Livre Blanc

LES ENJEUX DE LA CYBERSECURITE AU MAROC

LES ENJEUX DE LA CYBERSECURITE AU MAROC

9 780201 379624

Les enjeux de la cybersécurité au Maroc - 2018

Dépôt légal - Bibliothèque Nationale du Royaume du Maroc, 2018

TABLE DES MATIERES

Table des matières....I
Table des illustrations....III
Faits saillants....01
Préface....02
1.Avant-propos....07
1.1 – Qu'est-ce que la cybersécurité ?....07
1.2 – Évolution des tendances....08
1.3 – Place du Maroc dans le monde....09
1.4 – Intervention de l'État marocain....10
1.5 – Méthodologie et organisation de l'étude....11
1.6 – Pistes bibliographiques....12
2.Profil de l'industrie....13
2.1 – Localisation des organisations ayant répondu au sondage....14
2.2 – Taille des organisations ayant répondu au sondage....14
2.3 – Nature des activités des organisations ayant répondu au sondage....14
2.4 – Situation des marchés desservis par les organisations ayant répondu au sondage....15
3.Gestion de la cybersécurité....16
3.1 – Déploiement d'un programme de cybersécurité....17
3.2 – Structure de gouvernance de la cybersécurité....18
3.3 – L'équipe de cybersécurité....18
3.4 – Recrutement de la main d'œuvre en cybersécurité....19
3.5 – Formation et sensibilisation en cybersécurité....20
3.6 – Assurance cybersécurité....20
3.7 – Extension du programme de cybersécurité aux sous-traitants....21
4.Technologies de la cybersécurité....22
4.1 – Audit de sécurité....23
4.2 – Principales technologies de sécurité utilisées....24
4.3 – Plan de réponse aux incidents de sécurité....34
4.4 – Simulation de cyberattaques....25
4.5 – Surveillance permanente des événements de sécurité via un SOC....26
4.6 – Impartition des systèmes de cybersécurité....27
4.7 – Le cas des cyberattaques....27
5.Cadre légal et réglementaire....30
5.1 – Normes de sécurité les plus suivies par les organisations marocaines....31
5.2 – Suivi de la conformité aux normes....31
6.Niveau de l'investissement....32
6.1 – Investissement moyen en cybersécurité....33
6.2 – Prévisions d'investissements en cybersécurité....33
7.Conclusion et pistes de réflexion....34
7.1 – Maturité des organisations en matière de cybersécurité....35
7.2 – Grands enjeux de la cybersécurité au Maroc....35
7.3 – Rôle de l'État....35
Annexe 1 : Études de cas....36
Autoroute Du Maroc (ADM)....37
École nationale supérieure d'informatique et d'analyse des systèmes (ENSIAS)....39
Institut national des postes et télécommunications (INPT)....44
Groupe d'assurances Lyazidi....48
Groupe Managem....50
Ministère de la Réforme de l'Administration publique....52
Phone Group....54
TAREC....58
Annexe 2 : Questionnaire....60
Annexe 3 : Sigles et acronymes....68
Annexe 4 69

TABLE DES ILLUSTRATIONS

Figure 1 – *Importance du cybercrime dans les menaces qui pèsent sur la planète*.....06

Figure 2 – *L'environnement d'affaires de la sécurité avancée*.....07

Figure 3 – *Tableau de bord de la cybersécurité au Maroc*.....07

Figure 4 – *Localisation des organisations*.....12

Figure 5 – *Taille de l'organisation*.....12

Figure 6 – *Nature des activités de l'organisation*.....13

Figure 7 – *Où sont situés vos marchés ?*.....13

Figure 8 – *La grande majorité des organisations ont un programme de cybersécurité*.....15

Figure 9 – *Qui gère la cybersécurité ?*.....16

Figure 10 – *Nombre d'employés affectés à la cybersécurité*.....16

Figure 11 – *Recrutement des employés spécialisés en cybersécurité*.....17

Figure 12 – *Principales difficultés rencontrées*.....17

Figure 13 – *Formation et sensibilisation des employés*.....18

Figure 14 – *La majorité des entreprises n'a pas d'assurance cybersécurité*.....18

Figure 15 – *Les accords de sous-traitance prennent en compte la cybersécurité*.....19

Figure 16 – *La pratique des audits de cybersécurité est généralisée*.....21

Figure 17 – *Principaux systèmes de sécurité utilisés*.....22

Figure 18 – *Importance du plan de réponse pour les organisations*.....22

Figure 19 – *Simulations de cyberattaques effectuées par les organisations*.....23

Figure 20 – *Organisations affirmant disposer d'un SOC*.....24

Figure 21 – *La majorité des systèmes d'information sont gérés en interne*.....25

Figure 22 – *Un nombre relativement bas de cyberattaques*.....25

Figure 23 – *Les différents types de cyberattaques*.....26

Figure 24 – *Les différents types de ripostes*.....26

Figure 25 – *Normes de sécurité les plus généralement adoptées*.....29

Figure 26 – *Suivi des normes*.....29

Figure 27 – *Investissement en cybersécurité*.....31

Figure 28 – *Les investissements en cybersécurité augmentent peu*.....31

Figure 29 – *Satisfaction mitigée vis-à-vis de la maturité en cybersécurité des organisations*.....33

FAITS SAILLANTS

63% DES ORGANISATIONS ONT DEUX EMPLOYÉS OU MOINS AFFECTÉS A LA CYBERSÉCURITÉ

A l'échelle mondiale, le cybercrime est considéré comme un des risques les plus susceptibles de frapper les organisations au cours des 10 prochaines années. Les cyberattaques sont devenues une partie intégrante de la vie des entreprises privées et des administrations publiques.

Au Maroc, la très grande majorité des organisations est consciente de l'importance de la cybersécurité : 84% d'entre elles ont mis au point un programme de cybersécurité, 86% offrent des programmes de formation ou de sensibilisation à leurs employés et 86% ont adopté une ou plusieurs normes de sécurité (ISO 27001, DNSSI, etc.).

Par contre, le déploiement des mesures susceptibles de contrer la menace traîne de l'arrière : 63% des organisations ont deux employés ou moins affectés à la cybersécurité, 62% des organisations investissent moins d'un millions de dirhams par an dans la cybersécurité et seulement 45% prévoient d'augmenter ce montant au cours de l'année 2018.

Prise à la gorge par le manque de moyens, la cybersécurité est à la peine dans les organisations marocaines. Ainsi, plus des trois quarts des organisations ont procédé à un audit de cybersécurité, mais la majorité ne l'a fait qu'une fois, alors que pour être efficace, un audit doit être répété. Même chose pour les simulations de cyberattaques : 63% ont déjà pratiqué une simulation, mais seule une minorité le fait sur une base régulière. La quasi-totalité des organisations déploie des solutions de sécurité (antivirus, firewall...), mais 39% ne protègent pas leurs données (cryptage, anonymisation...).

Il ne faut pas s'étonner si 31% seulement des organisations déclarent avoir subi des cyberattaques – ce taux est de 80% en Europe. Cela ne signifie pas que les hackers interrompent leurs activités aux frontières du Maroc. Tout simplement, les responsables de la cybersécurité ne se sont pas aperçus de l'intrusion, sans doute faute de moyens. Parmi la minorité qui a réussi à déceler des incidents, les deux types de crimes les plus fréquents sont les attaques virales et demandes de rançons.

Au total, il apparaît que le top Management de l'organisation répugne à dégager les ressources nécessaires à l'établissement des bonnes pratiques de cybersécurité. Un hiatus existe à cet égard entre le top Management et les responsables de la cybersécurité, généralement bien formés, mais qui se plaignent du manque de valorisation de l'information par leurs organisations.

Un des points forts de la cybersécurité au Maroc est l'adoption des normes par la majorité des organisations. La promulgation de la loi 09-08 sur la protection des données personnelles et de la DNSSI sur les infrastructures critiques a eu l'effet d'un coup de fouet sur les organisations. L'État marocain a joué un rôle moteur dans ce phénomène d'établissement de normes pour les organisations et les professionnels, comme en témoigne l'Union internationale des télécommunications (UIT).

PREFACE

Par **Ali El Azzouzi**,
Président-Directeur Général, Dataprotect

Une cybersécurité limitée à son aspect économique

Les infrastructures critiques sont bien protégées, mais pas le reste du tissu industriel

La stratégie marocaine de cybersécurité est trop souvent limitée au seul aspect économique. En effet, ce sont les donneurs d'ordre européens qui, dans le cadre de leurs activités délocalisées, ont poussé les pouvoirs publics à se doter de structures de cybersécurité comparables à celles qui existaient chez eux. Aussi ne faut-il pas s'étonner si le champion de toutes ces réformes a longtemps été le ministère de l'Industrie, de l'Investissement, du Commerce et de l'Économie Numérique.

A l'inverse, dans de nombreux pays européens, l'initiative de la lutte contre la cybercriminalité est née autour de la problématique de défense des droits de l'homme et de la protection de la vie privée. Aux États-Unis, cela fait partie du cœur même de la mission du ministère de la Homeland Security. Partout, la sécurité et la sûreté sont indissociables. Faute de cette vision d'ensemble, la stratégie marocaine de cybersécurité demeure incomplète.

Un cadre juridique moderne mais incomplet

Des pas de géant ont néanmoins été accomplis depuis l'adoption de la DNSSI qui s'adresse aux organismes d'importance vitale. Des efforts considérables ont été consentis en termes de sensibilisation et d'obligation avec pour conséquence que ces organismes considèrent désormais la cybersécurité comme une priorité. Mais cet effort est limité par définition aux organismes d'importance vitale et laisse de côté la majeure partie du secteur privé.

Un arsenal juridique de pointe mais la mise en vigueur demeure déficiente

Depuis l'adoption de la DNSSI en 2013, l'arsenal juridique marocain n'a guère changé, si ce n'est la promulgation de quelques décrets d'applications au niveau de la loi 09-08. Les véritables enjeux résident dans la mise en vigueur des lois. Autrement dit, le Maroc dispose d'un arsenal juridique comparable à ce qui se fait de mieux dans le monde, mais il demeure de nombreux problèmes d'applicabilité.

Les magistrats continuent à se référer au droit commun pour incriminer des actes de cybercriminalité parce que c'est plus commode que de se référer aux nouvelles lois. A titre d'exemple, quand on confisque un disque de l'ordinateur d'un suspect, que va-t-on faire de cette pièce à conviction, quel type d'intervention pratiquer, combien de temps la conserver, comment déterminer si son propriétaire est bien responsable de son contenu, etc. Bien des zones de flou demeurent et pourtant, au même moment, on assiste à une recrudescence du nombre des actes criminels.

Les entreprises n'investissent pas assez en cybersécurité

Des ressources humaines de qualité, mais pas assez nombreuses.

Puiser dans le bassin des hackers repentis

Lutter contre le « brain drain » des ingénieurs marocains

Changer la culture d'affaires pour intégrer la « security by design »

Est-ce que la législation marocaine va évoluer? La CNDP a exprimé le vœu que le Maroc complète la loi 09-08 et se dote d'une législation comparable au RGPD. Il existe des pressions en provenance des donneurs d'ordre européens pour que la législation marocaine évolue dans ce sens-là.

Des investissements insuffisants

Les résultats de l'étude montrent que peu d'entreprises dépassent la barre des cinq millions de dirhams et plus en matière d'investissements en cybersécurité. La plupart des entreprises investissent moins d'un million de dirhams, ce qui est peu. Les répondants disent souvent qu'ils ont de la peine à convaincre leur direction générale d'investir dans la cybersécurité. Résultat : ils n'investissent que lorsqu'il y a un incident. C'est une problématique que tout praticien de cybersécurité rencontre tous les jours dans le cadre de ses fonctions.

Il y a aussi un problème de ressources humaines. Le Maroc compte trois fois plus d'habitants que la Tunisie et pourtant il forme deux fois moins d'ingénieurs : 7 500 diplômés par an au Maroc contre 15 000 en Tunisie. Comment expliquer une telle contre-performance? Il y a tout d'abord, une approche trop élitiste alors qu'il faudrait éliminer les barrières à l'entrée et encourager le maximum de jeunes à poursuivre des études d'ingénieur.

Ensuite, il faut aussi donner une chance aux gens qui ne sont pas ingénieurs mais ont développé une expertise en cybersécurité. Ainsi, DATAPROTECT compte parmi ses employés des jeunes qui n'ont même pas le baccalauréat mais qui sont des passionnés de cybersécurité et ont tout appris par eux-mêmes. Il est important d'aller puiser dans le vivier de ressources de l'underground des hackers repentis pour améliorer notre capacité de penser hors des chemins battus. Ce sont des gens qui sont techniquement à l'avant-garde de la cybersécurité. Ils réussissent tous les tests d'admission sans difficulté. Il nous reste à les former sur la communication, sur la rédaction de rapports, etc. On n'a pas besoin de les chercher longtemps, ce sont eux qui nous repèrent et nous offrent leurs services. Mais il s'agit de candidatures atypiques qui restent relativement peu nombreuses.

D'une façon générale, le Maroc ne produit pas assez d'ingénieurs spécialisés en cybersécurité et il doit affronter une concurrence mondiale féroce. A peine formés, nos meilleurs ingénieurs quittent le Maroc pour aller travailler à l'étranger. La conséquence de cette insuffisance quantitative et de ce « brain drain » qualitatif est qu'il y a inadéquation entre l'offre et la demande. Il faut multiplier les programmes universitaires en cybersécurité.

L'avenir de la cybersécurité au Maroc

Pour faire du Maroc une nation sécuritaire, il est fondamental de changer les mentalités et de rendre « naturelle » l'adoption de la « security by design ». Il faut que la sécurité soit intégrée systématiquement dans l'évolution technologique dès la conception des solutions, qu'elles soient informatiques ou autre. Pour traduire cette évolution dans les faits, il convient de considérer la cybersécurité sous deux angles : la souveraineté numérique et la confiance numérique.

1 - Souveraineté numérique. Trop souvent, il arrive que des organismes marocains hautement sensibles confient la surveillance de leurs actifs informationnels à des intervenants étrangers. Le Maroc a une industrie de la cybersécurité embryonnaire, il y a peu d'entreprises spécialisées et c'est dommage car il serait facilement possible de répondre à la demande locale. En outre, il s'agit d'un type de services doté d'un fort potentiel d'exportation qui pourrait générer une grande valeur ajoutée pour le Maroc. Il est important de favoriser l'émergence d'une industrie locale forte, ce qui peut être fait en misant sur l'ouverture des marchés publics à des acteurs locaux et en encourageant l'innovation dans le secteur.

Pour que les marchés publics deviennent un facteur dynamique de développement, il faut que l'État cesse d'organiser des appels d'offre basés sur le plus bas soumissionnaire au profit de l'établissement de

L'État doit utiliser les marchés publics pour créer une industrie domestique de la cybersécurité

La sensibilisation fait des progrès mais demeure freinée par manque de transparence

véritables partenariats public-privé. Pour cela, il est indispensable que les pouvoirs publics disposent d'une stratégie d'équipement à long terme et qu'elle la fasse largement connaître. En effet, les entreprises de cybersécurité ont besoin de connaître à l'avance les besoins du gouvernement pour mobiliser des ressources adéquates et engager les ressources humaines appropriées.

Au Maroc, les statistiques sur la cybercriminalité font défaut

2 - Confiance numérique. La confiance numérique a fait des progrès indubitables au Maroc depuis l'adoption de la DNSSI qui s'adresse aux organismes d'importance vitale. Des efforts considérables ont été consentis en termes de sensibilisation et d'obligation avec pour conséquence que ces organismes considèrent désormais la cybersécurité comme une priorité. Mais cet effort est limité par définition aux organismes d'importance vitale et laisse de côté la majeure partie du secteur privé ainsi que le grand public.

Qui plus est, le fait d'avoir confié la cybersécurité à la Défense nationale par le truchement de la DGSSI comporte un inconvénient. La culture de secret qui caractérise la Défense nationale a tendance à rendre inaccessible l'information colligée par la DGSSI. Tout est géré dans la plus grande discrétion alors que pour faire de la sensibilisation, il faudrait au contraire conférer la plus grande visibilité possible à cette activité.

Le Maroc ratifie en 2014 la convention de Budapest

Le résultat est que la sensibilisation du grand public progresse peu. Il y a de nombreux cas sociaux, surtout parmi les jeunes. Des cas de pédophilie en ligne sont signalés chaque année. Or, cela rentre bien dans le cadre de la lutte contre la cybercriminalité car ces actes sont perpétrés via des moyens technologiques. Le phénomène est comparable pour les PME. Bien du travail reste à faire dans ce domaine aussi. Or, le tissu économique marocain est surtout composé de PME.

L'indispensable coopération internationale

Il y a une géopolitique de la cybercriminalité. Le Brésil se spécialise dans le spam, l'Afrique subsaharienne dans les arnaques sur Internet, l'Europe de l'Est dans les fraudes à la carte bancaire, la Russie dans les dénis de services distribués, le Moyen-Orient et le Maroc dans le défacement de site web, etc. Il y a une spécialisation régionale du cybercrime. Malheureusement, au Maroc, il y a un manque de statistiques sur la cybercriminalité. On ne sait pas combien il y a eu de crimes, leur nature, leur impact, etc.

Pour qu'un CERT soit vraiment utile, il faut rendre obligatoire la déclaration d'incidents, notamment tout ce qui est violation de données. Les choses devraient changer en raison de l'adoption du RGPD par l'Union européenne qui devrait affecter le Maroc par ricochet. En effet, la cybersécurité est un phénomène transnational par définition.

C'est pourquoi, le Maroc a ratifié en février 2014 la convention de Budapest sur la cybercriminalité qui est le premier traité international à aborder les crimes informatiques et les crimes dans Internet en harmonisant certaines lois nationales, en améliorant les techniques d'enquêtes et en augmentant la coopération entre les nations et la protection adéquate des droits de l'homme et des libertés. Mais peu d'États africains ont ratifié la Convention de Budapest.

Le Maroc participe à la création de CyberSud en 2018

Signalons aussi la participation du Maroc à l'initiative CyberSud, un projet européen de coopération en matière de lutte contre la cybercriminalité dans le voisinage sud a été annoncé officiellement en mars 2018 à Tunis. L'objectif spécifique du projet est de renforcer la législation et les capacités institutionnelles en matière de cybercriminalité et de preuve électronique, conformément aux exigences relatives aux droits de l'Homme et à l'État de droit.

La coopération internationale est une nécessité absolue

La coopération internationale est une nécessité absolue car, en matière de cybercriminalité, on ne peut pas faire cavalier seul. Quand les attaques viennent d'intrus étrangers, une approche multilatérale est indispensable.

PREFACE

Par **Mohamed SAAD**,
Président AUSIM

Dans un monde qui fonce tout droit vers le tout digital, où les Technologies de l'Information s'installent comme outils incontournables dans la société, il est primordial que cette utilisation accrue s'accompagne d'une grande sensibilisation, d'un corpus réglementaire solide, et de bonnes pratiques pour en faire un meilleur usage.

« Le parti pouvait mettre à nu les plus petits détails de tout ce que l'on avait dit ou pensé, mais les profondeurs de votre cœur, dont les mouvements étaient mystérieux, même pour vous, demeuraient inviolables », écrivait George Orwell. Avec les Technologies d'aujourd'hui, on a dépassé le cauchemar de 1984. La matrice perce nos ressorts intimes, décèle le sens caché de nos comportements. Cela grâce aux métadonnées, ces informations qui disent tout d'une communication : date, heure, durée, lieu, humeur… Les Big Data, entre autres, ont rendu intelligible ce gisement intarissable. Moulinées par les algorithmes, ces métadonnées révèlent d'autres secrets que le contenu des courriers électroniques, des messages ou des conversations enregistrées. Qu'il s'agisse de transactions bancaires, de données de géolocalisation, de séquences génétiques, de fichiers d'électeurs ou de loueurs de vidéos en ligne, ces silos de données remplis de copeaux de vie anonymes trahissent, une fois traités, toutes les identités qui s'y entassent. Jamais l'homme n'avait été aussi dévoilé, aussi traçable, aussi transparent. Bientôt, plus aucun d'entre nous ne pourra avoir vécu sans que des millions d'informations, jusqu'aux plus intimes, aient été stockés sur lui, pour ne plus disparaitre. Ce phénomène, qui a conduit à l'explosion de la société de l'information, a favorisé l'apparition d'un nouveau type de crime, celui du 21ème siècle et des siècles qui viennent : le CyberCrime.

Lors d'un sondage, des jeunes gens aux Etats-Unis ont déclaré accepter d'échanger leurs données personnelles contre un cookie à la cannelle ! Cela montre le degré d'insouciance de la société mais surtout des générations futures à offrir à certains groupes malveillants l'opportunité de porter atteinte à leurs personnes. Les institutions peu soucieuses du risque « Cybercriminalité » se retrouvent aussi dans la même situation. Plusieurs organisations et non des moindres se sont vues subtiliser leurs données sensibles, voire rançonnées, et ont été contraintes de payer le prix de la délivrance.

Le cybercrime s'organise depuis deux décennies ; très exactement depuis l'avènement d'Internet, qui a servi de vecteur de transmission et de contagion pour les malwares.

Le crime s'est organisé et des bandes de malfaiteurs sévissent sur le net, profitant du manque de coopération inter-nations, dû aux disparités

juridiques. L'utilisation de l'underground et des outils très sophistiqués rendent les investigations très complexes.

Le Corpus réglementaire et le manque de montée en compétence des magistrats n'arrangent pas les choses, car on continue à incriminer les coupables sur la base de textes de lois obsolètes ou inadéquats, ce qui représente une aubaine pour les cybercriminels et crée le chaos dans ce capharnaüm.

L'AUSIM n'a cessé depuis 25 ans de sensibiliser, communiquer et former les acteurs de la société à se préparer à faire face aux risques « Cybercriminalité ». L'AUSIM œuvre bien évidement à accroitre la vigilance des utilisateurs et à mettre en place les mesures nécessaires afin d'inculquer la sécurité de l'information dans l'ADN de toute institution, et de faire également de cette démarche un axe de développement des ressources humaines.

L'AUSIM a édité durant les cinq dernières années des Livres Blancs en lien avec cette problématique. On citera par exemple :

- La loi 09-08
- La classification des données
- La conformité avec le Décret 02-15-712 (DNSSI) : Apport de la Norme ISO 27001

Plusieurs articles ont été publiés, plusieurs interventions en relation avec cette problématique ont été faites, et des séminaires traitant de ces sujets ont été organisés, dont un au profit d'enfants en bas âge pour les sensibiliser aux risques d'utilisation d'Internet.

L'AUSIM est partie prenante de la Campagne Nationale Maroc Cyberconfiance (CNMC), organisée par le Centre Marocain de Recherches Polytechniques et d'Innovation (CMRPI), qui regroupe des dizaines d'institutions de l'Administration et de la société civile et dont le programme très riche permet à notre pays de mettre en place une stratégie pour faire face à ce fléau. Je rappelle que la CNMC 2018-2022 a été lancée sous l'égide du Ministère de la Justice.

Les Assises de l'AUSIM, évènement incontournable, a toujours réservé à ce sujet une grande importance en invitant des sommités du monde de la sécurité IT et en traitant le sujet d'une manière stratégique.

L'AUSIM continuera à jouer son rôle d'acteur essentiel par rapport à l'utilisation des T.I. au Maroc, et c'est dans ce cadre que nous nous réjouissons de notre partenariat avec « DATA PROTECT », compétence majeure dans le secteur de la lutte contre la Cybercriminalité, la mise en place de stratégies de la sécurité IT, et la proposition de solutions et mesures nécessaires pour la lutte contre le Cybercrime.

Nous souhaitons à notre communauté une bonne utilisation de ce support inédit, qui vient nous donner une image de la situation au Maroc, ainsi qu'une proposition de pistes et mesures à mettre en place afin que notre société et notre économie soient plus résilientes, mieux préparées et à même de faire de ce risque une opportunité, en visant le leadership en matière d'expertise à travers le continent africain.

Je tiens à remercier la communauté AUSIM qui a répondu au questionnaire, ainsi que toutes les personnes qui ont contribué à la rédaction de ce Livre Blanc, sans oublier ceux qui ont lu et relu ce support afin d'en faire une référence en la matière.

01 AVANT PROPOS

1.1 – Qu'est-ce que la cybersécurité ?

La cybersécurité englobe toutes les technologies, politiques et actions qui visent à protéger les systèmes d'information. Avec le développement de l'industrie 4.0, on observe une tendance à relier les systèmes d'information aux systèmes opérationnels faisant appel à de l'équipement numérique (robots, machines à commande numérique, capteurs, systèmes de vision, imprimantes 3D, etc.). Cela a pour conséquence d'étendre le champ de la cybersécurité au monde physique.

Les objectifs généraux en matière de sécurité sont les suivants :

- La disponibilité qui garantit l'accessibilité des systèmes d'information par les utilisateurs.
- L'intégrité qui désigne l'authenticité des données.
- La preuve qui garantit la non-répudiation d'une transaction avec possibilité de pouvoir auditer les résultats fournis.
- La confidentialité qui prévient l'accès accidentel ou illicite à une information confidentielle[1].

1 Ali El Azzouzi, La cybercriminalité au Maroc, Casablanca 2010. Cf. p. 26-8.

01 AVANT-PROPOS

1.2 – Evolution des tendances

Le rapport sur les risques mondiaux publié en janvier 2018 par le Forum économique mondial de Davos situe les cyberattaques et le vol de données respectivement aux troisième et quatrième rangs des risques les plus susceptibles de se produire au cours des 10 prochaines années, derrière les conditions climatiques extrêmes et les catastrophes naturelles.

FIGURE 1 – IMPORTANCE DU CYBERCRIME DANS LES MENACES QUI PESENT SUR LA PLANETE

Rapport sur les risques mondiaux	*Les 5 risques les plus susceptibles de se produire au cours des prochains 10 ans*
Phénomènes climatiques extrêmes	*1*
Désastres naturels	*2*
Cyberattaques	*3*
Vol de données ou fraude	*4*
Échec de la limitation et de l'adaptation au changement climatique	*5*

Source: Global Risk Report, Executive Opinion Survey 2017, World Economic Forum

Cette perception du risque cyber ne doit pas nous surprendre. En effet, chaque 40 secondes, une compagnie reçoit une demande de rançon[2]. Les cyberattaques polluent l'environnement des affaires et frappent même la CIA. Les pertes vont au-delà des débours et des journées non travaillées. Cisco dans son étude « Cybersecurity as a growth advantage » estime qu'un tiers des entreprises nord-américaines abandonnent des projets innovants de crainte d'être trop exposées.

Pourquoi cette multiplication de crimes?

1 - La cybercriminalité est payante : les cyberattaques ont coûté quelques 450 milliards de dollars US aux entreprises, à l'échelle mondiale l'an dernier , et le montant est en pleine croissance (à titre de comparaison, le PIB du Maroc est de 110 milliards de dollars US)[3] .

2 - L'autre raison est que le nombre de cibles potentielles augmente rapidement avec la numérisation de l'économie, la transition vers la mobilité et le développement de l'infonuage. L'arrivée de l'Internet des objets (IdO) multipliera de façon exponentielle le nombre de cibles.

Paradoxalement, la sécurité accroit le danger dans la mesure où de plus en plus d'entreprises recueillent des données personnelles sur leurs employés, fournisseurs et clients, à commencer par des applications de gestion des mots de passe. L'accumulation de grandes quantités de renseignements personnels dans des bases de données accroit le risque d'accès non autorisé à ces informations. Une seule intrusion peut toucher des populations entières.

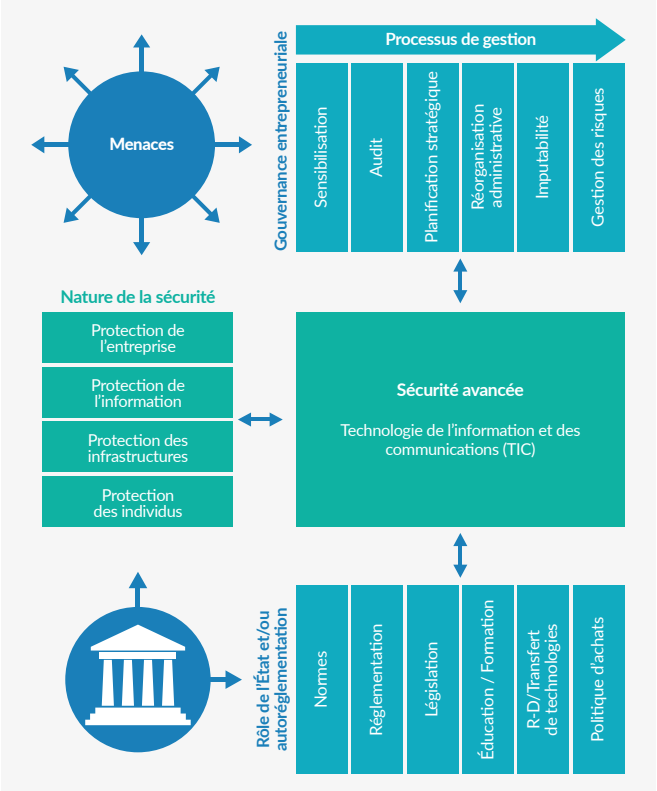
Autre tendance lourde : le glissement progressif de la sécurité hors du champ de la seule technologie. La sécurité est avant tout une affaire de gestion de l'entreprise, et cela au plus haut niveau – celui de la stratégie de gouvernance. Dès 2003, un des pionniers de la cyberdéfense, Robert Garigue annonçait ainsi la vraie nature de la cybersécurité :

> *La sécurité concerne la gestion globale de l'organisation. Elle demande à être traitée comme un enjeu d'affaires et non comme une simple question de technologie. Si nous acceptons ce postulat, il faut être prêt à affronter une série de conséquences qui modifient du tout au tout notre façon de travailler, et même de vivre*[4].

Tous les indicateurs montrent que la sécurité déborde du cadre de l'exploitation des TIC pour être redéfinie comme une fonction de gestion. Ce faisant, la place qu'occupe la sécurité dans les entreprises change, se veut plus stratégique et se rapproche de la haute-direction et du conseil d'administration.

2 Manage-Engine, Free book on ransomwave
3 CIA, The World Fact Book. Le montant de 110 milliards de dollars est calculé au taux de change officiel du dollar. Transposé en dollars PPP, cela donnerait 300 milliards de dollars (chiffres 2017).
4 Alliance CATA, La sécurité avancée au Québec, profil de l'industrie, Montréal, 2003.

FIGURE 2 - L'ENVIRONNEMENT D'AFFAIRES DE LA SECURITE AVANCEE



Source: Étude Alliance CATA – 2010

1.3 – Place du Maroc dans le monde

Selon l'Indice de la cybersécurité dans le monde (GCI-2017) de l'UIT, le Maroc occupe la 49e place parmi les 193 pays couverts. Les experts de cette agence onusienne spécialisée dans les technologies de l'information et de la communication passent au crible les approches liées à la cybersécurité au travers de cinq critères : juridique, technique, organisationnel, renforcement des capacités et de la coopération.
Selon le classement de l'UIT, le Maroc appartient aux 77 pays dits en voie de maturité (maturing stage), derrière les 21 pays avancés (leading stage) et devant les 96 pays en émergence (initiating stage). Au sein du groupe des pays arabes, il arrive en septième position – Oman et l'Égypte se classent parmi les pays avancés. Toutefois, cette performance relativement moyenne du Maroc s'appuie sur plusieurs points forts qui peuvent servir à bâtir une infrastructure sécuritaire à la hauteur du défi mondial.

Le Maroc atteint l'excellence en matière juridique et technique, tandis qu'il doit se contenter d'une note moyenne dans les critères des mesures organisationnelles, du renforcement des capacités et de la coopération. Au niveau des composantes de chacun de ces critères, il faut toutefois déplorer quelques faiblesses graves : CERT sectoriels, protection en ligne pour les enfants, stratégie, etc.

FIGURE 3 – TABLEAU DE BORD DE LA CYBERSECURITE AU MAROC

	Législation de la cybercriminalité
	Législation de la cybersécurité
	Formation en cybersécurité
	MESURES JURIDIQUES
	CERT/CIRT/CIRT national
	CERT/CIRT/CIRT gouvernemental
	CERT/CIRT/CIRT sectoriels
	Normes pour les organisations
	Normes pour les professionnels
	Protection en ligne pour les enfants
	MESURES TECHNIQUES
	Stratégie
	Responsabilité organisationnelle
	Indicateurs de cybersécurité
	MESURES ORGANISATIONNELLES
	Organisations de normes
	Bonnes pratiques en cybersécurité
	Programme de R-D
	Campagnes de sensibilisation publiques
	Cours de formation professionnelle
	Programmes éducatifs
	Mécanismes d'incitation
	Industrie domestique
	RENFORCEMENT DE CAPACITÉ
	Accords bilatéraux
	Accords multilatéraux
	Engagement international
	Partenariats public-privés
	Partenariats inter-organisationnels
	COOPÉRATION
	INDEX GLOBAL CGI

Source : UIT, Global Cybersecurity Index 2017 – Le vert indique le plus haut résultat, le rouge le plus bas

Une attention particulière doit être portée au critère de renforcement de capacité qui détermine l'avenir de la cybersécurité au Maroc. On y constate un manque d'incitatifs et une carence au niveau des entreprises spécialisées en cybersécurité. L'amélioration des mécanismes incitatifs devrait permettre d'encourager les utilisateurs de cybersécurité à prendre les mesures de protection nécessaires. Le développement d'une industrie domestique de la cybersécurité dynamique et concurrentielle est sans doute au cœur de la transition marocaine vers le groupe des pays avancés.

Pour rappel, l'Indice de la cybersécurité dans le monde, lancé en 2014, vise à promouvoir une culture mondiale de la cybersécurité et son intégration au cœur des TIC. Le GCI de 2017, qui est la deuxième édition, mesure l'engagement des États membres de l'UIT en matière de cybersécurité afin de stimuler les efforts de son adoption et son intégration à l'échelle mondiale.

1.4 – Intervention de l'Etat marocain

C'est tout naturellement que l'État marocain a été amené à jouer un rôle actif en matière de sécurité. Tout a commencé en novembre 2003 avec la promulgation de la loi 07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données. Cette loi comblait le vide juridique qui présidait aux activités informatiques en permettant pour la première fois de sanctionner les intrusions non autorisées dans un système de traitement automatisé de données.

Mais c'est en février 2009 avec l'adoption de la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel que la sécurité entre véritablement dans la gestion quotidienne de l'entreprise. Cette loi a pour objet de protéger la vie privée des personnes physiques contre les atteintes possibles à l'occasion du traitement des données les concernant.

La même loi instituait une Commission nationale de contrôle de la protection des données à caractère personnel (CNDP) pour sensibiliser la population, recevoir les plaintes, donner des avis juridiques lors de l'adoption de lois ayant une incidence sur la vie privée et accorder les autorisations nécessaires.

Pour collecter des données personnelles, une organisation doit faire une déclaration auprès de la CNDP – les données sensibles requièrent une autorisation préalable. Dans les deux cas, l'organisation qui collecte les données a l'obligation d'informer les individus concernés et d'obtenir leur consentement.

Au-delà de la loi, il y a l'arsenal réglementaire. Le Maroc a créé en septembre 2011 la Direction générale de la sécurité des systèmes d'information (DGSSI) relevant du ministère de la Défense nationale. Dans un premier temps, la DGSSI a repris certaines prérogatives qui incombaient jusque-là à l'Agence nationale de réglementation des télécommunications (ANRT) – cryptographie et certification électronique.

L'année suivante était adoptée une stratégie nationale de la cybersécurité avec pour objectif de doter les systèmes d'information marocains d'une capacité de défense et de résilience, à même de créer les conditions d'un environnement de confiance et de sécurité propice au développement de la société de l'information. Cette stratégie prévoyait l'élaboration d'une Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI) dont la mission consiste à élever et à homogénéiser le niveau de protection de l'ensemble des systèmes d'information des administrations et organismes publics ainsi que des infrastructures d'importance vitale.
La DGSSI a rendu public la DNSSI en décembre 2013. Cette directive décrit les mesures de sécurité organisationnelles et techniques qui doivent être appliquées par les organisations concernées. Ce socle de règles minimales est appelé à évoluer en fonction de l'évolution technique ainsi que de la cybercriminalité. Pour la mise en œuvre de cette directive, chaque organisation concernée doit définir un plan d'actions, élaborer les mesures organisationnelles et techniques nécessaires, puis assurer un suivi permanent.

En principe, seules les infrastructures critiques sont soumises à la DNSSI. Mais, dans la pratique, les fournisseurs réguliers des organisations chargées de la gestion des infrastructures critiques sont eux aussi assujettis à la DNSSI. Il y a donc actuellement une pression intense exercée par les pouvoirs publics pour que les entreprises marocaines se dotent des moyens les plus avancés en matière de cybersécurité.

L'État participe directement à cet effort via le Centre marocain d'alerte et de gestion des incidents informatiques (ma-CERT) relevant de la DGSSI. Mis au point avec la coopération de la Corée du Sud, le ma-CERT a été inauguré en janvier 2011 pour faire office de centre de veille, de détection et de réponse aux attaques informatiques. Ainsi, quand une infrastructure critique est victime d'une attaque, elle doit communiquer, dans les quarante-huit heures, au ma-CERT les informations relatives aux incidents majeurs affectant la sécurité ou le fonctionnement de ses systèmes d'information sensibles.

1.5 – Méthodologie et organisation de l'étude

L'Association des utilisateurs des systèmes d'information au Maroc – AUSIM – est une association à but non lucratif créée en 1993. Elle compte parmi ses adhérents de nombreuses structures (officces, banques, assurances, entreprises industrielles, ...) qui jouent un rôle de leadership sur le plan organisationnel et managérial au Maroc. L'AUSIM a pris les devants pour démontrer sa volonté de contribuer à la promotion des systèmes d'information au Maroc tout en s'associant aux autres acteurs du secteur, et s'est donné pour objectifs :

• La promotion de l'usage des systèmes d'information au profit de la création de valeur.

• La contribution à la protection des intérêts de ses adhérents.

• Le renforcement des liens qui l'unissent aux associations similaires au Maroc et à l'étranger.

• La diffusion entre les membres des connaissances et des informations relatives aux systèmes d'information.

• La participation aux grandes réflexions et réformes nationales sur le sujet.

Les administrations, établissements et entreprises publics et organisme disposant d'un agrément ou d'une licence de l'Etat pour exercer une activité réglementée. Ses entités soumettent conformément au programme des missions d'audit arrêté par l'autorité compétente, leurs systèmes d'information sensibles à un audit effectué par la Direction générale de la sécurité des systèmes d'information ou par des prestataires privés homologués par l'autorité compétente.

Un arrêté du Chef du gouvernement fixe les critères d'homologation des prestataires d'audit privés ainsi que les modalités de déroulement de l'audit.

S'inscrivant dans une démarche de sensibilisation de ses membres, l'AUSIM produit régulièrement des livrables thématiques (bulletins de veille SI périodiques, enquêtes...) visant à les informer régulièrement des dernières actualités, au Maroc et ailleurs, liées aux technologies et aux systèmes d'information ainsi que leur macro-événement. L'AUSIM réalise également des travaux à forte valeur ajoutée au profit de la communauté : des rapports d'études, des enquêtes et des livres blancs qui constituent une synthèse de bonnes pratiques dans le domaine des SI.

C'est dans ce cadre qu'aux termes d'un appel d'offre, l'AUSIM a confié à DATAPROTECT, une entreprise spécialisée en sécurité de l'information, le mandat de procéder à la réalisation d'un livre blanc portant sur la Cybersécurité au Maroc.

Le livre blanc de l'AUSIM porte sur une population de 4 600 organisations membres de l'AUSIM ou identifiées par l'AUSIM dans le cadre de ses activités. Le sondage a été administré en ligne par l'équipe DATAPROTECT entre février et mai 2018 sur le serveur spécialisé de SurveyMonkey. Cent vingt-six organisations ont répondu au questionnaire – 94 réponses ont été considérées comme complètes.

Ce sondage est la source principale (mais pas exclusive) de ce livre blanc. Dans la mesure du possible, nous avons établi une démarcation visible entre l'exposition des résultats et leur analyse.

Chapitre 2 : le profil de l'industrie.

Ce chapitre trace le portrait des entreprises ayant répondu au sondage. Où sont-elles situées géographiquement ? Quels sont leurs tailles, leurs marchés ? Comment se comparent-elles à la moyenne marocaine ?

Chapitre 3 : Gestion de la cybersécurité

Ce chapitre a pour objet de définir le niveau de préparation des organisations marocaines en matière de cybersécurité, tant au niveau du déploiement de programmes spécialisés que de la gouvernance et des processus.

Chapitre 4 : Technologies de la cybersécurité

Ce chapitre détaille le cadre technologique de la cybersécurité : fréquence des audits, existence d'un plan de relève, utilisation d'un SOC ainsi que la gestion des cyberattaques. Le panorama des technologies déployées et la façon dont elles sont employées, permettent d'évaluer les tendances lourdes de la cybersécurité.

Chapitre 5 : Cadre légal et réglementaire

Le Maroc s'est doté en quelques années d'un arsenal législatif et réglementaire destiné à encadrer les activités informatiques et à assurer la sécurité des citoyens et des infrastructures critiques (loi 09-08 et DNSSI). Il existe en outre des normes internationales très populaires parmi les organisations.

Chapitre 6 : Niveau de l'investissement

L'investissement moyen des organisations marocaines dans la cybersécurité est faible (moins d'un million MAD), mais il évolue à la hausse. Une légère majorité des répondants s'estiment bien outillées en matière de cybersécurité, mais de la place demeure pour l'amélioration.

Chapitre 7 : Conclusion et pistes de réflexion

Ce chapitre porte sur les grands enjeux auxquels est confrontée l'industrie. Il se fonde à la fois sur les résultats du sondage et sur les interviews qualitatives effectuées par l'équipe AUSIM/DATAPROTECT auprès des dirigeants de l'industrie.

Trois annexes complètent le livre blanc :

Annexe 1 : Les études de cas

Huit études de cas mettent en évidence des modèles d'affaires très différents les uns des autres. Le choix des entreprises étudiées ne relève pas d'un classement ou d'un palmarès. Il s'agit d'instantanés sur des entreprises qui illustrent les pratiques et processus identifiés dans les chapitres précédents.

Annexe 2 : Questionnaire utilisé pendant le sondage.

Annexe 3 : Sigles et acronymes utilisés dans le livre blanc.

01 AVANT-PROPOS

1.6 – Pistes bibliographiques

Deux études récentes portent sur la cybersécurité au Maroc. Les conclusions de ces deux études ont servi à alimenter la réflexion du présent livre blanc.

PWC - Cybersécurité : Global State of Information Security Survey, Focus Maroc, avril 2018.	**Kaspersky Lab et Averty – Comportements et attitudes des professionnels liés à la sécurité informatique au Maroc, novembre 2017**
• Les entreprises marocaines prennent conscience des risques encourus et des enjeux en matière de cybersécurité. Cependant, 70% des répondants déclarent que leur stratégie de cybersécurité n'est pas déployée à une vitesse suffisante. • L'utilisation de logiciels malveillants est le vecteur principal des cyberattaques au sein de l'entreprise au Maroc. En effet, 25% des entreprises interrogées estiment que ceux-ci sont à l'origine des incidents de sécurité. • Face à ces constats, les entreprises marocaines ont consacré en 2017 à leur cybersécurité des budgets en hausse significative par rapport à 2016, largement supérieur au panel mondial (11% du budget TI au Maroc contre 4% dans le monde). • Ce budget demeure insuffisant aux yeux de 72% des répondants.	• Plus de 21% des répondants affirment que leur entreprise a déjà été affectée par des menaces informatiques. • Les virus (63%), les logiciels malveillants (21,4%) et la perte de données (16,9%), sont dans le top 3 des menaces informatiques les plus fréquentes affectant l'entreprise. • L'antivirus reste l'outil de protection informatique le plus fréquent chez les professionnels marocains (84,6%). • En ce qui concerne les outils de sécurité informatique, 91% des professionnels restent convaincus de leur importance pour la protection des données professionnelles. • Néanmoins, 20% des professionnels sondés n'y ont pas recours, pensant ne pas en avoir besoin.
L'enquête a mobilisé 50 répondants issus de la grande entreprise (43%), de la moyenne entreprise (21%), de la petite entreprise (26%) et du secteur public (10%).	L'enquête a mobilisé 714 répondants, issus de plus de 26 secteurs d'activités et couvrant différentes tailles d'entreprises de moins de 10 personnes à plus de 500.

02 PROFIL DE L'INDUSTRIE

Ce chapitre trace le portrait des entreprises ayant répondu au sondage. Où sont-elles situées géographiquement ? Quels sont leur taille, leurs marchés ? Comment se comparent-elles à la moyenne marocaine ?

Rappelons à titre indicatif que le Maroc compte environ 500.000 entreprises. Avec 195.900 entreprises, le commerce détient une part de 33,9%. Il est suivi du BTP et activités immobilières. Ces branches détiennent 25,7% des parts, soit 153.067 entreprises[5].

Les PME représentent plus de 95% des entreprises marocaines, emploient 50% des salariés, réalisent 31% des exportations, 51% des investissements nationaux et 40% de la production[6].

5 Kawtar Tali, « Près d'un demi-million d'entreprises au Maroc », Aujourd'hui le Maroc, 21 mars 2016.
6 Fadoua Anari et Said Radi, « Difficulté du financement des PME marocaines », Finance & Finance Internationale, No 10, janvier 2018.

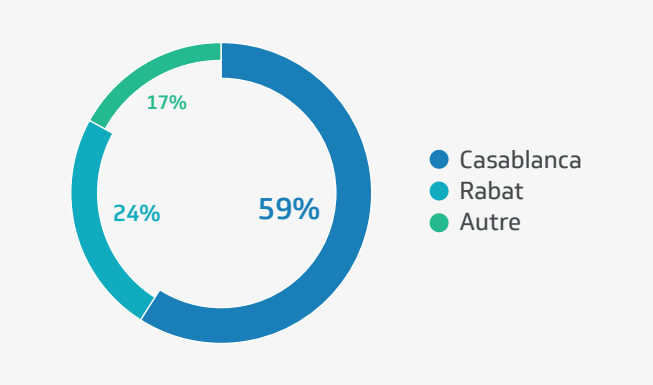
02 PROFIL DE L'INDUSTRIE

2.1 – Localisation des organisations ayant répondu au sondage

Les répondants à l'enquête proviennent de 12 villes. La grande majorité des organisations ayant répondu au sondage sont situées à Casablanca (59%) et Rabat (24%). Les autres villes les plus souvent mentionnées sont Marrakech et Tanger. Cette origine groupée des répondants s'explique car c'est dans ces deux villes que se trouvent le gouvernement et les sièges sociaux des grandes entreprises.

FIGURE 4 – LOCALISATION DES ORGANISATIONS

Veuillez indiquer vos coordonnées, SVP.



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – 94 répondants

2.2 – Taille des organisations ayant répondu au sondage

La majorité des organisations qui ont répondu au sondage sont de grande taille (59%), or comme nous l'avons vu, la très grande majorité des entreprises marocaines sont des PME. Les rares micro-entreprises qui sont présentes dans le sondage sont des filiales d'entreprises étrangères.

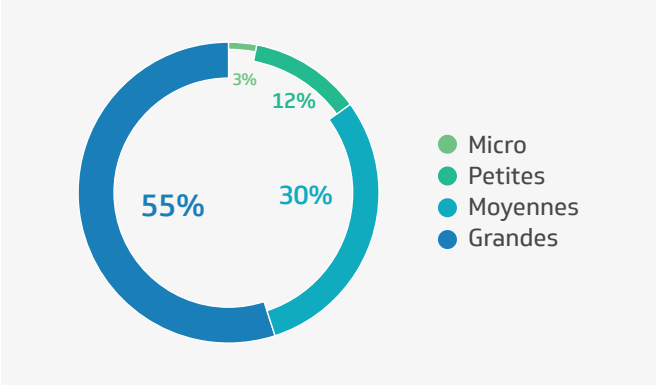
Typologie des entreprises	
Micro-entreprises	*1 à 10 employés*
Petites entreprises	*11 à 50 employés*
Moyennes entreprises	*51 à 250 employés*
Grandes entreprises	*251 à 1000 employés*
Très grandes entreprises	*Plus de 1000 employés*

Comme ce sont généralement les grandes entreprises qui investissent le plus en cybersécurité, cela signifie que nous avons affaire à une population qui devrait être mieux équipée que la moyenne nationale.

Notons que les petites entreprises qui ont répondu au sondage sont en majorité des entreprises de TI, voire même des entreprises spécialisées en cybersécurité. Elles ne représentent pas les petites entreprises marocaines qui appartiennent généralement au secteur commercial.

FIGURE 5 – TAILLE DE L'ORGANISATION

Combien d'employés travaillent dans votre organisation ?
[Veuillez indiquer le nombre approximatif d'employés à temps plein.]



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – 90 répondants

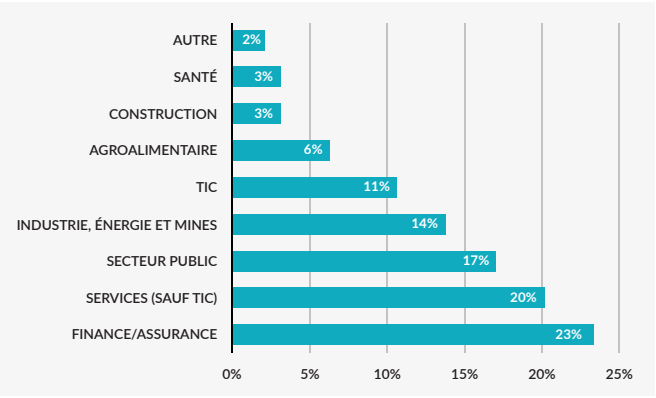
2.3 – Nature des activités des organisations ayant répondu au sondage

Les organisations qui ont répondu au sondage sont en majorité des institutions financières (23%), des entreprises de services (20%) et des administrations publiques (17%). Si on y ajoutait les TIC (11%), on obtient une représentation du secteur tertiaire de plus de 70%.

Ici encore, il ne s'agit pas d'un tertiaire représentatif de la moyenne marocaine. Il s'agit d'un tertiaire orienté vers le secteur financier qui est étroitement réglementé en matière sécuritaire, du gouvernement qui est lié au premier plan par les directives qu'il émet, et vers les entreprises de TIC. Le secteur commercial est à peine représenté par trois entreprises de distribution que nous avons englobées dans le secteur des services. Les BTP et l'immobilier ne sont guère mieux représentés.

FIGURE 6 – NATURE DES ACTIVITES DE L'ORGANISATION

Quel est votre principal domaine d'activité ?
[Par exemple : Banque, assurance, agroalimentaire, santé, machinerie électrique, électronique…]



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – 94 répondants

2.4 – Situation des marchés desservis par les organisations ayant répondu au sondage

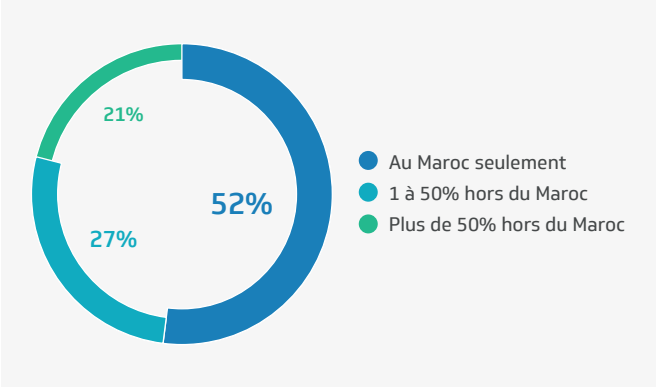
Près de la moitié des organisations ayant répondu au sondage exporte faiblement (27%) ou massivement (21%). Les marchés les plus souvent cités sont l'Afrique (21%) suivi de l'Europe (13%), le reste du monde étant à peine mentionné (4%).

Il n'y a pas de profil type de l'entreprise exportatrice. Des PME aussi bien que des grandes entreprises exportent massivement. Bien des grandes organisations sont des administrations publiques qui, par définition, se concentrent sur le territoire national. Cela fait diminuer la présence des grandes organisations sur les marchés extérieurs.

Cependant, au sein des répondants, il faut noter la présence active des petites entreprises parmi les exportateurs, en particulier les petites entreprises de haute technologie ainsi que les filiales marocaines de grands groupes étrangers.

FIGURE 7 - OU SONT SITUES VOS MARCHES ?

Quel pourcentage de chiffre d'affaires effectuez-vous : au Maroc ? hors du Maroc ?



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – 59 répondants

03

GESTION DE LA CYBERSECURITE

Ce chapitre a pour objet de définir le niveau de préparation des organisations marocaines en matière de cybersécurité, tant dans le domaine du déploiement de programmes spécialisés que dans celui de la gouvernance et des processus.

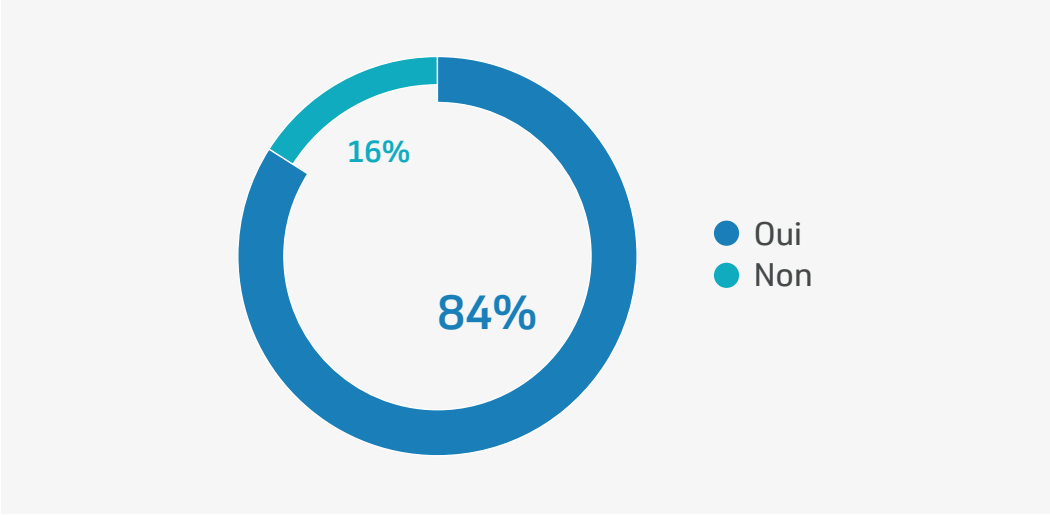
3.1 – Déploiement d'un programme de cybersécurité

La grande majorité des organisations affirme disposer d'un programme de cybersécurité (mesures à prendre en cas de failles ou d'incidents liés à la sécurité de l'information). Encore convient-il de mentionner que parmi les organisations qui ont répondu par la négative, certaines sont en train de s'équiper et d'autres ont mis en place des mesures ponctuelles.

Reste un petit groupe d'environ 16% des organisations qui déclarent que la cybersécurité n'est pas une priorité. Cela ne signifie pas que ces organisations soient complètement démunies en termes de cybersécurité, mais plutôt qu'elles n'ont pas formalisé les mesures prises.

FIGURE 8 - LA GRANDE MAJORITE DES ORGANISATIONS ONT UN PROGRAMME DE CYBERSECURITE

Votre organisation dispose-t-elle d'un programme de cybersécurité (mesures à prendre en cas de failles ou d'incidents liés à la sécurité de l'information) ?



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 94 répondants.

De prime abord, ces résultats sont encourageants, car ils indiquent une forte prise de conscience de l'importance de la cybersécurité au sein des répondants. Reste à évaluer la qualité des programmes mis en place.

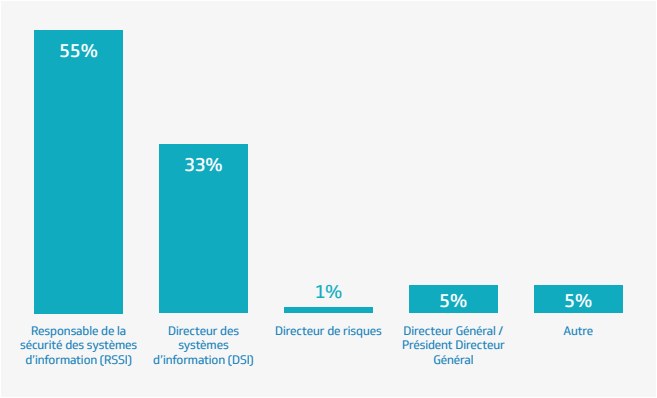
03 GESTION DE LA CYBERSECURITE

3.2 – Structure de gouvernance de la cybersécurité

Plus de la moitié des organisations (55%) confient la cybersécurité à un Responsable de la sécurité des systèmes d'information (RSSI). Toutefois, un tiers des entreprises confient la cybersécurité au Directeur des systèmes d'information (DSI). Parmi les entreprises qui ont répondu « autres », il faut noter des réponses comme « technicien réseau », « technicien spécialisé » ou encore « responsable infrastructure ». Un seul répondant a déclaré que l'ensemble de son programme de sécurité était confié à un prestataire externe.

FIGURE 9 – QUI GERE LA CYBERSECURITE ?

Qui est responsable de la cybersécurité dans votre organisation ?



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base 94 répondants.

Cette structure de gouvernance spécialisée est un signe qui ne trompe pas : la cybersécurité a atteint un degré de maturité suffisant pour devenir dans la majeure partie des cas une fonction autonome de l'entreprise. Quand la responsabilité de la cybersécurité est confiée au DSI, on court le risque de promouvoir dans l'organisation une approche strictement informatique de l'enjeu. Or, nous savons que la cybercriminalité nécessite une réponse globale, fortement axée sur la gouvernance.

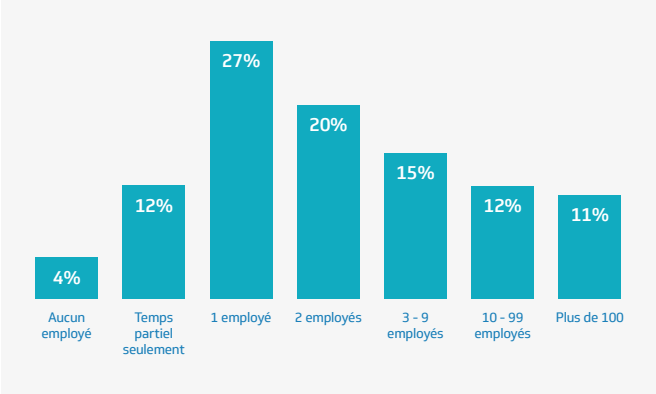
3.3 – L'équipe de cybersécurité

La majorité des organisations consultées ont deux employés ou moins affectés à la cybersécurité. Encore faut-il noter que lors des interviews téléphoniques effectuées en parallèle au sondage, nous avons constaté que plusieurs des répondants avaient gonflé leurs effectifs dans leurs réponses en ligne. Bien des emplois présentés comme à plein temps sont en réalité des emplois à temps partiel. Certains répondants ont aussi confondu le nombre d'employés affectés à la cybersécurité avec celui des employés affectés aux TI en général ou même à l'ensemble de l'organisation. C'est ainsi qu'il faut adopter la plus grande circonspection à l'égard des organisations qui affichent des effectifs de 100 spécialistes et plus en cybersécurité.

L'organisation marocaine moyenne compte un ou deux employés affectés à la cybersécurité, souvent à temps partiel. Dans bien des cas, le RSSI est un employé des TI à qui on a affecté la cybersécurité comme responsabilité additionnelle. Cela ne veut pas dire que le RSSI n'a pas les compétences voulues. Il est souvent passionné par son travail, mais il doit se battre contre sa hiérarchie pour dégager le temps nécessaire pour accomplir sa tâche.

FIGURE 10 – NOMBRE D'EMPLOYES AFFECTES A LA CYBERSECURITE

Combien d'employés dans votre organisation sont affectés à la cybersécurité ?



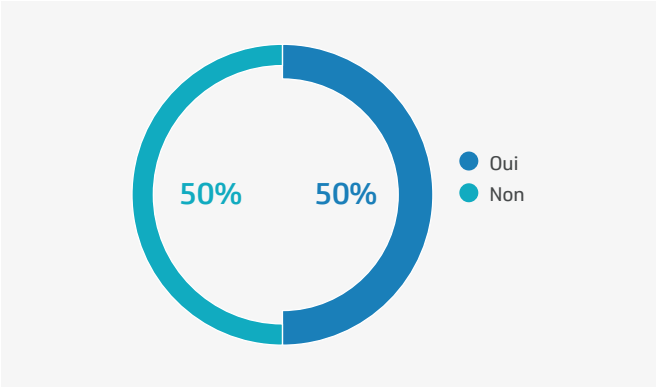
Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base 93 répondants

3.4 – Recrutement de la main d'œuvre en cybersécurité

Les organisations se divisent très exactement en deux sur la question du recrutement de main d'œuvre spécialisée en cybersécurité. Ce sont les organisations dotées de petites équipes (un ou deux employés de cybersécurité) qui disent éprouver le plus de difficultés à recruter.

FIGURE 11 – RECRUTEMENT DES EMPLOYES SPECIALISES EN CYBERSECURITE

Votre entreprise éprouve-t-elle des difficultés à recruter des employés spécialisés en cybersécurité ?

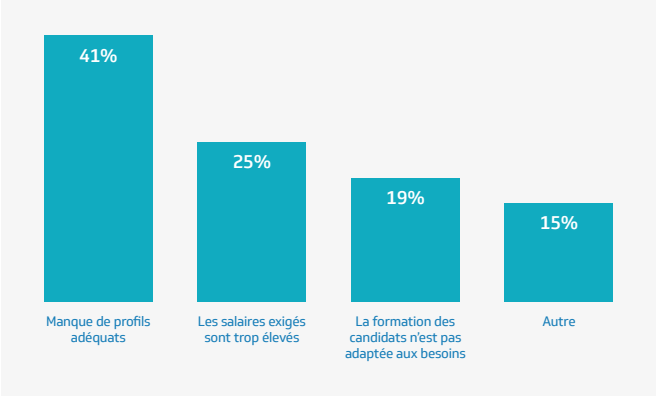


Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 94 répondants

La raison la plus souvent invoquée par les organisations qui éprouvent des difficultés de recrutement, est le manque de profils adéquats. Souvent, les mêmes organisations déplorent aussi l'inadaptation de la formation aux besoins – il était possible de donner plusieurs réponses à la question. Parmi les organisations ayant répondu « Autre », une estimait que les ingénieurs les mieux formés et les plus certifiés étaient recrutés par des sociétés à l'étranger.

FIGURE 12 – PRINCIPALES DIFFICULTES RENCONTREES

[Pour ceux qui ont répondu OUI à la question précédente seulement]
Quelles sont les principales difficultés rencontrées ?



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 47 répondants

La question des salaires avancée par un quart des répondants renvoie à la question plus fondamentale de l'engagement de l'organisation vis-à-vis la sécurité. Tant que la sécurité sera considérée comme un poste de dépenses parmi d'autres, il sera tentant de considérer que son coût est démesuré. La plupart des répondants ayant indiqué « Autre » expliquent qu'ils ont des difficultés internes : la haute direction refuse d'ouvrir des postes en cybersécurité, les formalités administratives sont excessives, ou encore, la grille salariale est inadéquate. Dans tous les cas, nous sommes renvoyés à une culture d'entreprise qui n'a pas pris la juste mesure de l'importance de la cybersécurité.

Même si la moitié de la population interrogée considère qu'il n'y a pas de problème de recrutement, il ne faut pas négliger les obstacles identifiés. Comme la menace de la cybercriminalité augmente de façon exponentielle, la demande en cybersécurité est appelée à croître en proportion.

03 GESTION DE LA CYBERSECURITE

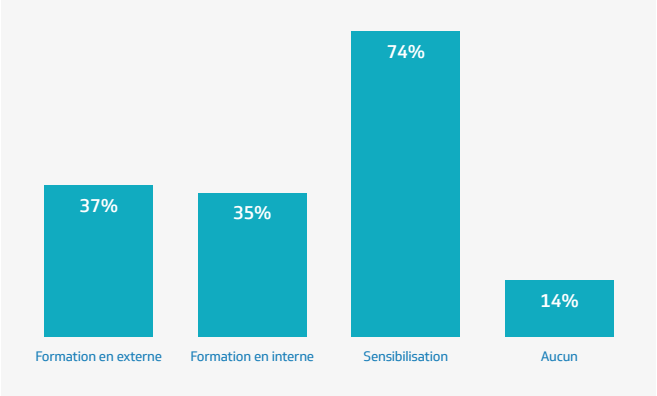
3.5 – Formation et sensibilisation en cybersécurité

La très grande majorité des organisations offrent à ses employés une forme ou l'autre de formation ou de sensibilisation (86%). Il existe même certaines organisations qui offrent concurremment les trois types de formation-sensibilisation (17%).

Parmi les programmes offerts, c'est la sensibilisation qui est la plus populaire (74%). Malheureusement, il ne nous a pas été possible d'obtenir des informations sur la nature de ces programmes de sensibilisation : messages sur l'intranet, courriels personnalisés, bulletins en ligne, affiches, capsules vidéo, etc. La formation externe (université, école spécialisée, etc.) et interne (conférences, cours, etc.) arrivent pour ainsi dire à égalité (35-37%).

FIGURE 13 – FORMATION ET SENSIBILISATION DES EMPLOYES

Dans votre organisation, en matière de cybersécurité, existe-t-il un programme de formation en externe (université, école spécialisée, etc.), un programme de formation en interne (conférences, cours, etc.), un ou des programmes de sensibilisation (messages sur l'intranet, courriels personnalisés, bulletins en ligne, affiches, capsules vidéo, etc.),



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 81 répondants

Sans surprise, la petite minorité qui n'offre ni formation ni sensibilisation appartient en entier au groupe des organisations qui n'ont pas de programme de cybersécurité.

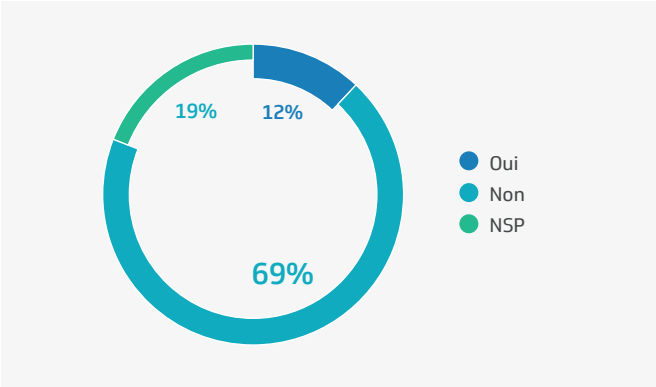
3.6 – Assurance cybersécurité

La grande majorité des organisations n'a pas d'assurance cybersécurité (69%). La réponse la plus souvent fournie pour expliquer ce manque est qu'il n'y a pas d'assurance disponible. Plusieurs répondants justifient leur décision de ne pas s'assurer par le fait qu'ils appartiennent à l'administration publique. Certaines entreprises affirment étudier la question et avoir planifié de s'assurer.

La petite minorité des entreprises qui est assurée est composée de grandes entreprises ou de filiales d'entreprises étrangères.

FIGURE 14 – LA MAJORITE DES ENTREPRISES N'A PAS D'ASSURANCE CYBERSECURITE

Votre entreprise a-t-elle contracté une assurance pour couvrir le risque en matière de cybersécurité ?



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 94 répondants

D'une façon générale, on peut conclure qu'il existe beaucoup d'incertitude vis-à-vis de l'assurance cybersécurité et que l'absence d'information est généralisée. Il s'agit d'un marché encore en friche. Encore une fois, il est à prévoir qu'avec la croissance rapide de la cybercriminalité, ce marché sera appelé à s'épanouir.

> Plus des 3/4 des répondants exigent que leurs sous-traitants aient des bonnes pratiques de cybersécurité.

3.7 – Extension du programme de cybersécurité aux sous-traitants

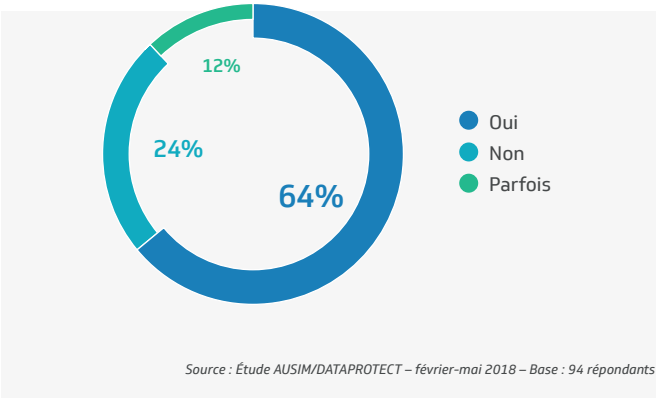
73% des répondants incluent une clause écrite sur les risques de cybersécurité dans les accords de sous-traitance – plus précisément, ils disent exiger que les fournisseurs respectent une norme de sécurité ou encore disposent d'un programme de sécurité. La plupart d'entre eux le font systématiquement (64%) et les autres le font parfois (12%).

Ces derniers le font chaque fois que des données personnelles sont en jeu afin de se conformer à la Loi 09-08 sur la protection des données à caractère personnel. La taille du projet peut aussi être une raison pour inclure une telle clause dans les accords de sous-traitance.

Parmi la minorité d'organisations (24%) qui ne prévoit aucune garantie dans les accords de sous-traitance. Fait plus troublant, certaines entreprises qui affirment disposer d'un programme de cybersécurité à l'échelle institutionnelle, n'exigent pas de disposition sur la cybersécurité dans les accords de sous-traitance.

FIGURE 15 – LES ACCORDS DE SOUS-TRAITANCE PRENNENT EN COMPTE LA CYBERSECURITE

Les risques de cybersécurité font-ils l'objet d'une clause écrite dans les accords de sous-traitance ? (Par exemple, exigez-vous que les fournisseurs respectent une norme de sécurité ou encore disposent d'un programme de sécurité ?)



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 94 répondants

04 TECHNOLOGIE DE LA CYBERSECURITE

Ce chapitre détaille le cadre technologique de la cybersécurité : fréquence des audits, existence d'un plan de relève, utilisation d'un SOC ainsi que la gestion des cyberattaques. Le panorama des technologies déployées et la façon dont elles sont employées, permettent d'évaluer les tendances lourdes de la cybersécurité.

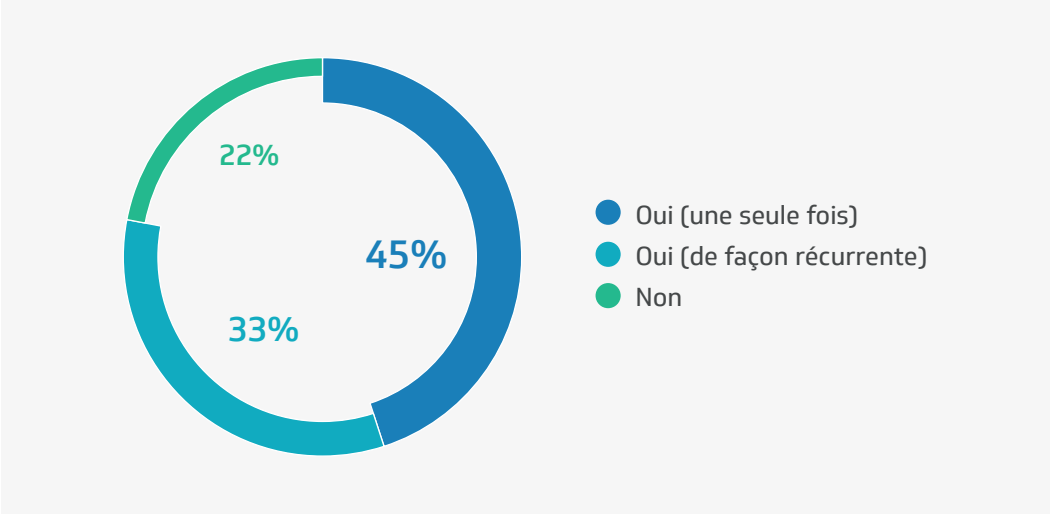
4.1 – Audit de sécurité

A la base de toute stratégie de cybersécurité se trouve l'audit. Il s'agit d'un processus exhaustif qui permet de s'assurer du bon déploiement de la stratégie de cybersécurité préalablement arrêtée.

La très grande majorité des organisations marocaines a déjà effectuée un audit complet de cybersécurité, ce qui montre le sérieux apporté par les organisations marocaines dans leur approche de la cybersécurité. Cependant, un tiers seulement d'entre elles le font de façon régulière. Ce groupe des « bons élèves » de la cybersécurité est composé presque exclusivement de grandes entreprises – les rares petites entreprises présentes sont des cabinets conseils en TI.

FIGURE 16 – LA PRATIQUE DES AUDITS DE CYBERSECURITE EST GENERALISEE

Votre organisation a-t-elle déjà effectué un audit complet de cybersécurité ?



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 93 répondants

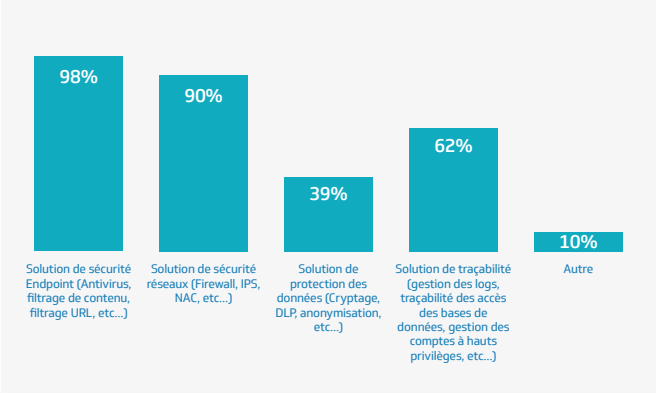
04 TECHNOLOGIES DE LA CYBERSECURITE

4.2 – Principales technologies de sécurité utilisées

La protection « endpoint » aussi bien que réseau est quasi universelle dans la population considérée. Les solutions de traçabilité sont aussi très majoritairement utilisées. Par contre, le taux d'utilisation baisse grandement quand il s'agit de protection des données (cryptage, DLP, anonymisation, etc.). Ce résultat est d'autant plus surprenant que la Loi 09-08 rend obligatoire la protection des données personnelles. Il existe encore certaines administrations publiques, entreprises de distribution et même des institutions financières qui n'ont pas encore adopté de solutions de protection des données.

FIGURE 17 – PRINCIPAUX SYSTEMES DE SECURITE UTILISES

Quels systèmes de sécurité utilisez-vous dans votre organisation ? [Plusieurs réponses possibles.]



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 93 répondants

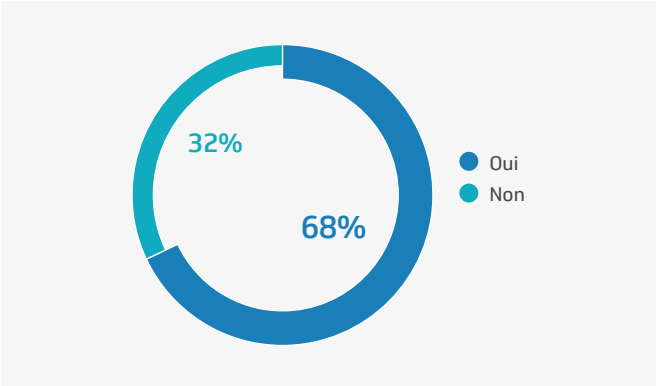
4.3 – Plan de réponse aux incidents

L'incident informatique quand il survient est instantané : impossible d'improviser. Tout le monde doit savoir quelles procédures et stratégies a appliquer sur le plan technique, bien entendu, mais aussi sur le plan des communications internes et externes (clients, fournisseurs et, le cas échéant, organisme de réglementation).

Plus des deux-tiers des répondants affirment disposer d'un plan de réponse aux incidents. Ceux qui n'en sont pas équipés correspondent aux habituels « ni-ni » : ils n'ont ni programme de cybersécurité, ni audit régulier ou même ponctuel. Ce sont généralement des PME, mais on y trouve quelques rares grandes organisations. Ce sont des organisations à haut risque où un simple incident a le potentiel de se transformer en catastrophe, faute de préparation.

FIGURE 18 – IMPORTANCE DU PLAN DE REPONSE POUR LES ORGANISATIONS

Votre organisation dispose-t-elle d'un plan de réponses aux incidents ?



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 93 répondants

LES ENJEUX DE LA CYBERSECURITE AU MAROC

4.4 – Simulation de cyberattaques

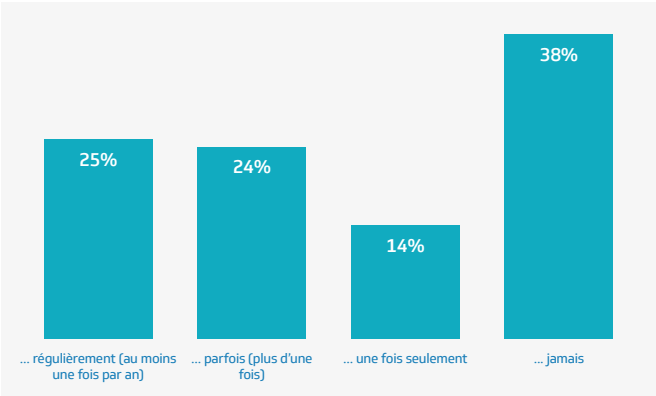
Plan de réponse et simulation de cyberattaques vont de pair : pour construire un plan de réponse, il est nécessaire de procéder à une simulation de cyberattaques. Aussi, ne faut-il pas s'étonner si 63% des organisations ont déjà procédé à des exercices de simulation. Ce sont presque toujours les mêmes organisations qui ont un plan de réponse.

Encore faut-il distinguer la minorité des organisations (25%) qui s'adonnent à des simulations annuelles de celles qui s'y adonnent irrégulièrement (24%) ou ponctuellement (14%). Pourtant, tout le monde s'accorde pour considérer que pour être valable, une simulation doit être répétée sur une base régulière.

Les organisations qui ne font pas de simulation ou qui le font sur une base irrégulière le reconnaissent. Elles invoquent alors le manque de ressources humaines ou de budget ou encore le manque de maturité du top Management. Une seule entreprise a répondu que « l'enjeu ne le justifiait pas ».

FIGURE 19 – SIMULATIONS DE CYBERATTAQUES EFFECTUEES PAR LES ORGANISATIONS

Votre entreprise effectue-t-elle des simulations de cyberattaques ?



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – 93 répondants

04 TECHNOLOGIES DE LA CYBERSECURITE

4.5 – Surveillance permanente des événements de sécurité via un SOC

Les organisations dotées d'un plan de réponse aux incidents doivent aussi surveiller les flux de données entrantes et sortantes. Il est important d'identifier l'incident aussitôt que possible en formalisant le traitement des incidents depuis leur détection jusqu'à leur traitement et centraliser les processus de façon à avoir une visibilité globale de la situation en temps réel. L'outil capable de satisfaire à ce double objectif est le centre d'opérations et de sécurité ou SOC selon son acronyme anglais (Security Operations Center).

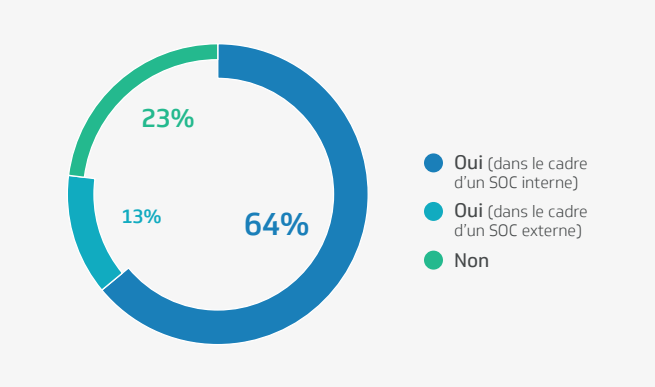
A la question sur la surveillance permanente des événements de sécurité, plus des trois-quarts des entreprises disposant d'un plan de réponse ont répondu qu'elles utilisaient un SOC à cet effet. La majeure partie utilise un SOC interne (65%) et un petit groupe un SOC externe (13%). Il s'agit évidemment le plus souvent de moyennes et grandes entreprises. Fait notable, la moitié des institutions financières déclare ne pas avoir recours à un SOC, ni interne, ni externe. Quelques rares administrations publiques et grandes entreprises privées n'ont pas de SOC.

Affirmer avoir un SOC est une chose. La qualité des SOC déployés en est une autre. Quand on voit des entreprises de taille moyenne affirmer avoir déployé un SOC en interne, il y a de quoi poser la question de la qualité. En effet, un SOC doit fonctionner 24/7 et employer au minimum cinq spécialistes à temps plein. Maintes entreprises possédant un ou deux employés en cybersécurité affirment avoir créé un SOC en interne… Il faut donc revoir à la baisse le taux réel d'entreprises disposant d'un SOC opérationnel en bonne et due forme.

La grande majorité des entreprises prétendant avoir des SOC internes ont en réalité déployé une solution de gestion des logs et, dans le meilleur des cas, un outil SIEM, mais pour être efficace, elle requiert une présence humaine constante. Notre conclusion est qu'il y a très peu d'organisations au Maroc équipée d'un SOC interne.

FIGURE 20 – ORGANISATIONS AFFIRMANT DISPOSER D'UN SOC

Votre organisation effectue-t-elle de la surveillance permanente des événements de sécurité ?



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 62 répondants

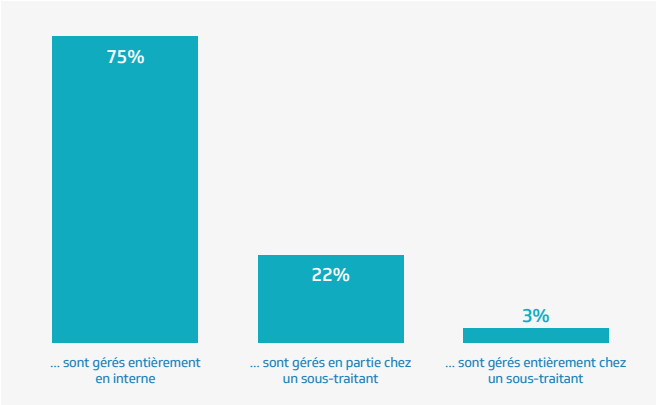
4.6 – Impartition des systèmes de cybersécurité

Les trois-quarts des organisations gèrent entièrement en interne leur système d'information et l'impartition (outsourcing) intégrale est l'exception. Reste une minorité appréciable d'organisations qui a recours à l'impartition partielle.

Les organisations qui recourent à l'impartition sont également divisées entre les « bons » et les « mauvais » élèves de la cybersécurité si on considère les critères de la formation-sensibilisation, de l'audit ou du plan de réponse. Il y a donc deux raisons pour sous-traiter la sécurité : le choix de confier en externe le mandat d'atteindre un niveau d'excellence qui ne peut être réalisé en interne ou, au contraire, le manque de maturité sécuritaire.

FIGURE 21 – LA MAJORITE DES SYSTEMES D'INFORMATION SONT GERES EN INTERNE

Vos systèmes de sécurité sont gérés entièrement en interne, sont gérés en partie chez un sous-traitant, sont gérés entièrement chez un sous-traitant.



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 93 répondants

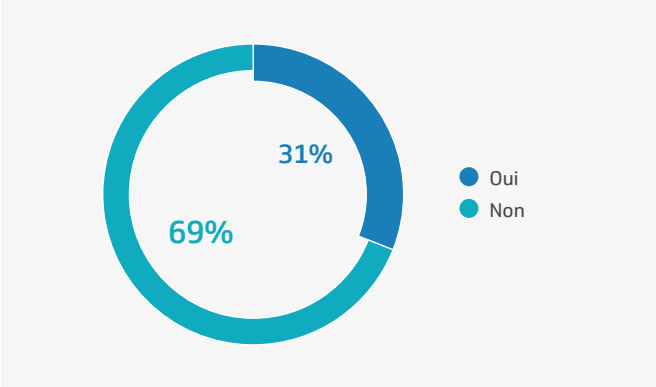
4.7 – Le cas des cyberattaques

Quand on demande aux organisations si elles ont déjà enregistré des cyberattaques, moins d'un tiers répond par l'affirmative. Parmi celles-ci, la plupart d'entre elles affirme avoir enregistré une seule cyberattaque. Pour la majorité d'entre elles, il s'agit d'organisations disposant d'un programme de cybersécurité, d'un plan de réponses aux incidents et ayant effectué au moins un audit de sécurité.

Il est assuré que le taux de cyberattaques est supérieur à ce qui est reporté car de nombreux types d'incidents passent inaperçus : intrusion informatique, vol de données, intégrité des données, etc. De nombreux incidents ne sont jamais décelés ou le sont après des années. Ainsi, à titre d'exemple, l'Union européenne estime que 80 % des entreprises européennes ont été touchées par des attaques de type demande de rançon au cours de l'année écoulée[7].

FIGURE 22 – UN NOMBRE RELATIVEMENT BAS DE CYBERATTAQUES

Votre entreprise a-t-elle déjà fait l'objet d'une cyberattaque ?



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 94 répondants

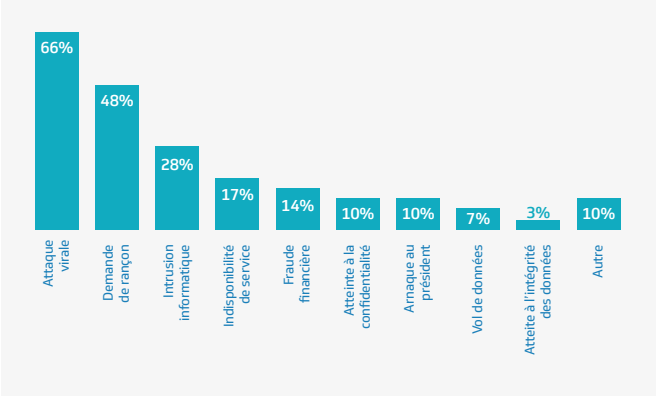
7 Commission européenne, fiche d'information : « État de l'Union 2017: la Commission renforce sa capacité de réaction face aux cyberattaques », 19 septembre 2017. http://europa.eu/rapid/press-release_MEMO-17-3194_fr.htm

04 TECHNOLOGIES DE LA CYBERSECURITE

Près des deux-tiers des cyberattaques sont effectuées par virus informatique. C'est de loin, le type d'incident le plus fréquent. Il est suivi par la demande de rançon avec près de la moitié des cas reportés. Dans la catégorie « Autre », il faut noter une usurpation d'identité, un cryptage des données et un défacement de pages web du site de l'organisation.

FIGURE 23 – LES DIFFERENTS TYPES DE CYBERATTAQUES

[Pour ceux qui ont répondu OUI à la question précédente.] [Plusieurs réponses possibles.]
Pouvez-vous définir de quel type de cyberattaques il s'est agi ?



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 29 répondants

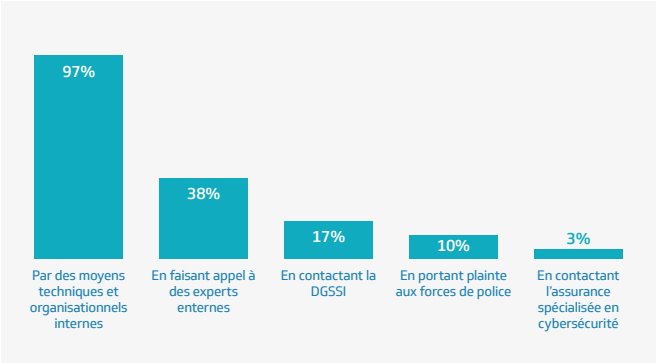
> Une étude rendue publique en novembre 2017 par Kaspersky Lab et Averty estimait que 21% des entreprises marocaines avaient déjà été victimes d'une cyberattaque et que la menace informatique la plus répandue était le virus (63%). L'étude ne couvrait pas la demande de rançon.
>
> **Reda Benomar,**
> « La cybersécurité n'est pas la priorité des dirigeants »,
> *L'Économiste*, 4 décembre 2017.

La quasi-totalité des organisations sujettes à des cyberattaques ont réagi avec des moyens internes – une forte minorité a aussi fait appel à des ressources externes. Notons qu'il ne s'agit pas d'un choix : interne ou externe. Une fois frappées, les organisations font appel à toutes les ressources disponibles.

Près de la moitié des organisations ayant subi des cyberattaques n'avaient jamais effectué de simulation (13 organisations sur 29) et plus du quart n'avaient jamais procédé à un audit (huit organisations sur 29). Elles ont dû entièrement improviser leur riposte. Or, il y avait parmi elles des administrations publiques et des grandes entreprises privées. Manifestement, le manque de maturité de certaines organisations a eu pour conséquence de transformer l'incident en crise.

FIGURE 24 – LES DIFFERENTS TYPES DE RIPOSTES

Comment votre entreprise a-t-elle réagi à la cyberattaque ?
[Plusieurs réponses possibles.]



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 29 répondants

05

CADRE LEGAL ET REGLEMENTAIRE

Le Maroc s'est doté en quelques années d'un arsenal législatif et réglementaire destiné à encadrer les activités informatiques et à assurer la sécurité des citoyens ainsi que des infrastructures critiques (Loi 09-08 et DNSSI). Il existe en outre des normes internationales très populaires parmi les organisations.

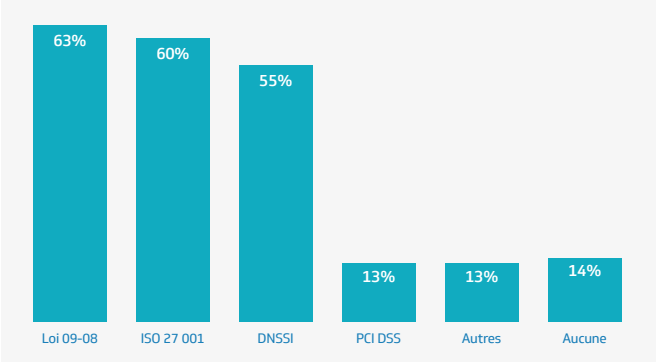
05 CADRE LEGAL ET REGLEMENTAIRE

5.1 – Normes de sécurité les plus suivies par les organisations marocaines

La plupart des organisations ont adopté une ou plusieurs normes de sécurité (86%), à commencer par celles qui sont obligatoires au Maroc – Loi 09-08 et DNSSI. Les organisations qui ont répondu « Autres » mentionnent la CNDP marocaine, le RGPD européen et le NIST CSF américain. Parmi celles qui ont répondu « aucune », deux d'entre elles affirment être en voie d'adoption d'une norme.

FIGURE 25 – NORMES DE SECURITE LES PLUS GENERALEMENT ADOPTEES

Votre organisation a-t-elle adopté une ou plusieurs des normes de sécurité suivantes : DNSSI (Directive Nationale de la Sécurité des Systèmes d'Information) ; ISO 27001 (management de la sécurité des informations) ; Loi 09-08 (Protection des personnes physiques) ; PCI DSS (Payment Card Industry Data Security Standard) ; Autre. [Plusieurs réponses possibles.]



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 94 répondants

La grande popularité des normes parmi les organisations marocaines est peut-être le signe le plus fort de l'engagement en matière de cybersécurité – avant même le déploiement d'un programme de cybersécurité. Certaines organisations ont adopté des normes de cybersécurité alors qu'elles n'ont même pas déployé de programme. Cela signifie que pour certaines organisations, l'adoption de normes tient lieu du programme.

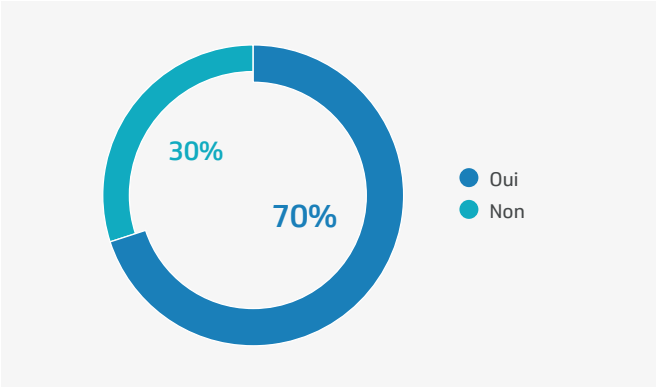
Comme deux des trois normes les plus généralement adoptées sont marocaines, cela souligne le rôle crucial que joue l'État dans le développement de la cybersécurité au Maroc.

5.2 – Suivi de la conformité aux normes

Soixante-dix pour cent des organisations ayant adopté des normes et règlements vérifient périodiquement leur conformité. Cela s'explique pour la DNSSI et la Loi 09-08 en raison du caractère contraignant du cadre réglementaire et législatif marocain. Qui plus est, les organisations qui ont adopté ISO 27001 en vérifient aussi la conformité. Cette qualité du suivi atteste de l'importance du cadre normatif pour les organisations marocaines.

FIGURE 26 – SUIVI DES NORMES

Votre organisation vérifie-t-elle périodiquement sa conformité aux normes sectorielles et à la réglementation ?



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 81 répondants

06

NIVEAU DE L'INVESTISSEMENT

L'investissement moyen des organisations marocaines dans la cybersécurité est faible (moins d'un million MAD), mais il évolue à la hausse. Une légère majorité des répondants s'estiment bien outillées en matière de cybersécurité, mais de la place demeure pour de l'amélioration.

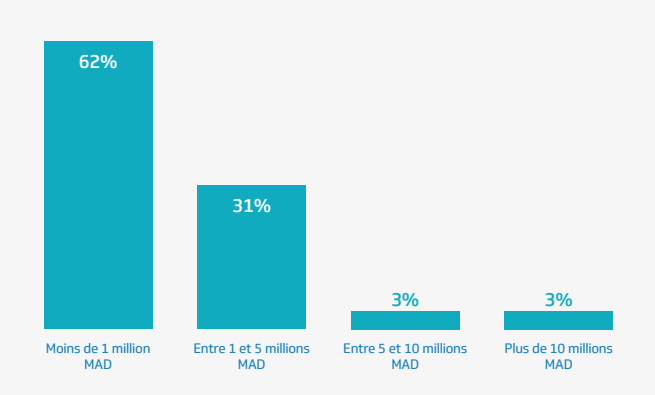
06 NIVEAU DE L'INVESTISSEMENT

6.1 – Investissement moyen en cybersécurité

La majeure partie des organisations investit moins d'un million de dirhams par an en cybersécurité[8] . Or, la grande majorité de ces firmes déclare avoir mis au point un programme de cybersécurité, un programme de formation-sensibilisation et adopté des normes, la moitié prétend avoir déployé un SOC en interne ou en externe. La modestie des moyens déployés indique l'état encore embryonnaire de la cybersécurité dans les organisations marocaines. La faiblesse des budgets est particulièrement frappante dans le secteur bancaire : près de la moitié des institutions financières investissent moins d'un million de dirhams par an.

FIGURE 27 – INVESTISSEMENT EN CYBERSECURITE

Quel est le montant approximatif que votre organisation investit en cybersécurité sur une base annuelle (montant pour 2017) ?



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 87 répondants

Les investissements conséquents en cybersécurité demeurent limités aux grandes organisations et quelques rares moyennes organisations : les trois quarts des organisations investissant entre un et cinq millions de dirhams sont grandes ; toutes les organisations investissant plus de cinq millions le sont.

6.2 – Prévisions d'investissements en cybersécurité

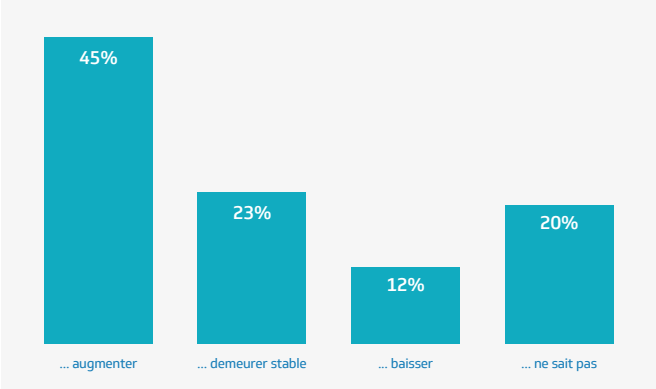
Les investissements en cybersécurité sont appelés à augmenter en 2018 dans 45% des organisations. C'est peu. Dans la majeure partie des cas, les investissements vont demeurer stables, baisser, ou encore, l'incertitude règne.

La quasi-totalité des organisations qui investissent plus de cinq millions de dirhams par an prévoient augmenter leurs budgets de cybersécurité – sauf une qui prévoit des investissements stables. Seule la moitié des organisations qui investissent moins d'un million par an prévoit augmenter ses investissements en cybersécurité.

D'une façon générale, ce sont les organisations qui investissent le plus qui prévoient d'augmenter leurs budgets de cybersécurité.

FIGURE 28 – LES INVESTISSEMENTS EN CYBERSECURITE AUGMENTENT PEU

Au cours de 2018, prévoyez-vous que ce montant sera amené à : augmenter ; demeurer stable ; baisser ; ne sait pas.



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 93 répondants

Face à la faiblesse des investissements actuels en cybersécurité, on devrait assister à un phénomène de rattrapage qui se traduirait par des injections massives de fonds. Ce n'est pas le cas. Manifestement, le grand décollage de la cybersécurité dans les organisations marocaines n'a pas commencé.

8 Un million MAD = 90 000 EUR ou encore 105 000 USD.

07

CONCLUSION ET PISTES DE REFLEXION

Ce chapitre porte sur les grands enjeux sécuritaires auxquels est confrontée le Maroc. Il se fonde à la fois sur les résultats du sondage et sur les interviews qualitatives effectuées par l'équipe AUSIM/DATAPROTECT auprès des responsables de la cybersécurité.

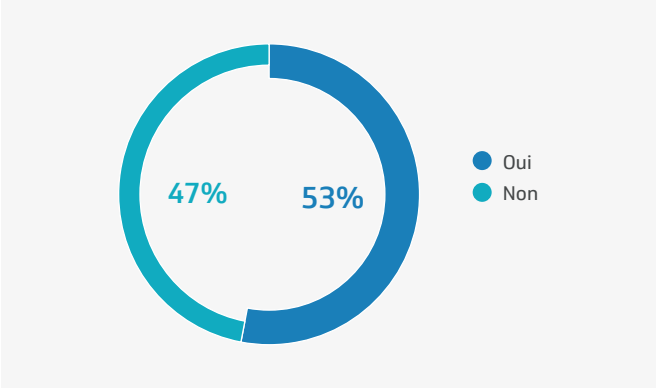
07 CONCLUSION ET PISTES DE RÉFLEXION

7.1 – Maturité des organisations en matière de cybersécurité

La dernière question du sondage portait sur l'évaluation globale des répondants par rapport à la situation de leurs organisations en matière de cybersécurité. A peine plus de la moitié affirmait que leur organisation était bien outillée. Les autres estimaient qu'il leur fallait faire plus pour améliorer la sécurité en termes de formation-sensibilisation, surveillance des activités de sécurité (SOC), audit, adoption de normes et recrutement de spécialistes.

FIGURE 29 – SATISFACTION MITIGEE VIS-A-VIS LA MATURITE EN CYBERSECURITE DES ORGANISATIONS

D'une façon générale, estimez-vous que votre organisation soit bien outillée en matière de cybersécurité ?



Source : Étude AUSIM/DATAPROTECT – février-mai 2018 – Base : 94 répondants

La moitié des organisations qui se disent bien outillés investissent moins d'un million de dirhams par an dans leur cybersécurité. La plupart affirment avoir mis au point un programme de cybersécurité, réalisé au moins un audit et même déployé un SOC.

7.2 – Grands enjeux de la cybersécurité au Maroc

Les organisations marocaines sont conscientes de l'importance de la cybersécurité, mais elles manquent de moyens pour mettre au point des mesures adéquates. La meilleure preuve de cette prise de conscience est le fort taux d'organisations qui se sont dotées d'un programme de cybersécurité (84%), qui offrent à leurs employés de la formation ou de la sensibilisation (86%) et enfin qui ont adopté une ou plusieurs normes nationales ou internationales (86%). Le plan de réponse aux cyberattaques est relativement bien déployé (68%) mais dans des conditions qui le rendent peu efficaces comme indiqué ci-dessous.

Au titre des faiblesses de la cybersécurité, il faut mentionner les audits qui sont effectués de façon ponctuelle (45%) ou pas du tout (22%), le peu de solutions de protection des données déployées (39%), la simulation effectuée irrégulièrement (24%), ponctuellement (14%) ou pas du tout (38%), ce qui rend inopérant le plan de réponses aux incidents. Ces faiblesses sont dues au manque de personnel et d'investissement, l'un renvoyant à l'autre.

Il y a donc un paradoxe au cœur de la cybersécurité marocaine : d'une part, les organisations affichent une sensibilité tout à fait adaptée au risque de la cybercriminalité, d'autre part, elles ne consentent pas les investissements nécessaires et engagent des ressources humaines au compte-gouttes. Un élément de réponse tient à la nature du sondage : il a fait appel aux responsables de la sécurité des systèmes d'information (RSSI) des organisations et non à la haute direction. A cet égard, plusieurs répondants ont déploré l'absence d'engagement de leurs dirigeants. Nous avons relevé plusieurs remarques de ce genre :

- « Ne valorise pas la valeur de l'information »,
- « Manque de maturité »,
- « Pas encore une priorité pour le top Management »…

7.3 – Rôle de l'Etat

La Stratégie Maroc Digital 2020 vise à mettre en ligne 50% des démarches administratives, à réduire de 50% la fracture numérique, à connecter 20% des PME et à faire du Maroc le premier hub numérique du continent africain d'ici 2020. La création de l'Agence du développement du digital (ADD) en décembre 2017 a pour objet de mettre en œuvre cette stratégie[9]. Pour atteindre ses objectifs, la nouvelle ADD aura besoin d'établir la confiance numérique au sein du tissu économique marocain.

Nous avons vu que l'un des points forts de la cybersécurité était l'adoption de normes par les organisations : 86% des organisations sondées ont adopté une ou plusieurs normes de cybersécurité. Étendre cette pratique aux PME apparaît comme une condition impérieuse à l'établissement de cette confiance numérique qui sous-tend l'atteinte de tous les autres objectifs. Il y a un défi de taille à relever pour l'ADD.

9 Mohamed Douyeb, « Le Maroc a besoin d'une Agence du digital indépendante », Huffpost Maghreb, 2 janvier 2018.

Annexe 01

ETUDES DE CAS

Les organisations qui font l'objet d'une présentation détaillée ont été choisies en fonction de leur appartenance aux différents segments de l'économie de façon à donner un aperçu aussi complet que possible de la variété des activités du secteur de la sécurité avancée au Maroc. Il ne s'agit donc pas d'un palmarès des meilleures organisations choisies en fonction d'un quelconque critère comparatif (innovation technologique ou marketing, chiffre d'affaires, meilleures pratiques, etc.).

La longueur des études de cas varie beaucoup d'une organisation à l'autre et il ne faut pas y voir un jugement de valeur : ce n'est pas parce qu'une étude de cas est détaillée que l'organisation est forcément plus innovante, active ou digne d'intérêt. Il faut plutôt y voir un reflet de la politique des dirigeants en matière de partage de l'information : certains d'entre eux ont été très généreux de leur temps, d'autres ont éprouvé des réserves devant certaines questions qu'ils considéraient comme confidentielles.

LISTE DES ETUDES DE CAS

- *Autoroute Du Maroc (ADM)*
- *Ecole nationale supérieure d'informatique et d'analyse des systèmes (ENSIAS)*
- *Institut national des postes et télécommunications (INPT)*
- *Groupe d'assurances Lyazidi*
- *Groupe Managem*
- *Ministère de la Réforme de l'Administration publique*
- *Phone Group*
- *Tarec*

Annexe 01

Autoroute Du Maroc (ADM)

Société Nationale des Autoroutes du Maroc
BP 6526, Hay Ryad,
Rabat, Maroc
Tél. (212) 06 6138 79 97
www.adm.co.ma

Entrevue	**M. Hassan Hamala** *Responsable de la sécurité des systèmes d'information (RSSI)*	
Données de base	Fondation Chiffre d'affaires Nombre d'employés Activité	1989 3,4 G MAD 540 Exploitation du réseau autoroutier du Maroc
Mission	✓ Aménagement du territoire favorisant un développement rapide du réseau autoroutier. ✓ Gestion, protection et conservation du domaine public dépendant du réseau de transport mis à la disposition d'ADM. ✓ Création et exploitation de services touristiques, d'hôtellerie et de tout autre service dans la proximité géographique de l'autoroute.	
Objectif	Satisfaction client par le développement de services innovants pour garantir leur sécurité, leur confort et leur faciliter toujours plus leur trajet.	
Moyens	Déploiement d'un système de télépéage destiné à fluidifier le trafic.	
Enjeux	Assurer la sécurité de l'information dans un contexte de télépéage.	

M. Hassan Hamala a travaillé pendant 20 ans aux systèmes d'information d'ADM. A compter de 2010, il a pris conscience de la montée en importance de la sécurité informatique dans le secteur des autoroutes. Il a alors passé un Master en gouvernance des systèmes d'information à l'Université internationale de Rabat. Il est aussi certifié, entre autres, ISO 27 001 et ISO 9 001. C'est en 2016 que le poste de RSSI a été créé. C'est le seul employé affecté à plein temps à la sécurité des systèmes d'information.

Depuis plus d'un an, ADM a commencé à s'intéresser à la sécurité de l'information car l'organisation est engagée dans un important programme d'automatisation du péage. Les voitures utilisent des « tags » pour passer dans les voies dédiées des postes de péage sans avoir besoin de s'arrêter et de payer en espèces. La dématérialisation du péage comprend aussi l'introduction des moyens de paiement monétique tels que l'acceptation des cartes bancaires, les bornes automatiques et le rechargement des cartes d'abonnement par internet.

Le télépéage avait débuté sur un plan modeste il y a quatre ou cinq ans. Le programme est passé à la vitesse supérieure en 2016 en faveur du partenariat entre ADM et la société française VINCI Autoroutes, prestataire technique en charge de la modernisation et de l'automatisation du système de péage. ADM enregistre à présent 200 000 « tags » et compte franchir le cap des 500 000 « tags » d'ici 2020. Depuis un an et demi, il est possible de circuler avec des « tags » sur les 1 800 kilomètres d'autoroute que compte le Maroc. Cette modernisation du système de péage a posé de façon nouvelle le problème de la sécurité des systèmes d'information chez ADM.

Annexe 01 Autoroute Du Maroc (ADM)

ADM vient de terminer un audit technique des systèmes d'information avec le support d'un cabinet conseil spécialisé en sécurité. Un bon de commande vient d'être émis pour mettre en place un véritable programme de sécurité de l'information. Le cahier de charge pour la mise en place d'un plan de renforcement de la sécurité vient tout juste d'être terminé. Cet ambitieux programme a été rendu possible par la haute direction d'ADM qui est consciente de l'importance de la sécurité de l'information dans le contexte de l'automatisation du péage. En effet, ADM fait partie de la liste des infrastructures d'importance vitale établie par la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) et, à ce titre, se trouve assujettie à la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI).

D'une valeur de huit millions de dirhams (± 700 000 euros), le plan de renforcement de la sécurité a pour objectif de rendre conforme à la DNSSI ainsi qu'aux meilleures pratiques internationales les systèmes d'information d'ADM[10]. Ce plan va concerner tous les aspects de la sécurité de l'information depuis la révision de la politique de sécurité, la charte des procédures jusqu'aux outils et aux moyens pour faire les tableaux de bords. Un système de gestion du risque va être mis en place. C'est un grand projet à la fois technique et managérial qui va toucher toutes les entités d'ADM, y compris les bureaux régionaux. Pour exécuter le plan d'action, il est prévu un accompagnement par un prestataire de services de sécurité de l'information.

Les principaux buts du plan de renforcement de la sécurité se déclinent comme suit :

- Disposer d'une vision globale et objective du niveau de sécurité du système d'information.
- Obtenir une liste détaillée de vulnérabilités présentes au sein du système d'information ainsi que des faiblesses au niveau organisationnel.
- Disposer de recommandations d'experts pour l'amélioration du niveau global de sécurité du système d'information.
- Obtenir une cartographie claire des risques de sécurité pesant sur le système d'information.
- Etablir un plan d'action d'amélioration basé sur des recommandations pragmatiques détaillées et chiffrées classées en deux catégories :
  - o Actions à mener à court terme;
  - o Actions à mener à moyen terme.
- Assurer des séminaires de formation et de sensibilisation en sécurité de l'information au profit du personnel ADM.
- Bénéficier de l'assistance d'experts en matière de sécurité pour la mise en œuvre des améliorations nécessaires au sein du système d'information.

Ce plan d'action repose sur une série d'audits : sécurité organisationnelle et physique, sécurité technique (tests d'intrusions externes et internes, configuration, architecture, applications, code source, performance des systèmes d'information) et audit spécifique de la sécurité du système d'information de péage. A partir de ces audits, un plan d'action sera élaboré qui hiérarchisera les recommandations en fonction de l'importance du risque :

- Les actions détaillées organisationnelles et techniques urgentes à mettre en œuvre dans l'immédiat, pour parer aux défaillances les plus graves ;
- Les actions stratégiques, organisationnelles et techniques à mettre en œuvre sur le court, moyen et long terme.

Les phases d'audit permettront aussi de mettre en œuvre une démarche d'analyse des risques à la lumière des meilleures pratiques dans le domaine et sur la base des normes et méthodologies internationales (ISO 27 005, EBIOS/MEHARI, etc.). Des scénarios de risques seront définis ainsi que les probabilités d'occurrence des incidents ainsi que leurs impacts potentiels.

La DGSSI accompagne ADM dans la mise au point de l'ensemble du programme de sécurité de l'information. Des réunions ont lieu entre le RSSI d'ADM et les spécialistes de la DGSSI où ces derniers peuvent émettre des recommandations au fur et à mesure du processus de préparation et, bientôt, de déploiement du plan d'action. Cet accompagnement est précieux car en tant qu'infrastructure d'importance vitale, ADM sera appelée à être auditée par la DGSSI. D'une manière générale, ADM prévoit être pleinement compatible avec la DNSSI vers la fin de 2018.

10 Mentionnons, entre autres, l'adoption de normes comme ISO 27002 version 2013, ITIL, COBIT, OSSTMM, OWASP, SANS, NIST, CIS, etc.

Annexe 01

Ecole nationale supérieure d'informatique et d'analyse des systèmes (ENSIAS)

Avenue Mohammed Ben Abdallah Regragui,
Madinat Al Irfane, BP 713,
Agdal Rabat,
Tél. (212) 06 63 01 86 67
www.ensias.um5.ac.ma

Entrevue	**Mme Hanan El Bakkali** *Professeur de l'enseignement supérieur* *Coordonnatrice de la filière Sécurité des Systèmes d'Information (SSI)*	
Données de base	Maison mère Fondation Nombre d'enseignants Nombre d'employés Activité	Université Mohammed V de Rabat 1992 67 46 Formation d'ingénieurs d'Etat et recherche en vue du développement technologique et économique du Maroc.
Mission	Les missions principales de l'ENSIAS sont l'enseignement, la recherche et la formation continue au profit du secteur socio-économique.	
Objectif	L'ENSIAS est appelée à multiplier les efforts pour former des femmes et des hommes capables d'intégrer le monde socio-économique et de soutenir pour le développement des technologies de l'information et de communication dans la société marocaine. Elle doit être à l'avant-garde dans ce domaine et jouer un rôle d'expertise, de veille technologique, de réflexion, de support et de conseil pour l'Université Mohammed V, pour le secteur public, et pour les opérateurs économiques du Maroc en général et de la région en particulier.	
Moyens	Le cursus de l'ENSIAS allie compétences scientifiques, techniques et ouverture sur l'entreprise. Une grande importance est accordée à la pratique et à la gestion de projets.	
Enjeux	Commercialisation des produits de la recherche.	

Ingénieure de formation, Mme Hanan El Bakkali est titulaire d'un doctorat de l'École Mohammadia d'Ingénieurs (2002). Sa thèse de doctorat porte sur les infrastructures à clé publique (PKI) et les modèles de confiance : comment utiliser une logique formelle pour analyser le niveau de confiance résultant de l'utilisation de certificats d'identité. Depuis lors, elle enseigne à l'ENSIAS.

Son premier centre d'intérêt portait sur la sécurité des transactions de commerce électronique et le rôle joué par les PKI. Elle a pu analyser à ce niveau le modèle de confiance utilisé par le protocole Secure Electronic Transaction (SET) qui est spécialement destiné à sécuriser les transactions Internet de paiement par carte bancaire. Bien que très sécuritaire, ce protocole n'a pas remporté le succès escompté sur le marché et a été remplacé par le Secure Sockets Layer (SSL), qui est un protocole de sécurisation des échanges sur Internet. Certes moins sécurisé que SET, mais qui a le mérite d'être moins coûteux en termes d'implémentation et plus facile d'utilisation.

« Trop de sécurité, tue la sécurité », conclut Mme El Bakkali en évoquant le débat SET-SSL et par la suite Transport Layer Security (TLS). C'est le protocole le moins sécuritaire qui l'a emporté pour des raisons d'acceptabilité – depuis lors, la technologie SSL-TLS est largement utilisée pour sécuriser les transactions de paiement électronique et a quelque peu gagné en fiabilité avec l'avènement du protocole 3D-Secure qui renforce la sécurité offerte par SSL/TLS

Annexe 01 Ecole nationale supérieure d'informatique et d'analyse des systèmes (ENSIAS)

Evolution de la formation en cybersécurité

L'ENSIAS a été la première institution universitaire au Maroc à offrir une option de cybersécurité en 2009 à ses élèves-ingénieurs. Cette option sera d'ailleurs transformée en filière Sécurité des Systèmes d'Information (SSI) en 2014. C'est en 2009 également que le gouvernement lançait le « Plan numérique 2013 » qui a depuis lors été reconduit sous diverses appellations. Mais le principe demeure que le gouvernement accompagne les entreprises dans leur effort de numérisation tout en œuvrant pour instaurer un climat de confiance numérique. Ce mouvement a gonflé la demande pour la formation de spécialistes en cybersécurité.

Pendant les premières années de l'existence de l'option Sécurité des Systèmes d'Information, il y avait une relative pénurie d'offre. La moitié des diplômés de la première promotion a dû accepter des emplois étrangers à la cybersécurité. Ils étaient embauchés comme informaticiens. Aujourd'hui, la situation est inversée : les entreprises recrutent les étudiants avant même qu'ils aient terminé leur formation (stage de fin d'études en pré-embauche). On note également une augmentation d'offre de stages de la part d'entreprises européennes. Il y a une pénurie mondiale en matière de spécialistes en cybersécurité.

Chaque génération de diplômés compte entre 20 et 30 étudiants et la plupart d'entre eux sont très motivés pour les métiers de la sécurité. En effet, il y a plusieurs facettes à la sécurité : gestion, analyse de risque, conformité aux normes et aux lois, sécurisation des réseaux, des applications, etc. A titre d'exemple, les spécialistes de tests de pénétration (pentests) doivent être prêts à passer de longues heures à analyser des codes et à chercher des vulnérabilités. Les plus enthousiastes participent à des concours de cybersécurité. D'une façon générale, ces dernières années la grande majorité des diplômés trouvent un emploi dans le domaine de la cybersécurité ou continuent leurs études dans le domaine.

Aujourd'hui, de nombreuses institutions universitaires au Maroc offrent des formations en cybersécurité, surtout au niveau Master. La faculté des sciences de l'Université Mohammed V offre un Master en cybersécurité axé sur la cryptographie, de même que l'Ecole nationale des sciences appliquées de Kénitra, l'Ecole nationale des sciences appliquées de Tanger, l'Ecole nationale des sciences appliquées de Marrakech, l'Ecole Mohammadia d'Ingénieurs, etc. D'une façon générale, il y a un intérêt croissant pour la cybersécurité dans le réseau universitaire marocain.

Bref aperçu sur la filière SSI de l'ENSIAS

La filière SSI vise à former des ingénieurs informaticiens spécialistes en sécurité des systèmes d'information. Conscients de son importance pour l'instauration de la confiance numérique qui constitue, sans aucun doute, la pierre angulaire pour le développement de l'économie numérique à l'échelle nationale.
Elle offre ainsi à l'élève-ingénieur une formation solide lui permettant d' :

- Avoir une base solide en informatique et en particulier en ce qui concerne les réseaux de communication, les systèmes d'exploitation et les technologies Web;
- Prendre conscience des différents enjeux liés à la gouvernance de la sécurité des systèmes d'information aussi bien au niveau organisationnel et managérial qu'au niveau juridique ;
- Avoir des connaissances approfondies en matière de cryptographie, pré-requis nécessaires pour la maîtrise des technologies et solutions utilisées pour la sécurisation des systèmes d'information et des e-sevices ;
- Acquérir une maîtrise des principaux concepts, technologies, outils et méthodes en matière de sécurité des systèmes d'information (sécurité physique, système, réseau et applicative);
- Prendre conscience des risques de sécurité inhérents à l'adoption de la virtualisation et du cloud computing;
- Acquérir -via les différents modules de la formation- des connaissances qui couvrent une grande partie du "Common Body of Knowledge" (CBK) de la certification CISSP (Certified Information Systems Security Professional);
- Avoir la possibilité d'obtenir la certification CEH (Certified Ethical Hacking), l'une des certifications les plus prisées dans le domaine de la sécurité.

En effet, pour un organisme, la sécurisation de son système d'information ne passe pas seulement par le biais de la mise en place de solutions technologiques, mais d'abord par l'existence de ressources humaines qualifiées maîtrisant aussi bien les technologies de sécurité que les aspects organisationnels, les normes, les méthodes et les référentiels de bonnes pratiques en matière de gouvernance de la sécurité des systèmes d'information.

La filière SSI vise aussi à ce que les élèves soient capables de prendre en compte les enjeux de Sécurité qui dépassent largement -et de plus en plus- les frontières d'une entreprise en raison du développement phénoménal de l'e-business et de la prolifération des e/m-services basés sur l'utilisation du Cloud et les technologies mobiles.

L'intelligence artificielle occupe une place croissante dans le domaine de la cybersécurité. Malheureusement, elle est aussi utilisée par les hackers. La filière SSI travaille sur les plateformes Security Information and Event Management (SIEM) qui font un recours massif à l'utilisation de l'intelligence artificielle pour détecter les incidents à un stage précoce.

Après un tronc commun d'une année avec les autres filières de l'ENSIAS, dédié à l'acquisition de connaissances de base et de compétences solides indispensables à tout informaticien, l'élève-ingénieur inscrit à la filière SSI va acquérir dans le troisième semestre des connaissances et des compétences complémentaires en technologies de l'information lui permettant de mieux comprendre les besoins et les évolutions des systèmes d'information ainsi que l'importance et la transversalité des aspects liés à la sécurité des systèmes. Les deux derniers semestres vont lui permettre d'acquérir les connaissances et les compétences lui permettant de devenir un ingénieur informaticien spécialiste en sécurité des systèmes d'information. Cette spécialité va lui permettre d'occuper et/ou d'évoluer vers les métiers suivants :

- ✓ Ingénieur en Sécurité des SI
- ✓ Membre de la Direction Audit et contrôle des SI
- ✓ Administrateur Systèmes
- ✓ Administrateur Réseaux
- ✓ Responsable sécurité des réseaux informatiques
- ✓ Responsable de la sécurité applicative
- ✓ Manager des Risques TI
- ✓ Consultant (junior puis senior) en Sécurité de l'Information
- ✓ Responsable de la Sécurité des Systèmes d'Information (RSSI)
- ✓ Auditeur en Sécurité de l'Information
- ✓ Expert en Sécurité des Systèmes d'Information
- ✓ Chargé de monitoring des incidents TI
- ✓ Directeur des Systèmes d'Information
- ✓ Directeur de l'Audit et contrôle des SI

Partenariats public-privé au profit de la filière SSI

En février 2014, un partenariat a été créé avec l'International Council of e-commerce Consultants (EC-Council) dans le cadre du programme EC-Council Academia, destiné exclusivement aux établissements universitaires pour offrir une certification qui vient compléter leurs acquis dans le cadre de leur formation d'ingénieur informaticien spécialisé en SSI, et faciliter leur insertion dans le monde professionnel. Il s'agit du certificat CEH (Certified Ethical Hacker) qui permet aux spécialistes en cybersécurité d'étudier et de comprendre les méthodes et les outils utilisés par les pirates informatiques. Les compétences ainsi acquises permettent de renforcer avec efficacité la sécurité de l'organisation. Mme El Bakkali a été certifiée CEH en 2015 et est l'interlocuteur côté ENSIAS avec EC-Council.

Depuis le lancement de son académie de formation en février 2014, IBM Maroc a noué plusieurs partenariats avec des établissements universitaires dont l'ENSIAS. Ces partenariats visent la mise en place de l'IBM Academic Program, un projet qui a pour objectif de créer et développer des cursus de formation autour des technologies TI au sein des universités partenaires, principalement dans les domaines du cloud, business analytics, cybersécurité et le social business.

Annexe 01 Ecole nationale supérieure d'informatique et d'analyse des systèmes (ENSIAS)

IBM a lancé également un programme de certification TI, le MEA University Program for Africa. Dans le cadre de ce programme, des professeurs de l'ENSIAS ont été formés et certifiés pour pouvoir offrir aux élèves de plusieurs filières des certifications sur le Big Data. Pour la filière SSI, Mme El Bakkali a été certifiée récemment comme Security Intelligence Specialist Academic-IBM QRadar SIEM v7.2, et elle peut désormais offrir cette formation/certification aux élèves de la filière. QRadar est une solution de type SIEM qui permet de détecter les anomalies, de découvrir les menaces perfectionnées et de supprimer les faux positifs. Pour cela, elle regroupe les données d'événements de journal et de trafic réseau enregistrées dans des milliers d'appareils, points d'extrémité et applications, répartis à travers un réseau. QRadar utilise ensuite un moteur Sense Analytics perfectionné pour normaliser et corréler ces données, puis identifie les atteintes à la sécurité qui doivent être analysées.

Dernièrement, un partenariat a été conclu avec Logpoint qui est l'un des concurrents européens d'IBM QRadar. De cette façon, les étudiants peuvent se certifier également sur cette technologie et se familiariser ainsi avec différentes solutions SIEM. C'est d'autant plus intéressant que de simples outils de collecte des logs, les SIEM se transforment peu à peu en véritables plateformes de traque des cyberattaques. Le « big data » et l'intelligence artificielle sont en passe de révolutionner ces applications.

Partenariats inter-universitaires

Depuis sa création, l'ENSIAS a conclu de nombreux accords de partenariat avec des universités étrangères. C'est ainsi, par exemple, qu'il existe une entente de double diplomation entre l'ENSIAS et l'École nationale supérieure d'informatique et de mathématiques appliquées (ENSIMAG). Chaque année, environ quatre ou cinq étudiants de l'ENSIAS -toutes filières confondues- vont suivre des cours à Grenoble (un an et demi) et obtiennent un double diplôme ENSIAS-ENSIMAG. Il existe aussi des partenariats avec d'autres établissements français comme l'Institut Supérieur d'Informatique, de Modélisation et de leurs Applications (ISIMA) à Clermont-Ferrand et avec l'École nationale supérieure d'électrotechnique, d'électronique, d'informatique, d'hydraulique et des télécommunications (ENSEEIHT) à Toulouse.

L'ENSIAS a conclu récemment une entente de mobilité avec l'Université de Sherbrooke au Canada. L'étudiant peut poursuivre sa dernière année d'étude à Sherbrooke. Il obtient son diplôme marocain et, ensuite, il a la possibilité de s'inscrire au doctorat à Sherbrooke. Deux étudiants de la filière SSI vont bénéficier cette année de ce partenariat. L'ENSIAS a également des accords de partenariat avec des universités américaines comme celui avec l'Université de Houston qui permet aux étudiants de deuxième année d'effectuer un stage d'été orienté recherche. Les plus qualifiés obtiennent la possibilité d'accomplir leur projet de fin d'études de la troisième année à l'Université de Houston et, le cas échéant, d'y poursuivre leur doctorat.

Evolution de la recherche à l'ENSIAS

Depuis un an, la recherche au niveau de l'Université Mohammed V de Rabat a été entièrement restructurée. Le Rabat Information Technology Center a été créé autour de l'ENSIAS, l'EMI et de la Faculté des Sciences de Rabat pour mettre en commun les ressources en recherche sur les technologies de l'information. Sa vision stratégique est de se positionner en tant que plateforme d'excellence en matière de Recherche, Développement et Innovation (R&D-I) en TIC.

Le Rabat IT Center regroupe plus de 100 professeurs spécialistes en diverses disciplines relevant des technologies d'information et de communication mais aussi en d'autres champs disciplinaires; mathématiques, gestion, économie et sciences humaines et sociales, pour un total d'environ 580 chercheurs. Ses membres sont répartis en trois laboratoires et huit équipes dont deux laboratoires et six équipes sont domiciliés à l'ENSIAS. La sécurité de l'information fait partie des axes de recherches Rabat IT-Center.

Principaux axes de recherche de Mme El Bakkali

Mme Hanan El Bakkali précédemment membre de l'équipe ISeRT (Information Security Research Team) de l'ENSIAS, est actuellement membre du Smart Systems Laboratory (SSL) et membre du conseil de gouvernance du Rabat IT Center. Ses axes de recherche relèvent de différentes problématiques de la Sécurité des systèmes d'Information comme :

- Contrôle d'accès dans des systèmes collaboratifs (notamment

les workflows). Cette recherche englobe les aspects inter-organisationnels qui se posent dans les secteurs de la santé, du commerce ou du tourisme. La multiplicité des intervenants implique que plusieurs politiques de contrôle d'accès sont confrontées. Il faut donc prévoir des méthodes de résolution de conflit en vue d'assurer la résilience de ces systèmes.

- Protection de la vie privée (privacy). Depuis l'adoption en février 2009 de la loi 09-08. La problématique de respect de la vie privée a été officiellement mise à l'ordre du jour à l'échelle nationale. L'entrée en vigueur du Règlement Général sur la Protection des Données (GDPR) par l'Union européenne en mai 2018 a encore accéléré cette problématique. La recherche entreprise porte sur le domaine de la télésanté (e-Health) où les questions de vie privée se posent avec une acuité particulière (données des patients) ainsi que dans le contexte Big Data.

- Systèmes de réputation et de confiance. Utilisation de l'intelligence artificielle et de l'analyse de sentiments pour rendre les plateformes de recommandations plus fiables : est-ce que les appréciations sur un produit ou un service ont été émis par des robots ou des agents payés à cette fin? L'algorithme étudie la concordance entre l'appréciation et sa sémantique avec les caractéristiques du produit. A titre d'exemple, est-ce que l'appréciation correspond avec des caractéristiques qui existent ou non dans le produit?

- Modèles de confiance des PKI tenant compte de la réputation et du niveau de sécurité des autorités de certification. La confiance numérique apportée par l'utilisation des certificats de clés publiques est certes basée sur la confiance dans les technologies cryptographiques, mais la confiance dans les autorités de certification (dites tierces parties de confiance) demeure l'élément déterminant de cette confiance. Comment évaluer cette confiance est la question que se posent plusieurs acteurs.

Parmi les tendances émergentes il convient de citer la technologie de la blockchain. C'est un moyen de renforcer la confiance dans les transactions électroniques. Mme El Bakkali entame une étude sur comment remplacer des systèmes centralisés de PKI par la technologie de la blockchain et des « smart contracts » ou par des systèmes hybrides.

Recherche, Développement et Innovation

Le grand défi consiste à faire passer les recherches entreprises à l'ENSIAS et au Rabat IT Center, du stade théorique au stade produit ou tout au moins prototype. C'est dans cette optique qu'une convention cadre a été conclue en décembre 2017 entre l'Université Mohammed V, le Rabat IT Center et l'entreprise privée DATAPROTECT dans le domaine de la CyberSécurité. Cette convention cadre définit la répartition de la propriété intellectuelle entre l'université, les doctorants et les investisseurs. Des conventions spécifiques seront ensuite négociées avec les doctorants et les entreprises concernées qui couvriront la mise au point du produit et, le cas échéant, le dépôt d'un brevet.

Des partenariats similaires sont en cours de discussion avec d'autres entreprises dans divers champs disciplinaires.

Annexe 01

Institut national des postes et télécommunications (INPT)

2 avenue Allal El Fassi,
Madinat Al Irfane,
Rabat, Maroc
Tél. (212) 06 61 89 02 77
www.inpt.ac.ma

Entrevue	**M. Abdellatif Mezrioui** *Professeur de l'enseignement supérieur*	
Données de base	Maison mère Fondation Nombre d'enseignants Nombre d'étudiants	ANRT 1961 90 (dont 50 permanents) 700
Mission	L'INPT a pour mission la formation, la recherche et l'expertise. Il est chargé de la formation initiale et de la formation continue dans les domaines des télécommunications, des technologies de l'information et de la communication et disciplines connexes. Cette mission concerne également la recherche scientifique et technique ainsi que toute autre formation rendue nécessaire au regard de l'environnement général ou de circonstances conjoncturelles.	
Objectif	La formation d'ingénieurs est le métier de base de l'INPT.	
Moyens	L'enseignement est réparti en filières. A compter de 2018, une filière sécurité a été créée.	

Professeur à l'INPT depuis 1995. Doctorat en génie logiciel à l'université de Nancy-1. A son retour au Maroc, il travaille un an dans un cabinet conseil en informatique qui réorientait ses activités vers la sécurité. A ce titre, il organise plusieurs séminaires de sensibilisation à la sécurité dans le secteur industriel en suivant la méthode d'analyse de risques informatiques orientée par niveau (Marion) mise au point par le Club de la sécurité de l'information français. La méthode Marion est une méthode d'audit visant à évaluer le niveau de sécurité informatique d'une entreprise.

En 1995, monsieur Mezrioui joint les rangs de l'INPT où il assure un certain nombre de cours en génie logiciel, conception de procédés logiciels, cours de base Unix, architecture réseau TCP-IP, etc. A compter de 2013, il a commencé à donner des cours sur la sécurité : exigences relatives aux systèmes de gestion de la sécurité des informations telles que définies par la famille de normes ISO 27 000, analyse de risques dans le cadre de la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), etc.

Au total, cinq enseignants se consacrent à la sécurité au sein du département MIR (Mathématique Informatique et Réseaux) de l'INPT. Traditionnellement, la formation en sécurité visait essentiellement les étudiants de deuxième et troisième année. L'ensemble des cours vient d'être révisé afin de proposer à compter de la prochaine année universitaire une nouvelle filière dite « confiance numérique » qui commence dès la première année par des cours de base et de sensibilisation à la sécurité. On escompte une cohorte de 30 à 40 étudiants dès l'entrée en vigueur de la filière.

Des stages sont effectués chaque année avec des entreprises privées, des banques et des organismes publics. L'INPT a noué des partenariats avec une quinzaine d'institutions universitaires de génie en France et même au Canada (Université de Sherbrooke). Les étudiants en sécurité ont tendance à se diriger vers l'Institut national des sciences appliquées Centre Val de Loire (INSA CVL), Télécom ParisTech, Télécom Sud Paris et l'École nationale d'ingénieurs de Brest (ENIB) qui sont spécialisés dans ce domaine.

Les étudiants de l'INPT peuvent poursuivre leur formation en génie jusqu'au niveau doctoral. Un groupe de recherche nommé RAISS (Réseau, Architecture, Ingénierie de Services, Sécurité) encadre une vingtaine de doctorants – dont cinq se consacrent à différents aspects de la sécurité. Parmi les principaux axes de recherche en sécurité il y a :

- L'Internet des objets.
- La détection des intrusions sophistiquées.
- La gouvernance dans l'infonuage.

Internet des objets.

La recherche entreprise à l'INPT porte sur la vulnérabilité des systèmes complexes composés d'objets connectés. Les protocoles utilisés, la disponibilité des équipements, l'accès aux données : tout est analysé depuis les capteurs jusqu'à l'utilisateur final. La recherche identifie les maillons faibles de la chaîne, quels sont les outils déjà disponibles, comment les renforcer, afin de faciliter les échanges entre les capteurs, les activateurs et les concentrateurs. Le but ultime étant bien entendu que les utilisateurs puissent obtenir des flux de données crédibles, intègres et correctes. Les expériences ont porté sur les réseaux électriques, mais les applications peuvent être étendus à plusieurs autres domaines : de la domotique jusqu'aux raffineries de pétrole. Même si les flux de données sont peu volumineux, leur intégrité doit impérativement être protégée. Or, malheureusement, les systèmes industriels contrôlés par la technologie SCADA ou autre, ne sont pas conçus comme les réseaux informatiques avec la sécurité intégrée dans leur architecture. Des protocoles vulnérables sont encore employés et le contenu n'est pas crypté. Bien des équipements sont encore livrés avec un mot de passe par défaut qui est indiqué sur le manuel en ligne. Les connexions avec des prestataires extérieurs ne sont pas toujours sécurisées.

Détection des intrusions

L'axe de recherche sur les intrusions porte sur la mise en place d'une architecture de détection-réaction en s'inspirant des réseaux à auto-défense. Le travail est, en effet, basé sur la vision des réseaux autonomes, des réseaux qui sont capables de s'autogouverner et de s'adapter sans aucune intervention humaine.
Le système cité fonctionne selon un cycle continu de détection, décision et réaction et en exploitant plusieurs connaissances sur le système d'information (biens sensibles, topologie du réseau, équipements actifs et leurs emplacements, utilisateurs et leurs rôles, etc). Le système est mis en œuvre au moyen d'outils comme Snort qui est un système de détection d'intrusion (ou NIDS) libre publié sous licence GNU GPL. Il s'agit aussi de mettre au point des scripts qui définissent un comportement normal sur une machine sensible. Dès qu'un écart est décelé, le système ainsi programmé va essayer d'inhiber cette action soit en désactivant le port du commutateur concerné, ou en fermant une session, ou encore en reconfigurant les autorisations du routeur. Cet ensemble d'actions est appliqué en fonction de la nature de l'incident. Le travail de recherche de l'INPT vise à créer une boucle de rétroaction plus puissante, plus raffinée et plus adaptable. C'est un système dans lequel on a injecté un surcroît d'intelligence pour enrichir la prise de décision.

On récupère de l'information sous diverses formes à partir de plusieurs éléments actifs sur le réseau, on uniformise ces différents types d'information, on réduit leur taille et ensuite on les achemine à un centre de décision de l'architecture où les anomalies sont traitées de façon adéquate. La plateforme contient aussi la modélisation du réseau afin de savoir d'où vient l'attaque, quel segment physique est affecté et sur quels routeurs intermédiaires il est possible d'agir pour contenir l'incident. De cette façon, on peut considérer que le réseau privé de l'organisation est protégé par la plateforme de détection-réaction ainsi mise au point.

Annexe 01 Institut national des postes et télécommunications (INPT)

Gouvernance de l'infonuage

Les solutions d'infonuage ne sont pas mûres car il y a des problèmes de migration des données depuis le système d'information physique vers le nuage. Il y a également un problème de verrouillage des données chez le fournisseur (une fois qu'un utilisateur a conclu un contrat avec un fournisseur de nuage, il ne peut plus en changer). Ceci nous mène évidemment aux questions purement contractuelles (niveau de sécurité garanti par le fournisseur, partage de responsabilités, etc.). Le travail entrepris à l'INPT porte sur les questions de gouvernance du nuage en matière de sécurité afin de dresser la liste des référentiels existants pour déterminer ceux qui peuvent répondre aux exigences de sécurité des utilisateurs. Un certain nombre de référentiels sont disponibles (ITIL, COBIT, ISO 27 001, etc.), mais une fois que les données ont migré sur l'infonuage, on ne maîtrise plus rien, personne ne sait ce qui se passe, on ne sait même pas dans quel pays se trouvent les données…

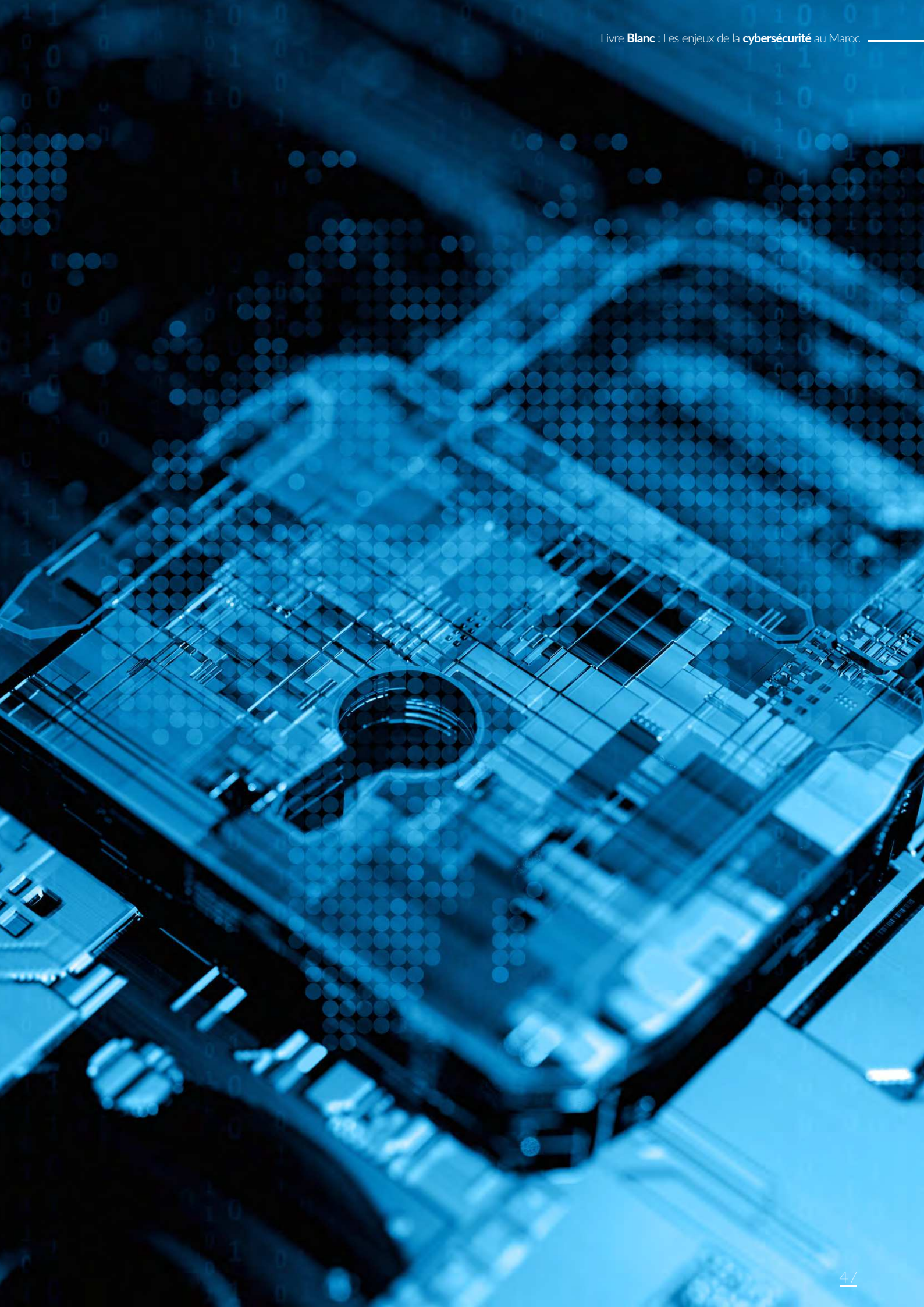
Voilà pourquoi, les chercheurs de l'INPT se sont penchés sur les référentiels pour examiner s'ils répondent toujours aux besoins d'une prise en main satisfaisante de l'infrastructure réseau et du système d'information de l'entreprise. Les chercheurs étudient aussi les nouveaux besoins qui sont apparus dans l'écosystème de l'entreprise à la suite de l'introduction de l'infonuage. Enfin, ils cherchent à unifier plusieurs référentiels existants pour répondre aux besoins en gouvernance de l'infonuage. De cette façon, quand un problème se présente, il n'est plus besoin de consulter toute une gamme de référentiels aux formulations disparates. A un problème donné, correspond donc un référentiel consolidé uniforme qui répond à tous les besoins en gouvernance de l'infonuage. Avant de pouvoir commercialiser un tel outil, il reste toutefois à effectuer une expérience pilote dans une entreprise privée ou une administration publique. Malheureusement, ce genre de projet entreprise-université est encore relativement rare au Maroc.

Prospectives

L'évolution de la technologie menace de faire de nombreux dégâts industriels, spécialement dans un contexte de généralisation de l'Internet des objets, de la domotique, des véhicules autonomes, etc. Voici les enjeux que doit relever le génie marocain en matière de sécurité :

- ✓ Renforcer la formation de tous les ingénieurs – pas seulement des spécialistes en sécurité, mais tous les ingénieurs.
- ✓ Inculquer des notions en culture technique et organisationnelle (référentiels, bonnes pratiques, etc.).
- ✓ Développer les bons réflexes en sécurité quand vient le moment de réaliser un grand projet (security by design).
- ✓ Cesser de réaliser un projet et de se poser ensuite la question de la sécurité pour inverser la démarche et procéder à la conception sécurisée des objets et des systèmes, même les plus simples.
- ✓ Favoriser une bonne connaissance des lois et des normes à respecter par les ingénieurs.
- ✓ Sensibiliser non seulement les ingénieurs, mais aussi les gestionnaires généralistes, à la valeur des données personnelles, ce que l'on peut en faire et ce que l'on doit protéger.

L'introduction de la DNSSI a grandement amélioré la situation au Maroc. Mais il faut maintenant favoriser une prise de conscience généralisée – ce qui n'est pas encore le cas. Informer les gestionnaires sur les enjeux de la sécurité ne suffit pas, il faut ensuite leur rappeler que c'est un processus permanent. Il faut maintenir les processus d'alerte à un niveau très élevé en tout temps. Le processus de formation et de sensibilisation à la sécurité n'a pas de fin. L'INPT applique à ses propres installations toutes les mesures de sécurité et de protection de la vie privée qui sont prescrits par la loi et la réglementation en vigueur au Maroc. Les enseignants de l'INPT baignent dans une culture sécuritaire d'avant-garde.



Annexe 01

Groupe d'assurances Lyazidi

Groupe d'assurances Lyazidi
16 avenue Moulay Youssef
Rabat, Maroc
Tél. (212) 06 61 08 16 08
www.lyazidi.co.ma

Entrevue	**Rachid Baarbi** *Chief Information and Innovation Officer (CIIO)*	
Données de base	Siège de l'organisation Création Nombre d'employés Activité Clients	Rabat 1954 95 Courtage d'assurance Entreprises et administration publique
Mission	Assister et accompagner les clients dans la gestion et le pilotage de leurs contrats d'assurances.	
Stratégie	Nouer des partenariats avec les grandes compagnies d'assurances.	
Moyens	Créer son propre système d'information indépendant.	
Enjeux	Assurer la sécurité du système d'information.	

Contexte

Dans le domaine de l'assurance, la plupart des courtiers travaillent avec le système d'information des grandes compagnies d'assurance (RMA Watanya, Axa Assurance Maroc, Wafa Assurance, Saham Assurance, Atlanta/Sanad, etc.). Ils sont connectés directement aux sites de ces compagnies qui gèrent la sécurité pour eux.

Dès 1982, le groupe d'assurances Lyazidi a créé son propre département d'informatique avec pour mission d'assurer la disponibilité des serveurs et fournir un service de « help desk » aux utilisateurs. Dans ce cadre, Lyazidi a développé en interne sa propre application de gestion de courtiers et intermédiaires d'assurance. Toute une série d'applications spécialisées ont ensuite été greffées sur cette base : comptabilité, ressources humaines, transactions commerciales, etc. Le département informatique s'est peu à peu transformé en système d'information doté de programmes de « business intelligence » et d'aide à la décision. Tous les processus qui s'y prêtaient, ont été automatisés. Aujourd'hui, Lyazidi est entré dans la phase de transformation numérique. Le centre de coût est ainsi devenu un centre de profit.

Le groupe d'assurances Lyazidi comprend cinq sociétés qui sont desservies depuis le même centre de systèmes d'information.

Groupe de sécurité

La sécurité du Groupe d'assurances Lyazidi est assumée par deux employés à temps partiel qui appartiennent à la cellule des Systèmes d'information (SI) – exploitation. Cela comprend la maintenance (help-desk) et la sécurité. Le cœur de la sécurité est constitué par des coupe-feux (firewalls).

Stratégie de sécurité

L'entreprise effectue en interne des audits de cybersécurité deux fois par an. Comme elle est certifiée ISO 9001 - version 2015 et en cours de certification ISO 27 001, elle doit répondre aux exigences de qualité les plus strictes. Dans cette optique, elle a fait appel à un cabinet de conseil externe pour procéder à l'audit. Ce processus a permis d'identifier des vulnérabilités mineures, ce qui a incité à mettre en place des solutions beaucoup plus avancées. A la faveur de ces audits réguliers, l'entreprise procède à la vérification des mots de passe : changements fréquents, robustesse, hiérarchisation (les mots de passe des développeurs n'est pas le même que celui des utilisateurs), etc.

Chaque poste de travail est régulièrement scanné de façon à vérifier que les antivirus ont bien été mis à jour. Un relevé des attaques est effectué et fait l'objet d'un suivi. Les collaborateurs nomades doivent accéder au système d'information de l'entreprise au moyen d'un réseau virtuel privé (VPN). Quand un nouveau virus est annoncé sur Internet, les responsables de la sécurité chez Lyazidi procèdent immédiatement aux mises à jour recommandées. Un service critique a déjà fait l'objet d'un « back-up » avec plan de continuité d'activité (PCA) complet. Il est prévu que l'ensemble du système d'information sera dédoublé géographiquement d'ici deux ans.

Enjeu actuel de Lyazidi

Lyazidi est engagé dans une logique de transformation numérique et d'ouverture vers l'extérieur, ce qui entraîne une mobilité accrue des agents. Ceux-ci doivent pouvoir se connecter par VPN aux systèmes de l'entreprise depuis les bureaux de leurs clients. Il a fallu développer des applications mobiles en tenant compte de toute une série de menaces nouvelles.

Perspective marocaine

Le Maroc poursuit une politique de numérisation qui s'incarne dans le projet Maroc 2020 et la création de l'Agence du développement digital (ADD) en décembre 2017 au sein du ministère de l'Industrie, du Commerce, de l'investissement et de l'Économie numérique. En multipliant les liens entre le gouvernement, les entreprises et les citoyens, ce processus de numérisation a mis de l'avant un nouvel impératif de sécurité. Même si toutes les entreprises ne sont pas soumises à la DNSSI, un grand nombre fait affaire avec l'administration publique et les infrastructures publiques et doivent donc respecter les directives prévues. On crée ainsi une culture de la sécurité dans le tissu économique marocain.

Annexe 01

Groupe Managem

Twin Center, Tour A, BP 5199,
Angle Boulevards Zerktouni et Al Massira Al Khadra, Casablanca, Maroc
Tél. (212) 06 08 86 11 53
www.managemgroup.com

Entrevue	**Mounir El Dhimni** *Responsable réseaux et télécommunications*	
Données de base	Fondation Chiffre d'affaires Nombre d'employés	1930 5,2 G MAD 5 660
Stratégie	Groupe industriel à vocation minière, Managem développe depuis 90 ans ses activités au Maroc et à l'international. La stratégie de développement du groupe s'appuie sur trois axes prioritaires : • *Renforcer les réserves et développer les projets existants.* • *Assurer une croissance organique grâce à l'extension des capacités des mines en exploitation.* • *Accélérer la croissance par de nouvelles acquisitions et partenariats, notamment en Afrique.*	
Objectif	Assurer les ressources et réserves pour au moins 10 ans de production de l'ensemble des métaux : argent, or, cuivre, cobalt et zinc.	

Le responsable des infrastructures du Groupe Managem est assisté de l'équivalent d'une personne à temps plein pour les questions de sécurité – l'entreprise avait un responsable sécurité à temps plein, mais il a quitté en 2017. Face à ce manque de ressources humaines en cybersécurité, le Groupe Managem envisage de recruter un spécialiste de niveau intermédiaire (trois ou quatre ans d'expérience). Le rôle de responsable de la sécurité des systèmes d'information (RSSI) continuera à être rempli par le responsable des réseaux et télécoms.

Stratégie de sécurité : audit et plan d'action

A la fin de 2017, le Groupe Managem a procédé à un audit de sécurité aussi bien sur le segment technologies de l'information (TI) de ses activités que sur le segment du système d'acquisition et de contrôle de données (SCADA). L'entreprise a vérifié la conformité de ses infrastructures par rapport aux principales normes en vigueur : ISO 27 001 pour les TI et ISC pour SCADA. L'entreprise a aussi adopté la norme DNSSI, même si elle n'est pas considérée comme une infrastructure critique. Il s'agit d'une mesure préventive destinée à évaluer le niveau de maturité de la sécurité du Groupe Managem.

LES ENJEUX DE LA CYBERSECURITE AU MAROC

A la suite du processus, un plan d'action en trois ans a été élaboré pour remédier aux vulnérabilités, avec des actions échelonnées en fonction de l'urgence et du niveau de complexité. L'ensemble du parc informatique du Groupe Managem compte environ 1 000 postes de travail ainsi que des serveurs (la classification des actifs informationnels est encore en cours). Tous les systèmes critiques sont dupliqués et, en cas de défaillance majeure, un plan de relève permettrait la poursuite sans interruption des activités. C'est d'autant plus important que plusieurs incidents de pirates informatiques ont déjà été enregistrés et déjoués par l'entreprise (attaque virale, demande de rançon, arnaque au président, fraude financière). Les sauvegardes sont fréquentes et reposent sur des systèmes situés dans des sites distants.

L'audit et le plan d'action ont été développés avec l'aide d'un cabinet-conseil en sécurité informatique. Ce support extérieur permet aussi d'effectuer un « benchmark » avec les autres entreprises de tailles et d'activités comparables à l'échelle internationale. C'est aussi une façon d'effectuer une veille constante en matière de gouvernance de la sécurité.

Formation et sensibilisation

La stratégie du Groupe Managem comprend des activités de formation et de sensibilisation. La formation consiste en des présentations effectuées à des groupes répartis par corps de métier. Les campagnes de sensibilisation touchent tout le personnel et se font par courriels et par notes sur les panneaux d'affichage. L'intensité de la formation-sensibilisation laisse cependant à désirer faute de moyens suffisants pour évaluer la compréhension et l'assimilation des thèmes abordés (rétroaction). Le plan d'action vise à remédier à cette carence. C'est d'autant plus important que le risque informatique concerne d'avantage les ressources humaines que la technologie.

Annexe 01

Ministère de la Réforme de l'Administration publique

B.P : 1076, Rue Ahmed Cherkaoui,
quartier administratif, Agdal, Rabat
Tél. (212) 0537 67 99 97
GSM (212) 0661 89 84 23
www.mmsp.gov.ma/fr/index.aspx

Entrevue	**Mohamed Moussa** *Chef de la division des systèmes d'information interne* *Direction des systèmes d'information*	
Données de base	Siège de l'organisation Nombre d'employés Activité Clients	Rabat 240 Fonction Publique et Modernisation de l'administration. Ensemble des employés du Ministère.
Mission	✓ Concevoir, développer et mettre en œuvre les systèmes d'information internes du Ministère tant au plan de la gestion administrative qu'au plan du cœur de métier. ✓ Assurer la maîtrise d'ouvrage des sites web du Ministère. ✓ Assurer le suivi et la mise à niveau du parc informatique et des réseaux informatiques et téléphoniques. ✓ Assurer l'assistance et la formation en matière de TIC.	
Stratégie	Conformité à la DNSSI.	
Moyens	Audit de cybersécurité.	
Enjeux	Satisfaire aux exigences les plus strictes de la cybersécurité avec des ressources humaines limitées.	

La Division des systèmes d'information interne (DSII) du Ministère de la Réforme de l'Administration et de la Fonction publique, compte 12 employés. Au sein de cette équipe, il y a un Responsable de la sécurité des systèmes d'information (RSSI) et deux employés affectés à la cybersécurité à temps partiel. Faute de ressources humaines en nombre suffisant, les spécialistes de sécurité doivent aussi prendre en charge d'autres projets. Le nombre de postes budgétaires alloués à la DSSI demeure insatisfaisant.

Audit de cybersécurité

En 2016, la DSII a procédé à un audit de sécurité (organisationnel, environnemental et technique) des systèmes d'information du ministère afin de s'aligner avec la Directive nationale de la sécurité des systèmes d'information (DNSSI). En tout le ministère compte 240 ordinateurs, plusieurs dizaines de serveurs, des sites web, un intranet et une plate-forme de virtualisation ainsi que des systèmes de gestion et de métier.

Un bureau d'étude en cybersécurité a été choisi au terme d'un appel d'offre ouvert afin de seconder la DSII. Le processus a duré six mois et a permis d'identifier les forces et faiblesses du ministère en matière de cybersécurité. La Direction générale de la sécurité des systèmes d'information (DGSSI) qui relève de l'administration de la Défense nationale.

Déploiement de la stratégie de cybersécurité

A la lumière de cet audit, toute une série de décisions ont été prises :

- Création d'un comité de sécurité des systèmes d'information qui est présidé par le secrétaire général du Ministère et qui comprend les directeurs de chaque entité de celui-ci.
- Création d'un poste de RSSI et désignation de son titulaire.
- Mise en place d'une politique de sécurité des systèmes d'information.
- Mise en place des procédures.
- Organisation de séances de sensibilisation : tous les fonctionnaires du Ministère sont réunis une fois par an sous forme de conférences suivies de débats ouverts (information sur la politique de sécurité du Ministère et des dispositions à prendre en fonction de l'actualité).
- Mise en conformité à la loi 09-08 sur la protection des données à caractère personnel.
- Plan d'action de sécurité sur trois ans élaboré pour renforcer la sécurité des systèmes d'information du Ministère à travers la réalisation de plusieurs projets en relation avec la sécurité : acquisition des solutions de renforcements de la sécurité, correction des vulnérabilités, renouvellement des licences de sécurité, etc.

Prévention et formation

La prévention des attaques demeure à la base de toute stratégie de cybersécurité. La collaboration de la DSII et du Moroccan Computer Emergency Response Team (maCERT) est permanente : échanges d'information, mises à jour des logiciels, alertes de nouveaux virus, etc. Le maCERT relève de la DGSII et assure la coordination de l'information sécuritaire entre tous les ministères.

Plusieurs activités sont organisées dans le cadre de la DGSII : un séminaire annuel sur la cybersécurité à l'intention des spécialistes en SI de la fonction publique et des formations sur les grands enjeux de l'heure (nuage, mobilité, IPV6, etc.).

La DGSII, en partenariat avec l'Agence Nationale de Réglementation des Télécommunications (ANRT) organise un Master en cybersécurité dans le cadre de l'Institut National des Postes et Télécommunications (INPT). Un ingénieur de la DSII a récemment terminé son Master en cybersécurité et accomplit actuellement son stage de fin d'études. Le tout est entièrement gratuit pour l'employé-ingénieur.

Actions en cours

Un plan d'action étalé sur trois ans a été déployé à compter de 2017. Celui-ci comprend un audit annuel des systèmes et processus mis en place. Chaque fois, les vulnérabilités décelées sont corrigées et le réseau est renforcé.

En parallèle, la division des TI a lancé un projet de classification des actifs informationnels du Ministère. En effet, la classification et la catégorisation des actifs informationnels est une étape indispensable dans le processus de gestion des risques du système d'information. Elle permet de déterminer la criticité des actifs informationnels du Ministère, en fonction des objectifs de sécurité de l'information, soit la disponibilité, l'intégrité et la confidentialité. Cette information servira d'intrant à l'évaluation des risques et permettra d'assigner à chacun des actifs un niveau de protection approprié. Les pratiques et les mesures de sécurité à mettre en œuvre seront modulées en fonction de la classification.

Place de la cybersécurité au Ministère

D'une façon générale, la cybersécurité est devenue une composante intrinsèque de la gestion des TI au Ministère. Chaque fois qu'un nouveau projet est lancé, il incorpore un volet sécurité. Le Système d'Information est en train d'être construit sous forme d'un centre de données intégré avec duplication des infrastructures. Le manque de ressources humaines disponible oblige toutefois la division des SI à prioriser les projets de sécurité et à étaler leur réalisation dans le temps. Chaque nouveau projet est précédé d'un audit de sécurité spécifique.

Annexe 01 Phone Group

Phone Group
26, rue Mohammed Kamal,
Casablanca
Tél. (212) 06-61-61-57-04
www.phone-group.ma

Entrevue	**Amina Gounajjar** *Directeur Adjoint Support des Systèmes d'Information*	
Données de base	Siège de l'organisation Création Nombre d'employés Activité Clients	Casablanca 2000 6000 Centre de contacts Entreprises ayant une forte relation client (depuis les entreprises de télécommunications jusqu'aux fournisseurs d'énergie en passant par des banques, détaillants d'e-commerce et compagnies aériennes).
Mission	✓ Le respect comme ciment de l'engagement des collaborateurs. ✓ Un climat de confiance qui retentit positivement sur l'expérience client et collaborateur. ✓ Des liens durables et équitables avec les collaborateurs, les clients et l'environnement.	
Stratégie	Phone Group se positionne comme la première entreprise de référence dans les métiers de la Relation-Client en Afrique.	
Moyens	Grâce à un accompagnement sur toute la chaîne de valeur client, allant de la conquête et acquisition jusqu'à la fidélisation, Phone Group propose des prestations hautement qualitatives couvrant une large diversité de secteurs, que ce soit en B2C ou en B2B, via des approches omni-canal et multilingues complètement intégrées.	
Enjeux	Le défi principal de Phone Group est de migrer ses activités sur Internet.	

Contexte

Phone Group a été créée en 2000 par le Groupe Saham. C'est un acteur de référence dans les secteurs de la finance, de l'offshoring et de la santé. En 2004, le Groupe Bertelsmann a pris une participation majoritaire dans Phone. Bertelsmann est une des plus grandes entreprises de médias du monde et il est également actif dans le secteur tertiaire ainsi que celui de l'enseignement. Il est plus particulièrement propriétaire d'Arvato, une entreprise internationale de prestations de services : Customer-Relationship-Management (CRM), Supply-Chain-Management (SCM), finances et technologies de l'information.

Phone travaille étroitement avec Arvato France. Elle compte neuf sites au Maroc, deux au Sénégal et un en Côte d'Ivoire.

Techniques de la sécurité

Les données sensibles (cartes bancaires, information personnelle) sont chiffrées. Mais Phone limite au maximum le stockage de ces données. Dans la mesure du possible, l'entreprise accède aux données des CRM des clients donneurs d'ordre via des lignes spécialisées hautement sécurisées. Pour certains clients aux besoins particulièrement exigeants, Phone va jusqu'à prévoir de façon contractuelle le chiffrement des courriels.

Phone subit l'impact direct du RGPD de l'Union européenne car la plupart de ses clients sont en Europe. Aussi un « task force » a été mis sur pied pour protéger le peu de données personnelles que Phone traite en interne.

Le plus important projet de 2017 a été la révision complète du système de sauvegarde de Phone pour être conforme au RGPD. La politique de stocker le moins de données possible a été renforcée en réduisant le temps de conservation de l'historique des courriels. En cas de réclamation sur le droit à l'oubli, cela évite d'avoir à faire des recherches interminables dans des vieilles bases de données. Le droit à l'oubli est une disposition de la réglementation qui est considérée avec la plus grande attention chez Phone.

La surveillance quotidienne du système d'information est assurée par un SOC externe. Il s'agit de prévenir toute attaque sur le SI. Une entreprise comme Phone ne peut se permettre de perdre son SI ne serait-ce qu'une heure, car non seulement cela occasionnerait un manque à gagner sur le plan de la facturation, mais la perte de confiance qui en résulterait serait incalculable. « Nous n'avons pas le droit à l'erreur », précise Amina Gounajjar.

Structure organisationnelle

Le responsable de la sécurité des systèmes d'information dépendait jusqu'ici de la Direction des SI. Il relève désormais de la Direction qualité de Phone, afin de ne pas être juge et partie.

Toujours dans la Direction qualité, il y a un responsable de la sécurité physique qui a pour rôle de vérifier si les consignes de sécurité sont bien appliquées au niveau des installations. Il dispose d'un « facility manager » sur chaque site pour s'occuper de tout ce qui est vigile, etc.

Enfin, il y a un responsable de la sécurité opérationnelle qui s'occupe de ce qui est lié aux activités quotidiennes en termes de métier. Rattaché à la Direction des infrastructures et systèmes d'information, il a sous ses ordres, un chargé de sécurité opérationnelle (CSO) pour chaque deux sites. A titre d'exemple, les CSO veillent à ce que les employés appliquent la politique bureau propre ou n'introduisent pas de sacs personnels dans les bureaux. Sur le plan des SI, ils vérifient que les mots de passe soient changés régulièrement ou que les profils d'accès au réseau soient bridés en fonction des responsabilités de chacun ou encore que les « whitelists » soient bien validées avec le client, etc. Ils sont en première ligne en cas de fraude.

D'une part, les trois groupes collaborent étroitement entre eux, d'autre part, ils collaborent avec celui des SI ainsi qu'avec les gestionnaires de sites. Le résultat de cet effort conjoint est qu'aujourd'hui, il n'y a pas une seule personne chez Phone qui ne soit pas sensibilisée à la sécurité. Aucun incident majeur n'a été à déplorer en termes de sécurité informatique.

Ce bon résultat est aussi dû à l'intégration de Phone à l'intérieur du périmètre global de sécurité du groupe Bertelsmann. Les équipes de sécurité de Phone échangent en permanence des informations avec les membres du groupe Bertelsmann – une conférence téléphonique mensuelle a lieu avec les équipes de sécurité du groupe européen. Cela permet un partage systématique des bonnes pratiques. Dès qu'une menace apparaît sur les tableaux de bord de veille du groupe, les équipes de sécurité de Phone sont alertées.

Stratégie de sécurité

La cybersécurité est la raison d'être de Phone : « Sans cybersécurité, nous n'aurions plus de raison d'exister, les clients ne nous feraient plus confiance. » Phone gère des données très sensibles comme les numéros des cartes bancaires des utilisateurs. C'est pour suivre la politique incitative de Bertelsmann que Phone a entamé en 2014 le processus de certification ISO 27 001. En absence de toute obligation, Phone a opté pour l'adoption de la norme afin de se différencier de sa concurrence.

Les premiers audits internes effectués par les experts de Bertelsmann ont eu lieu en 2014 et, un an plus tard, le premier site était certifié ISO. Tous les ans, prend place un audit de surveillance. Phone en profite pour élargir le périmètre de la certification ISO et en 2018, l'ensemble des 12 sites du groupe est conforme.

Annexe 01 Phone Group

La norme PCI-DSS a été aussi adoptée par étapes. D'abord au site de Marrakech qui était dédié au e-commerce, elle a ensuite été élargie au site de Dakar quand l'activité de e-commerce a gagné cette ville. C'est alors qu'un des plus importants clients de Phone a formulé une exigence contractuelle : tous les sites affectés à ses services devraient être certifié PCI-DSS. Il s'agit d'un opérateur de télécommunications pour qui les données personnelles sont considérées comme aussi confidentielles que les données bancaires.

Enjeux

Le défi principal pour Phone est de s'ouvrir sur Internet. Il est indispensable d'être attractif pour les ressources humaines. En effet, le métier de centre de contact est basé sur les ressources humaines. Or, le taux de roulement est important. Il faut sans cesse embaucher de nouveaux employés, donc ouvrir les infrastructures sur l'externe, miser sur les réseaux sociaux et d'une façon générale sur les canaux de communications utilisés par les jeunes.

Il faut aussi faire preuve d'agilité pour satisfaire les besoins des donneurs d'ordre. Il faut pouvoir déployer rapidement les fonctionnalités nécessaires à tout nouveau client sans avoir besoin d'intervenir physiquement dans le site local. On parle alors de « anytime, anywhere, any device ». Pour cela, il faut être connecté à Internet avec tous les dangers que cela comporte. Il faut donc accroître la cybersécurité des infrastructures.

Enfin, les canaux de communications avec les utilisateurs finaux migrent depuis le téléphone vers le courrier électronique, la messagerie instantanée, Skype, etc. Les utilisateurs doivent pouvoir gérer en direct leurs données confidentielles sur un certain nombre de plateformes. Au début, Phone recourait aux lignes dédiées pour les communications par visioconférence. Mais avec la multiplication de ce type d'échanges, ce n'est plus pratique et il devient indispensable de passer sur Internet.

L'ensemble de l'entreprise est au milieu d'une transition numérique, depuis le support client jusqu'aux différents corps de métiers. Il faut donc sécuriser l'architecture en conséquence. Voilà pourquoi, Phone a lancé le projet Olympus qui consiste à ouvrir les fonctionnalités sur Internet tout en les sécurisant avec plusieurs couches de « firewalls ». A l'intérieur de ce périmètre, le projet prévoit l'établissement de contrôles rigoureux et le traçage des accès.

A titre d'exemple, il y a deux ans encore, les ressources humaines géraient les demandes de congé au moyen de formulaires papier. Aujourd'hui, l'ensemble du processus est numérisé. En outre, le recrutement est entièrement effectué en ligne. Seule, la cybersécurité permet de déployer ces nouvelles applications sans lesquelles Phone perdrait son avantage différentiateur par rapport à ses concurrents. Selon Amina Gounajjar : « la sécurité est l'élément clé pour pouvoir satisfaire nos clients donneurs d'ordre, les ressources humaines et les utilisateurs finaux afin que cette entreprise puisse perdurer et aller de l'avant. »

La numérisation a déjà imposé de nombreux changements en matière de cybersécurité. Phone est extrêmement réactif à ces changements. Ainsi, plusieurs de ses clients procèdent à un audit de sécurité des infrastructures et des processus d'affaires de Phone sur une base annuelle. Le centre de contact évolue en fonction des résultats de ces audits. De par sa nature, l'entreprise est à l'écoute de toutes les exigences sécuritaires les plus pointues. « Nous devons arborer nos réalisations avec sérénité et même fierté, ajoute Amina Gounajjar. Cela fait partie de notre image de marque. »

Annexe 01 TAREC

Tarfaya Energy Company (TAREC)
6, rue Kadi Lass
Casablanca 20100
Tél. (212) 06-08-89-82-39
www.engie.com/groupe/notre-presence-internationale/maroc

Entrevue	**M. Yacine Yousfi** *Directeur des systèmes d'information (DSI)*	
Données de base	Fondation Chiffre d'affaires Nombre d'employés Activité	2013 768 millions de dirhams 30 Production d'énergie électrique
Mission	Développement des énergies renouvelables et de l'efficacité énergétique au Maroc.	
Objectifs	✓ Augmenter la part de l'énergie éolienne dans la capacité électrique totale à 14% à l'horizon 2020. ✓ Atteindre une capacité de production à partir de l'énergie éolienne de 2 GW et une capacité de production annuelle de 6 600 GWh, correspondant à 26% de la production électrique actuelle. ✓ Économiser en combustibles 1,5 million de tonnes équivalent pétrole annuellement, soit 750 millions de dollars US, et éviter l'émission de 5,6 millions de tonnes de CO2 par an.	
Enjeux de sécurité	Interconnexion d'un site d'exploitation situé dans le sud marocain avec Casablanca et le Danemark.	

Tarfaya Energy Company (TAREC) est une filiale d'ENGIE (ex-GDF SUEZ) et exploite un parc éolien à Tarfaya. Ce parc est actuellement le plus grand d'Afrique, avec 131 éoliennes d'une puissance de 2,3 MW chacune, réparties sur une zone de 10 000 hectares. La construction du parc a débuté en janvier 2013 et la mise en service a commencé en juin 2014, par tranches de 50 MW. Elle a nécessité un investissement total d'environ 450 millions d'euros. Cet effort s'inscrit dans la stratégie énergétique marocaine qui est de porter à 42% les actifs de production électrique issus d'énergies renouvelables à l'horizon 2020. A lui seul, le site de Tarfaya représente 15% de l'objectif fixé par le pays pour le développement des énergies renouvelables. La vente de l'électricité est régie par un contrat de fourniture d'électricité conclu avec l'Office National d'Électricité et de l'Eau potable (ONEE) pour une durée de 20 ans, sur une base « Build, Own, Operate and Transfer » (BOOT). Au terme de cette période, ONEE devient propriétaire des installations.

Le système d'information de TAREC est en ligne, En effet, la maintenance des éoliennes est assurée depuis le Danemark par l'entreprise Bonus Energy, filiale de Siemens Wind Power, qui a construit les turbines. Le site de Tarfaya, qui est situé dans le sud marocain, est aussi monitoré depuis le siège social de TAREC à Casablanca. Tout ce qui est purement logiciel, comme les mises à jour, est effectué à distance depuis le Danemark. Quand il faut une intervention physique sur les éoliennes, Siemens a des employés sur site qui sont chargés d'intervenir. La responsabilité de TAREC est située entre les éoliennes et le réseau électrique d'ONEE.

LES ENJEUX DE LA CYBERSECURITE AU MAROC

Le système d'information de TAREC-Casablanca est directement connecté aux bases de données sources des turbines. L'interconnexion des systèmes d'information et d'exploitation de TAREC nécessite des mesures de sécurité de haut niveau. Comme l'entreprise fait partie des infrastructures critiques, elle a dû se conformer à la DNSSI qui correspond à la norme ISO/CEI 27002. Afin de se conformer à ces exigences, TAREC a déjà procédé en 2016 à un audit sur l'informatique de gestion et s'apprête à faire un deuxième audit sur le périmètre industriel (mai 2018).

Le groupe des TI de TAREC comprend deux personnes. Au terme de l'audit en cours, un troisième employé sera vraisemblablement engagé afin de s'occuper exclusivement de la sécurité. Comme l'infrastructure TI de l'entreprise est robuste, il n'y a pas besoin de beaucoup de personnel pour la maintenance, y compris les aspects sécuritaires. La stratégie de sécurité de TAREC repose sur deux sites de relève (serveurs SCADA redondants) et les meilleures pratiques en vigueur dans l'industrie. Qui plus est, la partie la plus sensible du réseau interne n'est pas connectée à Internet. Le gros du danger provient donc de la menace interne et, en particulier, de la connexion avec Siemens. Les résultats de l'audit en cours vont être partagés avec Siemens pour s'assurer que les mesures de sécurité soient homogènes d'un bout à l'autre du réseau.

Une collaboration existe entre les différentes filiales éoliennes d'ENGIE au Maroc et ailleurs dans le monde pour évaluer les différentes solutions de sécurité. L'échange d'information est constant.

ANNEXE 02
QUESTIONNAIRE

Association des Utilisateurs des Systèmes d'Information au Maroc

PANORAMA DE LA CYBERSECURITE AU MAROC

Cette initiative vise à promouvoir la cybersécurité dans l'industrie et dans le secteur des services au Maroc. En dressant le panorama des mesures prises par les entreprises et les organismes publics en matière de cybersécurité, l'Association des utilisateurs des systèmes d'information au Maroc (AUSIM) vise deux buts : évaluer le degré de maturité du marché de la cybersécurité et faire connaître les meilleures pratiques dans ce domaine.

La cybersécurité est devenue un atout stratégique dans le développement des entreprises. De plus en plus, les contrats sont conditionnels à la présence de mesures adéquates de cybersécurité. Les entreprises marocaines ont déjà à leur actif de nombreuses réalisations. Trop souvent, ces réalisations sont méconnues. En participant à cette étude, vous permettrez de dresser un état de la situation et de le faire connaître non seulement au Maroc, mais aussi sur la scène internationale.

Nous comptons sur votre participation!

Mohamed Saad
Président

Annexe 02 QUESTIONNAIRE

IDENTIFICATION DE L'ORGANISATION

Q.01

Nom ..... Organisation .....

Pénom ..... Ville .....

Téléphone ou email ..... Région .....

Si différent, où se trouve votre siège social:

Ville ....., Région/Pays .....

Q.02

Votre organisation dispose-t-elle d'un programme de cybersécurité (mesures à prendre en cas de failles ou d'incidents liés à la sécurité de l'information) ?

Oui ☐ Non ☐

Si vous avez répondu « Non », veuillez préciser pourquoi :

.....

Confidentialité. Les réponses aux questions suivantes seront traitées de façon confidentielle. Elles n'apparaîtront pas dans la base de données et seront utilisées sous forme agrégée à des fins uniquement statistiques. Elles ne sont ni rétrocédées à des tiers ni utilisées à d'autres fins que celle requises à l'analyse des résultats de cette enquête.

Annexe 01 QUESTIONNAIRE

CADRE ORGANISATIONNEL

Q.03

Qui est responsable de la cybersécurité dans votre organisation ?

- Responsable de la sécurité des systèmes d'information (RSSI) ☐
- Directeur des systèmes d'information (DSI) ☐
- Directeur de risques ☐
- Directeur de conformité ☐
- Directeur de contrôle interne ☐
- Directeur Général / Président Directeur Général ☐
- Autre ☐

Si vous avez répondu « Autre », veuillez préciser la fonction, SVP :

.....

Q.04

Combien d'employés dans votre organisation sont affectés à la cybersécurité :

Nombre d'employés à plein temps ___
Nombre d'employés à temps partiel ___

Q.05

Votre entreprise éprouve-t-elle des difficultés à recruter des employés spécialisés en cybersécurité ?

Oui ☐ Non ☐

Q.06

[Pour ceux qui ont répondu OUI à la question précédente seulement]

Quelles sont les principales difficultés rencontrées ?

- Manque de main d'œuvre qualifiée ☐
- Les salaires exigés sont trop élevés ☐
- La formation universitaire des candidats n'est pas adaptée aux besoins ☐
- Autre ☐

Si vous avez répondu « Autre », veuillez préciser la fonction, SVP :

.....

Q.07

Dans votre organisation, en matière de cybersécurité, existe-t-il…

… un programme de formation en externe (université, école spécialisée, etc) ☐
… un programme de formation en interne (conférences, cours, etc) ☐
… un ou des programmes de sensibilisation* ☐

Pouvez-vous définir en quelques mots en quoi consiste ce ou ces programmes, SVP :

.....

** Il peut s'agir par exemple, de messages sur l'intranet, courriels personnalisés, bulletins en ligne, écrans de veille des ordinateurs, affiches, ou de capsules vidéo.*

Q.08

Votre entreprise a-t-elle contracté une assurance pour couvrir le risque en matière de cybersécurité ?

Oui ☐ Non ☐

Si vous avez répondu « Non », veuillez préciser pourquoi :
(par exemple : pas d'assurance disponible, prix trop élevé, etc.) :

.....

Q.09

Les risques de cybersécurité font-ils l'objet d'une clause écrite dans les accords de sous-traitance ?

Oui ☐ Non ☐

Si vous avez répondu « Parfois », veuillez préciser dans quelles circonstances, SVP :

.....

Annexe 01 QUESTIONNAIRE

CADRE TECHNIQUE

Q.10

Votre entreprise éprouve-t-elle des difficultés à recruter des employés spécialisés en cybersécurité ?

Oui (une seule fois)..... ☐ **Oui** (de façon récurrente)..... ☐ Non ☐

Q.11

Quels systèmes de sécurité utilisez-vous dans votre organisation ?

Solution de sécurité Endpoint (antivirus, filtrage de contenu, filtrage url, etc...) ☐
Solution de sécurité réseaux (Firewall, IPS, NAC, etc) ☐
Solution de protection des données (Cryptage, DLP, anonymisation, etc) ☐
Solution de traçabilité (gestion des logs, traçabilité des accès des bases de données, gestion des comptes à hauts privilèges, etc) ☐
Autre (veuillez préciser) ☐

Si vous avez répondu « Autre », veuillez préciser le ou les systèmes utilisés, SVP :

.....

Q.12

Votre organisation dispose-t-elle d'un plan de réponses aux incidents ?

Oui ☐ Non ☐

Q.13

[Pour ceux qui ont répondu OUI à la question précédente seulement.]

Votre organisation effectue-t-elle de la surveillance permanente des évènements de sécurité ?

Oui (dans le cadre d'un SOC interne) ..... ☐
Oui (dans le cadre d'un SOC externe) ..... ☐
Non ..... ☐

Q.14

Vos systèmes de sécurité...

... sont gérés entièrement en interne ☐
... sont gérés en partie chez un sous-traitant ☐
... sont gérés entièrement chez un sous-traitant ☐

Si vous avez répondu « en partie chez un sous-traitant », veuillez préciser quels systèmes sont sous-traités :

.....

Q.15

Votre entreprise effectue-t-elle des simulations de cyberattaques…

… régulièrement (au moins une fois par an) ☐
… de façon intermittente (plus d'une fois depuis le début du programme) ☐
… une fois seulement (depuis le début du programme) ☐
… jamais ☐

Si vous avez répondu « de façon intermittente », « une fois seulement » ou « jamais », veuillez expliquer pourquoi l'entreprise ne procède pas à des simulations régulières :

.....

Q.16

Votre entreprise a-t-elle déjà fait l'objet d'une cyberattaque ?

Oui ☐ Non ☐

Si « Oui », veuillez préciser à combien de reprises :

.....

Q.17

[Pour ceux qui ont répondu OUI à la question précédente.]

Pouvez-vous définir de quel type de cyberattaques il s'est agi :

attaque virale ☐
demande de rançon ☐
atteinte à la confidentialité ☐
intrusion informatique ☐
arnaque au président ☐
fraude financière ☐
indisponibilité de service ☐
vol de données ☐
atteinte à l'intégrité des données ☐
autre ☐

Si vous avez répondu « Autre », veuillez expliquer la nature de l'attaque :

.....

Q.18

[Pour ceux qui ont répondu aux deux questions précédentes.]

Comment votre entreprise a-t-elle réagi à la cyberattaque?

[Plusieurs réponses possibles.]

Par des moyens techniques et organisationnels internes ☐
En faisant appel à des experts externes ☐
En contactant l'assurance spécialisée en cybersécurité ☐
En portant plainte aux forces de police ☐
En contactant la DGSSI ☐
Autre ☐

Si vous avez répondu « Autre », veuillez préciser, SVP :

.....

Annexe 01 QUESTIONNAIRE

CADRE LEGAL ET REGLEMENTAIRE

Q.19

Votre organisation a-t-elle adopté une ou plusieurs des normes de sécurité suivantes :

DNSSI (Directive Nationale de la Sécurité des Systèmes d'Information) ☐
ISO 27001 (management de la sécurité des informations) ☐
Loi 09-08 (Protection des personnes physiques) ☐
PCI DSS (Payment Card Industry Data Security Standard) ☐
Autre ☐

Si vous avez répondu « Autre », veuillez préciser la ou les normes, SVP :

.....

Q.20

Votre organisation vérifie-t-elle périodiquement sa conformité aux normes sectorielles et à la réglementation ?

Oui ☐ Non ☐

Si vous avez répondu « Oui », veuillez préciser de quelles normes et règles il s'agit :

.....

INVESTISSEMENTS EN CYBERSECURITE

Q.21

Quel est le montant approximatif que votre organisation investit en cybersécurité sur une base annuelle (montant pour 2017) :

Moins de 1 000 000 mad
Entre 1 000 000 et 5 000 000 mad
Entre 5 000 000 et 10 000 000 mad
Plus de 10 000 000 mad ☐

Si vous avez répondu « Plus de 10 000 000 dirhams », veuillez préciser le montant approximatif, SVP :

.....

Q.22

Au cours de 2018, prévoyez-vous que ce montant sera amené à…

… augmenter ☐
… baisser ☐
… demeurer stable ☐

Q.23

D'une façon générale, estimez-vous que votre organisation est bien outillée en matière de cybersécurité ?

Oui ☐ Non ☐

Si vous avez répondu « Non », veuillez préciser ce qui devrait être fait, selon vous, pour améliorer la sécurité :

.....

INFORMATIONS GENERALES

Q.24

Quel est votre principal domaine d'activité ?

[Par exemple : Banque, assurance, agroalimentaire, santé, machinerie électrique, électronique…]

1 - .....

2 - .....

3 - .....

Q.25

Combien d'employés travaillent dans votre entreprise ?

[Veuillez indiquer le nombre approximatif d'employés à temps plein.]

Au Maroc .....

A l'étranger .....

Si vous avez répondu « A l'étranger », veuillez préciser dans quel(s) pays :

.....

Q.26

Quel pourcentage de chiffre d'affaires effectuez-vous…

…. % …au Maroc ?

…. % …à l'étranger ?

Pour ceux qui ont répondu « à l'étranger », veuillez préciser le ou les pays :

.....

PRIERE DE RENVOYER LE QUESTIONNAIRE

Par courriel **itourabi@dataprotect.ma**
Par télécopie **(+212) 522 218 396**

MERCI !

ANNEXE 03

SIGLES ET ACRONYMES

ADD	Agence de Développement du Digital
ANRT	Agence Nationale de Réglementation des Télécommunications
ASIS	American Society for Industrial Security
CNDP	Commission nationale de contrôle de la protection des données à caractère personnel
DGSSI	Direction Générale de la Sécurité des Systèmes d'Information
DLP	Data Loss Prevention
DNSSI	Directive Nationale de la Sécurité des Systèmes d'Information
DSI	Directeur des systèmes d'information
IPS	Intrusion Prevention System
ISC	Interagency Security Committee
ISO	International Organization for Standardization
ISP	Information Systems Professional
ITCP	Information Technology Certified Professional
MA-CERT	Morocco Computer Emergency ResponseTeam
NAC	Network Access Control
NIST-CSF	National Institute of Standards and Technology-Cybersecurity Framework
NIDS	Network Based Intrusion Detection System
PKI	Public Key Infrastructure
PME	Petites et moyennes entreprises
PMP	Project Management Professional
R-D	Recherche et développement
RFID	Radio Frequency Identification
RGPD	Règlement général sur la protection des données
RSSI	Responsable de la sécurité des systèmes d'information
RVP	Réseau virtuel privé
SIEM	Security information and event management
SOC	Security Operations Center
SSCP	Systems Security Certified Practitioner
TIC	Technologies de l'information et communications
TSCP	Transglobal Secure Collaboration Program
UIT	Union internationale des télécommunications

ANNEXE 04

Liste des secteurs d'activités d'importance vitale et autorités gouvernementales ou établissements publics ou personnes morales de droit public chargés d'assurer la coordination des secteurs

Secteurs	Autorités gouvernementales ou établissements publics ou personnes morales de droit public chargés d'assurer la coordination des secteurs
SECURITE PUBLIQUE	AUTORITE GOUVERNEMENTALE CHARGEE DE L'INTERIEUR
JUSTICE	AUTORITE GOUVERNEMENTALE CHARGEE DE LA JUSTICE
LEGISLATION	SECRETARIAT GENERAL DU GOUVERNEMENT
SECTEUR DES FINANCES	AUTORITE GOUVERNEMENTALE CHARGEE DES FINANCES
INDUSTRIE	AUTORITE GOUVERNEMENTALE CHARGEE DE L'INDUSTRIE
SANTE	AUTORITE GOUVERNEMENTALE CHARGEE DE LA SANTE
AUDIOVISUEL ET COMMUNICATION	AUTORITE GOUVERNEMENTALE CHARGEE DE LA COMMUNICATION
PRODUCTION ET DISTRIBUTION DE L'ENERGIE, ET MINES	AUTORITE GOUVERNEMENTALE CHARGEE DE L'INTERIEUR AUTORITE GOUVERNEMENTALE CHARGEE DE L'ENERGIE ET DES MINES
RESEAUX DES TRANSPORTS	AUTORITE GOUVERNEMENTALE CHARGEE DES TRANSPORTS
APPROVISIONNEMENT ET DISTRIBUTION D'EAU	AUTORITE GOUVERNEMENTALE CHARGEE DE L'INTERIEUR AUTORITE GOUVERNEMENTALE CHARGEE DE L'EAU
SERVICES POSTAUX	AUTORITE GOUVERNEMENTALE CHARGEE DES POSTES
SECTEUR BANCAIRE	BANK AL-MAGHRIB
TELECOMMUNICATIONS	AGENCE NATIONALE DE REGLEMENTATION DES TELECOMMUNICATIONS
SECTEUR DES MARCHES FINANCIERS	AUTORITE MAROCAINE DU MARCHE DES CAPITAUX
SECTEUR DES ASSURANCES	AUTORITE DE CONTRÔLE DES ASSURANCES ET DE LA PREVOYANCE SOCIALE

CYBERSECURITE MAROC 2018

Les attaques ciblant les données des organisations ont explosé. Les responsables de la cybersécurité ont tous une excellente vision de l'ampleur du danger. Mais l'investissement stagne. Quels sont les enjeux?

Plus de 90 organisations de tous les secteurs ont répondu au sondage et huit ont été interviewées sur une base personnalisée.

L'étude couvre plus précisément :

- ✓ Le profil des répondants
- ✓ Les stratégies de sécurité
- ✓ Les ressources humaines
- ✓ La technologie sécuritaire
- ✓ L'investissement
- ✓ Les enjeux

A qui s'adresse cette étude ?

- ✓ Les responsables de la cybersécurité
- ✓ Les décideurs de l'industrie et du gouvernement
- ✓ Les investisseurs publics et privés
- ✓ La communauté universitaire
- ✓ Les partenaires étrangers actuels ou potentiels
- ✓ Les médias spécialisés

Prix version papier :
Prix version électronique :
Rabais de 20% pour les membres des associations partenaires.
Par courriel :

Contact :

LES ENJEUX DE LA CYBERSECURITE AU MAROC

Livre Blanc

LES ENJEUX DE LA CYBERSECURITE AU MAROC

Dépôt légal :
Bibliothèque Nationale
du Royaume du Maroc, 2018

9 780201 379624