STRATÉGIE ***NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ II***

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

STRATÉGIE
NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ II

Approuvée et rendue exécutoire par le Conseil de gouvernement le 27.03.2015

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

AVANT-PROPOS DU PREMIER MINISTRE, MINISTRE D'ÉTAT

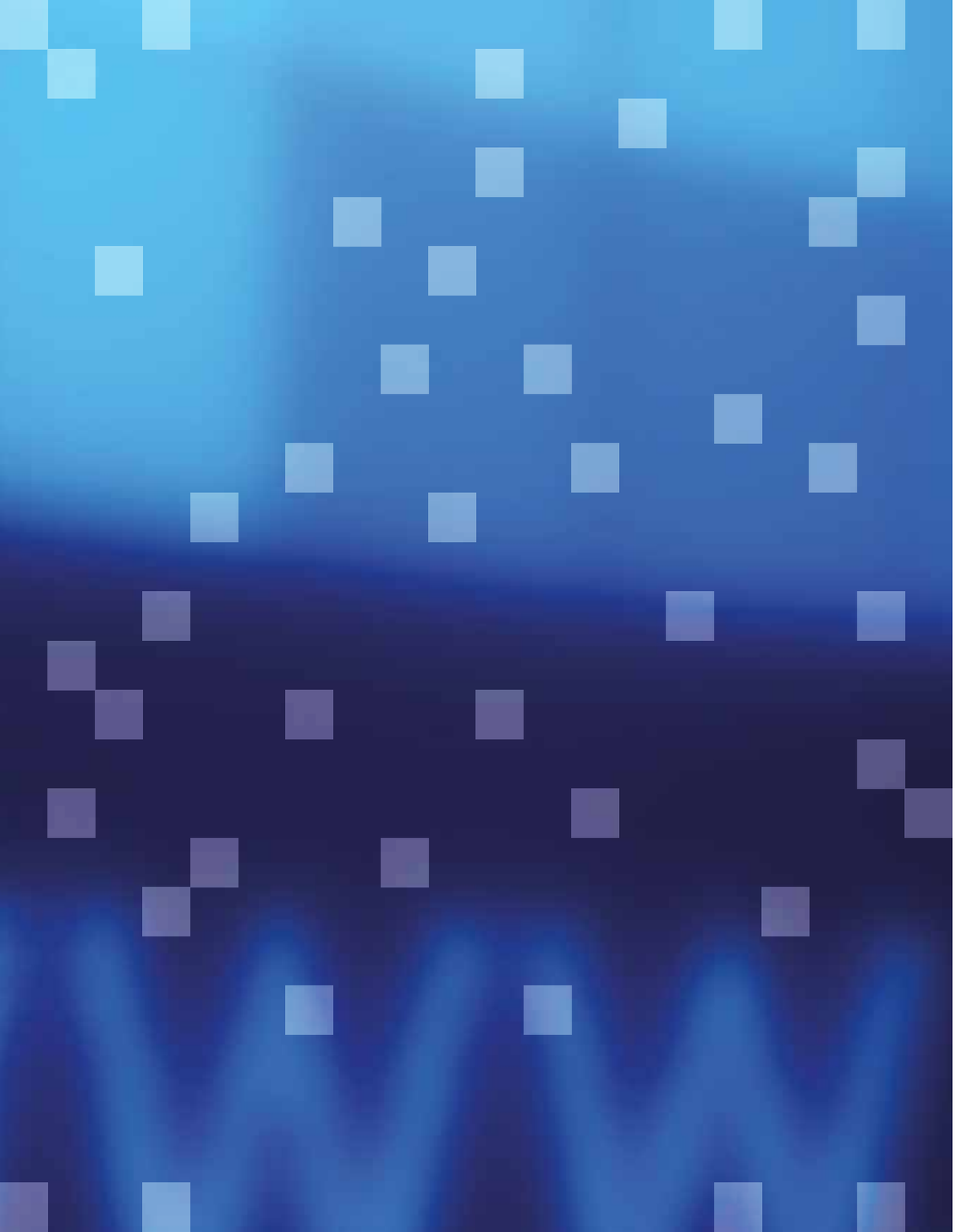
Vous tenez entre vos mains la deuxième version de la stratégie nationale en matière de cybersécurité approuvée par le gouvernement en date du 27 mars 2015. Le groupe de travail en charge des travaux de révision de la première version de 2012, présidé par le Haut-Commissariat à la Protection nationale et composé de représentants du Centre des technologies de l'information de l'État, du CERT gouvernemental, du Service des médias et des communications, du Ministère de l'Économie, du Centre de communications du gouvernement, du Service de renseignements, de la Police grand-ducale et de l'Armée, a tout d'abord procédé à l'analyse de l'impact de la stratégie adoptée en 2012 pour apporter ensuite les modifications qui se sont avérées nécessaires en fonction des conclusions de ladite analyse.

L'introduction de sept objectifs, complétés par des plans d'action se déclinant en des échéanciers précis et la détermination d'acteurs responsables pour la mise en œuvre des quelque quarante actions respectives, devra permettre une mise en œuvre adéquate de cette nouvelle stratégie nationale de cybersécurité d'ici fin 2017.

L'adaptation de ce document stratégique correspond aux axes définis en 2012 et reflète la volonté, voire la détermination du Luxembourg de doter le pays d'infrastructures de communication électroniques répondant aux standards internationaux de sécurité. Il s'agit là d'une condition préalable au développement de la société numérique, dans l'esprit de l'initiative « Digital Lëtzebuerg », car l'existence d'un environnement technologique sûr augmentera la confiance des citoyens et des entreprises dans ces technologies et permettra à terme de réaliser les objectifs de croissance économique que s'est fixés notre pays.

Xavier Bettel

SOMMAIRE



INTRODUCTION

Le programme gouvernemental de 2013 souligne l'importance de la cybersécurité pour le bien-être de la société. Conscient des risques liés aux technologies de l'information et de la communication (TIC), le « Cyber Security Board » (CSB) a développé une stratégie nationale en matière de cybersécurité en 2012. En date du 11 mars 2014, le CSB a chargé un groupe de travail, composé de représentants du Centre des technologies de l'information de l'État, du CERT gouvernemental, du Service des médias et des communications, du Ministère de l'Économie, du Centre de communications du gouvernement, du Service de renseignements, de la Police Grand-Ducale et de l'Armée, et opérant sous la direction du HCPN, d'élaborer une nouvelle version de ladite stratégie.

La cybersécurité est devenue un actif critique pour l'attractivité de notre économie. Pour cette raison, le gouvernement est déterminé à revoir de façon récurrente sa stratégie, de tenir à jour ses outils de gouvernance et de veiller à rester souverain dans certains services critiques liés à la sécurité.

Le gouvernement est conscient que la sécurité de l'information est un défi sociétal qu'il faut adresser en commun en adoptant les comportements adéquats, en mettant en place des mesures organisationnelles et techniques efficaces et efficientes tout en respectant les principes de proportionnalité et de nécessité.

Le gouvernement promeut la collaboration nationale et internationale, et est déterminé à démocratiser la sécurité de l'information en identifiant les synergies potentielles tout en réduisant les coûts ainsi que la complexité des procédures pour toutes les parties prenantes.

ÉTAT DES LIEUX DE LA STRATÉGIE DE CYBERSÉCURITÉ I

La stratégie de cybersécurité I prévoit une révision régulière de ses procédures. Le présent chapitre est dédié à cette tâche.

ÉTAT DES LIEUX DE LA STRATÉGIE DE CYBERSÉCURITÉ I

La stratégie de cybersécurité I prévoit une révision régulière de ses procédures. Le présent chapitre est dédié à cette tâche.

Axe 1 : Assurer la protection opérationnelle des infrastructures et systèmes de communication et de traitement de l'information

Volet opérationnel préventif

Le Luxembourg dispose de nombreuses initiatives dans le domaine de la prévention. Ces initiatives sont coordonnées par le « Cyber Security Board » (CSB) et exécutées pour la grande majorité par des acteurs publics. Dans le domaine préventif, une priorité a été accordée aux mesures organisationnelles de sécurité :

- Le gouvernement a identifié l'analyse des risques comme une priorité. En effet, ce n'est que suite à une telle analyse qu'une entité pourra identifier les mesures organisationnelles et techniques nécessaires. C'est elle qui veille à ce que les mesures mises en place respectent le principe de proportionnalité et de nécessité. Pour cette raison, CASES a développé une approche d'analyse des risques optimisée, basée sur une taxonomie commune, profitant des bases de connaissances sectorielles et offrant un grand potentiel synergétique : la méthodologie d'analyse des risques optimisée MONARC.

- CTIE, GOVCERT et CIRCL ont procédé à des analyses de risques internes.

- Un inventaire des bases de données traitant des données personnelles sous la responsabilité de l'État a été compilé par le GT « Base de données » du CSB.

- Le CSB a chargé un groupe de travail « Mobile devices » d'élaborer une proposition pour équiper les membres du gouvernement d'appareils de communication portables sécurisés. Les conclusions ont été présentées au CSB.

- Au niveau du traitement des risques, CASES a développé plusieurs guides de bonnes pratiques qui sont mis à disposition de toutes les entités concernées.

- Au niveau de l'identification des menaces, des outils d'échange d'information d'indicateurs de compromission ont été développés et mis à disposition de toutes les parties concernées.

Plusieurs acteurs nationaux (CSSF, ILR, CNPD, ILNAS et HCPN à l'avenir) exigent de leur constituante une analyse des risques réalisée suivant des critères spécifiques aux secteurs et aux missions attribuées. Le gouvernement doit s'efforcer à mieux harmoniser les approches préconisées ainsi que les référentiels d'exigence afin de pouvoir réduire l'effort individuel des entités régulées. La volonté du gouvernement consiste à faire de l'analyse des risques un outil de gouvernance qui respecte les principes de proportionnalité et de nécessité.

Volet opérationnel défensif

- Plan cyber : le gouvernement a adapté le plan d'intervention d'urgence en cas d'attaque contre les systèmes d'information ou de faille technique des systèmes d'information (« PIU Cyber ») en date du 19 mars 2014. Ce plan est régulièrement peaufiné lors des exercices cyber européens auxquels le Luxembourg participe activement.

  Le « PIU Cyber », élaboré sous la direction du HCPN, définit l'action du gouvernement en cas de problèmes d'envergure au niveau des systèmes d'information du secteur public et/ou du secteur privé, risquant d'entraîner un dysfonctionnement majeur, voire une indisponibilité de ces systèmes, qui menacerait les intérêts vitaux ou les besoins essentiels de tout ou partie du pays ou de la population du Grand-Duché. Rappelons que les incidents de routine sont gérés par les CERT opérationnels.

  Le plan détermine d'abord les organes de gestion de crise, tels que la cellule de crise, la cellule opérationnelle, la cellule d'évaluation du risque cyber et la cellule communication/information. Il fixe ensuite le déroulement de la diffusion d'alerte des autorités et de l'information au public, les mesures d'urgence, les actions y relatives ainsi que les responsables et acteurs respectifs. Lors de la mise en œuvre des différentes mesures de prévention et de protection, les ministères, administrations et services de l'État peuvent se faire assister par le CERT gouvernemental (axé prioritairement sur le secteur public et infrastructures critiques) et, en cas de besoin, par le CIRCL (axé prioritairement sur le secteur privé).

- En complément au CIRCL, qui consiste en un CERT dédié au secteur privé et aux communes, plusieurs CERT sectoriels privés et publics ont été créés : GOVCERT.LU pour le gouvernement et les infrastructures critiques, RESTENA-CSIRT en charge du secteur de l'éducation et de la recherche, ainsi que HealthNet-CSIRT couvrant le secteur de la santé. Il appartient à ces CERT de soutenir leur constituante respective.

- De même, en vue d'augmenter l'attractivité de la place économique, les CERT luxembourgeois offrent des services spécialisés dans le domaine de la sécurité de l'information :
  - Outils destinés à la réalisation d'indicateurs de santé des réseaux luxembourgeois. Il s'agit notamment des projets de BGP-Ranking[1] et de passive DNS[2] qui permettent une gestion plus efficace et rapide d'incidents.
  - Outils destinés à l'échange d'indicateurs de compromissions propres aux menaces estimées dangereuses, dont la plateforme MISP et l'outil d'analyse dynamique DMA[3]. Ces indicateurs permettent à toutes les entités concernées de détecter d'éventuels incidents dans leurs réseaux.
  - Outils destinés à fournir aux parties intéressées des informations individualisées concernant les vulnérabilités par rapport aux produits qu'elles utilisent.

Axe 2 : Moderniser le cadre légal

« Veille juridique »

Le cadre légal comporte plusieurs niveaux, à savoir :

- au niveau national :

Des réunions régulières ont lieu entre le Parquet, le GOVCERT, la Police grand-ducale, le RESTENA-CSIRT, le CIRCL, le Ministère de l'Économie, le SRE et la CNPD afin d'échanger sur l'évolution des menaces et discuter d'éventuelles solutions.

À cet égard, il convient de relever la loi du 18.7.2014 portant sur :

- l'approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001 ;

- l'approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à :
  - l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003 ;
  - la modification du Code pénal ;
  - la modification du Code d'instruction criminelle ;
  - la modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

1 http://circl.lu/ projects/#bgp-ranking
2 http://circl.lu/services/passive-dns/
3 http://circl.lu/services/dynamic-malware-analysis/

Suite à la ratification de la convention de Budapest en août 2014, des adaptations du cadre légal luxembourgeois ont été faites. Un article reprenant tous les textes en cause a été publié dans le journal des tribunaux luxembourgeois[4].

Par ailleurs, le gouvernement, conjointement avec la CNPD, a étudié la possibilité de créer une plateforme logicielle qui permettrait à toutes les entités concernées de réaliser des PIA (« Privacy Impact Assessment »), comme demandé par les textes européens sur la protection des données à caractère personnel.

- au niveau communautaire :

Des avis et des propositions de textes ont été rédigés concernant des projets de directives élaborés par les organes communautaires compétents (EFMS ; FOP). À titre d'exemple, citons la directive 2013/40/UE du Parlement et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil du 24 février 2005 ou encore la proposition de directive du Parlement et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux de l'information dans l'Union.

Axe 3 : Développer la coopération nationale et internationale

La coopération nationale et internationale en matière de cybersécurité a connu une attention particulière au Luxembourg au cours des dernières années. À titre d'exemple, citons :

- La participation active aux exercices Cyber Europe 2012 et 2014 de l'Union européenne.

- La participation aux exercices Cyber Coalition CC13 et CC14 de l'OTAN en tant qu'observateur.

- La signature d'un « MoU » concernant la cybersécurité entre le HCPN et le « Cyber Defence Management Board (CDMB) » de l'OTAN.

- La désignation de deux points de contact concernant la cybersécurité au GOVCERT.LU dans le cadre du « MoU » avec l'OTAN.

4 The ratification of the Budapest Convention on Cybercrime by Luxembourg; Max Braun; journal of Luxembourg courts; No. 35, 5th October 2014.

- La mise en place d'un service 24h/24 et 7j/7 chargé d'assurer la prise de contact nationale et internationale pour le traitement d'urgences informatiques à caractère de cyber crise dont la gestion est assurée en collaboration avec le « NATO Computer Incident Response Capability » sur leur plateforme de partage d'informations sur des incidents cyber.

- La participation du CIRCL au développement d'un logiciel facilitant le partage d'informations sur les indicateurs de compromission : « Malware Information Sharing Platform (MISP) ». Ledit logiciel fut mis à la disposition de tous les alliés de l'OTAN et utilisé par presque tous les CERT en Europe.

- La participation active des CERT luxembourgeois dans les réseaux internationaux (TF-CSIRT, FIRST, etc.) ; les CERT luxembourgeois jouissent d'une très bonne renommée.

- La collaboration du Luxembourg avec l'Allemagne et la Belgique au niveau de la gestion des risques.

- L'instauration d'une cellule d'évaluation du risque cyber (CERC) par le PIU Cyber, cadrant la coopération notamment entre le HCPN, le CTIE, le SRE, et les CERT concernés en cas d'incident significatif. Ladite cellule d'évaluation est présidée par le GOVCERT.LU.

- La participation du GOVCERT.LU à des conférences réunissant les GOVCERT de l'Europe.

- La participation des CERT luxembourgeois à différents projets de recherche européens, notamment dans le domaine du « phishing » et de la lutte contre les « botnets ».

Axe 4 : Informer, éduquer et sensibiliser sur les risques encourus

Les objectifs de sensibilisation, d'éducation et d'information des utilisateurs finaux

Le Luxembourg est conscient que la sensibilisation et l'éducation sont essentielles pour que toutes les personnes concernées adoptent les comportements adéquats dans le domaine de la sécurité de l'information. Nombreuses sont les menaces qui visent à exploiter des vulnérabilités humaines. Il est primordial de réduire ces vulnérabilités en sensibilisant et en formant toutes les personnes concernées :

- En ce qui concerne les utilisateurs/internautes, les actions suivantes ont été entreprises :

  - Sites Internet existants, respectivement à venir :
    - www.govcert.lu
    - www.circl.lu
    - www.bee-secure.lu
    - www.cases.lu
    - www.police.lu
    - Portail gouvernemental sur la cybersécurité

  - Articles récurrents dans la presse (de la part du CIRCL, CASES, BEE SECURE ou de la Police grand-ducale, en fonction des cas)
  - Campagnes de sensibilisation annuelles de CASES et de BEE SECURE
  - Alertes (de la part du CIRCL, de CASES, BEE SECURE ou de la Police grand-ducale, voire du Ministère de l'Économie en fonction des cas)
  - Des rapports et communications plus techniques à destination des utilisateurs avertis et informaticiens de la part du GOVCERT et du CIRCL[5]

- Pour ce qui est des élèves, des parents, des éducateurs et des professeurs, les autorités ont organisé des :

  - Formations obligatoires BEE SECURE (deux heures dans toutes les classes de 7e de l'enseignement secondaire et secondaire technique)
  - Formations facultatives BEE SECURE (deux heures dans les classes de l'enseignement fondamental)
  - Soirées de parents d'élèves (avec un peu de succès)
  - Formations pour éducateurs (avec un succès moyen)
  - Formations pour professeurs (avec peu de succès)

Le gouvernement est déterminé à étendre son offre de formations et de sensibilisation. Vu le grand besoin en experts IT durant les prochaines décennies, le

5 http://circl.lu/pub/

gouvernement poursuit ses efforts à stimuler l'intérêt de jeunes gens (garçons et filles) pour la thématique de l'informatique et de la programmation.

- Les fonctionnaires et employés publics bénéficient de :

  - Formations facultatives CASES (trois heures organisées par l'INAP dans ses propres locaux). Il s'agit de trois formations par an. Pour l'instant, cette formation n'est pas obligatoire pour l'ensemble des nouveaux agents de l'État.
  - Formations facultatives CASES (trois heures organisées par l'INAP dans les locaux de l'administration). Cette formation connaît un succès moyen : 4-5 administrations par an y font appel.
  - Formations spécialisées CASES (très peu de succès).
  - Formations du GOVCERT destinées aux correspondants informatiques.
  - Alertes et informations diffusées par le GOVCERT.
  - Publication de la Charte Informatique du CTIE.

Très peu de demandes émanent de petites et moyennes entreprises. Le gouvernement a mis en place un service de sensibilisation à prix réglementé et très avantageux, presté par des experts privés labellisés CASES.

Les objectifs de sensibilisation, d'éducation et d'information des prestataires de services

Bon nombre des acteurs soumis à un régime de régulation sont obligés de suivre des formations. Une bonne vue d'ensemble n'est cependant pas encore disponible.

Les obligations peuvent provenir :

- de standards de certification comme l'ISO/IEC 27001 (ISO/IEC 27002) auxquels se soumettent certaines entreprises ;

- des exigences des régulateurs :
  - la CSSF pour certains types de PSF ainsi que pour les instituts bancaires ;
  - l'ILNAS pour les Infrastructures à Clés Publiques (ICP) ainsi que pour les prestataires de services de dématérialisation et d'archivage électronique ;
  - la CNPD pour la sécurité des traitements (art. 22 et art. 23 de la loi du 27 juillet 2007).

GOVCERT.LU, CIRCL et CASES offrent des formations aux entreprises. Dans le cas de CASES, ces formations sont payantes et elles sont prestées par des intervenants labellisés d'entreprises spécialisées.

CASES met à disposition des entreprises un catalogue de services de gouvernance et d'analyse des risques, ainsi qu'une plateforme incluant les outils y associés :

http://my.cases.lu/.

Dans le cadre de la coordination et de la réponse aux incidents informatiques, le CIRCL met à disposition des entreprises, et plus particulièrement des équipes informatiques, des services et des outils proactifs dans le but de rendre plus efficace et efficiente la sécurité opérationnelle et réactive :

http://circl.lu/services/ et http://circl.lu/projects/.

Axe 5 : Mettre en place des normes et des standards contraignants

- Un nouveau régulateur au niveau des opérateurs d'infrastructures critiques :

Le projet de loi relative à la protection nationale prévoit l'instauration du Haut-Commissariat à la Protection nationale comme nouveau régulateur transversal, compétent pour tous les opérateurs d'infrastructures critiques dans les domaines de la sécurité physique ainsi que de la sécurité des systèmes d'information. Ainsi, les opérateurs seront à l'avenir tenus de mettre à la disposition du Haut-Commissariat à la Protection nationale toutes les données sollicitées aux fins du recensement, de la désignation et de la protection des infrastructures critiques. Ces données comprennent toutes les informations qui sont nécessaires dans le contexte de la prévention ou de la gestion d'une crise.

Les données relatives à l'infrastructure critique faisant l'objet d'un enregistrement, d'une communication, d'une déclaration, d'un recensement, d'un classement, d'une autorisation ou d'une notification imposés par la loi ou par la réglementation afférente sont communiquées au Haut-Commissariat à la Protection nationale, sur sa demande, par les départements ministériels, administrations et services de l'État qui détiennent ces données.

Le propriétaire ou opérateur d'une infrastructure critique est tenu d'élaborer un plan de sécurité et de continuité de l'activité, qui comporte les mesures de sécurité pour la protection de l'infrastructure. Le Haut-Commissariat à la Protection nationale adresse au propriétaire ou à l'opérateur d'une infrastructure critique des recommandations concernant ces mesures de sécurité qui permettent d'en améliorer la résilience et de faciliter la gestion d'une crise.

Le propriétaire ou opérateur d'une infrastructure critique est par ailleurs tenu de désigner un correspondant pour la sécurité, qui exerce la fonction de contact pour les questions liées à la sécurité de l'infrastructure avec l'autorité compétente.

Le propriétaire ou opérateur d'une infrastructure critique doit finalement notifier au Haut-Commissariat à la Protection nationale tout incident ayant eu un impact significatif sur la sécurité et la pérennité du fonctionnement de l'infrastructure.

- La gestion des PSDC (prestataires de services de dématérialisation et de conservation)

Conclusions de l'analyse de la stratégie de cybersécurité I

Lors de l'élaboration de la stratégie de cybersécurité I, l'organe compétent au niveau interministériel était le CSB. En ce qui concerne l'exécution des tâches, il a recours à la création de groupes de travail ad hoc au sein du CSB, respectivement à l'attribution de missions ponctuelles à des membres du CSB.

En tout état de cause, si le CSB constitue l'enceinte appropriée pour les réflexions et décisions d'ordre stratégique, il ne semble guère adapté pour exécuter la multitude des travaux requis dans le cadre de la mise en œuvre d'une stratégie de cybersécurité. Ces tâches pourraient être mieux coordonnées par un organe permanent à vocation opérationnelle.

C'est donc sur l'encadrement de la nouvelle stratégie et les modalités de la mise en œuvre qu'il faudra mettre l'accent à l'avenir, plutôt que sur une refonte de fond en comble des objectifs et des axes qui restent pertinents.

La stratégie de cybersécurité I à l'image d'autres stratégies nationales

La majorité des nations se sont dotées d'une stratégie de cybersécurité. Plusieurs organisations internationales[6], entreprises de conseil et universités ont compilé des comparaisons. Pour la présente analyse, deux documents ont été retenus, en l'occurrence la stratégie néerlandaise (NCSS2[7]) et une comparaison des stratégies des pays membres de l'Union européenne éditée par l'ENISA[8].

« ENISA National Cyber Security Strategies check-list »

Une analyse de la stratégie de cybersécurité de 2012 à l'aide d'un questionnaire de l'ENISA fait apparaître que le texte actuel comporte deux faiblesses qui méritent d'être remédiées à l'avenir : d'une part, la définition du terme cybersécurité et d'autre part, le dialogue avec le monde académique et industriel.

La stratégie néerlandaise

La deuxième version de la stratégie néerlandaise « NCSS2 » de 2013 s'aligne sur les objectifs de la première version et développe davantage le volet de la mise en œuvre. L'accent est mis sur la coopération avec le secteur privé ainsi que sur la responsabilisation de tous les acteurs (gouvernement, citoyens et acteurs économiques). Un plan d'action commun avec un échéancier sur deux années est présenté de manière détaillée dans le nouveau texte.

Conclusions de la comparaison

L'analyse comparative fait ressortir qu'il serait utile de développer plus amplement les éléments suivants dans le nouveau texte :

- Introduire une définition de la cybersécurité ;
- Engager le dialogue avec le monde académique et avec l'industrie ;
- Introduire la notion de cyberdéfense ;
- Charger formellement un organe de la coordination de la mise en œuvre de la nouvelle stratégie ;
- Mettre en place des plans d'action.

6 The OECD, OSCE, ENISA (European Network and Information Security Agency)
7 NCSS2: National Cyber Security Strategy 2
8 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

STRATÉGIE DE CYBERSÉCURITÉ II

Le gouvernement reconnaît que la sécurité de l'information ne doit pas être considérée comme un fardeau, mais plutôt comme une opportunité. Il s'agit de démocratiser la sécurité de l'information en promouvant la collaboration tout en réduisant la complexité et les coûts de toutes les parties prenantes.

STRATÉGIE DE CYBERSÉCURITÉ II

Définition de la cybersécurité[9]

« On entend par cybersécurité l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de sécurité sont les suivants :

- *Disponibilité ;*
- *Intégrité, qui peut englober l'authenticité et la non-répudiation ;*
- *Confidentialité. »*

9 Recommendation ITU-T X.1205 following UN resolution 181 (Guadalajara/2010)

Objectifs de la stratégie de cybersécurité II

De manière générale, cette stratégie de cybersécurité a pour but de protéger les acteurs publics et privés contre les cybermenaces tout en favorisant le développement économique et social dans le cyberespace.

Le gouvernement reconnaît que la sécurité de l'information ne doit pas être considérée comme un fardeau, mais plutôt comme une opportunité. Il s'agit de démocratiser la sécurité de l'information en promouvant la collaboration tout en réduisant la complexité et les coûts de toutes les parties prenantes.

Le gouvernement compte atteindre ce but en définissant les objectifs et les plans d'action suivants :

Objectif 1 : Renforcer la coopération nationale

Le besoin d'une approche globale soulève l'enjeu de la coordination gouvernementale afin que tous les acteurs concernés puissent travailler ensemble de manière cohérente, en évitant la duplication des fonctions et en favorisant le développement de synergies et le regroupement des initiatives afin de maintenir, voire de développer une image de qualité aussi bien à l'intérieur du pays qu'au niveau international.

Sur le plan national, une coopération accrue entre tous les acteurs concernés constitue un préalable à une mise en œuvre cohérente de la stratégie. La méthodologie de gouvernance doit se baser sur les concepts définis au niveau de la gestion des risques, tels que proposés par l'ISO/IEC 27005 :2011, à savoir la définition du contexte, l'identification des risques, l'estimation des risques, l'évaluation des risques, le traitement, l'acceptation et enfin la communication des risques ; le tout dans une optique d'amélioration continue.

Un objectif important du gouvernement est d'augmenter l'attractivité de la place économique en instaurant des outils de gouvernance souples, flexibles et modernes. La gouvernance doit être orientée sur les risques.

Sont visés par cette démarche :

- Les organes étatiques (HCPN, GOVCERT, SRE, CTIE, Armée) ;
- Les autorités de poursuite (Police grand-ducale et Parquet) ;
- Les autorités nationales indépendantes concernées (ILR, CSSF, CNPD) ;
- Les acteurs sectoriels (CIRCL, RESTENA, CERT privés) ;
- Les partenariats public-privé.

La création d'une agence nationale de la sécurité des systèmes d'information (ANSSI), facilitera la mise en place des plans d'action envisagés.

La création d'une agence nationale de la sécurité des systèmes d'information (ANSSI), décidée par le gouvernement en adoptant le projet d'arrêté grand-ducal y relatif dans sa séance du 21 janvier 2015, facilitera la mise en place des plans d'action envisagés.

L'ANSSI a pour mission de définir les politiques et les lignes directrices en matière de sécurité de l'information classifiée et non classifiée, de veiller à ce que des normes et standards soient définis, que les mesures nécessaires concernant la sécurité des systèmes d'information soient mises en place et que leur application soit garantie, de certifier les moyens de traitement de l'information non classifiée (systèmes, services, infrastructures numériques), et enfin d'assurer la fonction de CERT national et l'hébergement du CERT gouvernemental (GOVCERT.LU). Elle rassemblera sous une seule ligne de commandement tous les acteurs actifs dans le domaine de la cybersécurité en ce qui concerne le secteur public et les infrastructures critiques, et sera appelée à coopérer avec tous les acteurs convenant du secteur privé, si nécessaire par le biais d'accords de coopération formalisés.

Plan d'action objectif 1

#	Action	Remarque	Responsable, Acteur(s)	Échéancier
1	Création d'une ANSSI		HCPN, PGD, SMILE, GOVCERT, CTIE/CCG, SRE/ANS	2015
2	Identification et allocation des ressources humaines et budgétaires nécessaires au bon fonctionnement d'une ANSSI		HCPN, Ministère d'État	2015-2016
3	Mettre en place un accord de coopération entre l'ANSSI et le SRE	Formaliser l'échange d'information et la coopération entre les deux entités	ANSSI, SRE	2015
4	Mettre en place un accord de coopération entre l'ANSSI et SMILE	Idem	ANSSI, SMILE	2015
5	Favoriser la coopération avec les FSI		ANSSI, CERT	2015-2017
6	Fusion des opérateurs CTIE et CCG	Création d'un opérateur unique pour les réseaux classifiés et non classifiés de l'État	Ministère de la Fonction publique et de la Réforme administrative, CTIE, CCG	2015
7	Mise en place et exploitation d'un site unique sur la thématique de la cybersécurité		ANSSI, GOVCERT, SMILE, CTIE, SIP, SMC	2015-2016
8	Clarifier les missions du CSB suite à la création d'une ANSSI		CSB, SMC	2015
9	Adopter un système de gestion des risques liés à la sécurité des systèmes d'information basé sur la norme ISO/IEC 27005:2011		ANSSI, SMILE	2015-2016
10	Mise en place d'un groupe de travail « Gouvernance » aux fins de parfaire le modèle de gouvernance au niveau national		CSB	2015-2016

Objectif 2 : Renforcer la coopération internationale

Il est impératif de disposer d'un tissu de collaboration actif avec la communauté internationale.

La nécessité d'une coopération, tant sur le plan national entre tous les acteurs impliqués que sur le plan international, découle du caractère supranational des réseaux de communication. Il est dès lors impératif de disposer d'un tissu de collaboration actif avec la communauté internationale, en particulier au niveau des CERT et des forces de l'ordre. Le but de cette coopération est d'aboutir à un échange d'informations et d'entraide entre les services compétents des différents pays et au sein des enceintes internationales, ainsi qu'à la création d'approches et de solutions communes.

La coopération sur le plan international ne doit cependant pas se limiter à l'échange d'informations opérationnelles. Elle doit aussi porter sur les aspects méthodologiques et les outils dans le domaine de la gestion d'incidents, sur les systèmes de détection d'anomalies, les systèmes d'alerte rapide, la gestion des risques, les politiques de sécurité, la sensibilisation et l'éducation.

Sur le plan international, une collaboration peut prendre la forme de contacts bilatéraux ou encore s'appuyer sur des échanges multilatéraux au sein des institutions/groupes/communautés, tels que (liste non exhaustive) :

- Le Benelux
- L'Union européenne :
  - ENISA, NIS platform, EFSM et autres groupes de haut niveau
  - TF-CSIRT, EGC, CERT-Verbund, CLUSIx, clubs R2GS et autres groupes techniques
- L'Allemagne : BSI
- La Suisse : ISB
- L'Autriche : Ministère des Finances, A-SIT
- La France : ANSSI
- Le Conseil de l'Europe
- L'OTAN/CCDCoE/CDMB
- L'OCDE/OSCE
- Europol/Interpol/FBI
- FIRST (et autres communautés spécialisées du monde des CERT)

Plan d'action objectif 2

#	Action	Remarque	Responsable, Acteur(s)	Échéancier
1	Établir un inventaire de tous les accords, collaborations et participations au niveau bi-, voire multinational		CSB	2015
2	Identifier les bonnes pratiques en matière de coopération (en Europe et à l'international) et participer aux groupes, respectivement établir des partenariats clés		ANSSI, CERT, SRE, Armée	2015-2017

Objectif 3 : Augmenter la résilience de l'infrastructure numérique

La sécurité de l'infrastructure numérique réside dans sa capacité à garantir un certain niveau de disponibilité, d'intégrité et de confidentialité.

La sécurité de l'infrastructure numérique réside dans sa capacité à garantir un certain niveau de disponibilité, d'intégrité et de confidentialité. La sécurité de l'infrastructure numérique porte un coût et nécessite le savoir-faire d'experts. Il est pour cette raison avisé de profiter du mieux possible des synergies qui se présentent et de mutualiser autant que possible l'analyse des risques, l'établissement d'un état des lieux et la mise en place de mesures destinées à traiter les risques ainsi que les incidents.

Volet opérationnel préventif

Le gouvernement doit inciter toutes les parties concernées, en respectant le principe de proportionnalité et de nécessité, à mettre en place des mesures préventives. Des informations, formations, guides de bonnes pratiques ainsi que des méthodologies seront mis à disposition des parties prenantes. Le système de gouvernance mis en place par le gouvernement aidera tant les acteurs privés et publics que les régulateurs à identifier les traitements nécessaires, respectivement à définir les référentiels d'exigences dans le domaine de la cybersécurité. Les principes de nécessité et de proportionnalité sont essentiels au respect des besoins d'économicité, qui elle a un grand impact sur l'attractivité de la place économique.

Dans le domaine préventif, il est possible de capitaliser sur un grand nombre de synergies :

- Les outils de gouvernance pour l'analyse, la gestion des risques, ainsi que les métriques de menaces et de vulnérabilités (mis à disposition des CERT) peuvent être utilisés aussi bien par des régulateurs que des acteurs privés et publics.
- Les référentiels d'exigences élaborés par les régulateurs seront harmonisés grâce à l'utilisation d'une taxonomie et d'une méthodologie commune.
- Au niveau de la gestion des risques, des approches contextualisées seront proposées qui réduiront substantiellement l'effort et l'investissement dans des analyses des risques.
- Au niveau du traitement des risques, il est prévu de mutualiser certaines mesures de sécurité.
- Au niveau des CERT, des veilles au niveau des menaces et vulnérabilités sont faites. Le résultat de ces veilles est mis à disposition de tous les acteurs luxembourgeois et utilisé au niveau des outils de gouvernance et de gestion des risques.

Volet opérationnel défensif

Il faut partir du constat qu'aucun système d'information, quel que 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, pour traiter l'incident repéré de manière efficace et pour rétablir l'opérabilité des systèmes affectés.

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

- affiner les aspects opérationnels dans l'exécution du « PIU Cyber » pour les incidents cyber significatifs ;
- réaliser des simulations et/ou exercices sectoriels et nationaux portant sur la réponse en cas d'incident affectant la sécurité des systèmes d'information et de communication sensibles ou critiques, et participer aux exercices internationaux dans ce domaine ;
- améliorer la coopération entre les CERT lors de la prise en charge des incidents de routine par le biais d'accords de coopération et de la mise en place d'une plateforme d'échange d'informations.

Plan d'action objectif 3

#	Action	Remarque	Responsable, Acteur(s)	Échéancier
1	Proposer des outils de gestion de risques sectoriels		ANSSI, CASES, recherche	
2	Élaborer des bonnes pratiques sectorielles		ANSSI, CASES, CERT	
3	Intensifier les efforts de mutualisation des mesures de sécurité		ANSSI, ILR, CERT, secteur privé	2015-2017
4	Élaborer des indicateurs de performance au niveau de la sécurité, créer une veille de ces indicateurs		CERT	2015-2017
5	Mettre en place des outils et procédures détaillées pour la gestion des incidents significatifs	Mise en œuvre du « PIU Cyber »	HCPN, ANSSI, CIRCL, GOVCERT, CTIE, PGD, SRE	2016
6	Développer une doctrine militaire en matière de cybersécurité		EMA	2016
7	Participation à la préparation et l'exécution de l'exercice « Cyber Europe 2016 » de l'UE		HCPN, CERT, secteur privé	2016
8	Participation à la préparation et l'exécution de l'exercice « Cyber Coalition 2015 » de l'OTAN		EMA, HCPN, CERT	2015
9	Réaliser des exercices nationaux incluant le secteur privé		HCPN, CERT	2016
10	Élaborer des bonnes pratiques, méthodes et outils pour la promptitude, à différents niveaux (infrastructures critiques, opérateurs/ prestataires télécom, grandes entreprises, administrations, PME)		ANSSI, CERT	2015-2017

Objectif 4 : Combattre la cybercriminalité

L'évolution rapide des infrastructures numériques génère sans cesse de nouvelles menaces. Il est dès lors primordial d'évaluer régulièrement si les bases légales en vigueur sont toujours adaptées et si elles permettent de poursuivre et de sanctionner les nouvelles formes de cybercriminalité.

La veille juridique doit identifier les contradictions ou non-concordances au niveau des lois, règlements et circulaires, et veiller à harmoniser l'approche de tous les acteurs étatiques.

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 en partie dans un pays et en partie dans un autre, voire dans un troisième, alors que l'auteur 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.

L'évolution rapide des infrastructures numériques génère sans cesse de nouvelles menaces. Il est dès lors primordial d'évaluer régulièrement si les bases légales en vigueur sont toujours adaptées et si elles permettent de poursuivre et de sanctionner les nouvelles formes de cybercriminalité.

Plan d'action objectif 4

#	Action	Remarque	Responsable, Acteur(s)	Échéancier
1	Poursuivre les travaux du groupe de travail « Cybercrime »		Parquet, PGD, ANSSI, CIRCL, GOVCERT.LU, RESTENA CSIRT, CNPD, SRE	2015-2017
2	Création d'un GT juridique avec les missions suivantes : • Analyse du cadre légal actuel • Analyse des dispositions en vigueur à l'étranger • Transposition des directives européennes et adaptations du cadre légal national		Ministère de la Justice, Parquet, SMC, CNPD, ANSSI, PGD, SRE	2015-2017
3	Poursuivre la coopération internationale dans la lutte contre la cybercriminalité (EC3 Europol)	But : • Faciliter les actions communes dans la lutte contre la cybercriminalité • Centre de fusion des informations	PGD	2015-2017
4	Poursuivre la coopération avec l'EUCTF (« European Cybercrime Task Force »)		PGD	2015-2017
5	Poursuivre la coopération avec Interpol	via Europol	PGD	2015-2017
6	Poursuivre la coopération avec le FBI	Via l'officier de liaison à Bruxelles	PGD	2015-2017

Objectif 5 : Informer, former et sensibiliser sur les risques encourus

La sensibilisation des secteurs privé et public sur les risques encourus et les moyens de se protéger constitue un élément essentiel de la stratégie, qui 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 auprès de tous les acteurs concernés la prise de conscience qu'ils peuvent se protéger amplement contre les menaces et les dangers potentiels en adoptant un comportement responsable.

À 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. À titre d'exemple : la publication et l'application tardives de rectificatifs, la non-observation des procédures et 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, plus spécifiquement :
  - les enfants et les jeunes ;
  - les élèves, les parents, les éducateurs, les professeurs ;
  - les fonctionnaires et employés publics ;
  - les employés privés ;
  - les indépendants et autres professionnels ;
  - les informaticiens, spécialistes et autres experts TIC.

- Les décideurs et cadres à responsabilités
  - du secteur privé.

- Les prestataires de services :
  - d'hébergement physique (data centres) ;
  - de communication ;
  - de « cloud computing » ;
  - de signature électronique ;
  - de dématérialisation et d'archivage électronique ;
  - d'intégration et de fournitures d'équipements TIC ;
  - de consultance TIC ;
  - de sécurité de l'information.

- Les opérateurs des infrastructures critiques :
  - les décideurs ;
  - les opérateurs des infrastructures ;
  - les informaticiens ;
  - les employés/utilisateurs non avertis.

L'évolution permanente de la menace implique que les citoyens et les entreprises doivent régulièrement être tenus informés 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 permettront aux intéressés d'actualiser leurs connaissances, que ce soit au niveau des menaces potentielles ou des moyens de protection.

L'évolution permanente de la menace implique que les citoyens et les entreprises doivent régulièrement être tenus informés 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.

Plan d'action objectif 5

#	Action	Remarque	Responsable, Acteur(s)	Échéancier
1	Rendre la formation CASES obligatoire pour chaque nouveau fonctionnaire		CSB et MFPRA, CASES, prestataire de services externe	2015
2	Étendre le programme de formation de CASES aux aspects méthodologiques		CASES, prestataire de services externe	2016
3	Introduire des formations obligatoires au niveau de l'enseignement primaire et secondaire		CASES, Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse	2016
4	Établir un inventaire des obligations de formation incombant aux prestataires de services		CASES, associations professionnelles du domaine des TIC et/ou de la sécurité de l'information	2015-2016
5	Élaborer un programme de formation attrayant pour les PME		CASES, Chambre des métiers	2015-2016
6	Promouvoir les formations du post-secondaire dans le domaine de la sécurité		UNI, MESR	2015-2017
7	Élaborer un programme de sensibilisation/formation pour décideurs		CASES, Chambre des métiers, Chambre de commerce, Fedil	2015-2016
8	Élaborer un programme de formation pour opérateurs d'infrastructures critiques		ANSSI, GOVCERT, CASES, opérateurs IC	2016-2017

Objectif 6 : Mettre en place des normes, standards, certificats, labels et référentiels d'exigences pour l'État et les infrastructures critiques

La sécurité de l'information requiert un comportement adapté des acteurs ainsi que la mise en place de mesures organisationnelles et techniques appropriées. Avant la mise en place de mesures préventives de sécurité, il faut procéder à une analyse des risques pour pouvoir évaluer les pertes potentielles liées à une compromission de la disponibilité, de l'intégrité ou encore de la confidentialité des actifs. Il faut également considérer 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'État exige l'existence de méthodes d'analyse de risques, 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.

La mise en œuvre cohérente et efficace de systèmes sécurisés au sein de l'État exige l'existence de méthodes d'analyse de risques, de politiques et de standards de sécurité cohérents et adaptés aux contextes.

Dans le même ordre d'idées, les opérateurs d'une infrastructure critique ou sensible seront invités à se conformer à un certain nombre de référentiels, respectivement à viser une certification sectorielle pour prouver leur maturité au niveau sécuritaire.

Plan d'action objectif 6

#	Action	Remarque	Responsable, Acteur(s)	Échéancier
1	Analyse des risques pour les secteurs prioritaires		HCPN, ANSSI, SMILE	2015-2017
2	Mise en place de normes et standards SSI pour les réseaux classifiés et non classifiés du secteur public et des infrastructures critiques		ANSSI, HCPN	2015-2017
3	Établir un inventaire des standards et bonnes pratiques dans les différents secteurs		ANSSI, CSSF, ILR, CNPD, ILNAS	2015-2016

Objectif 7 : Renforcer la coopération avec le monde académique et de la recherche

L'Université et les centres de recherche publics spécialisés en ICT ont développé des compétences de pointe dans le domaine de la sécurité des systèmes d'information, du « big data » ainsi que dans l'utilisation des systèmes d'information en vue de contrôle de la qualité des services.

Il convient de mettre systématiquement ces compétences au service de l'amélioration de l'environnement cybersécurité national, tant par la recherche proprement dite que par l'intermédiaire de formations.

Dans ce même contexte, il faudra veiller à ce que ces compétences continuent à se développer en étroite concertation avec le secteur privé et les administrations gouvernementales, tout en favorisant la coopération internationale au niveau académique.

À moyen terme, des cursus universitaires ou modules de formation pourraient être développés à l'Université du Luxembourg, en concertation avec tous les acteurs tant privés que publics en vue d'adopter une réponse aux besoins en matière de cybersécurité, tout en prenant en considération les spécificités nationales.

Il faudra veiller à ce que ces compétences continuent à se développer en étroite concertation avec le secteur privé et les administrations gouvernementales, tout en favorisant la coopération internationale au niveau académique.

Plan d'action objectif 7

#	Action	Remarque	Responsable, Acteur(s)	Échéancier
1	Développer des protocoles et algorithmes cryptographiques		UNI, CRP	2015-2017
2	Développer un programme de formation cybersécurité		UNI, CRP	2015-2017

Mise en œuvre

La présente stratégie définit les objectifs qu'il importe d'atteindre dans les trois années à venir. Chaque objectif est complété par un plan d'action décrivant les mesures concrètes à mettre en œuvre suivant un calendrier déterminé, ainsi que les acteurs appelés à contribuer à leur mise en œuvre.

La stratégie de cybersécurité a vocation à évoluer dans le temps. Elle sera périodiquement révisée afin d'être adaptée aux nouvelles réalités.

La stratégie de cybersécurité a vocation à évoluer dans le temps. Elle sera périodiquement révisée afin d'être adaptée aux nouvelles réalités.

GLOSSAIRE

GLOSSAIRE

ANSSI
« Agence nationale de la sécurité des systèmes d'information » : autorité nationale en matière de sécurité des systèmes d'information classifiés et non classifiés installés et exploités par l'État et les opérateurs d'infrastructures critiques pour leurs besoins propres.

BEE SECURE stopline
Centre pour rapporter des contenus illicites et/ou préjudiciables en ligne.

CASES
« Cyberworld Awareness & Security Enhancement Services » : programme du groupement d'intérêt économique SMILE.

CC13
« Cyber Coalition » : exercice de cyberdéfense annuel de l'OTAN.

CCDCoE
« Cooperative Cyber Defence Centre of Excellence » : Centre d'excellence pour la cyberdéfense de l'OTAN à Tallinn (Estonie).

CDMB
« Cyber Defence Management Board » : organe de l'OTAN chargé des affaires relevant de la cyberdéfense de l'alliance.

CE2012
« Cyber Europe 2012 » : exercice biannuel de l'UE.

CERC
« Cellule d'Évaluation du Risque Cyber » : groupe d'experts en matière cyber constitué dans le contexte du « PIU Cyber ».

CERT
« Computer Emergency Response Team » : équipe prenant en charge des incidents de cybersécurité.

CIRCL
« Computer Incident Response Center Luxembourg » : CERT en charge des incidents cyber au niveau des secteurs privés et communaux, opéré par le groupement d'intérêt économique SMILE.

CNPD
« Commission Nationale pour la Protection des Données ».

CSB
« Cybersecurity Board » : créé par décision du Conseil de gouvernement le 18 juillet 2011. Le Cybersecurity Board luxembourgeois a la mission d'élaborer le plan stratégique national de lutte contre les cyberattaques. Il est présidé par le Ministre des Communications et des Médias.

CSIRT
« Computer Security Incident Response Team », synonyme de CERT.

CSSF
« Commission de surveillance du secteur financier ».

CTIE
« Centre des Technologies de l'Information de l'État ».

EC3
« European Cybercrime Centre ».

EFMS
« European Forum for Member States » on CIIP.

EMA
« État-Major de l'Armée ».

ENISA
« European Network and Information Security Agency ».

EUCTF
« European Cybercrime Task Force ».

FOP
« Friends of the Presidency ».

FSI
« Fournisseur de Services Internet ».

GOVCERT
« CERT gouvernemental » : CERT prenant en charge des incidents de cybersécurité du secteur public et des infrastructures critiques. Créé par l'arrêté grand-ducal du 30 juillet 2013 déterminant l'organisation et les attributions du Centre gouvernemental de traitement des urgences informatiques, aussi dénommé « Computer Emergency Response Team Gouvernemental ».

GT
« Groupe de travail ».

HCPN
« Haut-Commissariat à la Protection nationale ».

ICP
« Infrastructure de Clés Publiques » en l'occurrence LUXTRUST.

ILNAS
« Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et de la qualité des produits et services ».

ILR
« Institut Luxembourgeois de Régulation ».

MISP
« Malware Information Sharing Platform » : plateforme d'échange d'informations sur les logiciels malveillants.

MONARC
« Méthodologie d'analyse des risques de CASES ».

MoU
« Memorandum of Understanding » : accord de coopération.

NCSS2
« National Cyber Security Strategy 2 ».

PGD
« Police grand-ducale ».

PIU
« Plan d'Intervention d'Urgence ».

PSF
« Professionnels du Secteur Financier ».

RESTENA
« Réseau Téléinformatique de l'Éducation Nationale et de la Recherche ».

SMC
« Service des Médias et des Communications ».

SMILE
« Security Made In Lëtzebuerg » : g.i.e. opérateurs majeurs des initiatives gouvernementales BEE SECURE, CASES et CIRCL. SMILE est constitué de trois membres : l'État (représenté par trois ministères : Ministère de l'Économie, Ministère de la Famille, de l'Intégration et à la Grande Région, Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse), le SYVICOL (Syndicat des villes et communes luxembourgeoises) et le SIGI (Syndicat intercommunal de gestion informatique).

SSI
« Sécurité des Systèmes de l'Information ».

TIC
« Technologies de l'information et de la communication ».

ÉDITEUR / CONTACT
LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État
Haut-Commissariat à la Protection nationale
211, route d'Esch . L-1471 Luxembourg
Courriel : Secretariat@hcpn.etat.lu