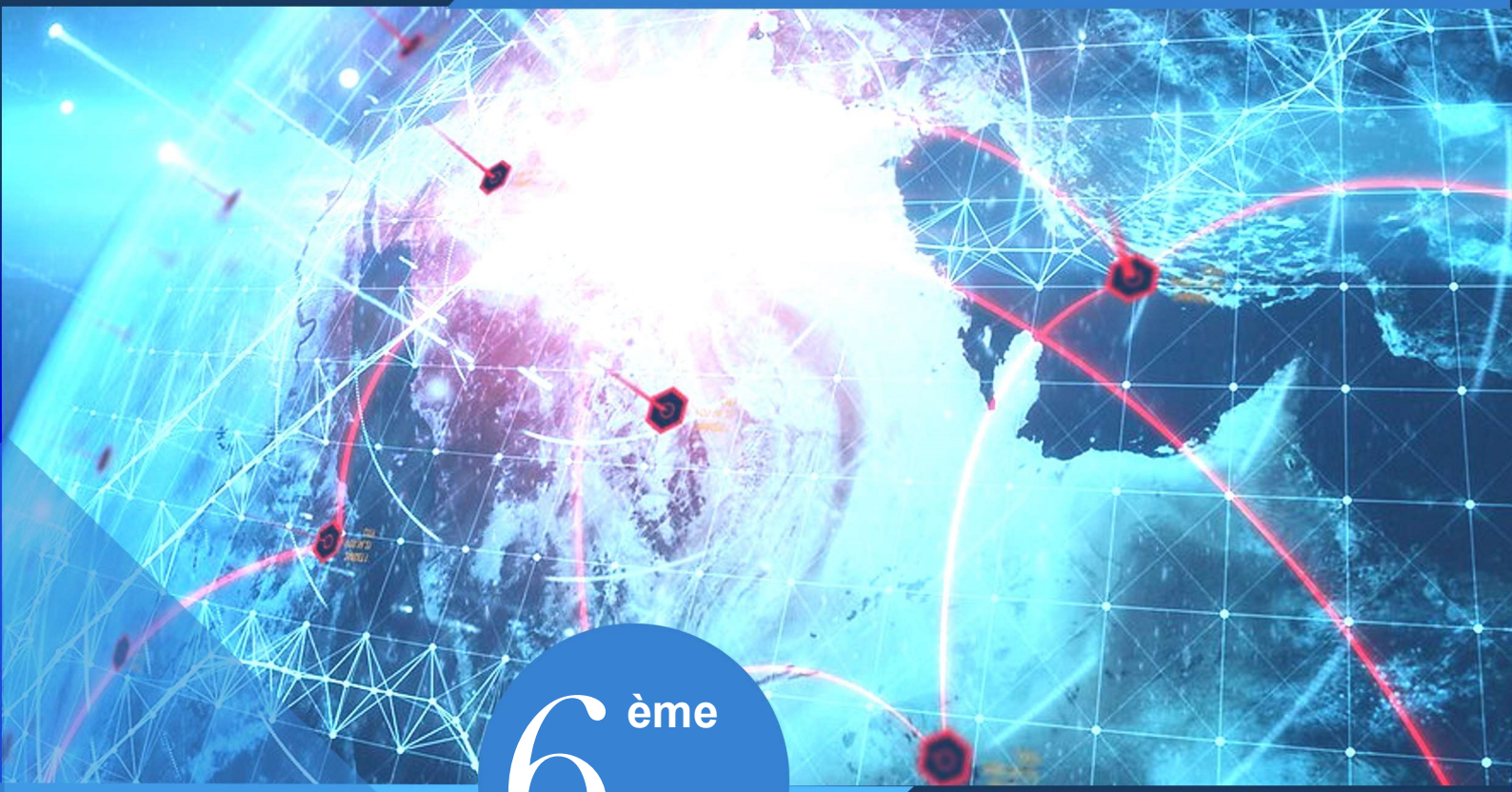
ROYAUME DU MAROC

Administration de la Défense Nationale

Direction Générale
de la Sécurité des Systèmes
d'Information

30 OCTOBRE 2018

Séminaire de sensibilisation sur la sécurité des systèmes d'information



6ème Edition

PROGRAMME

- Cyber résilience -
Nouvelle approche pour relever le défi du cyber risque

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 organise 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.

Trois sessions, animées par des experts nationaux et internationaux et des responsables de la DGSSI, seront 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 sera animée en partenariat avec la banque centrale.

INTERVENANTS

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.

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.

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).

Colonel Major Le 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).

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.

M. Nour-Dine HAJJAMI

Directeur Adjoint puis Directeur de l'Organisation et des Systèmes d'Information de Bank Al Maghrib depuis janvier 2005, Mr HAJJAMI a aussi exercé en tant que Directeur des Systèmes d'Information de Maroclear. 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. 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. 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 reatifs au "Data Mining" et "Machine Learning" au sein de l'Institut Universitaire de Lisbonne.

ROYAUME DU MAROC
Administration de la Défense Nationale
Direction Générale
de la Sécurité des Systèmes
d'Information

- Cyber résilience -
Nouvelle approche pour relever
le défi du cyber risque

6ème Edition

30 OCT 2018

PROGRAMME

08h30 à 09h00 : Accueil des participants

09h00 à 09h30 : Mots d'ouverture

- Mr. Le Ministre de l'Industrie, de l'Investissement, du Commerce et de l'Economie Numérique ;
- Mr. Le Wali Gouverneur de Bank Al Maghrib ;
- Mr. Le Ministre délégué, chargé de l'Administration de la Défense Nationale.

10h00 à 11h00 : Panel 1: Résilience vs Sécurité dans l'ère numérique

Modérateur : Colonel Abdellah BOUTRIG

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. Il s'agit lors de cette session de mettre en évidence les nombreuses menaces et vulnérabilités pouvant impacter non seulement les technologies de l'information mais également les autres dispositifs qui utilisent ces technologies tels que les systèmes de contrôle industriels, de gestion de bâtiments, d'automobiles, etc. Il est également question de présenter les normes et standards internationaux qui mettent en avant ce concept de résilience.

- La résilience vue au travers des standards internationaux (Colonel Abdellah BOUTRIG : Directeur à la DGSSI) : cas du standard NIST. Préparation, Protection, Détection, Remédiation et Récupération : les cinq piliers de la cyber-résilience.

- Les nouvelles menaces (Mr Kevin HENRI : Consultant sénior en cybersécurité) : Comprendre la menace est le premier pas vers une meilleure appréhension des risques. Il est désormais capital de considérer la nature changeante de ces menaces afin d'adapter les mesures.

- Cyber-résilience : Expérience de la Malaisie (Dr. AMIRUDIN BIN ABDUL WAHAB : CEO de Cyber-security Malaysia).

- Cyber-résilience : Expérience Espagnole (Mr. Alberto Hernandez Moreno :Directeur des Opérations de l'Institut National Espagnol de Cybersécurité INCIBE).

11h00 à 11h30 : Pause-café

11h30 à 13h00 : Panel 2: Construire un écosystème cyber-résilient

Modérateur : Colonel Major ElMostapha RABII

Cette session a pour objectif de répondre aux questions relatives à la construction d'un cadre complet de résilience à travers la mise en œuvre des nombreux éléments qui composent un programme de sécurité. 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. Les présentations durant cette session apporteront des réponses et des solutions pratiques pour se faire.

- Approche intégrée pour construire un écosystème résilient (Dr Lyron H. Andrews : Expert cybersécurité) : Comment faire concourir à la fois les moyens techniques et l'organisation dans l'objectif d'assoir la résilience du système d'information.

PROGRAMME (Suite)

- Adaptation des dispositifs de sécurité face à la menace changeante (CM EL Mostafa RABII : Directeur du ma-CERT) : Les chantiers phares entamés par la DGSSI pour une résilience des systèmes d'information à l'échelon national (Résilience des liens télécoms, mise en place des SOC (détection, coordination…)).

- L'évolution des SOCs (Paul DWYER: expert cybersécurité IBM) : Une organisation SOC est une structure qui évolue avec l'évolution des systèmes d'information et des innovations technologique. De la collecte d'événements jusqu'à la gestion des incidents et la remédiation quelles sont les problématiques courantes que l'on doit adresser pour la réussite d'un projet SOC.

- Rôle du dispositif réglementaire (Mr Hassan MOKHLIS : Directeur à la DGSSI) : Cyber résilience et apport des dispositions relatives à la Protection des Infrastructures d'importance vitale et à la Gestion des crises cyber.

13h00 à 14h30 : Panel 3 : Etude de Cas : Résilience du secteur financier

Modérateur : Monsieur Noureddine HAJJAMI

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. Selon une étude effectuée récemment par les services du Fonds Monétaire International, les pertes annuelles moyennes des institutions financières imputables aux cyberattaques avoisineraient près de 9 % du résultat net mondial des banques ce qui gruge le bénéfice de ces institutions et pourrait compromettre leur stabilité financière. Il convient de prendre les dispositions nécessaires pour parvenir à une meilleure compréhension des moyens de renforcement de la résilience des institutions et des infrastructures financières, pour à la fois réduire les probabilités de succès des cyberattaques et faciliter une reprise rapide des activités.

- Dispositifs en place ou à prévoir pour renforcer la résilience du secteur financier au Maroc (M. Nour-Dine Hajjami, Directeur des Systèmes d'Information à Bank Al Maghrib): dispositifs réglementaires et techniques (SOCs), rôle de la banque centrale, coopération avec la DGSSI.

- Cyber- résilience du système bancaire marocain (Monsieur Ismail DOUIRI, Directeur Général d'ATTIJARI WAFABANK).

- Enjeux de la cyber-résilience dans le secteur bancaire (M. Philippe Landucci, Responsable de la Division Informatique de la Banque Nationale de la Suisse et M. Luis Gonçalves expert en cyber-sécurité à la Banque Centrale du Portugal) : L'importante digitalisation du secteur financier associée à une inter-connectivité accrue des systèmes d'information pour répondre aux besoins des marchés interbancaires et de transfert font que les cyber-attaques constituent désormais un risque systémique pour le secteur.

14h30 : Mot de clôture du séminaire et pause déjeuner.