Les Rendez-Vous de l'AUSIM

La cybercriminalité : Les enjeux pour l'entreprise marocaine

Présenté par M. Ali EL AZZOUZI

Décembre 2015

Récit de la présentation par Mohamed SAAD, Président de l'AUSIM

Dans le cadre des « Rendez-vous de l'AUSIM », l'association a reçu le 11 Décembre 2016, Monsieur Ali EL AZZOUZI, consultant expert en sécurité de l'information, pour une présentation autour du thème « **La cybercriminalité : Les enjeux pour l'entreprise marocaine** »

L'image de l'adolescent cherchant désespérément à explorer une vulnérabilité d'un serveur sur l'internet depuis sa chambre au sous-sol est révolue. Aujourd'hui, de nouveaux groupes très structurés sont à l'origine d'actes cybernétiques visant à porter préjudice aux systèmes d'information des organisations privées et publiques. Le Maroc n'y échappe pas. Nous appartenons à ce village planétaire régi par les moyens de télécommunication les plus sophistiqués. Dans cette perspective, il est vital aujourd'hui pour les organisations marocaines de se préparer aux cyberattaques et de les confiner en identifiant leurs causes et leurs conséquences.

Ce rendez-vous a réuni une cinquantaine de participants venant de différents secteurs d'activités (banques, assurances, industries, holdings, administration, télécoms, marché des capitaux…), mais qui partagent tous la même préoccupation, celle de de la sécurité et de la protection de leurs informations et celles de leurs organisations.

L'expert a présenté son intervention selon les axes ci-dessous :

- **Les tendances de la cybercriminalité à l'international**
- **Les tendances au Maroc**
- **Les ripostes juridiques**
- **Conclusion en images**
- **Questions/Réponses**

Il y a dans le monde plus de six cents millions d'ordinateurs interconnectés en permanence, ce qui constitue un immense terrain de chasse pour ce que l'on appelle les cybercriminels. Et dans ce terrain, il y a le nôtre, ceux de nos organisations et ceux des hautes instances économiques et sécuritaires du pays. C'est ainsi, que nous essayons de protéger ces actifs informationnels grâce à des solutions logicielles, matérielles, et surtout à travers un processus continu de sensibilisation et de formation de l'être humain, car, comme expliqué ci-après, l'humain reste le garant fondamental de la bonne protection de l'information. Face à cela, on voit progresser une population de personnes avides de défis et d'innovation, chercheuses de failles, casseuses de codes de sécurité, capables de briser n'importe quel système d'information. D'après McAfee, on estime à 500 milliards d'USD les gains engrangés en 2014 grâce à ces activités illégales (http://www.mcafee.com/fr/resources/reports/rp-quarterly-threat-q3-

2014.pdf). L'expert a rappelé que cette économie souterraine dépasse même les chiffres du trafic de drogue.

Qui sont ces trafiquants qui revendent des secrets industriels ? Quels sont ces réseaux organisés qui pillent des comptes bancaires et qui usurpent des identités ?

Ce sont des individus qui ont fait de la cybercriminalité leur métier. C'est une économie « underground » qui échappe à la vigilance de la police, du fait des techniques ultra sophistiquées utilisées.
Aujourd'hui, nous parlons de différents objectifs et de différentes stratégies empruntées par les cybercriminels : Il s'agit entre autres de « Cyberterrorism », « Cyberextortion », « Cyberwarefare »…

Afin d'illustrer ces concepts, l'expert est revenu sur les techniques utilisées :

Les Botnets :

> Un **botnet** (de l'anglais, contraction de « robot » et « réseau ») est un réseau de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches.
>
> Historiquement, *botnet* désignait des réseaux de robots IRC. Le sens de *botnet* s'est étendu aux réseaux de machines zombies, utilisés pour des usages malveillants, comme l'envoi de spam et virus informatiques, ou les attaques informatiques par déni de service (DDoS). (Source wikipedia)

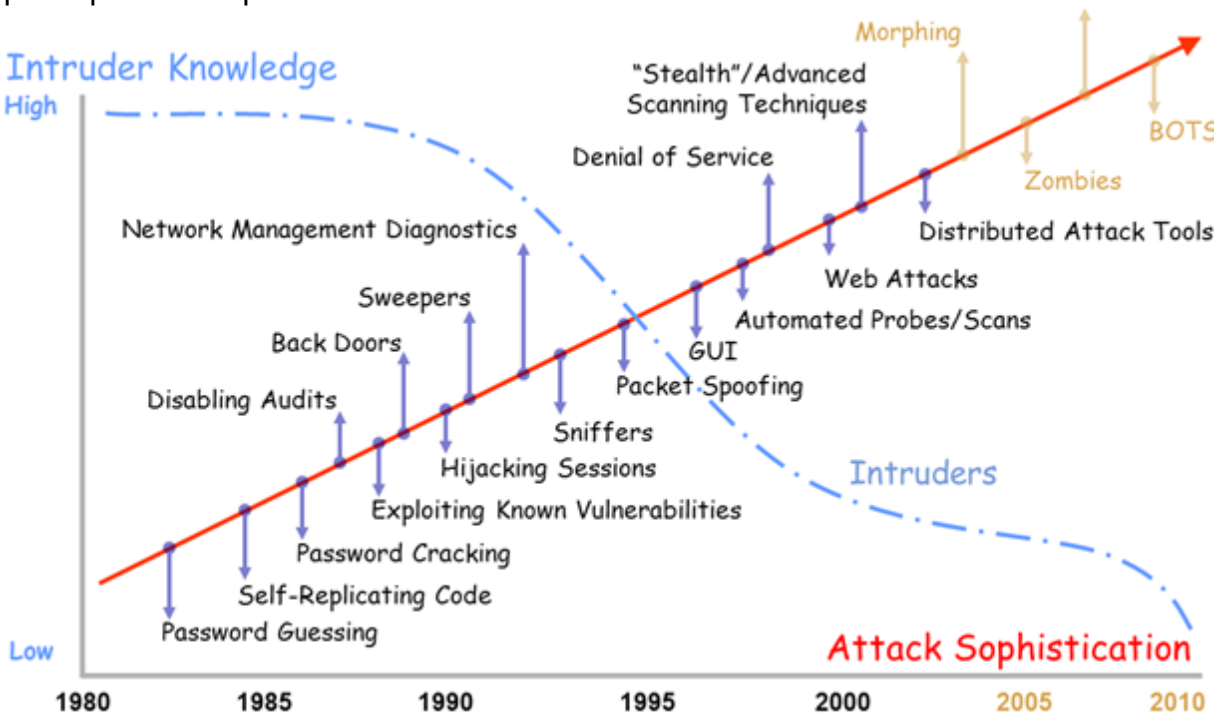
Les codes malveillants :

> Tout bout de code écrit dans l'intention de porter atteinte à autrui.
> L'expert a donné l'exemple de « Stuxnet » ;
>
> > **Stuxnet** est un ver informatique découvert en 2010, conçu par la NSA en collaboration avec l'unité 8200 pour s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium. Le programme a été initié sous l'administration Bush et a continué sous l'administration Obama. Il fait partie de l'opération Olympic Games, et ses caractéristiques le classent parmi les APT (Advanced Persistent Threat).
> >
> > Spécifique au système Windows, il a été découvert en juin 2010 par VirusBlokAda, société de sécurité informatique basée en Biélorussie. La complexité du ver est très inhabituelle pour un malware. Il a été décrit par différents experts comme *cyber arme*, conçue pour attaquer une cible industrielle déterminée. Il s'agirait d'une première dans l'histoire.
> >
> > C'est le premier ver découvert qui espionne et reprogramme des systèmes industriels, ce qui comporte un risque élevé. Il cible spécifiquement les systèmes SCADA utilisés pour le contrôle commande

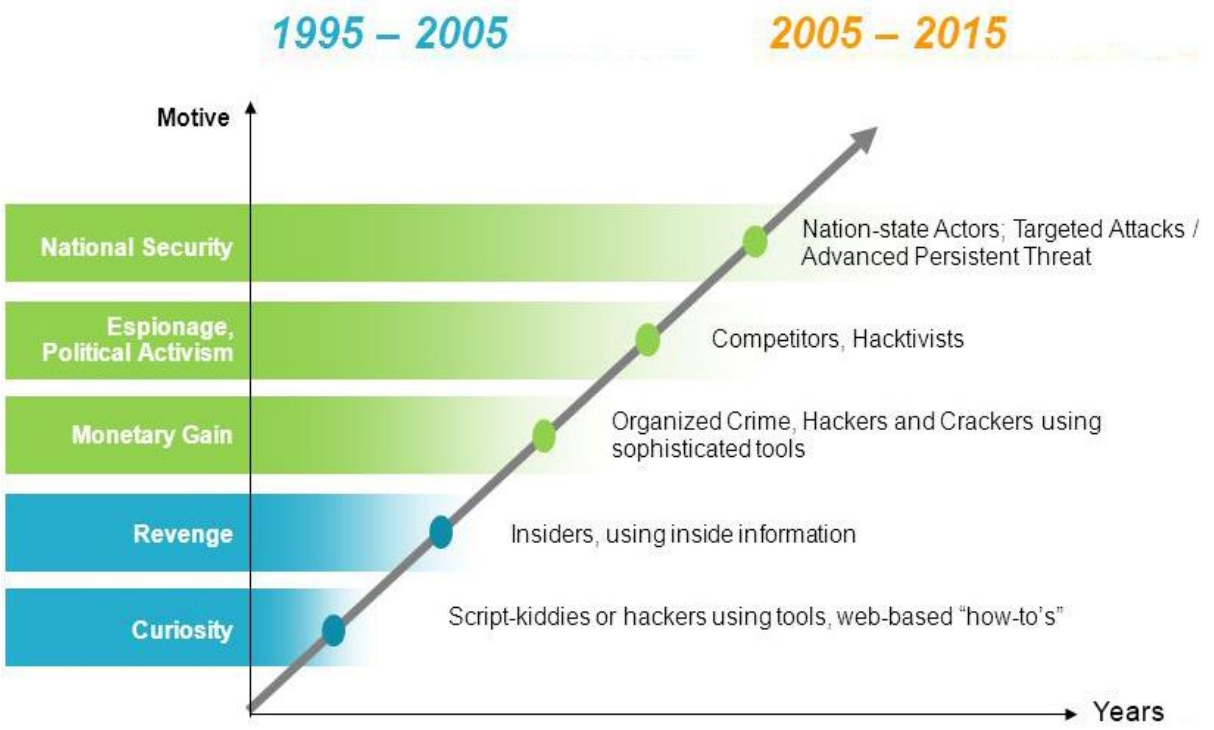
de procédés industriels. Stuxnet a la capacité de reprogrammer des automates programmables industriels (API) produits par Siemens et de camoufler ses modifications. Les automates programmables Siemens sont utilisés tant par quelques centrales hydro-électriques ou nucléaires que pour la distribution d'eau potable ou les oléoducs.

Le ver a affecté 45 000 systèmes informatiques, dont 30 000 situés en Iran, y compris des PC appartenant à des employés de la centrale nucléaire de Bouchehr. Les 15 000 autres systèmes informatiques sont des ordinateurs et des centrales situés en Allemagne, en France, en Inde et en Indonésie[9], utilisateurs de technologies Siemens. (Source Wikipedia)

L'expert a présenté un graphe qui illustre la sophistication des attaques Vs les prérequis techniques :



La motivation des cybercriminels a aussi évolué à travers les années ; Des jeunes scotchés devant leurs écrans dans les laboratoires d'universités, aux professionnels arborant des fortunes colossales et opérant à très haute échelle, ciblant les documents ultra confidentiels relevant du secret défense ou des secrets industriels comme le montre le graphe ci-après :



Se référant au rapport de Symantec 2014, notre expert est revenu sur l'état des lieux au Maroc, en insistant sur la situation alarmante qui place notre pays au troisième rang des pays ciblés par les cybercriminels.

Le développement des offres de solutions eBanking et du paiement en ligne augmente les risques du Phishing, et c'est pour cela que nous avons vu un certain nombre de parades permettant d'augmenter le contrôle et la sensibilisation des utilisateurs des moyens de paiements en ligne. Ceci dit, la communauté déplore l'absence de chiffres officiels des pertes, ou du nombre de cas d'actes de malveillance de cybercrime identifiés.
L'expert, d'après son expérience, estime ces pertes au Maroc à une centaine de millions de MAD par an.

A ce titre, un certain nombre de facteurs encourageant le développement de ces actes illégaux peuvent être cités :

- La prolifération de sites web peu ou pas du tout sécurisés ;
- Une activité hautement technique qui pose problème aux systèmes judiciaires ;
- L'absence d'experts assermentés ;
- La réticence d'expert à emprunter la voie de « l'expertise assermenté » faute de valorisation du travail par les autorités (honoraires ne correspondant pas aux efforts fournis) ;
- Le ma.Cert tarde à trouver sa place d'observatoire leader dans l'incident response, la centralisation des incidents, l'agrégation des incidents…
- Le Maroc constitue aussi une plateforme privilégiée pour les hackers de l'Afrique sub-saharienne ;

Néanmoins, il est à noter que les utilisateurs et les institutions au Maroc sont plus au moins épargnés grâce à la réglementation de changes.

Dans ce cadre, l'expert a présenté les ripostes juridiques à ce fléau :

- La loi n°07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données
    - **Les intrusions**
        - L'accès frauduleux dans un STAD (systèmes de traitement automatisé de données) ;
        - Le maintien frauduleux dans un STAD.
    - **Les atteintes**
        - Les atteintes au fonctionnement d'un STAD ;
        - Les atteintes aux données.
- Le Maroc est signataire de la convention de Budapest (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008156d)

A ce titre, il est à rappeler que les failles proviennent plus du manque de rigueur dans l'application des textes de loi que de l'absence de jurisprudence dans ce domaine. La situation est telle que l'on revienne au droit commun pour incriminer les actes informatiques frauduleux, impliquant une procédure pénale lourde et dont les techniques ne sont pas forcément appropriées et qui peuvent dans certains cas, porter atteinte aux libertés individuelles.

La conclusion de la présentation a été illustrée par des images ludiques :

La sécurité ne doit pas être une option

A partir du moment où les risques sont connus, il est extrêmement difficile de prendre la décision de ne rien faire.

Le risques Zéro ?
C'est quand la poule aura des dents.

L'être humain est le maillon faible de la sécurité.

La sécurité est un voyage, pas une destination…

La présentation s'est terminée sur une note positive :

La matinée s'est terminée par un flot de Questions/Réponses et interventions des participants qui ont trouvé le sujet très riche et captivant. Ils ont vivement encouragé les membres de l'AUSIM à étudier la possibilité de le prévoir lors des **Assises de l'AUSIM planifiées pour le mois d'octobre 2016**.

Next To come :

Rendez Vous de l'AUSIM : Janvier 2016

Retour d'expérience des entreprises certifiées ISO 27 001

Elles sont moins d'une dizaine au Maroc, les entreprises ayant relevé le défi de mettre en place un SMSI et de le certifier ISO 27 001. Ce thème sera présenté par des Responsables de sécurité de l'Information chevronnés, ayant plusieurs années d'expérience en matière de management de la sécurité de l'information et surtout ayant relevé le challenge de certifier leurs structures. Ils reviendront sur :

- ✓ La méthodologie de management de projet de mise en place d'un SMSI et de certification ISO 27 001
- ✓ L'apport des prestataires de service qui les ont accompagnés
- ✓ Le pré requis à la certification
- ✓ Les difficultés d'un projet de ce genre
- ✓ Les facteurs clés de succès
- ✓ Les couts estimatifs de ces projets
- ✓ La Certification ISO 27 001, so what Next !

Un témoignage pratico pratique, loin des discours standards formatés par les référentiels.

Pour plus d'information Mlle. Abla ELHOSNI se ferait un plaisir de vous renseigner : Abla.elhosni@ausimaroc.com

Au plaisir de vous voir.

Mohamed SAAD, Président de l'AUSIM