LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Stratégie nationale en matière de cyber sécurité

INTRODUCTION

- Le fonctionnement de notre société est aujourd'hui étroitement lié aux infrastructures et systèmes de communication et de traitement de l'information. Ces infrastructures, dans la mesure où elles sont utilisées dans des secteurs aussi variés que l'énergie, la communication, le transport ou la santé, contribuent à satisfaire les besoins vitaux des citoyens. Assurer la continuité au niveau de l'approvisionnement et empêcher toute interruption ou tout disfonctionnement qui pourrait avoir des conséquences néfastes, soit pour la santé et sécurité publique, soit pour l'économie constitue une des priorités de notre pays.

- Les citoyens ont de plus en plus souvent recours aux technologies de l'information et de communication que ce soit dans le cadre de leur vie sociale ou dans le cadre de leurs relations avec les administrations et acteurs de la vie économique. Nous assistons à une multiplication des plateformes de communication et d'échange d'information qui ont tendance à se substituer aux modes traditionnels de communication, à l'apparition de nouveaux modes de consommation en ligne des informations, des œuvres musicales, des œuvres audiovisuelles et littéraires ainsi qu'à une généralisation des échanges électroniques que ce soit au sein des administrations publiques ou dans le cadre de leurs relations avec les administrés. Ces changements qui affectent la vie de tous les jours créent auprès des utilisateurs le sentiment légitime de pouvoir compter sur un fonctionnement sans faille des infrastructures sous-jacentes à ces activités.

- A l'avenir, la croissance économique sera fortement stimulée par le développement du secteur des technologies de l'information et de la communication. Cette croissance qui est génératrice de nouveaux emplois repose sur l'existence d'infrastructures performantes, capables de répondre aux exigences en termes de vitesse et de qualité mais aussi de sécurité, des milieux professionnels concernés. Ceci est particulièrement vrai pour le développement du secteur financier dont la performance est étroitement liée à la qualité, la résilience et la pérennisation des systèmes informatiques. Soutenir l'économie numérique en créant les conditions favorables à son expansion figure dès lors parmi les préoccupations prioritaires de notre pays.

L'omniprésence du cyberespace dans la vie de tous les jours s'accompagne d'une certaine dépendance et vulnérabilité qui ne doivent pas être sous-estimées. Les infrastructures et systèmes de communication et de traitement de l'information sont de plus en plus exposés aux nouvelles formes d'activités illégales (infections virales, mises hors service, actes d'intrusion, usurpations d'identité, vols d'information, etc.) et la multiplication de celles-ci perpétrées moyennant l'utilisation des réseaux informatiques ainsi que la complexité croissante des actions malveillantes recensées tout comme l'ampleur des dégâts potentiels mettent en évidence la nécessité d'une réponse adéquate et efficace à ces menaces.

Partant de ce constat le gouvernement a décidé en juillet 2011 de mettre en place une stratégie globale en matière de cyber sécurité visant à renforcer la protection des infrastructures et systèmes de communication et de traitement de l'information.

L'élaboration de cette stratégie ainsi que sa mise en œuvre et le suivi de son exécution relèvent des missions du Cyber Security Board qui a été créé à la même occasion.

Le présent document précise les lignes d'action de cette stratégie dont la réalisation a pour but de renforcer la sécurité et la résilience des infrastructures et contribuera à assurer, dans l'environnement numérique, la protection des citoyens, des professionnels et des acteurs de la vie publique.

LES CINQ AXES DE LA STRATEGIE

I. Assurer la protection opérationnelle des infrastructures et systèmes de communication et de traitement de l'information

Une protection efficace et adéquate de ces systèmes contre toute forme d'incidents et d'activités illicites susceptibles de causer des dommages économiques importants ou de perturber le bon fonctionnement des institutions et infrastructures doit constituer une priorité pour notre pays. Le programme gouvernemental énonce à ce sujet:

> « Les infrastructures de communication et d'information exigent aujourd'hui tant une protection physique qu'une protection virtuelle, notamment contre les cyber attaques et les actes relevant du domaine de la cybercriminalité. Dans le domaine virtuel, il y a lieu d'accélérer, d'étendre et de systématiser les initiatives prises à ce jour pour protéger tant les infrastructures publiques que privées ».

La protection opérationnelle des systèmes d'information comprend deux volets : un volet préventif et un volet défensif.

Volet opérationnel préventif

Les mesures préventives à mettre en place ont pour objectif d'anticiper les menaces et de protéger à priori contre les risques qui découlent des menaces auxquelles sont exposés les systèmes d'information et de communication. Dans cette optique, une collaboration avec les centres de recherche et universitaires et notamment le Interdisciplinary Center for Security, Reliability and Trust (SnT) sera envisagée.

Elles comprennent, à titre non limitatif, les activités suivantes :

- procéder à des analyses de risques en fonction des menaces et des vulnérabilités existantes ;
- organiser, promouvoir et participer à la veille au niveau des technologies, des vulnérabilités et des menaces ; et
- promouvoir et réaliser la mise en place de systèmes de détection et de prévention d'intrusions au niveau des infrastructures et systèmes sensibles et critiques.

Volet opérationnel défensif

Il faut partir du constat qu'aucun système d'information, quelque soit son niveau de protection, n'est parfaitement sécurisé. Dès lors, il faut disposer de capacités suffisantes pour détecter des intrusions mais aussi pour réagir une fois l'incident détecté, de traiter l'incident repéré de manière efficace et de rétablir l'opérabilité des systèmes affectés.

Dans ce contexte, trois types de mesures opérationnelles visent à atteindre cet objectif, à savoir

- établir un plan d'urgence en cas d'incident majeur ;
- réaliser des simulations et exercices sectoriels et nationaux portant sur la réaction en cas d'incident affectant la sécurité des systèmes d'information et de communication sensibles ou critiques et participer aux exercices européens et paneuropéens dans ce domaine ;
- et mettre en place des équipes spécialisées (Computer Emergency Response team (CERT)) capables de prendre en charge des incidents de sécurité majeurs.

II. Moderniser le cadre légal

L'évolution rapide des technologies des infrastructures et des systèmes de communication et de traitement de l'information génère de nouvelles menaces. Il est dès lors primordial de vérifier régulièrement si les bases légales en vigueur sont toujours adaptées et si elles permettent de poursuivre et de sanctionner les nouvelles formes de cyber criminalité.

La nécessité d'une veille juridique découle encore du caractère transfrontalier des actes criminels qui remet en cause, dans une certaine mesure, le principe de l'application territoriale des règles légales. En effet, dans le domaine de la criminalité commise à l'aide d'un système ou d'un réseau informatique, le nombre de lieux et de pays impliqués dans l'acte frauduleux est susceptible d'augmenter. L'infraction peut être commise pour partie dans un pays et pour partie dans un autre, voire en partie dans un troisième alors que l'initiateur peut pratiquement se trouver n'importe où dans le monde. Il s'agit dès lors de suivre de près l'évolution aussi bien au niveau des technologies qu'au niveau des comportements frauduleux.

La veille juridique, afin d'être efficace, devra englober le suivi des initiatives lancées sur le plan communautaire, voire international. En effet, la nature globale des réseaux et systèmes nécessite une réponse globale et toute approche purement nationale serait d'avance vouée à l'échec.

III. Développer la coopération nationale et internationale

La nécessité d'une coopération que ce soit sur le plan national entre tous les acteurs impliqués ou sur le plan international découle du caractère par essence mondial des réseaux de communication. En effet, il ne suffit pas que notre pays soit bien préparé à l'intérieur de nos frontières car l'expérience montre que les attaques sont généralement planifiées et organisées de l'extérieur de notre territoire. Il est dès lors impératif de disposer d'un tissu de collaboration actif avec la communauté internationale, et notamment avec les CERT et les forces de l'ordre (militaire et civil). Le but de cette coopération étant d'aboutir à un échange d'information entre les services compétents des différents Etats et enceintes internationales ainsi qu'à la définition d'approches et de solutions communes.

Sur le plan national, une coopération et interaction effective entre tous les acteurs concernés sont le préalable à une mise en œuvre cohérente de la stratégie. Sont visés par cette démarche :

- les organes interétatiques
- les autorités de poursuite (Police grand-ducale et Parquet)
- les autorités nationales indépendantes concernées (ILR, CSSF, CNPD)
- les acteurs sectoriels
- les partenariats public-privé.

Sur le plan international, cette collaboration peut prendre la forme de contacts bilatéraux comme elle peut s'appuyer sur les rapports multilatéraux au sein des institutions suivantes :

- Benelux
- Interpol et Europol
- UE
- Conseil de l'Europe
- OTAN
- OCDE
- OSCE.

IV. Informer, éduquer et sensibiliser sur les risques encourus

La sensibilisation, l'éducation des secteurs privés et publics sur les risques encourus et les moyens de protection constitue un élément essentiel de la stratégie puisqu'il contribue dans une large mesure à réduire les vulnérabilités potentielles et à motiver les acteurs concernés à participer activement au renforcement de la sécurité. Il est important de provoquer une prise de conscience auprès de tous les acteurs concernés qu'ils peuvent, en adoptant un comportement responsable, se protéger dans une large mesure contre les menaces et les dangers potentiels.

A moyen terme, une amélioration de la sécurité dans le cyberespace ne saura se faire sans responsabiliser davantage tous les acteurs des secteurs en cause. Une grande partie des failles exploitées par les cybercriminels sont rendues possibles par des négligences dans la conception et l'utilisation des systèmes qui sont sur le marché. A titre d'exemple: la publication et l'application tardives de correctionnels, la non-observation des procédures, la prévalence de la commodité sur la sécurité. Le législateur, les propriétaires et les opérateurs des infrastructures, les utilisateurs ainsi que les fournisseurs de solutions informatiques devront réunir leurs efforts afin de sécuriser le cyberespace au bénéfice de la collectivité.

Toute démarche de sensibilisation, d'éducation et d'information doit s'adresser à l'ensemble des acteurs, à savoir

- les utilisateurs finaux
    - les utilisateurs/internautes
    - les élèves, les parents, les éducateurs, les professeurs
    - les agents de l'Etat
    - les petites et moyennes entreprises

- les prestataires de services
    - d'hébergement physique (data centres)
    - de communication
    - de cloud computing
    - de signature électronique
    - de dématérialisation et d'archivage électronique

- les opérateurs d'infrastructures critiques.

L'évolution permanente de la menace implique que les citoyens doivent être tenus informés régulièrement de la nature et de l'envergure des attaques en cours, ainsi que des outils à mettre en place et des procédures à appliquer afin de se protéger efficacement.

Des formations (notamment dans les écoles, dans les administrations et dans les « Internetstuffen ») permettront aux intéressés d'actualiser leurs connaissances, que ce soit au niveau des menaces potentielles ou des moyens de protection.

V. Mettre en place des normes et des standards contraignants

Parmi les moyens des plus efficaces pour prévenir des cyber-attaques figurent la réduction des surfaces d'attaque et la réduction des vulnérabilités tant humaines que techniques.

Avant la mise en place de mesures préventives de sécurité, il faut procéder à une analyse des risques pour pouvoir estimer les pertes potentielles liées à une compromission de la disponibilité, de l'intégrité ou encore de la confidentialité des actifs sans pour autant perdre de vue que l'impact majeur est souvent la perte de renommée et de confiance.

La mise en œuvre cohérente et efficace de systèmes sécurisés au sein de l'Etat exige l'existence de méthodes d'analyse de risque, de politiques et de standards de sécurité cohérents et adaptés aux contextes. Les mesures de sécurité organisationnelles et techniques décrites dans ces politiques et standards doivent être appliquées par les différentes administrations. Sont notamment à inclure dans ces politiques des sujets comme la sécurisation des terminaux mobiles ou l'introduction généralisée de l'authentification forte pour tous les systèmes sensibles et accessibles depuis l'Internet.

Dans le même ordre d'idées, les opérateurs d'infrastructures critiques ou sensibles devront se conformer à un certain nombre de référentiels respectivement viser une certification sectorielle pour prouver leur maturité au niveau sécuritaire.

MISE EN ŒUVRE DE LA STRATEGIE

La présente stratégie définit les objectifs qu'il importe d'atteindre. Elle sera complétée par un inventaire des mesures existantes et par des plans d'actions opérationnels qui devront pour chaque domaine décrire les mesures concrètes à mettre en œuvre suivant un calendrier déterminé ainsi que les acteurs appelés à contribuer à leur accomplissement. Dans ce contexte, les centres universitaires et de recherches, qui constituent des centres d'excellence et disposent de connaissances et compétences pointues, seront invités à contribuer à la réalisation des objectifs de la stratégie.

La stratégie ci-avant décrite a vocation à évoluer dans le temps. Elle sera périodiquement révisée afin d'être adaptée, si besoin en était, aux nouvelles réalités. A cette fin, il sera périodiquement procédé à une réévaluation des menaces et des risques, accompagnée, si nécessaire, de propositions ayant pour objet d'actualiser la présente stratégie.