LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Plan d'intervention d'urgence
en cas d'attaque contre les systèmes d'information
ou de faille technique des systèmes d'information
« PIU Cyber »

(version publique)

Ministère d'État

Ministère de l'Économie

Approuvé et rendu exécutoire par le Conseil de gouvernement le 19 mars 2014

Le plan d'intervention d'urgence « PIU Cyber » définit l'action du gouvernement en cas de faille technique ou d'attaque d'envergure contre les systèmes d'information du secteur public et/ou du secteur privé. Les mesures concrètes à respecter seront décidées par les autorités compétentes en matière de protection nationale au moment opportun, communiquées au public, et mises en œuvre par les administrations et services compétents.

Sommaire

1. Introduction et objectifs

Le plan d'intervention d'urgence « PIU Cyber » définit l'action du gouvernement en cas de faille technique ou d'attaque d'envergure contre les systèmes d'information du secteur public et/ou du secteur privé.

Arrêté par le Conseil de gouvernement le 19 mars 2014, le « PIU Cyber » a pour **objectifs** :

- d'arrêter les mesures de prévention et de protection,
- de déterminer les organes de gestion de crise,
- de définir les mesures d'urgence, les actions y relatives ainsi que les responsables et acteurs respectifs,
- de fixer le déroulement de la diffusion d'alerte des autorités et de l'information au public.

La situation d'urgence cyber désigne une situation qui découle d'un incident ou d'une attaque risquant d'entraîner un dysfonctionnement majeur, voire une indisponibilité de systèmes de communication et de traitement de l'information qui menace les intérêts vitaux ou les besoins essentiels de tout ou partie du pays ou de la population du Grand-Duché de Luxembourg.

Dans l'optique d'une multitude d'incidents possibles, ayant des impacts et des répercussions variés, ce plan met à disposition des responsables en charge de son exécution les outils essentiels afin de pouvoir réagir de façon appropriée et flexible aux événements et de protéger au mieux les citoyens, voire les secteurs concernés, leurs intérêts vitaux et les intérêts économiques nationaux.

L'exécution du plan, élaboré sous la direction du Haut-commissariat à la protection nationale (HCPN), relève du Premier ministre, ministre d'État, du ministre des Communications et des Médias et du ministre de l'Économie. Tous les ministères, administrations et services de l'État sont tenus à coopérer par tous les moyens disponibles à la réalisation des objectifs fixés par le présent plan.

2. Organes de gestion de crise

Le « PIU Cyber » détermine les organes de gestion suivants en situation d'urgence:

2.1. Cellule de crise (CC)

La Cellule de crise (CC) est activée par le Premier ministre, ministre d'État, en cas d'imminence ou de survenance d'une crise. Elle initie, coordonne et veille à l'exécution de toutes les mesures destinées à faire face à la crise et à ses effets, respectivement à favoriser le retour à l'état normal. Elle prépare les décisions qui s'imposent et les soumet au gouvernement aux fins d'approbation. En cas d'intervention opérationnelle sur le terrain, sa mission s'étend à la coordination et au contrôle de l'exécution.

Dans le contexte d'une situation d'urgence, la composition de la Cellule de crise comporte au moins les personnes suivantes:

- le Haut-commissaire à la protection nationale ;
- le directeur général de la Police grand-ducale ;
- le directeur du Service de renseignement de l'État ;
- le chef d'État-major de l'Armée ;
- le directeur du Centre des technologies de l'information de l'État,
- le chargé de direction du Service des médias et des communications ;
- le chargé de direction du Centre de communications du gouvernement ;
- le directeur du CERT gouvernemental (*Computer Emergency Response Team*);
- le directeur du CIRCL (*Computer Incident Response Center Luxembourg*) ;
- le directeur du Service de la communication de crise.

La CC fonctionne pendant toute la durée de la crise jusqu'au retour à l'état normal.

En fonction des circonstances, la CC peut être élargie à des représentants des départements ministériels concernés et peut être complétée par des représentants des fournisseurs d'accès internet (FAI) et des secteurs visés par l'attaque.

La Cellule de crise suit l'évolution de la situation sur base des informations préparées pour son compte par la Cellule d'évaluation du risque cyber (CERC.

2.2. Cellule opérationnelle (CO)

La CC peut déléguer à une cellule opérationnelle notamment l'exécution, la mise en œuvre et le contrôle des mesures et activités ordonnées.

2.3. Cellule d'évaluation du risque cyber (CERC)

En matière de gestion de crise, le rôle de la CERC est de suivre l'évolution de la situation et d'en informer la CC. Composée d'experts, elle procède à une évaluation de la situation et à une veille renforcée en amont de l'activation éventuelle de la CC. Elle est présidée par le directeur du CERT gouvernemental.

2.4. Cellule communication/information (CCI)

La CCI est en charge de la communication et de l'information aux médias et aux citoyens. La coordination horizontale de l'organisation de la communication externe incombe au Service de la communication de crise.

3. Mise en oeuvre du plan

La prise de connaissance d'un incident ou d'une attaque cyber par les organes de gestion de crise se fait en principe soit par l'analyse d'informations disponibles au niveau national, soit par des acheminements internationaux suivants des accords en vigueur. À ces fins, un point de contact unique « SPOC Cyber » (Single Point of Contact Cyber) est opéré en mode 24/7 afin de donner la possibilité aux acteurs nationaux et internationaux de signaler à tout moment les incidents majeurs dans le domaine cyber aux autorités luxembourgeoises compétentes.

Dès la prise de connaissance d'un incident cyber, la CERC est alertée et procède à une évaluation des informations disponibles.

Si l'incident est de nature à engendrer un impact significatif, le Haut-Commissaire à la protection nationale est alerté et en informe le Premier ministre, ministre d'État, qui décide de l'opportunité d'activer la Cellule de crise.

4. Mesures à prendre

Le plan met à disposition des responsables en charge de son exécution les outils essentiels afin de pouvoir réagir de façon appropriée et flexible aux événements et de protéger au mieux les citoyens, voire les secteurs concernés, leurs intérêts vitaux et les intérêts économiques nationaux.

4.1. Évaluation

Il s'agit de la première mesure dans le cycle de gestion de crise. Elle permet d'évaluer le degré d'urgence et l'impact de l'incident sur le territoire luxembourgeois.

4.2. Veille renforcée

La mesure « veille renforcée » regroupe les actions à mettre en œuvre lors d'une situation à risque. Il s'agit surtout

- de réaliser des rapports de situation du trafic réseau, sur l'état d'infection des réseaux et sur l'efficacité des contre-mesures mises en place ;
- d'évaluer toutes les statistiques et données disponibles pour déterminer le degré de gravité de la situation afin de pouvoir réagir instantanément le cas échéant.

4.3. Analyse technique

La mesure « analyse technique » regroupe les actions nécessaires pour analyser en détail une attaque, une intrusion ou tout autre incident informatique qui serait lié à la situation de crise ou qui aurait provoqué la situation de crise.

Il s'agit également d'identifier tous les systèmes impactés de près ou de loin (dommages collatéraux) pour organiser la coordination et la coopération entre les acteurs impliqués ainsi que la communauté CERT internationale.

4.4. Cloisonnement

La mesure « cloisonnement » agit sur le trafic réseau pour contrer d'éventuelles attaques de déni de service (distribuées ou non). Elle peut aussi être appliquée pour isoler efficacement des systèmes menacés et éviter ainsi des fuites d'informations.

4.5. Mise à niveau et protection des systèmes

La mesure « mise à niveau et protection des systèmes » a pour objectif la prise de contact avec des cibles potentielles, listées selon le type d'attaque, afin de vérifier l'existence de certaines vulnérabilités qui risqueraient ainsi d'être exploitées par une menace. Cette liste concerne également les systèmes qui pourraient faire l'objet d'une attaque.

Sur base de la vérification de la situation au niveau des vulnérabilités, la CERC propose à la CC de mettre en place

- soit des mesures préventives au niveau des cibles potentielles,
- soit des mesures protectrices au niveau des cibles,
- soit même de procéder à une déconnection partielle ou totale d'une cible.

La mesure « cloisonnement » est déclenchée lorsque la déconnection d'une cible potentielle s'avère opportune.

4.6. Activation de la réserve nationale cyber

La mesure « activation de la réserve nationale cyber » a pour objectif de faire appel aux experts de l'administration publique dans le domaine de la sécurité des systèmes d'information et de communication. En cas de besoin et pour des domaines spécifiques, la réserve peut être complétée par des experts issus du secteur privé ou d'organisations internationales dont le Luxembourg fait partie.

Cette mesure n'est déclenchée qu'en cas de crise ayant une envergure significative et un impact considérable.

4.7. Rétablissement des services

La mesure « rétablissement des services » regroupe les actions nécessaires pour assurer une reprise des activités impactées par l'incident. Le rétablissement peut se faire par étapes et/ou par niveau de priorité et est clôturée dès le retour à la situation normale.

5. Collaboration et assistance internationale

Toute crise cyber étant susceptible d'avoir une dimension internationale, une collaboration internationale est garantie et une assistance internationale est possible tant au niveau des CERTs que dans le cadre des organisations internationales dont le Grand-Duché de Luxembourg fait partie (Union européenne, Benelux, OTAN, ONU, OSCE).

6. Information du public

Le grand public est informé de l'évolution de la situation par le gouvernement ainsi qu'à travers le site www.infocrise.lu.