6ème Edition du Séminaire de Sensibilisation sur la Sécurité des Systèmes d'Information

« Cyber résilience »

Nouvelle approche pour relever le défi du cyber risque

DGSSI 30 Octobre 2018

NOTE DE PRESENTATION

Avec la montée en puissance des menaces cybernétiques, toute organisation se doit de mettre en œuvre les mesures adéquates pour assurer la sécurité de son infrastructure, de ses systèmes et l'intégrité de ses données. Cependant, dans le contexte actuel d'hyper connectivité des systèmes, il devient de plus en plus difficile de se prémunir contre les cyberattaques. Aussi, il n'est plus question de savoir si oui ou non on pourrait être victime d'une attaque mais plutôt sommes-nous capables d'y faire face lorsqu'elle se produira tout en garantissant une reprise de l'activité dans des délais acceptables? On parle alors de cyber-résilience.

La cyber-résilience se veut une approche pragmatique, qui impose une modification de la perception de la sécurité par les organisations. En effet, si la cybersécurité s'attèle à améliorer les capacités d'une organisation à détecter et empêcher la réussite de cyberattaques, la cyber-résilience en revanche couvre un spectre plus large ; car il s'agit aussi et surtout d'améliorer les capacités de remédiation et de reprise d'activité.

Un autre aspect de la cyber-résilience consiste à concevoir et à mettre en œuvre des dispositifs robustes, susceptibles de s'organiser rapidement face aux nouvelles menaces. En effet, les attaques sont de plus en plus intelligentes et se présentent sous des formes diverses et de plus en plus difficiles à prédire. Il convient donc de mettre en place des mécanismes d'adaptation basés sur des processus d'évaluation continue des risques.

Le concept de cyber résilience est de plus en plus mis en avant par les référentiels spécifiques à la protection des infrastructures d'importance vitale tels que le framework NIST (National Institute of Standards and Technology) développé par les Etats-Unis. En effet, les secteurs d'importance vitale constituent désormais des cibles privilégiées pour les attaquants compte tenu des enjeux qui s'y présentent. Le secteur financier est l'un des exemples les plus illustratifs, en témoignent les pertes annuelles des institutions financières imputables aux cyberattaques qui s'élèveraient à près de cent milliards de dollars selon une modélisation effectuée en 2018 par les services du Fond Monétaire International (FMI). D'ailleurs, cette institution recommande de s'orienter vers une meilleure maitrise des moyens permettant de renforcer la résilience des institutions et des infrastructures financières, pour à la fois réduire les probabilités de succès des cyberattaques et faciliter une reprise rapide et en douceur des activités

Aujourd'hui, il convient aussi aux acteurs nationaux d'intégrer la cyber-résilience dans leurs stratégies opérationnelles afin d'être mieux préparés à faire face aux cyber-menaces. C'est dans ce sens que sont inscrites plusieurs actions entreprises jusque-là par la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) et qui ont visé à renforcer la résilience des systèmes d'information nationaux. Il s'agit notamment du :

- Renforcement de la résilience de l'Internet national, principal médium assurant l'interconnexion entre les systèmes de tous les acteurs aussi bien publics que privés. Dans ce

sens, des études techniques et des projets ont été menés en partenariat avec l'ANRT pour la sécurisation des protocoles BGP et DNS et la mise en place de systèmes autonomes ;
- Protection des systèmes d'information sensibles des infrastructures d'importance vitale à travers la mise en œuvre de directives et de mécanismes réglementaires pour le contrôle et le suivi des incidents de sécurité ;
- Amélioration de la gestion des crises et événements cyber majeurs à travers la mise en place et l'animation d'un dispositif interministériel de gestion de crises cyber.

Aussi, et dans la continuité de l'initiative menée par la DGSSI pour le déploiement des Centres Opérationnels de Sécurité (SOC) au sein même des entités publiques et Infrastructures d'Importance Vitale afin de les doter de capacités propres de supervision, il est question aujourd'hui de les inciter à renforcer davantage la résilience de leurs systèmes internes. Il s'agit pour eux de gérer la sécurité en adoptant une approche qui implique les individus, les processus et la technologie afin de renforcer les cinq piliers de la cyber-résilience :

- la ***préparation*** par l'identification des informations essentielles à l'activité, leur emplacement, leur degré de vulnérabilité ainsi que la tolérance aux risques.
- La ***protection*** par la mise en œuvre de mesures de protection destinées aux infrastructures et aux services critiques afin de limiter l'impact d'une attaque.
- La ***détection*** par la mise en place de moyens adéquats permettant de surveiller de manière continue les événements internes de sécurité et leur mise en corrélation avec les menaces externes.
- La ***remédiation*** par la définition de procédures claires à suivre en cas d'incident et la mise en place d'équipes d'intervention avec des rôles et responsabilités prédéfinis.
- Enfin, la ***récupération*** par la mise en œuvre de systèmes et plans appropriés pour restaurer les données et les services susceptibles d'avoir été impactés.

Dans ce contexte, la DGSSI a organisé la 6ème édition de son séminaire annuel de sensibilisation sous le thème : «***Cyber-résilience : Nouvelle approche pour relever le défi du cyber-risque*** ». L'objectif étant de présenter les différents aspects relatifs à cette notion ainsi que les démarches et retours d'expériences permettant de construire un écosystème cyber résilient.

Le séminaire a eu lieu le **30 Octobre 2018** 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 et des organismes publics ainsi que ceux des Infrastructures d'Importance Vitale.

Trois sessions, animées par des experts nationaux et internationaux et des responsables de la DGSSI, ont été au programme de ce séminaire dont deux consacrées à la définition du concept de cyber résilience et son implémentation. La troisième session est une étude de cas relative à la cyber résilience dans le secteur financier qui a été animée en partenariat avec BANK AL-MAGHRIB.

Mots d'ouverture :

Mr. Abdellatif Jouahri, Wali de Bank Al-Maghrib,

Mr. Abdeltif Loudiyi, Ministre délégué, chargé de l'Administration de la Défense Nationale.

Mr. Azzelarab Hassibi, Directeur Général de L'Agence Nationale de Réglementation des Télécommunications (ANRT)

Monsieur Le Wali de Bank AL-MAGHRIB a salué les efforts déployés par la DGSSI pour relever le niveau de maturité de la sécurité des systèmes d'information au niveau national. Il a aussi souligné l'importance qu'accorde Bank AL-MAGHRIB à la cyber sécurité et la cyber résilience en tant qu'institution et régulateur du secteur banquier national.

La cyber résilience constitue un réel enjeu de stabilité financière. A ce titre, les exigences règlementaires n'ont cessé de se renforcer, qu'il s'agisse de celles applicables aux organismes de crédit ou aux gestionnaires des systèmes de paiement et de règlement.

Dès 2005, les directives de la Banque Centrale exigeaient la mise en place par les établissements de crédit de plans de continuité d'activité, leur permettant de se prémunir contre des perturbations opérationnelles majeures dont les attaques d'ampleur sur leurs systèmes d'information. Aussi, afin de renforcer la sécurité de ces systèmes, une directive définissant le cadre de conduite de tests d'intrusion a été adoptée en 2016 imposant aux banques la mise en œuvre de programmes annuels de tests dont les résultats font l'objet de reporting à Bank Al-Maghrib.

En outre, en application des dispositions réglementaires établies par la DGSSI, relatives à la protection des Systèmes d'Information sensibles des Infrastructures d'Importance Vitale, Bank Al Maghrib, en tant que coordinateur du secteur, a procédé à l'identification des établissements à caractère vital et a veillé à l'harmonisation et à la cohérence des déclarations des SI sensibles.

Actuellement, la banque centrale travaille sur la mise en place d'un cadre de stabilité financière et de surveillance macro-prudentielle qui tient compte du caractère systémique du cyber risque. Des exercices de simulation de crise autour de scénarii de cyberattaque sont prévus dans le cadre de la coordination de la continuité d'activité de la place afin de mieux se préparer à des crises opérationnelles majeures pour lesquelles les réponses individuelles des opérateurs pourraient s'avérer insuffisantes.

Monsieur le Wali a souligné l'importance qu'accorde Bank Al Maghrib à la conformité par rapport aux dispositions réglementaires élaborées par la DGSSI. Le pilotage de cette conformité s'inscrit dans le cadre du système de management de la sécurité de l'information de la Banque. L'institution a également déployé un plan de continuité d'activité supporté par un site de secours et mis en place un centre opérationnel de sécurité (SOC) qu'elle ambitionne de faire évoluer en CERT.

Enfin, Monsieur le Wali a rappelé l'importance et la nécessité de la coordination, de l'échange et du partage, à l'instar de cet événement organisé par la DGSSI, pour mieux se préparer aux cyber risques.

Selon Monsieur le Ministre délégué, chargé de l'Administration de la Défense Nationale, la cyber résilience suscite l'intérêt à tous les niveaux par l'approche qu'elle propose pour faire face aux menaces grandissantes du cyber espace. L'ensemble des secteurs d'activité sont désormais impactés par le digital ce qui a élargi les surfaces d'attaque au niveau des systèmes d'information. Par conséquent, les experts s'accordent sur le fait que les cybermenaces constituent désormais un défi de premier plan, en particulier pour les décideurs.

Dans ce contexte, on ne parle plus seulement de cyber sécurité, qui consiste à protéger les systèmes d'information par des moyens physiques ou par des mesures de protection contre les intrusions, les attaques ou les effets des catastrophes , on parle aussi de cyber résilience, qui consiste outre la réduction des risques, à développer la capacité d'une organisation à résister et à pouvoir reprendre et continuer une activité normale.

La réponse aux menaces actuelles devra passer ainsi par une approche plus pragmatique faisant appel à des dispositifs robustes impliquant à la fois l'organisation et les moyens informatiques et susceptibles de s'adapter rapidement aux nouvelles menaces par la mise en place de processus d'évaluation continu des risques.

Mr. Le Ministre a insisté sur la nécessité d'adopter une attitude de vigilance pour relever le défi de l'hyperconnexion et de la résilience et tirer profit des avantages concurrentiels et de productivité offerts par le développement des systèmes d'information. Il a ainsi rappelé les différentes actions menées par la DGSSI dans ce sens en commençant par la Directive Nationale de la Sécurité des Systèmes d'Information mise en place en 2014 et qui avait pour objectif d'homogénéiser et de relever le niveau de maturité de la SSI des organismes de l'Etat et intégrait déjà certains aspects relatifs à la résilience.

Les exigences de sécurité, ont pris une dimension encore plus importante dès 2016, notamment en ce qui concerne les infrastructures d'importance vitale et ce à travers la mise en place d'un cadre réglementaire qui s'oriente davantage vers les aspects de cyber résilience. Ce cadre prévoit la mise en place de centres opérationnels de sécurité (SOC), précise les

modalités de préparation des plans de continuité et de reprise d'activité et instaure la déclaration obligatoire des incidents de sécurité à la DGSSI ainsi que la réalisation d'audits réguliers de la sécurité des systèmes d'information.

Au nom de Monsieur le Ministre de l'Industrie, de l'Investissement, du Commerce, et de l'Economie Numérique, Monsieur le directeur général de l'ANRT a affirmé dans son mot d'ouverture que les enjeux de la cyber sécurité peuvent être vus sous différents angles à savoir : économique, industriel, sociétal ainsi que celui de la souveraineté. La cybersécurité et la confiance numérique représentent ainsi une nouvelle donne stratégique dans le développement du Digital notamment au Maroc.

La transformation digitale requière l'adoption rapide de nouvelles technologies et l'ouverture des SI aux partenaires et aux clients. En parallèle, les cybers attaques et la criminalité ne cessent de croitre de manière exponentielle. Conscients de ces risques, les Etats et régulateurs augmentent leur actions et exigent une meilleure gestion de ces risques, espérant ainsi garantir une protection améliorée et une réaction appropriée en cas d'incident majeur.

Pour le Maroc, le gouvernement a déjà entrepris un certain nombre de mesures pour le développement de la cyber sécurité et l'instauration de la confiance numérique, notamment par le renforcement du cadre juridique à travers un certain nombre de Lois comme la Loi 09-08 pour la protection des données à caractère personnel, la Loi 53-05 relative à l'échange électronique de données juridiques, la Loi 31-08 relative à la protection du consommateur en particulier dans le contexte de l'e-commerce ou le projet de Loi 121-12 qui traite des infrastructures vitales et précise les responsabilités des opérateurs télécom.

S'agissant de ses relations avec les pays partenaires, le Maroc a ratifié la convention du Conseil de l'Europe sur la cybercriminalité et son protocole additionnel, ainsi que la convention de l'Union Européenne relative à la protection des données personnelles et son protocole additionnel et la convention des pays arabes sur la cybercriminalité.

Néanmoins, ces efforts devraient être poursuivis à travers le renforcement du cadre juridique notamment en matière d'hébergement des données. La sensibilisation et la communication au profit des citoyens. L'accompagnement des entreprises notamment les PME pour développer des dispositifs fiables de détection d'attaques et de protection.

La nouvelle Agence de Développement du Digital est à disposition de la DGSSI pour contribuer dans les chantiers de

sensibilisation, de vulgarisation et de formation en cybersécurité.

PANEL N°1 : RESILIENCE VS SECURITE DANS L'ERE NUMERIQUE :

Modérateur : Colonel Abdellah BOUTRIG

Directeur de l'Assistance, de la Formation, du contrôle et de l'Expertise au sein de la DGSSI.

INTERVENANTS

Mr. Kevin Henry : Expert en cybersécurité ;

Dr. Haji Amirudin Abdul Wahab : Directeur général de « Cyber Security Malaysia » ;

Mr. Alberto Hernandez Moreno : Directeur des Opérations de l'Institut National Espagnol de Cyber sécurité INCIBE.

Cette session avait pour objectif de répondre aux questions relatives à la construction d'un cadre complet de résilience à travers la mise en œuvre de nombreux éléments qui composent un programme de sécurité. Il était également question de présenter les normes et standards internationaux qui mettent en avant le concept de résilience.

Le Colonel BOUTRIG a présenté des éléments de réflexion pour monter un programme de cyber résilience au sein d'une organisation après avoir défini la cyber résilience comme étant la capacité d'un système à continuer à fonctionner dans des conditions défavorables ou sous stress, même dans un état dégradé ou affaibli, tout en maintenant des capacités opérationnelles essentielles et retrouver une posture opérationnelle efficace dans un délai conforme aux besoins de l'organisation.

Le programme de cyberrésilience doit faire l'objet d'une stratégie portée par le top management et avec l'engagement de tous les responsables au sein de l'organisation. La stratégie présentée pourrait s'articuler sur cinq piliers à savoir :

- La préparation du personnel par la sensibilisation sur les politiques et les procédures existante en matière de cyber sécurité. Ce personnel doit être conscient de la valeur des informations sensibles et maitriser leur gestion ;
- L'identification des actifs informationnels de l'organisation, puis, l'évaluation des risques sur ces actifs et l'identification des mesures à prendre pour gérer ces risques ;
- La protection qui consiste à implémenter les mesures préalablement identifiées et puis renforcer leur efficacité et efficience par la conduite d'audits périodiques ;
- La détection qui concerne la mise en œuvre des moyens appropriés afin d'identifier les attaques et évaluer les systèmes pouvant être affectés tout en garantissant une réponse en temps voulu ;
- La résolution des problèmes, qui est susceptible de réduire le délai de réaction aux incidents de sécurité et limiter l'impact de l'attaque détectée ;
- La récupération qui implique le développement et la mise en œuvre des systèmes et des plans appropriés pour restaurer les données et les services

susceptibles d'avoir été impactés lors d'une cyberattaque, l'objectif étant d'être en mesure de reprendre l'activité et de restaurer les processus et systèmes stratégique sans délais. Pour cela, il faut disposer d'un plan clair et détaillé.

Selon le cabinet Forreter, une autre approche pour appréhender les attaques ciblées et renforcer la résilience consiste à adresser la problématique selon une hiérarchisation des besoins de sécurité en 6 niveaux :

- Une stratégie de sécurité actualisée ;
- Une politique adaptée pour le recrutement et la fidélisation du personnel ;
- Un renforcement des fondamentaux de la sécurité ;
- Un portefeuille intégré de solutions pour l'orchestration des actions de sécurité ;
- Une consolidation des capacités de prévention ;
- Une détection rapide conjuguée à une réponse efficace aux incidents.

Par la suite, l'intervenant a cité quelques standards internationaux qui intègrent dans leurs recommandations des contrôles pour mettre en place un programme de cybersécurité et de cyber résilience à savoir :

- Le cadre de gouvernance de l'institut national américain des standards et de la Technologie (NIST) ;
- La directive sur la sécurité des réseaux et des systèmes d'information « NIS » de l'agence Européenne chargée de la sécurité des réseaux et de l'Information (ENISA) ;
- Le standard de Gouvernance et de Gestion des risques liés à la cybersécurité ;
- Le standard ISO 27001 sur les exigences relatives aux systèmes de management de la sécurité des informations ;
- Ainsi que le standard ISO 22301 sur les systèmes de management de la continuité d'activité.

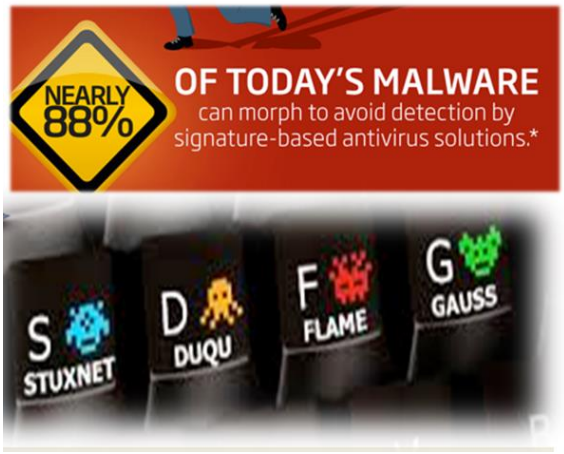
Mr. Kevin HENRI, consultant sénior en cybersécurité, a précisé qu'il est possible de sécuriser nos systèmes de manière à obtenir une meilleure résilience. Cette résilience nous donnerait la souplesse nécessaire pour nous adapter aux nouvelles menaces grâce à une stratégie, une bonne gouvernance et une étroite collaboration entre départements.

Toutefois, force est de constater qu'un grand gap réside entre les stratégies et les actions menés pour leur concrétisation. Des organismes reconnus mondialement ont dépensé beaucoup de ressources en technologies et en plans d'actions, alors que finalement leurs systèmes présentent des manquements graves à la sécurité.

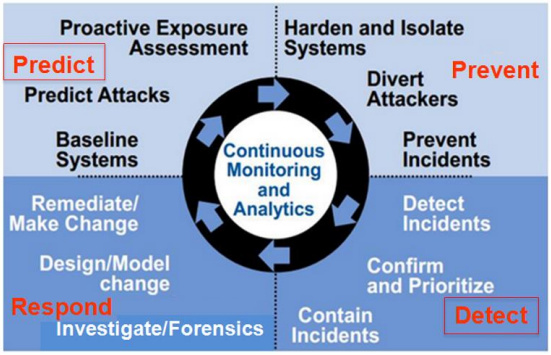
La solution ne réside pas toujours dans la mise en place de nouvelles technologies, mais plutôt d'offrir aux gens la possibilité de reconnaitre les menaces et les risques en premier lieu, puis de prendre les mesures nécessaires afin d'y faire face lorsqu'il y a lieu.

Il est aussi primordial de souligner l'importance d'analyser les incidents et les expériences passés et de prendre des actions concrètes et rapides avec un engagement clair pour construire et renforcer les défenses face aux attaques et pouvoir s'en prémunir dans le futur.

Dr. HAJI AMIRUDIN ABDUL WAHAB, Directeur général de Cyber Security Malaysia, a partagé avec les participants au séminaire l'expérience de la Malaisie en matière de cyber résilience. Ce pays a connu une émergence importante dans l'usage des nouvelles technologies dans à peu près tous les secteurs, ce qui a augmenté de manière substantielle les risques liés aux cyberattaques. Pour s'en prémunir, Ils ont adopté une approche préventive qui porte sur la sensibilisation et la formation à la cybersécurité, la mise en place d'une politique nationale depuis 2006, la conformité des processus aux standards internationaux et la promotion des bonnes pratiques de déploiement associées aux technologies utilisées.



Cependant, cette approche s'est avérée insuffisante face aux attaques qui ne cessent d'évoluer avec a peu près 88% des Malwares qui ont des capacités de mutation leur permettant d'esquiver la détection par les outils traditionnels. L'adoption d'une nouvelle approche, qui n'est pas focalisée uniquement sur la prévention, mais plutôt sur le renforcement des capacités de prédiction et de détection s'avère plus efficace. D'où la mise en place en Malaisie d'un service nommé CyberDEF.



Ceci dit, il est toujours nécessaire de suivre l'évolution des technologies émergentes et d'avoir une stratégie adaptée pour appliquer efficacement les principes fondamentaux de la cybersécurité avec des fonctionnalités et des techniques innovantes, ainsi que de renforcer les collaborations et partenariats à l'échelle internationale afin d'être cyber résilient.

Mr. Alberto Hernandez Moreno de l'Institut National Espagnol de Cyber sécurité (INCIBE) a présenté quant à lui le retour d'expérience Espagnol.

L'institut en question a pour but de protéger les citoyens espagnols et le secteur privé, par le développement de la cybersécurité et la confiance numérique.

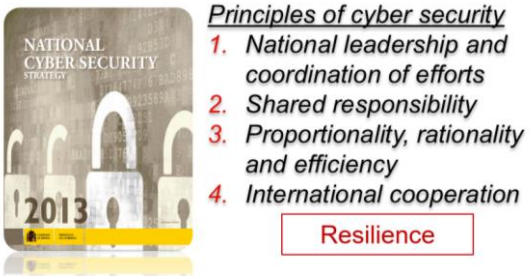
L'intervenant a dressé un portrait de la cybersécurité dans ce pays à travers des statistiques sur le nombre d'incidents de sécurité déclarés et leur étendue sur le territoire espagnol ainsi que la contribution d'INCIBE dans leur gestion.

Il a ainsi confirmé que des secteurs d'importance vitale, comme le secteur financier, de transport ou de l'énergie, sont les cibles privilégiées des attaquants.

S'agissant de la stratégie de cybersécurité espagnole, il a affirmé qu'elle vise la résilience à travers quatre principes :

- Le leadership national et la coordination des efforts ;
- La responsabilité partagée ;
- La proportionnalité, rationalité et efficience ;
- Et la coopération internationale.

Cette stratégie a été notamment déclinée en un plan national de cybersécurité et un cadre réglementaire spécifique composé de Lois et Décret Royaux pour la protection des infrastructures critiques ainsi que de guides, outils et instruments sectoriels de cybersécurité.



L'Espagne a aussi reconnu l'importance de la recherche et du développement et a pu focaliser ses efforts sur la mise en place d'activités basées sur la recherche, la fourniture de services et la coordination avec les universités et les spécialistes en la matière.

Ainsi, l'INCIBE contribue à renforcer la cybersécurité et la cyber résilience au niveau national et international en contribuant massivement à supporter des projets de recherche liés à la cybersécurité.

PANEL N°2 : CONSTRUIRE UN ECOSYSTEME CYBER RESILIENT :

Modérateur : Colonel Major EL Mostapha RABII

Directeur du Centre de Veille, de Détection et de Réponse aux Attaques Informatiques (MaCERT) au sein de la DGSSI

INTERVENANTS :

Dr. Lyron H. Andrews : Expert en cybersécurité ;
M. Paul Dewyer : Expert en cybersécurité IBM ;
Lt-Colonel Khalil NOSSAIR : Chef de la Division Contrôle et Expertise au sein de la DGSSI

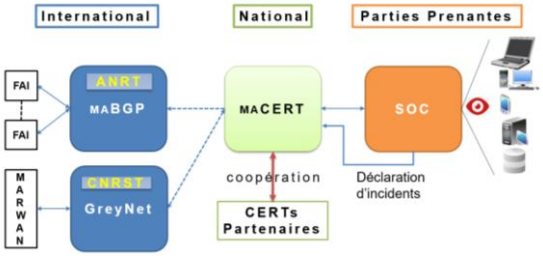
Si la cybersécurité consiste à protéger les systèmes d'information contre les menaces cyber en empêchant l'exploitation des vulnérabilités, la cyber résilience se veut plus pragmatique en cherchant en plus à minimiser l'impact suite à des attaques de plus en plus inéluctables. Mettre en place un système résilient consiste à le construire de manière à rendre une rupture ou une défaillance, improbable, de courte durée et avec un impact minimal sur les objectifs et la mission d'un organisme.

Le Colonel Major EL Mostapha RABII, Directeur du Centre de Veille, de Détection, et de Réaction aux Attaques Informatiques a mis l'accent sur la diversification et le perfectionnement des vecteurs d'attaques dans le cyberspace. Il a présenté dans ce sens des statistiques dévoilant la domination des attaques de crypto-mining suivies par les attaques de type « détournement de comptes » avec presque 15% des attaques de type phishing et enfin des attaques liées à l'exploitation des vulnérabilités. Les systèmes de contrôles industriels sont devenus également la cible privilégiée des cyber-attaquants. En effet, dans un rapport publié en 2017 par « **BUSINESS ADVANTAGE** », sur un échantillon de 359 entreprises industrielles interrogées dans 21 pays, plus de 54% ont subi un incident relatif à la sécurité de leurs systèmes industriels durant les 12 derniers mois.

A partir de ces constats, il apparait que face à un cyberspace aussi fragile, instable et potentiellement hostile il faut désormais se préparer à subir des attaques et avoir la capacité à continuer et à reprendre rapidement une activité normale. Pour ce faire, le plan de continuité d'activité constitue l'élément majeur de la stratégie de résilience à condition de l'adapter au caractère particulier du cyber-risque pour ne pas se retrouver en cas de crise avec des dispositifs de continuité d'activité inefficients.

Dans ce registre, la DGSSI a mené plusieurs études sur la résilience du réseau Internet au niveau national étant donné qu'il

constitue l'épine dorsale des systèmes de communication pour la grande majorité des organismes nationaux et que la continuité de leurs activités en dépend étroitement. En collaboration avec l'ANRT, la DGSSI a identifié et mesuré des indicateurs pertinents et représentatifs de cette résilience, notamment, l'Etat des protocoles BGP et DNS chargés du bon fonctionnement d'internet ainsi que le service TLS utilisé par les navigateurs Web pour le chiffrement des communications. Le but étant d'encourager notamment les fournisseurs d'accès à internet à s'approprier les bonnes pratiques d'ingénierie admises pour que ces deux protocoles soient bien implémentés afin de réduire l'effet de menaces cyber telles que les attaques par déni de service distribuées (DDOS) ou l'usurpation des préfixes (DNS Hijacking). Ce projet a été accompagné par le déploiement d'une plateforme de supervision du protocole BGP intitulée « maBGP ».



Le système de veille et de détection déployé par la DGSSI a aussi été revu dans le but d'améliorer la réactivité des parties prenantes et de renforcer leur résilience. En effet, en plus de la supervision des frontières des systèmes d'information et de la connexion Internet prises en charge jusqu'à maintenant par le maCERT, les parties prenantes se doivent désormais d'assurer la supervision interne par des SOC (centres opérationnels de sécurité). La DGSSI continuera à assurer les fonctions de veille, d'analyse et d'assistance en cas d'attaque.

Enfin, et dans le but de rester informé de l'évolution de la menace, le maCERT a mis en place un système GreyNET en collaboration avec le Ministère de l'Education Nationale et le Centre National pour la Recherche Scientifique et Technique (CNRST). Ce GreyNET va permettre de détecter les attaques automatisées et d'étudier dans un environnement restreint les tendances et les nouvelles techniques d'attaques.

S'exprimant au sujet de la construction d'un écosystème cyber résilient en alliant à la fois technologie et organisation, M. Lyron H. Andrews, expert en cyber sécurité, a entamé son intervention en expliquant que l'histoire est riche d'exemples qui démontrent que les personnes ou institutions ayant réalisé le plus grand nombre d'exploits sont également ceux qui ont essuyé le plus grand nombre d'échecs. Autrement dit, c'est en apprenant de son échec qu'on peut rebondir et réaliser un exploit.

Il a affirmé que le meilleur moyen de bâtir et de confirmer la résilience d'un système est de le soumettre régulièrement à des défaillances programmées afin de corriger au fur et à mesure les dysfonctionnements perçus. Cette démarche, qualifiée

d'ingénierie du CHAOS, a fait le succès du géant américain Netflix qui en a fait usage pour assurer la résilience de son fameux système de diffusion de contenu en ligne dont la continuité de service est capitale.

Le principe de l'ingénierie du chaos est d'établir une référence comme étant un état stable et souhaité du système d'information dans des conditions optimales, ensuite de stimuler des pannes en conditions réelles sur des systèmes de production pour en évaluer la résilience puis de trouver et corriger les faiblesses identifiées. Cette démarche peut se faire de manière progressive tel qu'illustré par le cas de Netflix qui a commencé par mettre une instance hors service puis une zone et enfin toute une région.

S'agissant d'atteindre un état de résilience à travers une organisation adéquate, l'intervenant a mis l'accent sur l'importance de privilégier une approche axée sur le développement d'une architecture globale d'entreprise plutôt que celle axée sur la conception immédiate de solutions techniques adhoc pour répondre à des besoins ponctuels. En effet, l'approche basée sur le développement d'architectures permet de penser des solutions cohérentes en abordant les problèmes sous différents angles (ex : sur les plans technologique, organisationnel et métier).

Sur cet aspect en particulier de développement des architectures, il existe des Framework tel que ZACHMAN, SABSA ou ISO 27034-1, qui représentent des approches intéressantes. Ces frameworks commencent tous dans un premier temps par la compréhension du contexte d'un point de vue métier, puis la définition de l'architecture qui peut répondre aux besoins métier pour arriver enfin à la phase de conception et de choix des solutions techniques.

M. PAUL DWYER, spécialiste en cyber sécurité chez IBM, a confirmé le constat de ses prédécesseurs quant à l'importance de la gestion de la compétence des équipes aussi bien que celle de la technologie pour le développement de la résilience. En effet, en se basant sur le retour d'expérience d'une centaine de centres opérationnels de sécurité (SOC) qu'elle équipe un peu partout dans le monde, IBM a pu évaluer les priorités selon sept dimensions à savoir : Technologie, processus, métriques, rapports, gouvernance, source de données et cas pratiques. La dimension qui a affiché la plus grande maturité partout dans le monde dans les SOC est celle de la technologie. Toutefois, bien que le fait d'acheter des outils et des solutions soit essentiel pour résoudre des problèmes technologiques, c'est aux équipes que revient le rôle primordial de savoir les employer correctement et c'est ce qui

compte le plus pour réussir les missions d'un SOC.

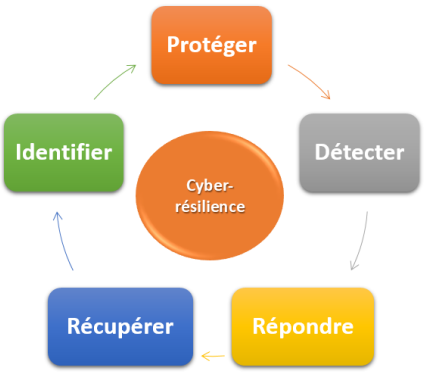
Dans le contexte de cyber résilience, la mission principale des SOCs est la coordination d'une défense multicouche permettant de détecter, de protéger et de répondre aux menaces pouvant toucher une organisation. L'intervenant a expliqué comment intégrer la mise en place d'un SOC dans le plan global de résilience d'une organisation à travers l'adoption d'un modèle opérationnel qui repose principalement sur quatre niveaux : donnée, technologie, opération et gouvernance et ce en faisant ressortir les principales recommandations à prendre en considération lors de la mise en place des SOC.

Pour le niveau technologique, il devient important de combiner les outils SIEM et Big Data afin de pouvoir détecter même les attaques inconnues et qui représentent actuellement plus de 42% des attaques.

Pour le niveau opération, l'automatisation des activités d'opérations du SOC est le mot d'ordre désormais afin de réduire le taux d'erreurs et aussi le cout de gestion et pouvoir se focaliser sur les autres dimensions et pas seulement sur les opérations. Il s'agit d'optimiser les processus et les personnes. Cela représente la vision future pour les SOC et les dernières tendances dans ce domaine avec la mise en place d'indicateurs clés de performance (KPI) permettant de mesurer leur efficacité en temps réel.

Dans son intervention, le Lt-Colonel NOSSAIR a affirmé que la cyber-résilience est un nouveau concept qui vient s'ajouter au panorama des concepts de la sécurité des systèmes d'information mais qui ne change pas pour autant les fondamentaux de la sécurité. Il met juste l'accent sur des aspects particuliers inhérents à la continuité d'activité.

S'agissant de l'apport de la stratégie et de la réglementation, il a expliqué que ces deux composantes ont certainement contribué d'une manière ou d'une autre dans le renforcement d'un ou plusieurs des piliers de la résilience préalablement évoqués (à savoir Préparation, Identification, Protection, Détection, Résolution et Récupération)



A titre d'illustration, dans la stratégie nationale de cybersécurité adoptée par le MAROC en 2012, les actions liées au recensement, à l'identification et à la

classification des systèmes d'information et aussi à l'évaluation des risques ont un impact direct sur le pilier « Identification ». La mise en place d'un réseau de transmission sécurisé de l'état, l'implication des opérateurs et des fournisseurs d'accès Internet, la sécurisation des sites web et des services publics en ligne et enfin les actions relatives au renforcement des fondements de la sécurité comme la formation et la sensibilisation ont un impact direct sur le pilier de « Protection ».

L'intervenant a ainsi fait la correspondance entre les programmes et actions de la stratégie nationale et le reste des piliers de la résilience.

En ce qui concerne l'apport de la réglementation, une correspondance a été faite entre le développement de la résilience et la mise en place de trois dispositifs réglementaires.

Tout d'abord la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI) qui comprend 104 règles de sécurité reparties sur 11 chapitres inspirés de la norme ISO 27002 :2005 et représentant le socle commun et minimum que tous les départements publics sont appelés à implémenter. Il a souligné que des chapitres entiers de cette directive sont consacrés à la gestion des incidents et à la continuité de l'activité ce qui représente un lien direct avec la résilience.

Deuxièmement, le dispositif de protection des systèmes d'information sensibles des infrastructures d'importance vitales qui a été mis en place au travers d'un décret en mars 2016. Ce dispositif a permis d'une part l'élargissement du champs de compétence de la DGSSI aux entités privées faisant partie des secteurs d'importance vitale mais aussi d'autre part de mettre en place des mesures obligatoires comme l'identification des systèmes d'information sensibles, la mise en place de moyens de supervision et de détection, la déclaration et le traitement des incidents de sécurité et la mise en place des plans de continuité et de reprise d'activités ainsi que la réalisation d'audits de sécurité périodiquement menés par la DGSSI ou pas des prestataires homologués par la DGSSI.

Dans ce sens, la DGSSI a déployé quelques mesures d'accompagnement. Il s'agit notamment de la directive qui fixe les règles de sécurité et les modalités de déclarations des systèmes sensibles, des guides et des référentiels techniques de sécurité et du dispositif d'homologation des prestataires d'audit. Ce dernier permettra d'ailleurs de créer un écosystème d'expertise dans l'évaluation et l'audit au niveau national et de désigner des prestataires qui sont à même de réaliser cette activité selon les normes et les bonnes pratiques en vigueur.

Le troisième dispositif qui a été mis en place par la DGSSI, est celui de la gestion des crises cybernétique. C'est un dispositif interministériel dont l'objectif est d'assurer une meilleure réactivité, de coordonner l'action et d'éviter l'improvisation. Ce dispositif qui a été mis en place via une organisation à deux niveaux : un niveau décisionnel qui approuve l'activation du dispositif, qui invite les départements concernés à se faire représenter en fonction de la situation, qui peut faire appel à l'expertise externe et qui assure aussi la communication vis à vis du public. Et un niveau opérationnel chargé de la gestion opérationnelle et technique de la crise depuis l'identification des éléments déclencheurs jusqu'à la clôture.

PANEL N°3 : Etude de Cas : Résilience du Secteur Financier

MODERATEUR :

M. Nour-Dine HAJJAMI (Maroc)

Directeur Organisation et Système d'Information de Bank Al-Maghrib

INTERVENANTS :

M. Ismail DOUIRI (Maroc)

Directeur Général d'ATTIJARI WAFABANK

M. Philippe LANDUCCI (Suisse)

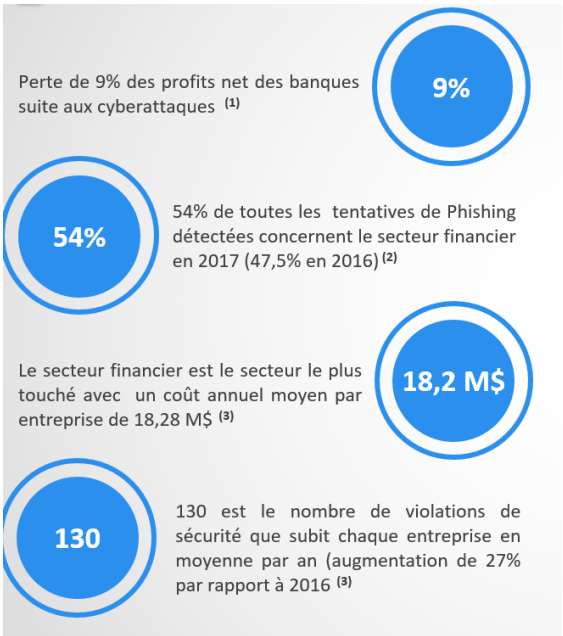
Responsable de la Division Informatique de la Banque Nationale Suisse

M. Luis Gonçalves (Portugal)

Responsable cyber-sécurité de la Banque Centrale du Portugal

La bonne tenue du système financier dépend de la résilience opérationnelle collective des institutions et des infrastructures financières. La montée en puissance des cyberattaques soulève toute une gamme de nouveaux défis en matière de résilience opérationnelle de ces systèmes. Il convient de prendre les dispositions nécessaires pour parvenir à une meilleure compréhension des moyens de renforcement de la résilience, pour à la fois réduire les probabilités de succès des cyberattaques et faciliter une reprise rapide des activités.

M. HAJJAMI, Directeur Organisation et Système d'Information de Bank Al-Maghrib**,** a rappelé que la complexité numérique a atteint un point critique en matière de cybersécurité car l'évolution des menaces et l'élargissement de la surface d'attaque (Mobilité, Cloud, réseaux sociaux, etc.) ont évolué d'une manière exponentielle ces dernières années. En contrepartie, la réponse en matière de cyber sécurité à ce genre de risques se doit d'être double. Tout d'abord une convergence devrait être assurée en matière d'architecture et de démarche mais en même temps une divergence doit être assurée en matière de livraison des solutions et en matière de prise de décision.



Des statistiques illustrant l'impact des cyberattaques sur le secteur financier ont été présentées pour démontrer que ce secteur compte parmi les plus ciblés. En effet, les pertes annuelles moyennes des institutions financières imputables aux cyberattaques avoisineraient près de 9% des profits nets des banques. De même, 54% de toutes les tentatives de Phishing détectées ont concerné le secteur financier

en 2017 (47,5% en 2016). En plus, chaque entreprise subit en moyenne près de 130 violations de sécurité par an (augmentation de 27% par rapport à 2016).

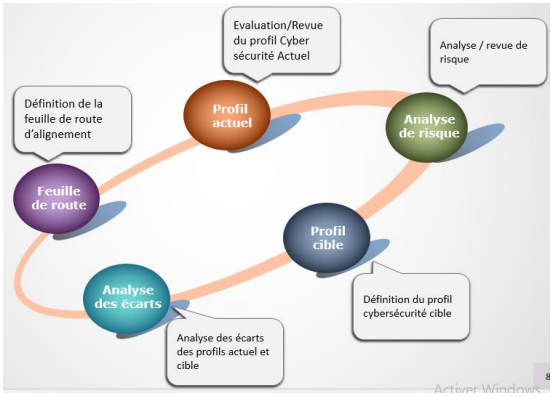
Il devient ainsi primordial de penser à la cyber résilience avant de mettre en place une activité ou une structure opérant dans le secteur financier en particulier. En effet, la résilience organisationnelle se base sur 5 principaux axes, notamment, le leadership, la culture, les processus, les personnes, et l'infrastructure.

L'intervenant a ensuite présenté les résultats de deux études menées en 2017 par le cabinet de recherche *Gartner.* La première démontre le manque d'alignement entre la stratégie de sécurité et la stratégie de l'entreprise à cause de la subsistance d'un gap entre ce que pensent les responsables de la sécurité et ce qu'attendent les responsables métiers. La deuxième étude expose le cycle de 5 phases (Hype Cycle) par lequel passent les nouvelles technologies ou les nouveaux concepts, en général, et la gestion de la continuité d'activité et la résilience IT en particulier.

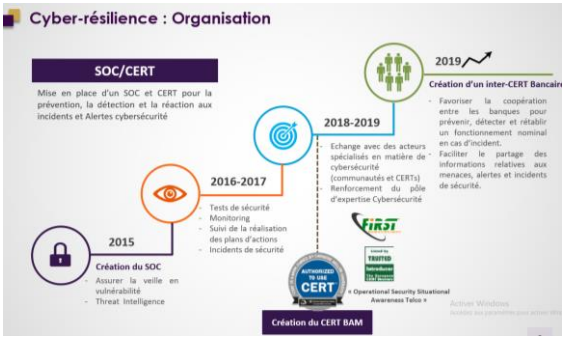
Il a expliqué qu'en matière de Résilience, les outils utilisés peuvent être localisés au sein de l'entreprise ou bien mis en place au niveau du Cloud à travers des partenariats permettant d'assurer la flexibilité et l'élasticité de l'offre en fonction de la demande. Il s'agit de profiter des technologies offertes tout en maitrisant les risques qui en découlent.

La Banque Centrale dispose d'une structure organisationnelle composée d'une entité chargée des risques, d'une autre chargée du Système d'Information, des entités métiers et d'un comité de gouvernance stratégique qui veille à assurer l'alignement entre la stratégie IT et celle de l'institution. D'ailleurs, depuis plusieurs années, il n'existe plus une stratégie informatique au niveau de la banque centrale mais plutôt une stratégie de l'entreprise dans laquelle l'élément digital est bien intégré.

Bank Al-Maghrib s'est basé, comme la plupart des entreprises, sur des référentiels reconnus et a mis en place une démarche qualité, depuis 2006. A cet effet, plusieurs mesures de sécurité ont été mises en œuvre, notamment, la certification de tous les processus selon la norme ISO 9001, la mise en place d'un système de management de la sécurité de l'information (SMSI) et sa certification selon la norme ISO 27001 et l'intégration du Framework NIST (National Institute of Standards and Technology) avec les 20 contrôles du référentiel de sécurité SANS.

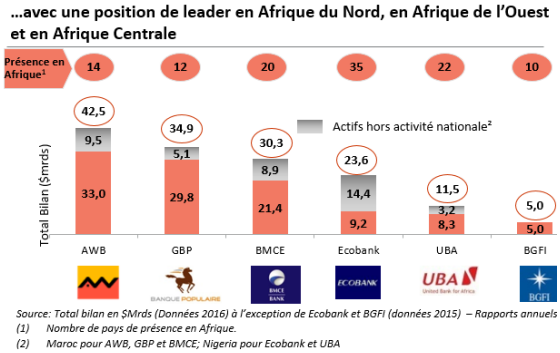


En plus de ces mesures de sécurité , un SOC a été créé en 2015 au niveau de Bank Al-Maghrib avec une perspective de le faire évoluer vers un CERT dédié à la Banque Centrale en premier lieu, puis créer un CERT interbancaire.



Enfin, pour améliorer la résilience du système d'information de la banque, des tests de sécurité et du monitoring ont été réalisés depuis 2016 et 2017, et des plans d'actions en réponse aux vulnérabilités, ont été élaborés.

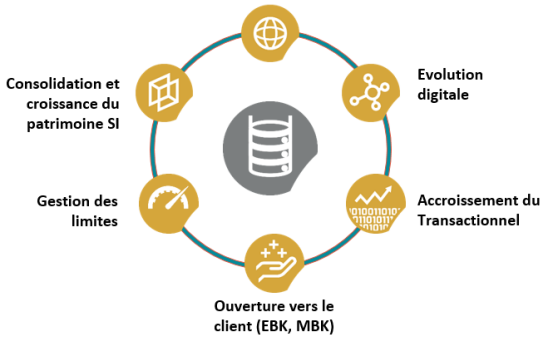
Au début de son intervention, M. DOUIRI, Directeur Général d'ATTIJARI WAFABANK, a mentionné qu'avec un bilan total dépassant les 50 milliards de dollars et une présence importante dans différents pays, ATTIJARI WAFABANK est le 5ème plus grand groupe financier à l'échelle du continent et que son patrimoine SI est le reflet de son histoire et le vecteur de sa future stratégie.



Source: Total bilan en $Mrds (Données 2016) à l'exception de Ecobank et BGFI (données 2015) – Rapports annuels
(1) Nombre de pays de présence en Afrique.
(2) Maroc pour AWB, GBP et BMCE; Nigeria pour Ecobank et UBA

Dans ce sens, il a soulevé la complexité de prendre des décisions en matière de cyber sécurité lorsqu'il s'agit d'une multitude d'activités et d'une aussi grande couverture géographique. En tant qu'institution financière, ATTIJARI WAFABANK est exposée aux risques et n'a pas seulement l'obligation de protéger l'activité de ses clients mais également l'image du pays.

Le système d'information de la banque est passé par trois phases. La première phase « post fusion » entre BCM et WAFABANK a permis de créer ATTIJARI WAFABANK. Durant cette phase, il y avait le e-Banking rudimentaire avec du contenu essentiellement informationnel et quelques transactions avec gestion stricte du risque induit qui a perduré jusqu'aux années 2004-2005. Depuis, il y avait eu une élimination progressive de la séparation physique entre le réseau interne et le réseau externe. Par la suite, la mise en place du premier schéma directeur SI post fusion identifiant d'importants besoins de transformation de l'architecture SI et indiquant la nécessité de créer une Couche d'intégration (middleware) permettant l'échange entre un back-office métier « LEGACY » et un front plus agile.



Ensuite une deuxième phase où a eu lieu une ouverture croissante avec le renforcement de l'infrastructure à travers plusieurs actions, notamment, le développement de nouveaux canaux et

l'investissement pour l'acquisition de deux datacenters conformes aux normes.

Enfin, une troisième phase durant laquelle, plusieurs actions ont été mises en place, dont principalement l'utilisation des services transactionnels par des centaines de milliers d'utilisateurs actifs et le déploiement des investissements progressifs pour renforcer les dispositifs de sécurité.

Dans le même cadre, la transformation d'ATTIJARI WAFABANK a été faite d'une manière progressive et une évolution de la maturité a été faite en parallèle avec les besoins des clients ou suite aux changements réglementaires. Néanmoins, il est désormais difficile de le faire d'une manière incrémentale, il s'agit plus d'une logique de rupture que d'une logique de continuité de la sécurité.

En matière de lutte contre les cybers menaces, une approche de minimisation des dégâts a été appliquée : (mesures de confinement, PATCHING, HARDENING), avec l'activation de la recherche et la surveillance permanente au niveau des plateformes de SIEM et ENDPOINTS et partage de l'information en interne et avec l'écosystème, ce qui a engendré une augmentation du niveau de dépense en matière de sécurité au niveau d'ATTIJARI WAFABANK. Ainsi le budget d'investissement en cyber sécurité a augmenté de 160% par rapport à l'année dernière et le budget de fonctionnement en sécurité informatique a augmenté de 60%.

Pour clore son intervention, M. DIOURI a souligné l'importance de mettre en place des mesures pour renforcer la cyber résilience face aux menaces et aux attaques d'ampleur mondiale, notamment le fait :

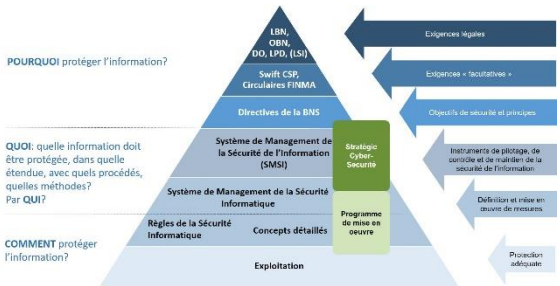
- d'agir sur tous les projets IT en intégrant la sécurité dans le cycle de vie des projets ;
- de renforcer les dispositifs d'audit automatisés et proactifs de la sécurité des infrastructures, réseaux, codes sources et applications ;
- de poursuivre et d'accélérer l'atterrissage des plans d'actions sécurité visant la conformité des plateformes sensibles par rapport à la DNSSI ;
- de renforcer la vigilance quant aux choix des solutions orientées Cloud en termes d'analyse des risques, de classification et de cartographie des risques ;
- de former et de sensibiliser les équipes et utilisateurs ;
- de renforcer la gouvernance de la sécurité à travers la mise en place d'un SMSI et la certification ISO 27001
- et de renforcer les dispositifs de surveillance SIEM et SOC pour la banque et ses filiales.

M. Philippe LANDUCCI, Responsable de la Division Informatique de la Banque Nationale Suisse (BNS), a mentionné que la BNS applique une approche « Top DOWN » systématique selon, les exigences légales et les exigences facultatives comme SWIFT CSP, Circulaires FINMA, les directives de la

DNS, les contrôles de la sécurité de l'information et les règles de sécurité Informatique et de l'Exploitation.

En effet, la BNS est composée d'une part, d'une entité de gestion des risques, responsable du système de contrôle interne des risques opérationnels (500 risques) et de la direction des exercices de la continuité de l'activité, et d'autre part d'une entité informatique qui assure le management de la sécurité informatique à travers les applications de banque centrale et la gestion interne et de l'infrastructure. Les deux entités coopèrent selon une gouvernance de stratégie commune et une mise en œuvre intégrée.

La BNS étant une société anonyme, elle est régie par une loi spéciale, la loi sur la banque nationale (LBN). Cette loi définit quelques aspects de la sécurité de l'information et de la gestion des risques opérationnels, tant pour la BNS que pour les infrastructures financières d'importance systémique. Une nouvelle loi fédérale sur la sécurité de l'information, applicable aux entreprises liées à la confédération - dont la BNS - est actuellement en préparation et devrait entrer en vigueur en 2019. En outre, la BNS a développé une stratégie « cyber sécurité » et un plan de mise en œuvre basés sur le cadre standard du NIST qui devraient lui permettre de se conformer aux régulations à venir et de faire face aux menaces émergentes.



La stratégie Nationale de protection de la Suisse contre les cyber-risques a été revue et étendue pour mieux tenir compte de leur importance. En effet, elle contient des mesures qui s'appliquent plus particulièrement au secteur financier notamment :

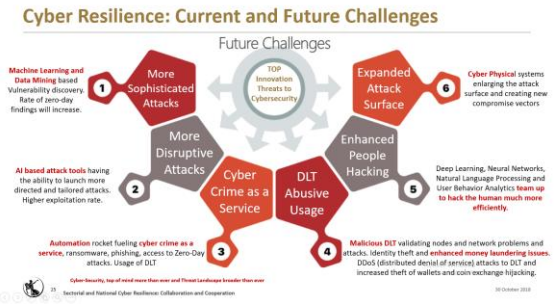
- l'extension des capacités permettant d'analyser et de présenter la situation de la cybermenace ;
- l'amélioration de la résilience informatique des infrastructures d'importance Vitale ;
- l'examen d'une obligation de notifier les cyber incidents et la décision quant à son introduction dans la Loi ;
- le développement de MELANI (Centrale d'enregistrement et d'analyse pour la sûreté de l'Information en SUISSE) en tant que partenariat public-privé pour les exploitants d'infrastructures critiques ;
- et la réalisation des exercices communs de gestion de crise au niveau de toutes les confédérations.

En relation avec la confédération et le secteur financier, la centrale MELANI, qui inclut le GovCert national, n'a pas un rôle de protection mais plutôt un rôle d'information, et elle a un groupe fermé d'utilisateurs de secteur financier (Uniquement les Banques Suisses). En outre, le secteur financier dispose d'une organisation de crise incluant l'opérateur de l'infrastructure financière (SIX), l'autorité de surveillance (FINMA), la BNS et les principales institutions financières en suisse. La BNS veille à partager ses informations sur les menaces et les attaques avec MELANI, avec le «**Working Group Information Technologie Security**» des banques suisses et avec un groupe d'environ 30 banques centrales afin

de permettre aux autres entités de profiter de ses expériences.

Après avoir rappelé l'évolution de la cybercriminalité, M. LUIS GONÇALVES, Expert en cybersécurité à la Banque Centrale du Portugal, a mentionné que nous vivons dans l'aire de cyber insécurité à travers l'augmentation du nombre de cybercriminels qui sont devenus plus professionnels, inconnus et malintentionnés. L'expert a incité les participants à être vigilants lors du recours au Cloud, à maitriser les risques qui en découlent et à mettre en place les mesures nécessaires surtout au niveau des institutions financières, qui représentent une cible favorisée des attaquants indépendamment de la taille de la banque concernée.

En effet, la transformation en cours des services financiers et les nouveaux services numériques créent de nouveaux points d'entrée pour les cyberattaques, ce qui crée de nouveaux défis. Dans ce cadre, M. GONÇALVES a évoqué l'importance de la cyber résilience qui permet aux services financiers d'être « élastiques » et de continuer à fonctionner après une cyberattaque. La cyber résilience est donc un objectif commun pour toutes les institutions financières, car elles constituent une chaine unique dont la force est égale à celle de son maillon le plus faible.



Avec la multitude de ces cybermenaces relatives au secteur financier, aucune institution financière ne peut survivre ou prospérer seule. Dans ce sens, une collaboration étroite et approfondie entre les institutions financières, publiques et privées, est le seul moyen de permettre une compréhension des vulnérabilités et des menaces qui pèsent sur le secteur financier, minimisant ainsi les cybermenaces susceptibles de perturber les fonctions économiques essentielles et mettant ainsi en péril la stabilité financière. Pour ce faire, l'Expert a insisté sur la création des relations de travail et des chaines de coopération pour pallier les risques existants et bien se préparer aux différentes cyberattaques. A cet effet, il existe un ensemble de Frameworks sur lesquels les institutions financières peuvent se baser, notamment l'iso 27001, Top 20 de SANS, NIST, PCI, etc.

En guise de conclusion, M. GONÇALVES n'a pas manqué à son tour d'inciter les institutions financières à une forte et efficace collaboration pour constituer les futurs services financiers et pour faire face aux différentes cybermenaces.

Conclusions

Il ressort de ce séminaire que la cyber résilience doit constituer une priorité à intégrer dans les stratégies opérationnelles des organismes nationaux afin qu'ils soient mieux préparés à faire face aux cyber-menaces et en mesure de reprendre une activité normale dans des délais acceptables en cas d'occurrence d'un incident majeur.

Plusieurs mesures ont été identifiées et mises en avant pour le renforcement de cette résilience. Il s'agit notamment de :

- Poursuivre et accélérer l'atterrissage des plans d'actions sécurité visant la conformité des plateformes sensibles par rapport à la DNSSI ;
- Renforcer la gouvernance de la sécurité à travers la mise en place de Systèmes de Management de la sécurité en définissant les rôles et responsabilité en la matière ;
- Intégrer la sécurité dans le cycle de vie de tous les projets IT et renforcer la vigilance quant aux choix des solutions en termes d'analyse et de cartographie des risques, de classification des actifs, de formation et de sensibilisation des équipes et des utilisateurs ;
- mettre en place des SOC (Centres Opérationnels de Sécurité), des plans de continuité et de reprise d'activité et des mécanismes pour la gestion des incidents et leur déclaration à la DGSSI ;
- Analyser les incidents et les expériences passés et prendre des actions concrètes pour construire et renforcer les défenses et pouvoir s'en prémunir dans le futur ;
- Systématiser l'audit périodique et renforcer les dispositifs d'évaluation automatisés et proactifs de la sécurité des infrastructures, réseaux, codes sources et applications.

En ce qui concerne le secteur financier, l'un des plus visés par les cyberattaques, les conclusions du séminaire ont porté sur la nécessité de renforcer la résilience à travers notamment :

- La prise en compte du caractère systémique du cyber risque dans l'élaboration du cadre de stabilité de la place financière ;
- La conduite d'exercices de simulation de crise pour vérifier l'efficacité des plans de continuité d'activités exigées par la DNSSI et les directives de la banque centrale ;
- La veille permanente pour l'anticipation des vulnérabilités et menaces susceptibles de perturber la stabilité financière et mettre en péril les fonctions économiques essentielles de l'Etat.

Par ailleurs, le séminaire a été l'occasion de rappeler que la résilience ne repose pas uniquement sur la technologie mais aussi sur l'organisation et la bonne gouvernance ainsi que de souligner l'importance et la nécessité de la coordination, de l'échange et du partage entre les institutions.

Intervenants

M. Kevin Henry

Expert en cybersécurité, Kevin HENRI a travaillé dans de nombreux domaines des technologies de l'information, notamment l'analyse des systèmes et l'audit des technologies de l'information. Après 20 ans dans le secteur des télécommunications, Kevin a été nommé vérificateur principal auprès de l'État de l'Oregon, où il a été membre du sous-comité du gouverneur sur la sécurité informatique. Coprésident du CBK pour le CISSP et plusieurs autres certifications, ainsi qu'auteur d'articles publiés dans plus de dix livres et magazines, Kevin est le directeur de « KMHenry Management Inc.» et occupe actuellement le poste de responsable de l'éducation pour (ISC)² et vice-président de l'ITPG.

Dr. Haji Amirudin Abdul Wahab

Actuellement directeur général de « CyberSecurity Malaysia ». Il a environ 25 ans d'expérience professionnelle dans les secteurs des télécommunications et de l'informatique au sein du gouvernement, du secteur semi-gouvernemental et privé. Dr. Amir est titulaire d'un doctorat en philosophie de l'Institut de technologie de l'information et génie électrique (ITEE) à l'Université du Queensland, en Australie, d'un MBA et d'un master en technologies de l'information. Dr Amir est professeur adjoint à l'Université islamique internationale de Malaisie (UIAM) et à l'Université Kebangsaan Malaisie (UKM) et membre du comité consultatif au sein de 3 autres universités.

M. Alberto Hernandez Moreno,

Directeur des opérations de INCIBE depuis février 2014, il est ingénieur en télécommunications de l'École technique supérieure d'ingénieurs en télécommunications de l'Université polytechnique de Madrid. Alberto Hernandez a cumulé une expérience de plus de 14 ans dans le domaine de la cybersécurité et de la cyberdéfense au sein de sociétés de premier plan telles que INDRA et ISDEFE.

Dr. LYRON H. ANDREWS

Lyron a travaillé en tant que Directeur principal des technologies de l'information chez BMG, Vice-président du« Workforce Opportunity Services » et Doyen du « Technology for learning and development» chez BNY Mellon. il a intégré la gestion de la sécurité de l'information en tant qu'enseignant à l'Université de Columbia et à d'autres institutions dans 30 pays du monde. Il est co-auteur de la 5e édition du guide « Certified Information Systems Security Professional » pubiée en 2018. En 2014, Dr. Andrews a mené des recherches au « Teachers College Columbia » concernant l'utilisation d'installations critiques dans un environnement de travail. En plus de travailler en tant qu'instructeur principal pour (ISC)²,

M. Paul Dwyer

Inventeur avec de nombreux brevets en cyber-sécurité, en analyse de détection avancée et en modélisation de capacité. Il est le responsable des activités de conseil en gestion d'optimisation de la sécurité globale d'IBM avec plus de 300 collaborateurs dans le monde et plus de 200 clients concentrés dans les secteurs des services financiers, de la défense et des télécommunications. Il dispose d'une grande expérience dans la stratégie de sécurité d'entreprise, ainsi que dans la conception, la mise en œuvre, l'exploitation et l'optimisation des centres d'opérations de sécurité (SOC).

M. Philippe Landucci

Après des études comme ingénieur électronicien à l'Ecole Polytechnique Fédérale de Zurich, Philippe Landucci a d'abord été entrepreneur pendant plus de dix ans, ses clients étant la recherche fondamentale, l'industrie, les Services du Parlement et - les banques - pour lesquelles il quitta en 1996 son activité indépendante. Ses fonctions pendant deux ans au sein de l'informatique de l'Union de Banques Suisses puis pendant treize ans auprès de celle du Crédit Suisse lui auront permis de connaitre de nombreuses facettes du métier. Ce parcours est complété avec la Division Informatique de la Banque Nationale Suisse, qu'il dirige depuis septembre 2011.

M. Luis Gonçalves

Actuellement responsable de la cybersecurité au sein de la banque centrale portugaise, Luis Gonçalves est aussi membre fondateur du chapitre portugais de "Cloud Security Alliance". Il enseigne la Gouvernance de la Cybersécurité, la Stratégie et la Cyberrésilience du secteur Financier en tant que professeur à l'Institut de Formation Bancaire au Portugal. Il enseigne également des modules relatifs au "Data Mining" et "Machine Learning" au sein de l'Institut Universitaire de Lisbonne.

M. Ismail DOUIRI

Ayant débuté sa carrière à Westinghouse Electric Co. aux USA, puis à Casablanca Finance Group, il a collaboré avec Morgan Stanley à Londres et avec McKinsey & Co. au sein de l'Initiative Afrique du Nord, et a fondé une startup dans l'Internet mobile basée à Casablanca. Actuellement, Mr DOUIRI est Directeur Général d'Attijariwafa Bank, il est également Administrateur de la Bourse de Casablanca, ainsi que de la plupart des filiales d'Attijariwafa bank au Maroc et en Afrique. Nommé 'Young Global Leader' par le World Economic Forum en 2010, Il est lauréat de l'Ecole Polytechnique et de Telecom Paris et titulaire aussi d'un MBA de Harvard University.

M. Nour-Dine HAJJAMI

Lauréat de l'Ecole Mohammedia des Ingénieurs, il est aussi titulaire d'un DESS en commerce international de l'ISCAE Casablanca / Université de Lille, M. Nour-dine HAJJAMI a commencé sa carrière en 1994 à la Direction du Trésor et des Finances Extérieures avant d'être détaché auprès du Dépositaire Central des Titres (MAROCLEAR) dès son démarrage en 1997. Il y a été en charge des Systèmes d'Information jusqu'en 2005 lorsqu'il a rejoint Bank Al-Maghrib en tant qu'Adjoint au Directeur de l'Organisation et des Systèmes d'Information (DOSI). A la tête de la DOSI depuis janvier 2010, il a une vue transversale de tous les métiers de la Banque et des projets engagés aussi bien à travers le pilotage du Système de Management Intégré (Qualité/ Santé-sécurité / Environnement) qu'à l'occasion des projets de transformation de processus ou de leur dématérialisation.

Colonel Major El Mostapha RABII

Lauréat de de l'Académie Royale Militaire (promotion 1986) et titulaire d'un Diplôme des Etudes Approfondies en Informatique de l'Université Technique de Munich (Allemagne) et d'un master en sécurité et défense du collège Royal des études militaires supérieures, le Colonel-major El Mostafa RABII a occupé notamment la fonction de chef de la Division Veille Electronique au sein de l'Arme des Transmissions. Le Colonel-major El Mostafa RABII a rejoint l'Administration de la Défense Nationale en 2011 pour participer à la mise en place de la Direction Générale de la Sécurité des Systèmes d'Informations. En décembre 2012, il a été nommé Directeur du centre de veille de détection et de réaction aux attaques informatiques (maCERT).

Colonel Abdellah BOUTRIG

Ingénieur de formation et lauréat de l'Académie Royale Militaire de Meknès (1987), il a notamment occupé les fonctions de commandant d'un bataillon des Transmissions et de chef de la division informatique de l'Inspection des Transmissions où il a participé à la réalisation de projets informatiques et de télécommunication au sein de l'Arme. Le Colonel BOUTRIG assure actuellement la fonction de directeur de l'Assistance, de la Formation, du contrôle et de l'Expertise au sein de la Direction Générale de la Sécurité des Systèmes d'Information. Il est titulaire du diplôme du cours d'Etat-major, du Cours supérieur de défense et d'un master sécurité et défense du collège Royal des études militaires supérieures.

M. Hassan MOKHLIS

Inspecteur des Finances de Grade Exceptionnel, et titulaire d'un Doctorat en Economie Internationale à l'Université de Paris I Panthéon-Sorbonne. Il est titulaire également d'un Master en Administration Publique obtenu à l'ENA de France en 2009. Après avoir exercé au sein de l'Inspection Générale des Finances depuis 1997 il a occupé respectivement en 2010 et 2011 des fonctions de chargé de mission à l'Office National Marocain du Tourisme et de conseiller technique auprès des ministres chargés de l'Education Nationale et de l'Administration de la défense nationale. En décembre 2012, il est nommé au poste de Directeur de la Stratégie et de la Réglementation à la Direction Générale de la Sécurité des Systèmes d'Information.

Lt-Colonel Khalil NOSSAIR

Ingénieur en aéronautique et en systèmes embarqués, lauréat de l'Ecole Royale de l'Air (1993-1998) et de l'Ecole Nationale des Ingénieurs de Construction Aéronautique (ENSICA, Toulouse), il est aussi titulaire d'un DEA en systèmes informatique. Le Lt-Colonel NOSSAIR a cumulé plus de 17 ans d'expérience en management et exploitation des systèmes d'information en tant que responsable du système d'information du pôle plan et équipement de l'Etat-Major Air puis de l'Administration de la Défense Nationale avant d'exercer en tant qu'auditeur sécurité puis chef de la Division Audit et contrôle au niveau de la Direction Générale de la sécurité des Systèmes d'Information.