cybersécurité pour l'Algérie ?

et alerter au niveau national les parties qui peuvent être victimes de la même attaque. Selon le rapport annuel de la compagnie Dell, le nombre de cyberattaques contre les Systèmes de contrôle et d'acquisition de données (Scada) des infrastructures sensibles a doublé en 2014, que la majorité de ces incidents n'ont pas été signalés alors que dans la plupart des cas il s'agissait d'attaques du type APT (Advanced Persistent Threat) à motivation politique. L'initiative de rapporter les attaques est donc dans l'intérêt de l'ensemble, elle permet le partage des informations, comme celles sur les cybermenaces, sur les vulnérabilités des systèmes, une meilleure compréhension des attaques, l'identification des faiblesses dans les réseaux et de partager les enseignements.

Dans le cas de la récente cyberattaque contre la chaîne de télévision française TV5 Monde, le ministre de l'Intérieur français a annoncé l'ouverture d'une enquête et l'Agence nationale de la sécurité des systèmes d'information (ANSSI), rattachée au Premier ministre, a dépêché 13 ingénieurs en sécurité informatique pour déterminer les contours de cette attaque. La ministre de la Culture, Fleur Pellerin, a déclaré qu'elle réunirait «très prochainement l'ensemble des dirigeants de grands médias audiovisuels» et de la «presse écrite» pour les faire bénéficier des enseignements.

Occulter les cyberattaques constituerait un délit et équivaut à permettre la répétition des mêmes attaques contre d'autres organismes nationaux. Des textes pour la notification des violations de données existent déjà aux Etats-Unis, Allemagne, Australie, France, Royaume-Uni, etc. Cependant, une entreprise attaquée pourrait être réticente à rendre publiques ces informations privées dans la mesure où une exploitation de cette intrusion pourrait lui faire courir le risque d'une perception négative conduisant à inquiéter les clients, voire à créer une relation de défiance. De plus, des inquiétudes existent selon lesquelles le partage de l'information peut faciliter l'accès à des informations commerciales confidentielles et à la propriété intellectuelle par des concurrents. Des parties ont aussi exprimé des préoccupations selon lesquelles le gouvernement peut utiliser contre elles les renseignements obtenus à des fins qui n'ont aucun lien avec la cybersécurité.

La protection des données

Plus de 1 500 intrusions dans les réseaux ont conduit à un milliard de paquets de données volées en 2014. Par rapport à 2013, ces chiffres représentent une augmentation de 49% du nombre d'intrusions pour voler des données et une augmentation de 78% du nombre de paquets de données volées.

La principale motivation de ces intrusions est le vol d'identité puisqu'elles représentent 54% de l'ensemble des données volées, plus que toutes les autres catégories de données volées y compris celles financières. Alors que la confidentialité est essentielle, les opérateurs économiques et fournisseurs de services recueillent et stockent des données relatives à l'identité, à la situation professionnelle, aux activités, aux contacts, aux habitudes, à la situation financière, à l'état de santé, au contenu des emails, des SMS, à la position géographique, etc. Cette pratique du stockage de données (Mass Data Collection) ainsi que leurs utilisations par les opérateurs économiques du secteur public et privé devraient être réglementées par une loi. Son objectif principal serait aussi de rendre les données imperméables aux intrusions.

Cloud Computing

Le cloud permet de mettre à disposition des données partout pour une facilité d'utilisation par les employés souvent au détriment de la sécurité des données qui jouent un rôle important pour la survie d'une entreprise. Il semble donc essentiel que la loi rappelle le caractère primordial de la sécurisation des données et la nécessité de ne pas les héberger en dehors de l'Algérie.

Les services cloud étrangers stockent les données des clients dans des serveurs localisés dans différents pays et peuvent les transférer à volonté d'un pays à l'autre, y compris dans des pays réputés hostiles à l'Algérie ou avec lesquels elle n'a aucune relation (Israël), sans accord préalable du client. Par ailleurs, les serveurs et les données obéissent aux lois du pays étranger d'accueil. Une des conséquences serait l'accès aux données, sans l'autorisation du propriétaire et sans le prévenir, par des représentants des autorités du pays d'accueil si leur loi les y autorise. La loi sur la cybersécurité devrait exiger des infrastructures sensibles de ne recourir qu'aux services cloud nationaux et dont l'hébergement des données est national. Selon une directive de l'actuel chef de gouvernement français «l'hébergement des données sensibles sur le territoire national est obligatoire». Son prédécesseur avait déclaré quant à lui que «la France soutenait une politique nationale ambitieuse d'autonomie stratégique dans le domaine du numérique afin de ne pas dépendre de tiers pour héberger et traiter les données des entreprises et des citoyens».

Obligation de faire des audits

La loi doit rendre obligatoire des évaluations régulières de sécurité (audits internes et externes) pour les entreprises et organisations pour les protéger contre les intrusions. A titre d'exemple, dans le secteur des banques, l'Etat de New York impose par un texte de loi aux banques locales depuis mai 2014 des audits de sécurité périodiques. En juin 2014, le secteur britannique des banques a suivi en mettant en place un processus obligatoire de «tests» pour protéger les institutions financières britanniques contre les cyber-attaques. En Afrique, le Cameroun définit l'audit de cybersécurité dans la loi n°2010/012 du 21 décembre 2010, le cadre juridique qui régit cette activité, qui peut auditer les organisations qu'il faut auditer, la fréquence, etc.

Respect des exigences de sécurité par les fournisseurs des produits TIC

Les logiciels sont l'une des vulnérabilités majeures des produits TIC et il n'existe aucune règle en Algérie pour définir les normes de développement et d'acquisition de logiciels qui soient de haute qualité, fiables et sécurisés pour être utilisés par les organisations gouvernementales et les autres infrastructures sensibles. Comme le cancer, un logiciel imparfait se réplique, envahit et infecte les autres logiciels du réseau causant des dommages aux systèmes et la perte des données. Les infrastructures sensibles ne doivent utiliser que les produits et services TIC dont la sécurité est évaluée et attestée. Une association de compagnies privées américaines et européennes a élaboré un document (Process Control Domain Security Requirements for Vendors) qui définit les normes de sécurité à mettre en place obligatoirement par leurs fournisseurs de hardwares et logiciels afin de protéger leurs réseaux contre les cyberattaques. Conscientes de la menace, ces compagnies privées n'ont pas attendu les lois de leurs gouvernements respectifs.

Plusieurs Etats ont repris à leur compte, après l'affaire Edward Snowden, cette initiative sur les exigences sécuritaires à l'égard des fournisseurs à l'exemple de l'Allemagne qui exige depuis quelques mois de ses fournisseurs de produits TIC de signer un engagement selon lequel les hardwares ou logiciels fournis n'ont pas été manipulés par les services de sécurité étrangers.

Charte pour l'utilisation des ressources informatiques

En général, ce genre de charte définit les règles d'utilisation des ressources informatiques par les employés, leurs responsables, prestataires, etc. Elles s'appliquent à toute personne, quel que soit son statut. Elle invite par un engagement écrit au respect des règles sur la cyber-sécurité et est souvent un élément du règlement intérieur d'une organisation. Des lois imposent l'existence des chartes au niveau des infrastructures sensibles.

La cybersécurité est une question de sécurité nationale et est de la responsabilité de l'Etat qui intervient pour protéger le pays et la vie privée des citoyens internautes. Il met en place un mécanisme de supervision pour protéger la vie privée et empêcher la surveillance internet inappropriée. Ce mécanisme de supervision devrait exister pour assurer le caractère raisonnable des recherches et procédures gouvernementales dans le domaine de la cybersécurité et pour qu'elles soient contenues dans un cadre légal.

La cybercriminalité

La cybercriminalité est devenue très attrayante, elle génère des revenus élevés et les risques sont limités comparativement aux autres activités criminelles. Elle est devenue plus lucrative que le trafic de drogue dans le monde entier, une tendance inquiétante. Il est évident que les autorités n'arrivent pas à la contrer efficacement.

La mauvaise ou l'absence de perception des préjudices de la cybercriminalité par les autorités législatives et judiciaires est parmi les éléments qui facilitent la propagation rapide de ce type d'activités illégales. Par ailleurs, les forces de l'ordre concentrent toujours les efforts sur les crimes «hors ligne», alors que les organisations criminelles s'organisent et s'investissent dans les activités «en ligne». Le vol des données personnelles et le cyber-harcèlement en ligne sont les activités les plus communes (en Algérie aussi) et les plus rentables pour les cybercriminels. Les citoyens semblent rarement être au centre des politiques de cyber-sécurité alors qu'un grand nombre d'utilisateurs d'Internet sont régulièrement victimes de la cybercriminalité. Pour donner une idée de l'impact économique de la cybercriminalité, les dix fraudes en ligne les plus communes sont responsables de la perte en 2014 de 15 milliards de dinars dans un pays européen. Et il ne s'agit ici que de la face émergée de l'iceberg car la majorité des crimes en ligne ne sont pas rapportés à la justice par les citoyens et entreprises.

Selon des experts de la criminalité, le problème est que les lois existantes se sont figées alors que les crimes en ligne connaissent une constante évolution et adaptation aux mesures de sécurité. La loi algérienne d'août 2009 sur la cybercriminalité dont les points saillants sont la création d'un organe national de coordination, l'usage des données électroniques par la justice, la surveillance des communications électroniques à des fins préventives et la coopération internationale nécessite une adaptation à la «vitesse des crimes électroniques».

Campagnes de sensibilisation

Les campagnes de sensibilisation sont essentielles car aujourd'hui la façon la plus simple de réussir une cyberattaque consiste en l'exploitation des vulnérabilités humaines alors que de nombreuses organisations continuent à mettre l'accent uniquement sur l'acquisition des équipements, très coûteux d'ailleurs, pour la sécurisation des réseaux. Malheureusement, sans «la sécurisation de l'homme» grâce à des campagnes de sensibilisation régulières, ces efforts seront vains. La sensibilisation doit cibler non seulement les employés mais tous les citoyens internautes car la cybersécurité et le cyberespace national sont une responsabilité partagée. Les Etats-Unis ont fait depuis des années, grâce à la loi sur la cybersécurité, du mois d'octobre le mois de la sensibilisation sur la cybersécurité. Depuis 2012, les pays de l'Union européenne ont fait la même chose du mois d'octobre (European Cyber Security Month, ECSM). Ces initiatives, qui ont été aussi suivies par d'autres pays d'Asie et d'Afrique, visent à promouvoir la cyber-sécurité parmi les citoyens, les organisations et les entreprises, pour changer leur perception sur la cybermenace par l'éducation et d'accroître la résilience du cyberespace national. Les campagnes de sensibilisation définies par des textes de loi revêtent ainsi un caractère obligatoire.

La protection de la vie privée et des libertés civiles

La cybersécurité est une question de sécurité nationale et est de la responsabilité de l'Etat qui intervient pour protéger le pays et la vie privée des citoyens internautes. Il met en place un mécanisme de supervision pour protéger la vie privée et empêcher la surveillance internet inappropriée. Ce mécanisme de supervision devrait exister pour assurer le caractère raisonnable des recherches et procédures gouvernementales dans le domaine de la cybersécurité et pour qu'elles soient contenues dans un cadre légal. Certaines lois existantes privilégient une forme de contrôle indépendant car souvent les organismes dépendant de la Défense (cas de la NSA) ne sont pas soumis à la même surveillance et transparence que les organismes civils.

Conclusion

Malgré les investissements financiers continus et croissants dans la sécurité informatique (13 milliards de dollars dépensés par les entreprises en une année en parefeu et systèmes de prévention des intrusions), il est clair que la guerre contre les logiciels malveillants, de plus en plus sophistiqués, est loin d'être gagnée. Les lois sur la cybersécurité sont un moyen pour atténuer et contrer cette menace asymétrique qui pèse sur les infrastructures sensibles, elles permettent d'armer un pays de la connaissance de base nécessaire pour protéger les biens vitaux de la nation et les citoyens.

L'Algérie connaît un retard certain dans la production de solutions nationales de cybersécurité et surtout dans la mise en place de son cadre juridique et organisationnel. Concernant ce cadre, le plus important est de faire démarrer le processus car, comme l'expérience des autres pays le montre, son contenu ne peut être applicable immédiatement. Les Etats-Unis, le Royaume-Uni et la France qui ont déjà défini leurs cadres juridiques et organisationnels ont accordé un délai de 2 à 3 années aux institutions, organisations et entreprises pour qu'elles s'y préparent et s'y conforment strictement.

A. D.