de taille plus modeste. Aussi, parmi les nombreux secteurs qui font aujourd'hui appel à l'externalisation, ceux de la banque et de l'assurance représentent une majorité. Le secteur public n'est pas exclu de la tendance. On y remarque d'ailleurs un intérêt croissant pour les offres en Cloud.

Malgré tous les risques précités, l'externalisation est devenue en quelques années une tendance en vogue à laquelle de nombreuses structures ont déjà eu recours ou envisagent de le faire prochainement. En effet, externalisation et sécurité ne sont pas toujours contradictoires. Le recours à un prestataire peut s'avérer dans certains cas un choix souhaitable notamment, lorsque les ressources financières ou les compétences disponibles en interne sont insuffisantes. Allier externalisation et sécurité suscite de nombreuses questions auxquelles les responsables des systèmes d'information doivent apporter une réponse afin de maitriser les risques tout en tirant profit de cette évolution technologique :

A qui confier son système d'information ? Quel prestataire serait en

mesure de faire valoir sa capacité à procurer des services de sécurité qui permettent d'assurer la confidentialité, la disponibilité et l'intégrité des données hébergées.

Quelles données peut-on externaliser ? La réglementation en vigueur au Maroc stipule, entre autres, que les données sensibles doivent être obligatoirement hébergées sur le territoire national. Ce qui induit pour les organisations le besoin fondamental de mettre en place un projet de classification des données et une démarche d'analyse de risque pour définir exactement quelles sont les données susceptibles d'être externalisées de celles qui appellent un traitement particulier.

Quel impact sur l'entité ? Il s'agit notamment, de l'impact sur l'organisation interne de l'entité et du traitement à réserver à l'existant informatique ainsi que de la problématique de réversibilité en cas de ré-internalisation des systèmes et services préalablement externalisés.

Tant de questionnements et bien d'autres qui doivent constituer des éléments de prise de décision susceptibles de permettre d'allier à la fois le besoin d'externaliser à celui d'assurer la protection du patrimoine informationnel sensible des organisations.

Pour apporter un éclairage à ces questions et disposer d'éléments susceptibles d'aider à la maitrise des problématiques liées à l'externalisation au sein de nos administrations, organismes publiques, infrastructures d'importance vitale et opérateurs du secteur privé, la DGSSI organise la 7° édition du séminaire d'information et de sensibilisation sur la cybersécurité. La thématique retenue à cet effet porte sur « l'externalisation des Systèmes d'Information et les enjeux de la cybersécurité ».

Cette manifestation inscrite dans le plan d'action 2019 de la DGSSI vient en complément à d'autres actions menées au cours des dernières années dans le but d'aider les organismes nationaux à évaluer les avantages et à maitriser les risques liés à l'externalisation de leurs systèmes d'information. Il s'agit, d'une part de la publication de plusieurs guides et référentiels en rapport avec la problématique, comme le guide d'externalisation des systèmes d'information, le guide de gestion des risques de sécurité SI ou le référentiel de classification des SI. L'ensemble de ces documents est mis en ligne sur le site web de la DGSSI (www.dgssi.gov.ma).

Le séminaire a eu lieu le 12 novembre 2019 au Club de Bank Al Maghrib. Y étaient conviés, les directeurs des systèmes d'information et les responsables de sécurité des systèmes d'information des administrations, des organismes publics, des entreprises marocaines privées ainsi que ceux des Infrastructures d'Importance Vitale.

# Séance Inaugurale

En exécution des Hautes Instructions Royales, la Direction Générale de la Sécurité des Systèmes d'information (DGSSI) de l'Administration de la Défense Nationale a organisé, le 12 novembre 2019 au sein du Club de Bank Al Maghrib à Rabat, la 7° édition du séminaire annuel sur la cybersécurité, sous le thème « Externalisation des Systèmes d'information et enjeux de la cybersécurité ».

Présidée par M. Abdeltif LOUDYI, Ministre délégué chargé de l'Administration de la Défense Nationale, la séance inaugurale de ce séminaire a été rehaussée par la présence de M. M.BENCHAABOUN, Ministre de l'Economie, des Finances et de la Réforme de l'Administration, de M. M.H. EL ALAMY, Ministre de l'Industrie, du Commerce et de l'Economie Verte et Numérique et de M. O. SEGHROUCHNI, Président de la Commission Nationale de Contrôle de Protection des Données à Caractère Personnel.

Dans une allocution prononcée en la circonstance, M. Abdeltif LOUDYI, Ministre délégué auprès du Chef du Gouvernement, chargé de l'Administration de la Défense Nationale a souligné que l'externalisation des systèmes d'information est un phénomène en constante évolution qui concerne désormais bon nombre de secteurs d'activités et se présente comme une tendance durable et irréversible. Il a dans ce sillage précisé que le recours à l'externalisation des SI offre des avantages importants en termes d'accessibilité et d'élasticité tout en favorisant la réduction des coûts d'investissement et de fonctionnement des systèmes d'information.

Le Ministre A. LOUDYI n'a pas manqué de préciser que la décision d'externalisation des SI demeure tributaire de la maîtrise de certains risques juridiques, techniques et de sécurité. Il a par ailleurs avancé que la sécurité n'est pas antinomique à

l'externalisation et qu'il est indispensable de prendre en compte les préoccupations légitimes des utilisateurs. A ce titre, M. LOUDYI a fait référence à la possibilité de développement d'installations souveraines et d'une offre nationale de cloud qui permettrait non seulement de satisfaire aux besoins des organismes nationaux et à la maîtrise des enjeux de cybersécurité, mais aussi d'ériger le Maroc en plate-forme régionale d'IT Outsourcing pour ainsi enrichir son écosystème numérique.

Monsieur LOUDYI a clôturé son intervention en relatant certaines actions réalisées par la DGSSI, dans le cadre du renforcement de l'arsenal juridique cyber au Maroc, et ce à travers la conduite d'un projet de mise en place d'une loi sur la cybersécurité, ainsi qu'une loi relative aux services de confiance pour les transactions électroniques. Ces projets de loi sont en cours de finalisation en concertation avec les départements concernés.

Pour sa part, le Ministre de l'Economie, des Finances et de la Réforme de l'Administration a salué les avancées réalisées sur le plan national en matière de Sécurité des Systèmes d'information au travers de la stratégie nationale adoptée à cet effet et les efforts soutenus déployés par la DGSSI, depuis sa mise sur pied, pour diffuser la culture de la sécurité informatique tant auprès des Départements ministériels qu'auprès des infrastructures d'importance vitale et du secteur privé.

Il a en outre mis l'accent sur la feuille de route mise en place par le Département de l'Economie et des Finances pour moderniser ses SI en précisant que la bonne gestion des bases de données occupe une place centrale dans les organisations modernes et nécessite une vigilance de tous temps face aux cybermenaces.

Monsieur BENCHAABOUN a enfin mis en exergue l'importance de la thématique choisie pour ce séminaire annuel considérant que l'externalisation des SI est une problématique d'actualité qui retient l'attention des responsables à tous les niveaux à l'heure où la digitalisation constitue un enjeu important de développement pour le Royaume. Il a ainsi souligné que l'externalisation offre des opportunités certaines mais comporte aussi des risques liés à l'hébergement et au

traitement des données dans un environnement externalisé, qu'il faudrait maîtriser.

A l'entame de son intervention, M. Moulay Hafid EL ALAMY, Ministre de l'Industrie, du Commerce et de l'Economie Verte et Numérique, a souligné quant à lui que le numérique constitue l'un des piliers majeurs du développement à l'heure actuelle. C'est à ce titre que la stratégie "Maroc Digital" a été adoptée dans l'optique de faire du Royaume un centre régional des technologies de l'information et de communication. C'est dans ce cadre également que l'Agence de Développement du Digital a été créée pour mettre en œuvre la stratégie de l'Etat dans le domaine digital.

L'externalisation des SI pourrait, selon le Ministre EL ALAMY, constituer une option intéressante au regard des avantages certains qu'elle offre (concentration sur le métier de base, accès à une expertise accrue dans le domaine IT et à des compétences mutualisées et adaptation agile du budget IT au besoin de productivité). Elle renferme, par ailleurs, des risques qu'il faudrait analyser et mieux appréhender pour en tirer le meilleur parti.

Rappelant les actions déployées pour doter notre pays d'un cadre juridique moderne en phase avec les enjeux du numérique notamment dans sa dimension « cybersécurité », le Ministre EL ALAMY a souligné que la transformation digitale requiert l'adoption rapide de nouvelles technologies et l'ouverture des SI aux partenaires et au clients. Elle nécessite de surcroît le renforcement de la confiance numérique qui va de pair avec la mise en place d'un système de cyber sécurité efficace.

Enfin, en clôture de la séance inaugurale, le Président de la Commission Nationale de Contrôle et de Protection des Données à Caractère Personnel (CNDP) a axé son intervention sur les enjeux liés à l'externalisation des SI au regard des impératifs de protection des données personnelles. A cet égard, il a souligné la nécessité de trouver le juste équilibre entre le besoin d'utiliser ces données par les

organismes et le respect des droits des personnes concernées.

Le Président de la CNDP a ajouté que le transfert et le traitement des données devrait garantir un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes. M. SEGHROUCHNI a clôturé son intervention en soulignant qu'il était opportun de développer une offre nationale en matière de protection des données dans le cadre de l'externalisation IT, qui constituerait un avantage concurrentiel à mettre en œuvre dans le cadre d'une offre de service en la matière.

# 1er Panel :
# Externalisation et enjeux de sécurité.

**Modérateur :**

**M. Hassan MOKHLIS**, Directeur de la Stratégie et de la Réglementation à la Direction Générale de la Sécurité des Systèmes d'Information.

**Intervenants:**

**M. Aziz SAWLI**, Chef du département de Coordination et des Infrastructures à l'Agence du Développement Digital.

**M. Popescu ZELETIN**, Professeur à l'Université Technique de Berlin.

**M. Cyril CIVILIER**, Sous-Directeur Adjoint Stratégie à l'ANSSI.

**M. Duncan KUSHMAN**, Représentant du Ministère de Défense Britannique

**M. Pablo LOPEZ**, Représentant du Centre Cryptographique National d'Espagne

## 1ère intervention : M. Aziz SAWLI, Chef du département de coordination et des infrastructures à l'Agence de Développement du Digital (ADD).

M. SAWLI, a précisé que l'Agence de Développement du Digital est très concernée par l'externalisation des SI en tant qu'accélérateur de développement du Digital dans le Pays et qu'elle est consciente des enjeux de sécurité liés à cette pratique.

*" Promouvoir l'IT Outsourcing est un des chantiers majeurs qui composent la feuille de route de l'Agence de Développement du Digital au Maroc. "*

Dans ce contexte, l'Agence nouvellement instituée, a inclus dans sa feuille de route de développement plusieurs chantiers en rapport avec l'externalisation. Il s'agit notamment de:

- L'accompagnement des acteurs publics et privés dans le processus de déploiement d'une externalisation maitrisée ;

- L'assistance dans la mise en place des infrastructures télécoms et informatiques (matériel et logiciel) pour accueillir les systèmes d'information externalisés des secteurs public et privé;

- La mise en place d'une cartographie des infrastructures présentes sur le territoire national, en termes de data-centres, afin de promouvoir les offres cloud au niveau national tenant en compte la souveraineté des données ainsi que les exigences de la DNSSI ;

- L'initiation de projet de partenariats au niveau national et international dans le but de promouvoir les offres d'externalisation sur le territoire national.

Par ailleurs, l'intervenant a précisé que promouvoir l'« IT Outsourcing » à travers la mise en place d'infrastructures fiables et sécurisées s'inscrit dans le cadre de la stratégie nationale du développement digital au Maroc.

## 2ème intervention : M. Popescu ZELETIN, Professeur à l'Université Technique de Berlin.

Le Cloud Computing est un modèle qui permet un accès réseau pratique et sur demande à un pool partagé de ressources informatiques configurables (par exemple, des réseaux, des serveurs, du stockage, des applications et des services), qui peut être rapidement approvisionné et disponible avec un minimum d'efforts de gestion ou d'interaction d'opérateurs. Telle est la définition du « cloud » donnée par NIST et rappelée en l'occasion par M. Popescu ZELETIN.

Ce dernier a enchainé par l'énumération des différentes catégories du cloud qui sont : le « cloud privé », le « cloud communautaire », le « cloud public » ou « le cloud hybride », ayant chacun ses propres spécificités. Selon le niveau d'abstraction des services fournis, ces catégories englobent généralement trois modèles de services cloud, à savoir :

- Infrastructure as a Service (IaaS) : L'IaaS fournit aux organisations des ressources matérielles pouvant être utilisées au besoin. L'avantage est

qu'au lieu d'acheter des serveurs, des logiciels et de payer l'espace du centre de données, le fournisseur de services loue ces ressources. Et par location de ressources, on entend toutes les ressources qu'une personne peut imaginer, notamment l'espace serveur, les équipements réseau, la mémoire, les cycles de CPU, l'espace de stockage, etc.

- Platform as a Service (PaaS) : PaaS fournit toutes les ressources nécessaires pour créer des applications et des services entièrement à partir d'Internet, sans avoir à télécharger ou installer aucun type de logiciel. Les services fournis dans le modèle PaaS incluent la conception, le développement, les tests, le déploiement, l'hébergement, la collaboration en équipe, l'intégration de services Web et de bases de données, ainsi que la gestion des versions.

- Software as a Service (SaaS) : SaaS est un modèle de distribution de logiciels dans lequel les applications sont hébergées par un fournisseur de services et mises à la disposition des clients via Internet. Les applications sont accessibles à partir de divers périphériques clients via une interface de client léger, telle qu'un navigateur Web (par exemple, une messagerie Web), ou une interface de programme. Le SaaS est le plus souvent implémenté pour fournir des fonctionnalités logicielles professionnelles aux entreprises.

Dans le secteur public, la législation, les exigences en matière de sécurité et la nature des services à offrir aux citoyens jouent un rôle majeur dans le choix de la combinaison, catégorie et modèle de service cloud à adopter. L'option du cloud privé est souvent privilégiée, suivie en deuxième lieu par le cloud hybride (privé, communautaire).

Le panéliste a rappelé les multiples avantages que présente le cloud, notamment la consolidation des expertises IT, l'allocation dynamique des ressources (notion de pay as you go), la gestion de services, la supervision globale du système (system landscape) ou encore la surveillance et le traitement des données (monitoring and processing). Ainsi, la transition des structures IT des data-centres en interne (on premise) vers le cloud est de nature à fournir plus de flexibilité et d'efficience.

*" Par l'adoption du modèle cloud adéquat, une administration publique allemande est en capacité de fournir ses services à tous les citoyens ou entreprises, tenant compte de leur mobilité en interne (municipalité, land, Etat) ou, à une plus grande échelle, dans l'espace européen. "*

M.Popescu ZELETIN affirme que l'administration publique allemande a choisi d'aller vers le cloud, et que cette infrastructure cloud a constitué son gage de réussite. Ainsi, de par sa structure politique et administrative représentant un maillage entre à la fois le gouvernement central, les länder et les municipalités, le cloud s'avère le plus approprié à ce modèle et ce dans un total respect des règles de sécurité des données. Il est à préciser que chaque land est constitué de plusieurs municipalités et jouit d'une grande autonomie d'infrastructures et de législations.

De surcroît, Outre Le règlement général sur la protection des données RGPD entré en vigueur le 25 mai 2018 au niveau de l'espace Européen, l'Allemagne adopte d'autres règles à diffèrent niveau pour renforcer la protection et la sécurisation des données. Ainsi, par l'adoption du modèle cloud adéquat, une administration publique allemande est capable de fournir ses services à tous les citoyens ou entreprises, tenant compte de leur mobilité en interne (municipalité, land, Etat) ou, à une plus grande échelle, dans l'espace européen. A ce titre, le panéliste a mis en évidence que la mobilité des citoyens et des entreprises a contraint aussi la Commission Européenne à envisager de mettre en place un cloud souverain, dit Cloud for Europe.

Enfin, M.Popescu ZELETIN a affirmé qu'il a personnellement beaucoup appris de la CSA «  Cloud Security Alliance » en matière de sécurité du cloud. En effet, la CSA est un organisme à but non lucratif dont la mission est de promouvoir l'utilisation des meilleurs pratiques pour assurer la sécurité de l'information en cloud et d'assurer des formations sur l'utilisation de l'informatique en nuage. Il a précisé que cette Alliance a acquis une réputation mondiale en 2011 lorsque l'administration présidentielle américaine a choisi le sommet de la CSA pour annoncer la stratégie cloud du gouvernement fédéral. En outre, CSA dispose d'une plateforme d'échange riche en expériences partagées par des acteurs dans différents secteurs d'activités, notamment banques, assurances et industrie. Le paneliste a invité l'audience à se tenir informée des guides et référentiels publiés par CSA.

## 3ème intervention : M. Cyril CUVILLIER, Sous-Directeur Adjoint Stratégie à l'ANSSI France.

Au début de son intervention, M.CUVILLIER de l'ANSSI, a remercié la DGSSI de l'invitation et s'est félicité de la coopération fructueuse qui lie les deux institutions. Il a ensuite salué l'initiative de la DGSSI pour l'organisation du séminaire sur l'externalisation et les enjeux de cybersécurité qu'elle suscite.

Le paneliste a tenu à préciser que le recours à l'externalisation et en particulier au cloud computing est une décision qui requiert une réflexion très poussée. Le recours au cloud est considéré souvent comme une alternative prometteuse pour certaines organisations dépourvues de capacités techniques suffisantes. En effet, le cloud leur permettra d'assurer une gestion optimale de leurs SI et de disposer de structures de production robustes et sécurisées.

Pour d'autres organismes opérant dans des secteurs sensibles, cette option renferme des risques qu'il faudrait appréhender avant toute décision et recours au cloud. Ces organismes ayant investi pour développer leurs propres compétences techniques pour la protection de leurs systèmes sensibles, doivent procéder à une analyse de risque très fine pour confronter les avantages indéniables des technologies du cloud, avec les risques qu'elles peuvent générer.

Plusieurs questions doivent être posées à cet égard : qui va héberger mes données et où ? combien de fois et dans quels pays seront recopiées mes données ? comment la mutualisation des ressources est gérée pour l'hébergement de mes applicatifs ? comment est géré le compartimentage entre les données et les applications des différents clients ? Toutes ces questions et bien d'autres seront nécessaires pour aller vers le cloud d'une maniéré réfléchie.

Consciente de cette problématique et soucieuse d'accompagner les administrations publiques dans leurs stratégies de digitalisation, la République Française dispose d'une agence gouvernementale, en l'occurrence, la Direction Interministérielle du Numérique qui œuvre pour la modernisation du secteur public en accompagnant les

administrations notamment dans leurs stratégies de passage au cloud. Cette direction travaille en tandem avec l'ANSSI pour s'assurer que sa démarche se fasse dans un climat de confiance et de sécurité.

Dans ce cadre, le rôle de l'ANSSI porte sur la rédaction de guides et la mise en œuvre des processus de qualification pour les opérateurs du cloud. A ce titre, l'agence agit sur deux flancs. D'une part, elle formule des exigences à mettre en place par les fournisseurs du cloud pour sécuriser leurs prestations. Et d'autre part, elle met à la disposition des dirigeants, une méthode d'analyse de risques pour les aider à comprendre les défis du recours au cloud.

" les OIV en France sont responsables de leurs politiques de sécurité. Certes l'ANSSI peut « aiguillonner » ces organismes, les auditer, les contrôler ou leur faire des recommandations, mais en aucun cas assumer leurs propres risques "

M. CUVILLIER a affirmé qu'une réglementation particulière aux Organismes d'Importance Vitale (OIV) concernés par l'externalisation est inscrite dans la loi de programmation militaire publiée en 2013. De même, à l'échelle européenne, il a été procédé, comme une première mesure, au recensement des opérateurs des services essentiels à la prospérité de l'économie européenne. Ces opérateurs ont été amenés à répondre à un certain nombre d'exigences en terme de sécurité.

Ainsi, les OIV en France sont responsables de leurs politiques de sécurité. Certes l'ANSSI peut « aiguillonner » ces organismes, les auditer, les contrôler ou leur faire des recommandations. Cependant, elle ne peut pas prendre les risques que les OIV refusent de prendre eux-mêmes, en particulier pour la question du cloud. En contrepartie, cette dernière est exigeante sur un certain nombre d'aspects, notamment en obligeant les OIV connectés à internet à placer des sondes de sécurité qualifiées par l'ANSSI.

En France, plusieurs acteurs sont déjà passés vers le cloud par besoin d'agilité, de disponibilité, de passage à l'échelle ou de rapidité de déploiement, tout en comprenant les risques y afférents. Par conséquent, le pays s'est engagé dans une dynamique visant à sécuriser les offres cloud. Un équilibre économique s'installe dès lors entre le coût d'une solution cloud sécurisée et le besoin et l'intérêt de l'adopter. Ceci est décliné à l'échelle de l'Etat par l'organisation d'un accès au cloud au niveau de l'Administration sur trois cercles de confiance :

Le 1er cercle vise à supporter des applications et des bases de données particulièrement sensibles au titre de leur caractère critique pour la nation, des bases

de données personnelles de l'Etat, de citoyens français, des processus sensibles, etc… Ces solutions sensibles seront installées sur un cloud qui sera opéré avec l'aide du prestataire, mais par l'Etat lui-même. Ces clouds sont des plateformes hébergées en France sous l'égide de ministères français, qui ont des grosses DSI et qui sont en mesure de mettre en place des clouds sécurisés, au niveau des exigences demandées par l'ANSSI. Sur ce cloud, le problème de territorialité des données ne se pose pas car c'est l'Etat qui gère ce cloud.

Ensuite, le deuxième cercle dans lequel est fait appel à des acteurs industriels de très haut niveau. Ces professionnels qui vont héberger et offrir ces services cloud doivent répondre à un niveau d'exigence plus élevé en terme de sécurité. Dans ce cas, l'ANSSI va leur imposer un certain niveau de supervision de la qualité de sécurité dans ces cloud. L'agence vise ainsi, à mettre à la disposition des demandeurs une offre de cloud hautement sécurisée, mais non étatique. Les offreurs de cloud doivent répondre à des questions très spécifiques, précisées dans le cahier de charges, telles que la question de territorialité et l'assujettissement au cadre européen.

Enfin, il y a un troisième niveau de cercle qui consiste à faciliter l'accès au cloud dans le marché, compte tenu du nombre croissant des demandeurs. D'où la nécessité d'organiser le marché du cloud à travers son inscription sur des dispositifs d'achat public. La France dispose à ce propos de l'UGAP (Unité Générale d'Accès aux Prestations), dont le rôle est de faciliter l'accès à des offres cloud pour les administrations publiques. Les dirigeants de ces dernières doivent procéder à une analyse de risques pour savoir sur lequel de ces trois cercles se situent les données qu'ils manipulent.

*" L'accès au cloud est organisé à l'échelle de l'Etat sur trois cercles de confiance allant du tout opéré par l'Etat au cloud public en passant par un niveau intermédiaire ou la gestion est confiée aux industriels de haut niveau."*

## 4ème intervention : M. Duncan KUSHMAN, Représentant du Ministère de la Défense Britannique

L'intervention de M. KUSHMAN s'est articulée principalement sur l'approche conceptuelle du Royaume-Uni en matière de cyber sécurité et la projection de cette approche sur le rôle du Ministère de la Défense britannique dans l'écosystème cybernétique du pays. L'intervenant a clôturé son exposé par la mise en exergue des recommandations du Centre National de la Cyber sécurité au Royaume-Uni.

Pour ce qui est de la vision du Royaume-Uni en matière de cyber sécurité, le gouvernement britannique vise la promotion durable d'un cyberespace libre, pacifique et sécurisé. Le cyber espace constitue, en effet, à la fois un moteur de la croissance économique et un défi pour la sécurité nationale. Ainsi, il requiert la mise en œuvre d'un modèle de gouvernance flexible capable de répondre au développement technologique rapide et de satisfaire les exigences de la sécurité nationale.

*" L'Etat doit mettre à la disposition des propriétaires de risque (risk owners), une méthode de raisonnement leur permettant d'abord de formuler leurs exigences en matière de sécurité, et de déterminer, ensuite, les fournisseurs de cloud pouvant satisfaire les exigences de la sécurité nationale "*

Sur fond des exigences pour sécuriser le cyber espace, l'externalisation des systèmes d'information constitue un défi sécuritaire majeur pour le Royaume Uni. Dans ce cadre, le gouvernement britannique a adopté une série de mesures à l'effet de maitriser cette externalisation et de prévenir les actions nuisibles ou illégales. Il a notamment élaboré en avril 2019 un « livre blanc », dans lequel il a mis en avant un système global pour responsabiliser les différents acteurs concernés par cette forme d'externalisation (parties prenantes, fournisseurs de service d'externalisation et la société en général). En outre, ce livre oblige les propriétaires des systèmes d'information à procéder à une analyse de risques avant toute opération d'externalisation.

S'agissant du ministère de la défense (MoD), il a pour rôle de mettre en œuvre la stratégie nationale britannique en matière de cyber sécurité, et ce à travers la mise en place de mécanismes robustes de cyberdéfense, la projection de puissance au besoin et la participation à l'action du Royaume-Uni en cas d'un cyber incident majeur ou d'une attaque cybernétique en général.

Dans un contexte opérationnel spécifique à ce ministère, l'externalisation apporte un défi supplémentaire par rapport au degré d'efficience et de sécurité requis. Ainsi, l'approche du MoD pour appréhender la sécurité dans le cyberespace, consiste à

placer les services opérationnels selon leur criticité dans l'une des trois zones ci-après:

- Zone de proximité, où le réseau est totalement contrôlé par le MoD ;
- Zone du milieu, où se déroulent les opérations critiques du réseau. Cette zone n'est pas contrôlée uniquement par le MoD, mais aussi par des tiers ;
- Zone éloignée, où se trouvent les réseaux pouvant avoir un impact critique sur les opérations et qui échappent au contrôle du MoD (gérés uniquement par des tiers).

Les deux dernières zones étant les plus vulnérables dans la mesure où elles sont facilement influencées par des adversaires ou des parties tierces.

Outre les actions assurées par le département de la défense, Il va sans dire qu'agissant seul, le MoD ne peut pas garantir la cyber sécurité dans tout le pays. Son action doit être coordonnée avec d'autres acteurs du gouvernement. Fort de cette conviction, le Royaume–Uni a procédé à la création du Centre National de Cyber sécurité servant de plateforme unifiée et agissant comme interlocuteur avec le secteur privé.

M. KUSHMAN a précisé qu'en rapport avec la mise en œuvre du cloud, comme étant la forme d'externalisation des SI la plus sollicitée actuellement, le Centre National de Cyber sécurité a publié un framework englobant 14 principes de sécurité, visant à mettre à la disposition des propriétaires de risque (risk owners), une méthode de raisonnement leur permettant d'abord de formuler leurs exigences en matière de sécurité, et de déterminer, ensuite, les fournisseurs de cloud pouvant satisfaire ces exigences.

Enfin, il a ajouté que les termes et les conditions du contrat de sous-traitance doivent être adaptés au niveau de sécurité requis pour le passage vers le cloud. Le demandeur de service doit être en mesure de formuler clairement ses exigences au niveau de granularité requis. Le gouvernement britannique a mis en place, à cet effet, un outil appelé «Cyber Essentials» fixant les exigences minimales à inclure dans les contrats avec les fournisseurs de cloud.

## 5ème intervention : M. Pablo LOPEZ, Représentant du Centre Cryptographique National d'Espagne

M. Pablo LOPEZ a affirmé que s'agissant de l'externalisation, l'Etat est responsable de préparer un écosystème favorable notamment en ce qui concerne le passage vers le cloud, et ce à travers la production et la promulgation de guides, de conseils et de recommandations, ainsi que l'adoption de standards de sécurité valables pour la fourniture des services et la manipulation des données.

Eu égard à tous ses avantages, le Cloud ne peut être abandonné pour la simple raison qu'il présente des risques. L'Etat doit mettre en place les moyens nécessaires pour bâtir un climat de confiance (Building Trust) dans lequel la question de conformité réglementaire revêt une importance capitale. Il s'agit notamment d'arrêter les exigences légales (Territorialité, réversibilité, etc) et de disposer de mécanismes pour la certification de cette technologie.

Dans le sillage de la question de confiance, il est du ressort de l'organisme ayant recours à l'externalisation de faire appel à des fournisseurs de service compétents, en leur imposant des standards de sécurité au niveau des contrats de sous-traitance. Il convient de préciser qu'il ne s'agit pas ici du SLA (Service Level Agreement), mais plutôt des exigences de sécurité proprement dites. A ce sujet il est du devoir du gouvernement de spécifier les exigences minimales pour garantir un écosystème sécurisé.

Constituant un élément clé dans l'approche du gouvernement espagnol de la question du cloud, la réduction de la surface d'exposition aux risques constitue un pilier de base du cadre de travail (National Security Framework) mis en place. Sous forme de procédures et de conseils, ce cadre de travail a pour objectif de développer la sécurité dans le cloud et prévenir les risques y afférents.

> " l'Etat est responsable de préparer un écosystème favorable notamment en ce qui concerne le passage vers le cloud, et ce à travers la production et la promulgation de guides, de conseils et de recommandations "

Un défi relevé par l'approche du gouvernement espagnol consiste à adapter

le savoir-faire développé et accumulé à ce stade dans le domaine du cloud, par les fournisseurs et les différentes agences responsables de la sécurité, pour répondre aux besoins spécifiques de l'écosystème espagnol et accompagner les organes de l'Etat dans leur démarche de passage vers le cloud.

L'accès à la technologie cloud en Espagne doit se faire en plusieurs étapes. Il faut d'abord procéder à une analyse de risque à travers laquelle se dégage le risque résiduel. Ensuite, implémenter les paramètres de sécurité découlant du National Security Framework. A l'issue de cette étape, dérouler et appliquer les règles traitant la sécurité de la configuration au niveau du cloud. Quand toutes ces étapes sont parcourues, on se retrouve avec un modèle qui permet de mettre en place tout le processus de la sécurité dans le cloud.

A ce titre, le gouvernement Espagnol est actuellement en train de développer, de concert avec Microsoft, des configurations de sécurité et des PowerShell scripts dans le but d'améliorer le volet sécurité dans le cloud Microsoft. Ce faisant, la surface d'exposition est réduite et est probablement meilleure par rapport à une configuration par défaut. Cette initiative avec Microsoft, verra le jour en décembre ou en début de l'année 2020, sous forme de guide servant à implémenter une configuration sécurisée au sein d'Azure et Office 365.

En résumé, la technologie Cloud présente plusieurs avantages mais aussi plusieurs risques à prévenir ou à gérer. Pour ce faire, il faut implémenter ses propres paramètres de sécurité et ne pas se fier aux paramètres par défaut pour réduire la surface d'exposition. Cela se fait à travers la promulgation de guides et de procédures pour assister les organismes à profiter de cette technologie.

# 2ème Panel :
# Offres Cloud et garanties de sécurité.

**Modérateur :**

**Général EL Mostafa RABII**, Directeur du maCERT de la Direction Générale de la Sécurité des Systèmes d'Information.

**Intervenants :**

**Mr. Lyron H. ANDREWS**, Consultant Cyber sécurité.

**Mr. Amine KANDIL**, Directeur Général de N+ONE Datacenters.

**Mr. Hicham IRAQI HOUSSAINI**, Directeur Général Microsoft Maroc.

**Mr. Khalid LAMKINSI,** Expert cybersécurité chez INWI Datacenter.

**Mr. Rachid RESSANI**, PDG IT Road.

## 1ère intervention : Mr. Lyron H. ANDREWS, Consultant Cyber sécurité.

Mr Lyron a invité les participants au séminaire à considérer dans leurs stratégies de migration vers le Cloud, le concept du Zero Trust. Ce concept tranche avec l'approche classique qui se base sur la segmentation DMZ ( trusted et untrusted zone) et estime qu'elle est insuffisante et qu'il faut désormais implémenter ce qu'on appelle la micro segmentation.

Zero Trust est un modèle de sécurité informatique qui élimine la notion de confiance pour protéger les réseaux, les applications et les données. Cela contraste fortement avec le modèle de sécurité périmétrique traditionnel, qui suppose que les mauvais acteurs sont toujours du côté non fiable du réseau, et que les utilisateurs dignes de confiance sont toujours du côté interne. Avec Zero Trust, ces hypothèses sont annulées et tous les utilisateurs sont présumés non fiables.

*" Les organismes doivent mettre en place une architecture de sécurité unique et unifiée qui donne aux utilisateurs un accès sécurisé aux applications et aux données quel que soit leur emplacement et applique les politiques de sécurité sur une base continue "*

Une solution Zero Trust doit :

- Assurer que seul le trafic connu ou autorisé ou la communication d'application légitime est autorisée en segmentant et en activant la stratégie au niveau de la couche 7 du modèle OSI.
- Tirer parti d'une stratégie d'accès à moindre privilèges et appliquer strictement le contrôle d'accès à tous les niveaux.
- Inspecter et enregistrer tout le trafic.

Ces principes peuvent être plus simples à mettre en œuvre dans un réseau d'entreprise sur lequel l'organisation détient le contrôle total. Or, force est de constater qu'aujourd'hui, il est souvent plus rentable d'héberger une application dans le cloud au lieu d'un centre de données. Ces environnements cloud, exploités par des fournisseurs de services cloud, ne font pas partie du réseau interne d'une organisation. Le même type de contrôles réseau ne s'applique donc pas.

En conséquence, la plupart des organismes ayant des applications et des données hébergées en cloud, ont peu de visibilité sur qui accède à leurs applications et données, comment les données sont utilisées et partagées ou même quels appareils sont utilisés pour y accéder (smartphones, tablettes, ordinateur portable, etc.), car la plupart de leurs actifs se trouvent sur une infrastructure tierce.

Pour résoudre ces problèmes, les organismes utilisent souvent une variété de solutions et de passerelles pour assurer un accès sécurisé à moindres privilèges à leurs plateformes Cloud et qui diffère des solutions utilisées en interne. Ce mélange de technologies crée une architecture de sécurité fragmentée dans laquelle il est difficile de savoir quelles politiques sont en place pour protéger les données en interne et dans le cloud.

Pour réussir ce challenge, les entreprises doivent mettre en place une architecture de sécurité unique et unifiée qui donne aux utilisateurs un accès sécurisé aux applications et aux données quel que soit leur emplacement : Cloud public, applications SaaS ou Cloud privé / Datacenter, et qui inspecte le trafic et applique les politiques de sécurité sur une base continue.

À mesure que les organisations migrent vers le cloud, il est important d'intégrer le Zero Trust dans la conception de toute nouvelle infrastructure cloud. Cette

construction se fait en utilisant une méthodologie en 5 étapes :

Étape 1: Identifier le type d'applications (par exemple, publiques, privées, SaaS, etc.) et les données (par exemple, confidentielles, sensibles, sans importance) que l'organisme possède, où elles se trouvent et qui y accède et les utilise. Ensuite, définir la surface de protection : les données, les applications, les actifs et les services les plus critiques pour votre entreprise.

Étape 2: Elaborer une cartographie des flux de transactions (c.-à-d. Comment fonctionnent réellement les applications).

Étape 3: Architecturer la nouvelle infrastructure cloud et créez des frontières entre les utilisateurs et les applications.

Étape 4: Élaborer les stratégies Zero Trust de l'organisme en fonction de qui doit avoir accès à quoi et appliquer des contrôles d'accès contextuels basés sur les principes de moindre privilège. Informer les utilisateurs sur les politiques de sécurité de l'organisme et sur ce que l'on attend d'eux lorsqu'ils accèdent et utilisent les applications et les données dans le cloud.

Étape 5: Surveiller et maintenir l'environnement Zero Trust. Cela signifie inspecter et enregistrer en permanence tout le trafic pour identifier les activités inhabituelles et décider de la manière de sécuriser les stratégies. Avec une surveillance active, la surface de protection peut grandir, permettant d'apporter des modifications à l'architecture pour améliorer la sécurité de manière continue.

## 2ème intervention : Mr. Amine KANDIL, Directeur Général de N+ONE Datacenters et Mr. Hicham Iraqi Houssaini, Directeur Général Microsoft Maroc.

Dans son intervention, Mr. Amine KANDIL a mis l'accent sur la problématique de territorialité des données au niveau du Cloud, dès lors qu'elles peuvent être stockées dans des pays autres que ceux des clients. La question de la protection des données et la position géographique du datacenter est primordiale. Le pays de localisation des serveurs où sont stockées les données conditionne les lois qui seront

appliquées et auxquelles les entreprises seront soumises.
En lien avec cette question, le panéliste exprime la volonté de son entreprise de mettre en place un cloud souverain permettant l'hébergement des données au niveau du territoire Marocain sous un cadre juridique national.

> " La notion du cloud souverain répond parfaitement à la problématique de territorialité dans le cloud.
> Afin de permettre une migration sécurisée vers le Cloud, il convient d'étudier la sécurité du prestataire du cloud et, au besoin, d'intégrer dans son architecture des couches de protection supplémentaires "

En effet, la notion du cloud souverain répond parfaitement à la problématique de territorialité dans le cloud. Il s'agit d'un modèle de déploiement dans lequel l'hébergement et l'ensemble des traitements effectués sur des données par un prestataire de cloud sont physiquement réalisés dans les limites du territoire national selon les lois et normes nationales en vigueur. La présence d'un tel cloud permet de préserver la sécurité et la confidentialité de ces données.
Les spécificités du cloud souverain sont d'être hébergé et géré par un prestataire national, non affilié à une entreprise étrangère, et disposant d'infrastructures situées à l'intérieur du pays. Cette certification garantit que les données stockées soient soumises au contrôle des autorités nationales compétentes et que les hébergeurs soient en règle avec la loi.

En règle générale, afin de permettre une migration sécurisée vers le Cloud, il convient d'étudier la sécurité du prestataire du cloud et, au besoin, d'intégrer dans son architecture des couches de protection supplémentaires. Pour sa part, N+ONE Datacenters met à la disposition de sa clientèle une plate-forme cloud répondant à de nombreuses exigences de sécurité et certifiée PCI-DSS, ISO27001...

M. Kandil et M. Iraqi Houssaini ont profité de l'occasion pour informer les participants du lancement d'une plateforme Cloud Azure Stack destinée aux institutions et entreprises qui souhaitent héberger leurs données sensibles dans un cloud marocain. Cette plateforme propose des solutions IAAS (Infrastructure as a service), et PAAS (Platform as service), aujourd'hui indispensables pour accompagner la transformation digitale au Maroc. Les deux intervenants ont affirmé que beaucoup de leurs clients sont habitués à la puissance d'AZURE, et doivent également se conformer à la législation en termes de souveraineté et de territorialité des données.

Mr KANDIL a expliqué que ce choix de partenariat renforcé avec l'un des leaders mondiaux du cloud, les a amenés à développer une approche concrète et éprouvée d'un cloud souverain, qui permettra d'accompagner de manière opérationnelle leurs clients dans leurs projets de transformation digitale.

Pour M. IRAQI, le lancement de cette plateforme s'inscrit dans le cadre de la volonté de Microsoft de répondre à un nombre de besoins exprimés par les entreprises et institutions marocaines et d'accélérer l'adoption du cloud au Maroc. Microsoft continue ainsi de contribuer au développement de l'économie locale et des communautés, et met à présent l'accent sur l'accélération de la transformation numérique à travers le Cloud computing auprès des entités des secteurs public et privé marocains.

Enfin, M. IRAQI a ensuite mis l'accent sur la manière avec laquelle Microsoft gère ces solutions Cloud, qui se base sur trois principes importants :

- La transparence, qui consiste à communiquer au client l'emplacement de stockage de ces données
- La protection des données personnelles, ou Microsoft assure la protection des données de sa clientèle en conformité avec le GDPR et la loi 09-08
- La conformité, ou Microsoft est certifié dans la plupart des domaines

## 3ème intervention : Mr. Khalid LAMKINSI Expert cybersécurité chez INWI Datacenter.

Mr. Khalid LAMKINSI a expliqué au début de son intervention que d'une manière générale, le passage vers le cloud pour la majorité des clients se fait pour :

- Répondre à un besoin d'agilité,
- Assurer rapidement une mise à niveau vers de nouvelles technologies
- Avoir des coûts optimisés tout en profitant des outils, des compétences et des investissements existants.

Le panéliste a précisé que dans la tendance actuelle de migration vers le tout Cloud, il y'a une problématique qui se fait de plus en plus récurrente, il s'agit de celle de préservation des données de

souveraineté. Le Maroc, à travers le décret 2-15-712 fixant le dispositif de protection des systèmes d'information sensibles des infrastructures d'importance vitale, exige que toute externalisation fasse l'objet d'un contrat de droit marocain et que l'hébergement des données sensible des entités se fasse sur le territoire marocain.

Notre pays ne fait pas l'exception dans ce cadre, d'autre pays ont adopté la même posture. En France par exemple, une commission d'enquête vient de publier un rapport en Octobre 2019 favorisant le déploiement des infrastructures critiques sur le territoire français, et la nécessité de mobiliser le capital humain et financier pour y arriver.

*" Dans la tendance actuelle de migration vers le tout Cloud, il y'a une problématique qui se fait de plus en plus récurrente, il s'agit de celle de préservation des données de souveraineté. "*

Répondre à cette problématique de souveraineté des données requièrt le développement d'une offre nationale à même de supporter toutes ces exigences. Dans ce contexte, les opérateurs d'infrastructure Télécom sont des acteurs privilégiés car ils sont amenés à répondre au même type de problématiques côté réseau de communication. Pour cette raison, l'Opérateur Inwi a récemment développé une offre d'hébergement Cloud.

Pour Mr. Khalid LAMKINSI l'objectif d'Inwi est d'assurer à ses clients un passage maitrisé vers le cloud. Elle propose à cet effet une démarche graduelle qui consiste à encourager en premier lieu la migration des environnements non critiques et des environnements de test et de recettes avant de passer à des environnements de production plus sensibles. Il y a lieu de signaler que cette démarche permet d'assurer, notamment pendant la transition vers le cloud, une meilleure compatibilité entre d'une part l'environnement déployé côté client (au niveau d'un datacenter interne) et d'autre part l'environnement cloud (cloud privé ou public).

Il a ajouté que la question de sécurité reste celle qui fait l'unanimité de tous les demandeurs des services cloud. A ce propos, les méthodes et les techniques utilisées évoluent quasiment au même rythme que celui de la croissance de la demande sur ces prestations. A cet effet, dans la perspective de sécuriser son Datacenter INWI a :

- Recruté des experts en cybersécurité ;
- Acquis une panoplie de solutions de sécurité et ce en collaboration avec

des partenaires de sécurité de renommée ;

- Mis en œuvre un portefeuille de services cyber sécurité ;
- Mis en œuvre un centre opérationnel de sécurité (SOC).

Enfin, s'inscrivant dans la dynamique d'externalisation, Inwi a mis à la disposition de ses clients plusieurs Datacenter à Rabat, Casablanca et à Marrakech constituant ainsi la plus grande infrastructure Datacenter certifiée Tier3.

## 4ème intervention: Mr. Rachid RESSANI, PDG IT Road.

PDG d'une société spécialisée en infogérance, Mr. Rachid RESSANI a axé son intervention sur les services d'infogérance IT, comme étant la forme traditionnelle et la plus répandue d'externalisation.

Il a ainsi présenté les différents modèles d'infogérance qui existent sur le marché et auxquels fait appel sa clientèle :

- L'infogérance globale : qui consiste à confier l'intégralité du système d'information à un prestataire tiers. Cela concerne donc à la fois les infrastructures techniques et les applications logicielles.
- L'infogérance partielle : qui consiste à ne confier qu'une partie du système d'information à un prestataire tiers. Il peut s'agir d'un ou de plusieurs services, ou encore, d'une partie des données.
- L'infogérance applicative : qui consiste au développement, l'exploitation et la maintenance d'une ou de plusieurs applications de l'entreprise.
- L'infogérance d'exploitation : qui concerne plus particulièrement l'hébergement, la fourniture de matériel ou de logiciels et la supervision du système informatique (administration des serveurs, gestion des sauvegardes…)
- Enfin, un dernier modèle qui existe et qui ne rentre pas dans le portfolio d'IT-Road et qui est l'externalisation d'un ou plusieurs processus métier. Il s'agit donc dans ce cas d'externaliser une fonction complète de l'entreprise.

Mr RESSANI a précisé que les problématiques de sécurité dans une prestations d'infogérance sont assez similaire aux problématique Cloud, le Cloud étant lui-même une forme particulière d'infogérance. L'évaluation initiale du risque et les mesures techniques et contractuelles relatives au choix du bon prestataire et au suivi de la prestation sont tout aussi similaires.

L'intervenant a ajouté qu'en plus des prestations d'infogérance classiques, forte de son expertise en la matière, d'un potentiel humain qualifié et une demande de plus en plus importante, IT road accompagne souvent ses partenaires pour le passage vers le cloud en adoptant une approche basée sur la conformité aux textes règlementaires et sur l'analyse des risques.

Et d'ajouter que l'activité de conseil qui constitue un volet de plus en plus important de son activité tourne désormais autour d'une offre taillée pour répondre aux besoins clients ci-après :

- L'Accompagnement dans des audits de conformité SSI, et de conformité à des standards industriels ;
- L'analyse des risques ;
- La mise en œuvre de SOCs et NOCs ;
- L'élaboration de schémas directeurs ;
- L'élaboration de plans de transformation digitale ;
- La formation au profit des clients.

" les problématiques de sécurité dans une prestation d'infogérance sont assez similaires aux problématiques Cloud. L'évaluation initiale du risque et les mesures techniques et contractuelles relatives au choix du bon prestataire et au suivi de la prestation sont tout aussi similaires.

Enfin, en dépit du caractère séduisant des offres Cloud, Mr RESSANI a exhorté les participants à s'inscrire dans une orientation technologique progressive afin d'assurer un passage vers le cloud dans un respect total des textes règlementaires en vigueur, et des exigences de la sécurité nationale. Il a aussi rappelé que le Maroc dispose d'un capital humain mature et en capacité de répondre aux exigences de l'externalisation dans un cadre de souveraineté nationale.

# 3ème Panel :
# Solutions de sécurité pour le cloud.

**Modérateur :**

**COL. MAJ. ABDELLAH BOUTRIG**, Directeur de l'Assistance, de la Formation, du Contrôle et de l'Expertise.

**Intervenants :**

**M. Mohamed MALKI**, Enterprise Security Architect – Colorado, Etats-Unis.

**M. Ehab MARZOUKI**, Senior System Engineer at VMware North & West Africa.

**M. Yassine MALKI**, Consultant chez NUTANIX.

**M. Abderrahman ERROUSSI**, Ingénieur chez SYMANTEC.

## 1ère Intervention : M. Mohamed MALKI, architecte de sécurité d'entreprise à l'Etat du Colorado aux Etats-Unis d'Amérique

S'exprimant au sujet de la sécurité lors du passage vers le Cloud, M. MALKI a entamé son intervention en expliquant la stratégie du « Cloud first ». Cette initiative adoptée par le gouvernement américain depuis 2011, consiste à encourager les grandes entreprises à aller de plus en plus vers le cloud public et à choisir le cloud pour tous leurs projets technologiques. Cette tendance a été établie en partant du principe que les fournisseurs de cloud public étaient les mieux armés pour proposer des solutions pouvant répondre aux différents besoins fonctionnels des entreprises, tout en créant de la valeur et en réduisant les coûts.

Néanmoins, face aux nouveaux défis que présente le passage vers le cloud, il s'avère nécessaire de se poser certaines questions.

Est-ce vraiment la meilleure stratégie à adopter dans tous les cas ? Peut-elle évoluer et s'adapter pour répondre à tous les besoins futurs de l'entreprise ? Dans ce sillage, M. Malki a précisé qu'il serait plus judicieux de définir les exigences opérationnelles et de sécurité de chaque entreprise avant de choisir le type de cloud le mieux adapté. On parle alors de l'approche « Cloud Smart » qui est de toute évidence plus rationnelle que l'approche précédente. Il a également affirmé l'obligation de se conformer dans tous les cas à la réglementation en vigueur, en l'occurrence celle relative à l'hébergement des données sensibles au niveau du territoire national.

*" A force de parler du « cloud first » on finit par le prendre pour un « business case : pourquoi pas le cloud ? ». Cependant, il est judicieux de parler « cloud smart » et donc de répondre à la question : « pourquoi le cloud ? "*

La question de conformité aux exigences réglementaires relatives à la protection des données confidentielles a été résolue au niveau des Etats-Unis à travers la mise en place d'un cloud gouvernemental appelé « GOV-CLOUD ». En effet, les fournisseurs du Cloud public, notamment AWS, AZURE et GOOGLE, ont conçu, en concertation avec le gouvernement américain, un service cloud dédié pour permettre aux agences gouvernementales américaines de placer leurs données confidentielles dans le cloud, tout en répondant à des exigences réglementaires spécifiques.

Il a précisé également que dans tous les cas il est indispensable de spécifier au niveau du contrat établi avec un fournisseur cloud, les conditions de réversibilité qui permettront à l'entité de pouvoir assurer la reprise partielle ou complète de ses données ou système en cas de rupture de service ou de passage vers un autre fournisseur. Il a réaffirmé par ailleurs que l'adoption d'une stratégie « multi-cloud » est le meilleur moyen pour se libérer de l'enfermement propriétaire « Vendor Lock-in ».

Enfin, le panéliste a affirmé que le passage vers le cloud s'avère dans certaines situations plus sécurisé que l'hébergement en local. Il a justifié cette position par le fait que les fournisseurs du Cloud sont les mieux armés pour proposer les Datacenters les plus sécurisés et les plus résilients du marché grâce à leur taille et à leur expertise.

## 2ème Intervention : M. Ehab MARZOUKI, Senior System Engineer chez VMware North & West Africa

M. MARZOUKI a axé son intervention sur la vision de VMWARE en matière de sécurité pour les systèmes virtualisés, en particulier ceux utilisés par les grands fournisseurs du Cloud. Cette vision s'articule autour de quatre piliers à savoir :

- La Prédiction : par la création d'un système capable de prédire tous les risques de sécurité futurs en étudiant les attaques passées et en s'appuyant sur un mécanisme d'Intelligence Artificielle ;

- La Prévention : à travers l'élaboration et la mise en place de guides de bonnes pratiques relatifs au durcissement des bases de données, des hyperviseurs, et des systèmes d'exploitation. Dans ce cadre, VMware a également mis sur pied un mécanisme de micro-segmentation dans l'hyperviseur qui permet l'isolation entre toutes les briques d'un data-centre.

- La Détection : par la mise en place de systèmes permettant la détection des différentes menaces ;

- La Remédiation : à travers l'automatisation de la réponse à un large éventail d'attaques connues.

M. MARZOUKI a souligné par ailleurs, qu'il s'avère difficile de prédire les dangers se rapportant au cloud en l'absence d'un écosystème puissant. C'est dans ce sens que VMware a adopté un modèle de sécurité proactif. En effet, la sécurité est nativement incluse « built-in » dans les différentes solutions de virtualisation offertes. De plus, plusieurs partenariats ont été conclus avec les plus grands acteurs de sécurité dans le monde pour tirer profit de leur expérience et leur savoir-faire.

*" Dans le cloud public, on n'est pas dans un aquarium mais dans un océan. On ne peut pas prévoir tous les dangers qui s'y rapportent de nos jours en l'absence d'un écosystème puissant "*

## 3ème Intervention : M. Yassine MALKI, Consultant . NUTANIX

Au début de son intervention M. Y.MALKI a évoqué l'importance de cartographier et de classifier les biens informationnels d'une organisation, en termes de confidentialité et de criticité, avant de prendre la décision stratégique du passage vers le cloud public. Il a également attiré l'attention sur le fait que la sécurisation des données mises sur un cloud public demeure, dans la plupart des offres cloud du marché, sous la responsabilité des clients et qu'il faudra prendre les dispositions nécessaires pour en assurer la protection.

Selon M. Y.MALKI, la meilleure approche serait d'adopter le cloud hybride. Le Cloud hybride consiste à connecter un ou plusieurs Cloud publics à un Cloud privé ou à une infrastructure de Data Center sur site traditionnel. De manière plus élaborée, le Cloud hybride est un environnement Cloud constitué de ressources de Cloud privé sur site combinées avec des ressources de Cloud public tiers connectées entre elles par un système d'orchestration.

*Le cloud hybride offre l'avantage de la flexibilité tout en répondant aux contraintes de préservation des données sensibles.*

Le cloud hybride a pour principal avantage la flexibilité. En effet, si les ressources du cloud privé ne suffisent plus à un moment donné, l'organisation a la possibilité d'ajouter instantanément des ressources du cloud public pour répondre à ses nouveaux besoins. Cette possibilité fait partie de la capacité by design de NUTANIX à gérer du multi-cloud.

L'autre avantage majeur du cloud hybride est d'ordre sécuritaire. Une infrastructure cloud hybride donne la possibilité à une organisation de conserver ses données les plus critiques en interne et d'utiliser en continu des applications hébergées dans le cloud public. Pour ce qui est de la confidentialité des données, il est possible de s'assurer de l'intégrité des données hébergées et de les crypter en appliquant le chiffrement au repos « At Rest data Encryption ». De plus la solution que propose NUTANIX est aussi capable d'assurer la sécurisation des données par la micro-segmentation et peut ainsi assurer le

cloisonnement des données sensibles dans un environnement virtuel.

## 4ème Intervention : M. Abderrahman ERROUSSI, Ingénieur sécurité, SYMANTEC

Dans son intervention, **M. ERROUSSI** a affirmé qu'en général, les engagements des fournisseurs de cloud public portent plutôt sur la disponibilité des systèmes que sur les données elles-mêmes. Il en résulte que la sécurisation et la protection de ces dernières s'avèrent la responsabilité de l'organisation.

Le cycle de sécurité dans le Cloud comporte cinq briques à savoir :

- L'identification des applications qui existent au niveau du cloud et qui ne sont pas visibles au niveau de l'entreprise, appelées « Shadow IT ». La classification des données hébergées dans le cloud et l'élaboration d'une stratégie cloud ;
- La protection à travers l'implémentation des politiques de sécurité en vigueur au sein de l'organisme et la mise en place de solutions de contrôle des applications cloud, de solutions de chiffrement, de classification de données...etc.
- La détection des incidents et violations survenus au niveau des applications et du système d'information de l'organisme ;
- La réponse aux incidents afin de réduire l'impact que peuvent générer les incidents de sécurité ;
- La récupération par la mise en place d'un programme de reprise et de continuité d'activités.

*" Dans un modèle cloud, l'organisme est le premier responsable de la sécurité et de la protection des données et non le fournisseur de service cloud "*

L'intervenant a également présenté les six recommandations de Symantec en matière de sécurité dans le cloud. Il s'agit de :

- La création d'un programme de sécurité dans le cloud adapté aux

besoins de sécurité au sein de l'organisation ;

- L'Elargissement des stratégies et des workflows de surveillance des données sensibles en intégrant des solutions DLP en local et dans le cloud ;

- La Réorientation de l'organisation pour adopter une approche de sécurité dans le cloud et recenser régulièrement les utilisateurs pour l'amélioration continue des processus internes ;

- L'assurance que les données sensibles qui sont réglementées soient stockées dans des espaces qui respectent la politique de sécurité de l'organisation ;

- L'Implémentation d'une solution CASB capable de détecter et d'évaluer le risque des applications cloud, de détecter les activités malveillantes dans les comptes cloud, ainsi que de classifier et de contrôler les données qu'elles contiennent, quel que soit le lieu de l'utilisateur ou du Endpoint.

# Conclusion

Il ressort de ce séminaire que l'externalisation dans toutes ses formes, en particulier celle du Cloud, est une tendance irréversible en constante évolution. Elle offre certes de multiples avantages mais présente également des risques qu'il convient de maitriser.

En effet, le recourt à l'externalisation est une problématique d'actualité qu'il s'agit d'aborder aussi bien à l'échelle de l'Etat que celle des organismes et institutions.

De prime abords, il est désormais indispensable pour l'Etat de préparer un écosystème favorisant une externalisation encadrée, dont les risques sont maitrisés, notamment pour les organismes publics et infrastructures d'importance vitale. Ceci peut être réalisé à travers la production et la promulgation de lois, de guides, et de référentiels en la matière. Il s'agit aussi d'organiser l'accès au cloud selon le niveau de criticité des données et des applications pour l'Etat (à titre d'exemple : cloud géré par l'Etat, cloud souverain, cloud public ou privé). Enfin, encourager et accompagner des acteurs économiques pour la création d'une offre nationale à même de répondre aux impératifs précités.

Par ailleurs, à l'échelle des organismes et institutions, plusieurs mesures ont été identifiées et mises en avant afin d'assurer un niveau adéquat de sécurité lors de l'externalisation. Il s'agit notamment de :

- Effectuer une analyse de risque pour définir les mesures de sécurité appropriées à exiger du prestataire ou à mettre en place en interne ;
- Procéder à une classification des données afin de déterminer les données passibles d'un traitement particulier au regard de la réglementation en vigueur ;
- Elaborer un document contractuel qui décrit l'ensemble des dispositions spécifiques que le prestataire s'engage à mettre en œuvre pour garantir le respect des exigences de sécurité de l'entité et qui prévoit les conditions de réversibilité.
- Mettre en place une architecture de sécurité unifiée garantissant un accès sécurisé aux applications et aux données quel que soit l'emplacement des utilisateurs et le modèle d'externalisation adopté (Cloud public, applications SaaS ou Cloud privé).