Chambre des Députés
GRAND-DUCHÉ DE LUXEMBOURG

PN/CSC P.V. AI 06

Commission des Affaires intérieures

Procès-verbal de la réunion du 7 février 2024

Ordre du jour :

1. Approbation du projet de procès-verbal de la réunion du 13 décembre 2023

2. Demande du groupe politique LSAP du 30 janvier 2024 concernant les deux nouveaux arrangements administratifs portant sur le renforcement des patrouilles mixtes entre le Luxembourg et la France, sur les axes routiers, autoroutiers et à bord des trains transfrontaliers, signés le 25 janvier 2024 par Monsieur le Ministre des Affaires intérieures et son homologue français

3. Demande de la sensibilité politique déi gréng du 31 janvier 2024 concernant l'usurpation d'identité (« *smishing* ») du système d'alerte national LU-Alert

4. Divers

*

Présents : Mme Barbara Agostino (en rempl. de M. Luc Emering), M. Guy Arendt, Mme Nancy Arendt épouse Kemp, M. Gilles Baum (en rempl. de M. Gusty Graas), M. Dan Biancalana, Mme Taina Bofferding (pour le volet « Police » et en rempl. de Mme Liz Braz pour le volet « Affaires intérieures »), M. Emile Eicher, M. Georges Engel (en rempl. de M. Claude Haagen), M. Paul Galles (en rempl. de M. Max Hengel), M. Marc Goergen, M. Fernand Kartheiser, M. Marc Lies, Mme Nathalie Morgenthaler, M. Laurent Mosar, Mme Lydie Polfer, M. Meris Sehovic

M. Marc Baum, observateur délégué

M. Léon Gloden, Ministre des Affaires intérieures

M. Alain Becker, M. Pol Henrotte, de la Direction générale de la sécurité civile (DGSC), Mme Sarah Harik, de la Direction générale de la sécurité intérieure (DGSI) ; du Ministère des Affaires intérieures

M. Guy Bley, Haut-Commissaire adjoint, du Haut-Commissariat à la Protection nationale (HCPN)

M. Paul Rhein, Directeur du *Computer Emergency Response Team* (CERT) gouvernemental (GOVCERT.LU)

M. Luc Tapella, Directeur, M. Tom Weber, de l'Institut luxembourgeois de Régulation (ILR)

M. Grégory Redavid, Chef de la Division « Organisation et support », du Centre des Technologies de l'Information de l'État (CTIE)

Police Lëtzebuerg :

M. Pascal Peters, Directeur central de la Police administrative

M. Philippe Neven, Mme Fabiola Cavallini, de l'Administration parlementaire

*

Présidence : M. Marc Lies, Président de la Commission

*

1. Approbation du projet de procès-verbal de la réunion du 13 décembre 2023

Le projet de procès-verbal est approuvé.

2. Demande du groupe politique LSAP du 30 janvier 2024 concernant les deux nouveaux arrangements administratifs portant sur le renforcement des patrouilles mixtes entre le Luxembourg et la France, sur les axes routiers, autoroutiers et à bord des trains transfrontaliers, signés le 25 janvier 2024 par Monsieur le Ministre des Affaires intérieures et son homologue français

Monsieur le Ministre souligne que les deux arrangements conclus entre la République française et le Grand-Duché de Luxembourg constituent des arrangements administratifs et non des traités.

Lesdits arrangements ont été négociés, sous le Gouvernement précédent, par son prédécesseur, l'ancien ministre de la Sécurité intérieure, M. Henri Kox. À cause d'un empêchement du ministre de l'Intérieur et des Outre-Mer de la République française, M. Gérald Darmanin, les deux arrangements n'ont pas pu être signés à la date initialement prévue, raison pour laquelle ils ont été signés le 25 janvier 2024 par le successeur de l'ancien ministre de la Sécurité intérieure luxembourgeois, à savoir l'actuel ministre des Affaires intérieures[1].

Les deux arrangements, qui entrent en vigueur le 1er mars 2024, ont été élaborés en réponse au mécanisme d'évaluation et de contrôle destiné à vérifier l'application de l'acquis de Schengen, mais aussi en vue des Jeux olympiques et paralympiques se déroulant en été 2024 à Paris.

L'objectif des deux arrangements consiste à encadrer les patrouilles mixtes, composées de policiers français et luxembourgeois, qui circulent entre les deux pays sur les axes routiers, autoroutiers et à bord des trains transfrontaliers. Ces deux arrangements précisent en outre les modalités pratiques du déploiement desdites patrouilles, autorisées par l'accord bilatéral de coopération transfrontalière en matière policière et douanière du 15 octobre 2001 et du droit de l'Union européenne. Ainsi, une patrouille mixte est soumise à la direction opérationnelle luxembourgeoise si elle se trouve sur le territoire du Grand-Duché de Luxembourg et sous la direction opérationnelle française, si elle se trouve sur le territoire de la République française.

[1] Depuis le début de la législature 2023-2028, la sécurité intérieure fait partie des attributions du ministère des Affaires intérieures.

L'orateur précise qu'il n'est pas prévu de doter les agents desdites patrouilles mixtes d'un uniforme commun, de sorte que les policiers luxembourgeois et français garderont leurs uniformes respectifs. À cela s'ajoute que les policiers français ne sont pas autorisés à utiliser leur arme à feu sur le territoire luxembourgeois et *vice versa*, sauf en cas de légitime défense.

Échange de vues

- Estimant que les textes d'accords bilatéraux entre pays, au même titre que les traités, nécessitent d'être ratifiés par les parlements concernés, M. Fernand Kartheiser (ADR) exprime son souhait d'avoir accès aux textes des deux arrangements administratifs en question. Il propose également que les textes soient annexés au procès-verbal de la présente réunion, dans la mesure où ils ne contiennent pas d'informations confidentielles.

  Bien que l'orateur apprécie l'intention du Luxembourg et de la France de renforcer leur coopération transfrontalière en matière policière et douanière, il donne à considérer que, sur le plan opérationnel, toute une série de questions se posent, notamment en ce qui concerne la définition concrète de la mission des patrouilles mixtes, la coordination et la responsabilité opérationnelle des interventions au cours desquelles surviennent des problèmes nécessitant l'utilisation d'armes à feu, les démarches administratives (dont l'établissement de procès-verbaux) qui doivent être entamées ou pas, en vertu du droit français ou luxembourgeois, et la formation afférente des agents de police concernés.

  Monsieur le Ministre souligne que les deux arrangements précités constituent des arrangements administratifs qui ne doivent pas être ratifiés par la Chambre des Députés, contrairement aux traités.

  L'orateur fait remarquer qu'il ne refuse pas aux députés l'accès à ces documents, mais que pour des raisons de sécurité liées aux Jeux olympiques et paralympiques, il n'est pas possible de partager ces informations avec le public.

  Soulevant qu'une certaine transparence vis-à-vis des députés doit être garantie, M. Fernand Kartheiser indique qu'il serait prêt à se rendre au ministère des Affaires intérieures pour pouvoir consulter sur place les textes en question.

  Monsieur le Président précise que, pour les raisons évoquées, il n'est pas possible d'annexer les textes des arrangements administratifs au procès-verbal de la présente réunion. Partant, il recommande aux députés intéressés de s'adresser à la Direction générale de la sécurité intérieure (DGSI) du ministère des Affaires intérieures afin de pouvoir consulter lesdits textes dans les locaux ministériels.

  Monsieur le Ministre informe que les bureaux de la DGSI se trouvent au Kirchberg, à l'adresse suivante : 10, Avenue John F. Kennedy L-1855 Luxembourg.

- M. Dan Biancalana (LSAP) se félicite que les députés aient la possibilité d'étudier le contenu desdits arrangements dans les locaux de la DGSI, notamment parce que les communiqués de presse publiés sur les sites web du ministère des Affaires intérieures luxembourgeois ainsi que du ministère de l'Intérieur et des Outre-mer français ne contiennent pas d'informations supplémentaires par rapport à ce qui a été relaté dans la presse.

  Dans ce contexte, l'orateur souhaite savoir si l'initiative du renforcement des patrouilles mixtes a été prise par les autorités françaises ou par les autorités luxembourgeoises.

Considérant que cette mesure vise à renforcer la sécurité en vue des Jeux olympiques et paralympiques, l'orateur demande si les deux arrangements administratifs sont limités dans le temps, c'est-à-dire jusqu'à la fin dudit évènement sportif, ou s'ils perdurent au-delà.

Monsieur le Ministre souligne qu'il s'agit d'une initiative conjointe entre le Grand-Duché de Luxembourg et la République française.

En ce qui concerne la durée de validité desdits arrangements, l'orateur informe que ceux-ci cesseront de s'appliquer lorsque l'accord franco-luxembourgeois précité du 15 octobre 2001, actuellement en cours de révision, cesse d'être en vigueur.

L'orateur ajoute que l'Unité de la police de la route de la Police grand-ducale, ainsi que le Bureau de la coopération transfrontalière de la gendarmerie zonale et la Direction zonale de la Police nationale figurent comme points de contact entre les autorités françaises et luxembourgeoises.

- Mme Barbara Agostino (DP) demande si les nouveaux arrangements administratifs prévoient également l'utilisation de l'hélicoptère de la Police grand-ducale.

  Monsieur le Ministre répond par la négative.

3. Demande de la sensibilité politique déi gréng du 31 janvier 2024 concernant l'usurpation d'identité (« *smishing* ») du système d'alerte national LU-Alert

M. Meris Sehovic (déi gréng) rappelle qu'en date du 27 janvier 2024, à savoir une dizaine de jours après l'alerte rouge émise pour verglas forts au Luxembourg, lors duquel des messages d'alerte ont été envoyés à la population à travers le système d'alerte national LU-Alert, le ministère des Affaires intérieures a confirmé que ce même système d'alerte a été victime d'une usurpation d'identité, aussi appelé « *smishing*[2] ». Lors de cet incident, des messages frauduleux au nom de la Caisse nationale de santé (CNS) ont été transmis *via* ce même canal, de sorte qu'ils se sont affichés côté à côté des messages d'alerte relatifs au verglas sur les appareils des destinataires, ce qui a probablement conféré une plus grande plausibilité et légitimité à l'arnaque.

En même temps, il a été communiqué que le système LU-Alert n'a pas été compromis et que les mesures appropriées ont été mises en place par les autorités et les opérateurs des réseaux de téléphonie mobile. Dans ce contexte, il se pose la question comment l'incident a pu avoir lieu, tout en préservant la confidentialité de ce système relevant de l'infrastructure critique.

Le fait que cet incident se soit produit constitue un grave problème selon la sensibilité politique déi gréng, qui estime que les citoyens devraient avoir confiance dans les infrastructures critiques ainsi que dans le système d'alerte à la population LU-Alert.

[2] Le « *smishing* », « SMS *phishing* » ou hameçonnage par SMS (abréviation de « *Short Message Service* »), est une méthode d'arnaque semblable à l'hameçonnage par courrier électronique (« *phishing* ») qui s'opère *via* le service de messagerie de téléphonie mobile SMS. Un SMS de *smishing* annonce par exemple au destinataire qu'il doit entreprendre une action, comme le paiement immédiat d'un abonnement prétendument en retard ou l'annulation d'une commande qu'il n'a jamais passée, sur un site Internet qui lui demande ses identifiant et mot de passe et/ou ses coordonnées bancaires (compte, carte bancaire). Le SMS comprend un lien hypertexte vers le faux site piège. Comme pour l'hameçonnage, les émetteurs de *smishing* se font souvent passer pour des établissements bancaires, des messageries, des opérateurs télécom ou des réseaux sociaux (source : https://fr.wikipedia.org/wiki/SMiShing).

L'orateur explique que la sensibilité politique déi gréng s'interroge, d'une part, sur les détails techniques qui ont conduit à l'incident de « *smishing* » et, d'autre part, sur les flux d'informations et le processus de décision entre les différents acteurs nationaux, impliqués dans la gestion de cet incident.

Faisant remarquer que la population en a été informée par le biais d'un communiqué de presse[3] du ministère des Affaires intérieures, l'orateur demande s'il n'aurait pas été plus efficace d'envoyer une communication *via* le système d'alerte national LU-Alert pour sensibiliser les citoyens aux messages frauduleux, étant donné que l'on ne peut pas nécessairement supposer que tous les destinataires du message SMS frauduleux ont également lu le communiqué de presse en question.

En outre, l'orateur demande de quelle manière le Haut-Commissariat à la Protection nationale (HCPN) a été impliqué dans la réaction à l'usurpation d'identité du système LU-Alert et de quelle façon la coordination entre le ministère des Affaires intérieures et le HCPN sera assurée à l'avenir en cas d'incidents similaires.

Monsieur le Ministre informe que les autorités étatiques impliquées dans la gestion dudit incident ont été le HCPN, qui est une administration placée sous l'autorité du ministère d'État, l'Institut luxembourgeois de Régulation (ILR) et le ministère des Affaires intérieures.

Il rappelle que le *smishing* du système d'alerte et d'information LU-Alert a eu lieu en soirée du 26 janvier 2024.

En réaction à cet incident, il a été d'abord analysé, en étroite collaboration avec les opérateurs des réseaux de téléphonie mobile (POST Luxembourg, Orange et Tango) pour déterminer comment l'usurpation d'identité a pu se produire. Aucune cyberattaque n'a été détectée contre le système LU-Alert du côté étatique, ce qui permet de conclure que le système est resté opérationnel à tout moment.

Par la suite, les opérateurs précités ont renforcé la surveillance dans leurs réseaux respectifs et ont mis en place une série de blocages. Sur demande du CERT gouvernemental[4] (ci-après « GOVCERT.LU), le lien contenu dans le message de *smishing* a été bloqué. Une demande a également été adressée à *Amazon Web Services* pour bloquer le site web vers lequel a mené le lien précité.

En date du 31 janvier 2024, une nouvelle tentative d'envois de SMS frauduleux au nom de LU-Alert a eu lieu. Comme la tentative avait échoué, les cybercriminels ont inversé le nom indiqué dans le message, c'est-à-dire le nom « LU-Alert » a été remplacé par « Alert-LU ».

Suite à la détection de cette nouvelle tentative de *smishing* par les opérateurs des réseaux de téléphonie mobile, ceux-ci ont de nouveau renforcé la surveillance dans leurs réseaux et ont mis en place des blocages. GOVCERT.LU a également bloqué le lien de ces SMS frauduleux et la Police grand-ducale a demandé le blocage du site web en question auprès de son hébergeur *Amazon Web Services*.

---

[3] https://maint.gouvernement.lu/fr/actualites.gouvernement%2Bfr%2Bactualites%2Btoutes_actualites%2Bcommuniques%2B2024%2B01-janvier%2B27-maint-sms-frauduleux.html

[4] L'équipe d'intervention en charge des urgences informatiques pour le Gouvernement du Grand-Duché de Luxembourg (GOVCERT.LU), également dénommée « équipe de réponse aux incidents de sécurité informatique (CSIRT) », supervise la prise en charge d'incidents de sécurité informatique qui compromettent le Luxembourg, ses citoyens ou son économie. Il est chargé de recevoir, d'examiner et de répondre aux rapports de tels incidents.

Une plainte pour usurpation de nom, sur base des articles 231 et 231*bis* du Code pénal[5], a également été déposée auprès de la Police.

En outre, l'ILR a invité les trois opérateurs de réseaux précités à prendre les mesures nécessaires pour protéger le nom « LU-Alert » dans leurs réseaux respectifs.

À cet égard, l'orateur tient à souligner que d'autres institutions étatiques ont également été victimes de tentatives similaires de *smishing* par le passé.

La population a été informée dudit incident de *smishing* du 26 janvier 2024 par le biais de deux communiqués de presse du ministère des Affaires intérieures, diffusés le 27 janvier 2024 et le 2 février 2024[6].

En réponse à une question de M. Sehovic, l'orateur fait remarquer qu'il n'a pas été possible de sensibiliser les destinataires par rapport aux SMS frauduleux *via* le canal du système LU-Alert, étant donné que les personnes concernées ne sont pas connues par les autorités. De l'autre côté, l'orateur estime que si un tel message avait été envoyé, par le biais de LU-Alert, à l'ensemble de la population, cela aurait probablement provoqué une réaction de panique inutile. À cela s'ajoute le fait que le nombre de caractères pour la rédaction des messages d'alerte est limité.

Le Directeur du CERT gouvernemental, qui préside également la Cellule d'évaluation du risque cyber[7], qui a été activée dans le cadre de l'incident de *smishing*, explique que le service d'envoi de SMS existant se fait à travers le protocole SS7[8], datant des années 1990, et qui ne permet malheureusement pas d'authentifier l'identité de l'expéditeur d'un message. Il s'ensuit qu'il est possible, pour des tiers malveillants, d'usurper l'identité de l'expéditeur ainsi que d'autres paramètres d'envoi de SMS, ce qui explique, dans le cadre du *smishing* du système national LU-Alert, pourquoi les messages truqués se sont affichés côté à côté des véritables messages d'alerte du Gouvernement relatives au verglas sur les appareils des destinataires.

L'orateur souligne, qu'aux yeux de la Cellule d'évaluation du risque cyber, l'incident peut clairement être qualifié d'une usurpation d'identité et non de cyberattaque, étant donné que le système LU-Alert lui-même n'a pas été attaqué.

En ce qui concerne la provenance des SMS frauduleux, une analyse a révélé qu'ils ont tous été envoyés à partir de l'étranger, notamment depuis la Lituanie, la France et la Belgique. Néanmoins, la Cellule d'évaluation du risque cyber n'a aucune connaissance de

---

[5] Art. 231 Quiconque aura publiquement pris un nom qui ne lui appartient pas sera puni d'un emprisonnement de huit jours à trois mois, et d'une amende de 251 euros à 3.000 euros, ou d'une de ces peines seulement.

Art. 231*bis* Quiconque, dans le but de troubler la tranquillité d'un tiers, ou dans le but de porter atteinte à l'honneur ou à la considération d'un tiers, aura pris un nom ou un identifiant qui ne lui appartient pas sera puni d'un emprisonnement de trois mois à deux ans, et d'une amende de 251 euros à 3.000 euros, ou d'une de ces peines seulement.

Le délit prévu par le présent article ne pourra être poursuivi que sur la plainte de la victime, de son représentant légal ou de ses ayants droit.

[6] https://gouvernement.lu/fr/actualites/toutes_actualites/communiques/2024/02-fevrier/02-arnaques-sms.html

[7] Le rôle de la Cellule d'évaluation du risque cyber (CERC) est de surveiller tout incident ou toute menace critique de sécurité informatique nationale et d'informer la Cellule de crise en continu. La cellule est constituée d'experts et offre une surveillance et une analyse de vulnérabilité accrues dans le cadre du plan national d'urgence. Elle identifie des cibles potentielles, classées selon le type d'attaque, et elle assure l'optimisation et la protection des systèmes d'information menacés. L'unité peut mettre en œuvre des mesures de protection là où des cibles ont été confirmées ou des mesures de prévention là où des cibles potentielles ont été identifiées. Si nécessaire, elle peut également isoler une cible, en partie ou en totalité.

[8] Abréviation de « *Signaling System #7* »

la manière dont les cybercriminels se sont procurés les numéros de téléphones portables luxembourgeois auxquels les messages usurpés ont été envoyés.

Étant donné que la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques[9] ne prévoit pas d'obligation pour les opérateurs des réseaux de téléphonie mobile d'analyser les messages envoyés *via* leur réseau, les SMS frauduleux ont été transmis aux détenteurs des numéros de téléphone concernés.

Concernant la réaction gouvernementale au *smishing* du système LU-Alert, l'orateur rapporte que le Haut-Commissaire adjoint du HCPN avait signalé l'incident le 26 janvier 2024, vers 20:00 heures. Une heure plus tard, vers 21:00 heures, les acteurs impliqués dans l'analyse dudit incident ont été relativement certains qu'il s'agissait d'une attaque de *smishing*, raison pour laquelle les opérateurs de réseaux précités ainsi que l'ILR ont été contactés afin de se concerter sur les mesures à prendre.

Par la suite, il a été décidé d'établir une « *black list* » contenant de nombreuses combinaisons de caractères en relation avec le nom « LU-Alert », que les cybercriminels pourraient potentiellement utiliser afin de tenter de nouvelles attaques de *smishing* (par exemple « LU_Alert », « Alert.lu », « Alerte.lu », etc.). La liste finalisée a été envoyée à l'ILR, qui a transmis une réglementation aux opérateurs de réseaux afin de les inviter à bloquer tout message SMS provenant de l'étranger et contenant l'un des noms figurant sur la liste.

Quant aux liens qui se trouvent dans les SMS frauduleux et qui mènent souvent vers des sites web malveillants, l'orateur fait remarquer que ceux-ci peuvent être identifiés par une URL[10] atypique. Pour piéger les destinataires, les cybercriminels pourraient ainsi utiliser une URL comme « www-cns.lu » (dont le caractère « - » après « www » semble inhabituel) pour imiter l'adresse web de la CNS (dont l'URL réelle est « www.cns.lu »).

Dès que de telles URL falsifiées sont détectées, GOVCERT.LU lance une procédure de blocage et de retrait (« *takedown* ») du site web en intervenant auprès de son hébergeur. Lorsqu'une plainte a été déposée, la Police grand-ducale peut également intervenir auprès des hébergeurs de sites web.

Dans le cas de l'usurpation d'identité du système d'alerte national LU-Alert, GOVCERT.LU a également formulé une demande de retrait du DNS[11] auprès de la POST Luxembourg, de sorte que le nom de domaine ne soit plus accessible *via* Internet.

Bien que les acteurs concernés puissent donc prendre toute une série de mesures en cas d'attaque de *smishing*, l'orateur déplore que les faiblesses du protocole SS7 et l'absence de cadre légal afférent ne permettent, à l'heure actuelle, pas d'empêcher de telles attaques de *smishing*.

[9] Loi du 17 décembre 2021 portant transposition de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen et portant modification de la loi modifiée du 30 mai 2005 portant : 1) organisation de l'Institut Luxembourgeois de Régulation ; 2) modification de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'État.

[10] Une URL (sigle de l'anglais : *Uniform Resource Locator*), couramment appelée « adresse web », est une chaîne de caractères uniforme qui permet d'identifier une ressource du *World Wide Web* par son emplacement et de préciser le protocole Internet pour la récupérer (par exemple « http » ou « https »).

[11] Le *Domain Name System* (service de nom de domaine) ou « DNS » est un service informatique qui permet d'associer un nom compréhensible, à une adresse IP. Le DNS est un composant essentiel du développement du réseau informatique.

Au vu des explications du Directeur du CERT gouvernemental quant aux faiblesses du protocole SS7, M. Meris Sehovic demande s'il existe éventuellement un protocole alternatif qui permettrait d'authentifier l'identité d'un expéditeur lors de l'envoi d'un SMS.

À part cela, l'orateur demande s'il n'est pas possible de prendre d'autres mesures, éventuellement en modifiant les textes législatifs en la matière, pour empêcher des attaques similaires de *smishing* à l'avenir.

Le Directeur du CERT gouvernemental explique qu'il n'existe que très peu de protocoles alternatifs, étant donné que le SMS est pratiquement devenu le canal de communication standard pour atteindre l'ensemble d'une population ou au moins un maximum de personnes en cas de situation de crise.

L'orateur estime que le « *Whitelisting* » pourrait être une méthode qui permet d'empêcher que des SMS frauduleux ne parviennent aux destinataires, mais souligne que ceci devrait encore être évalué entre l'ILR et GOVCERT.LU. Le *Whitelisting* (ou « liste blanche » en français) est une approche restrictive dans laquelle seules les entités préapprouvées sont autorisées à accéder à un service ou à un environnement spécifique, tandis que toutes les autres sont automatiquement refusées par défaut.

Le Directeur de l'ILR indique qu'il partage les affirmations du Directeur du CERT gouvernemental et confirme que son administration analyse de manière récurrente le développement croissant du phénomène du *smishing* dans le domaine des télécommunications.

Selon l'orateur, il s'agit d'un phénomène auquel d'autres pays étrangers sont plus confrontés que le Luxembourg, en raison de la taille de leur population et donc du nombre plus élevé de détenteurs de cartes SIM qui pourraient, pour les cybercriminels, devenir des cibles potentielles pour l'hameçonnage par SMS. L'orateur ajoute que le nombre de cartes SIM au Luxembourg s'élève à approximativement 1 million d'unités, ce qui est un chiffre relativement faible par rapport à la plupart des pays étrangers.

Étant membre dans plusieurs groupes de travail au niveau européen, l'ILR et les autres régulateurs analysent régulièrement quelles solutions pourraient être mises en place dans la lutte contre la problématique du *smishing*. Soulignant qu'une autorité de régulation ne peut agir dans les limites qui lui sont imposées par le législateur, l'orateur regrette que, malgré l'existence de plusieurs directives européennes, les législations nationales des différents États membres de l'UE divergent, ce qui empêche de lutter plus efficacement contre le *smishing*.

En ce qui concerne l'incident du *smishing* du système d'alerte LU-Alert, l'orateur soulève que la collaboration entre l'ILR, le HCPN, GOVCERT.LU et les opérateurs des réseaux de téléphonie mobile a été bonne, ce qui a permis au régulateur national d'agir rapidement en émettant, conformément à la loi précitée du 17 décembre 2021, une recommandation aux opérateurs de bloquer tout message SMS frauduleux contenant des noms de la « *black list* » précitée.

L'orateur estime que les acteurs étatiques précités devraient se réunir avec les opérateurs des réseaux de téléphonie mobile pour évaluer sous quelle forme un « *Whitelisting* » pourrait être mis en place, sans pour autant bloquer le trafic commercial de données mobiles.

M. Fernand Kartheiser (ADR) demande sous quelle forme les autorités nationales coopèrent avec les pays précités d'où sont provenus les SMS frauduleux. Cette coopération se fait-elle par le biais d'une enquête policière ?

Monsieur le Ministre répète qu'une plainte a été déposée auprès de la Police grand-ducale et que celle-ci collaborera avec les forces policières des pays concernés dans le cadre de l'enquête afin d'identifier les auteurs de l'attaque de *smishing*.

Le Directeur de l'ILR souligne que le rôle de son administration consiste à mettre en place des solutions proactives en concertation avec des instances nationales et internationales afin d'éviter que certains problèmes qui se posent dans le domaine des télécommunications ne se propagent. Dans ce contexte, l'orateur fait remarquer que l'ILR participe régulièrement aux réunions du BEREC (*Body of European Regulators for Electronic Communications*[12]), une instance européenne indépendante qui rassemble notamment les régulateurs des vingt-sept États membres de l'Union européenne. Lors de ces réunions, qui se tiennent plusieurs fois par an, les régulateurs échangent sur différentes problématiques qui surgissent dans le domaine des télécommunications.

À titre d'exemple, l'orateur fait savoir que l'ILR a récemment émis une recommandation aux opérateurs de réseaux au sujet des numéros de téléphones géographiques luxembourgeois. Ces numéros, qui sont typiquement associés aux téléphones fixes luxembourgeois, peuvent être utilisés par des criminels pour passer des appels depuis l'étranger afin de pratiquer le *phishing* par téléphone. Afin d'éviter ceci, l'ILR a mis en place une réglementation invitant les opérateurs de réseaux de bloquer tout appel d'un numéro géographique luxembourgeois depuis l'étranger.

Un représentant ministériel de la DGSC souhaite ajouter que, suite à l'attaque de *smishing* du système d'alerte national LU-Alert, le Centre national de crise de la Belgique a contacté le ministère des Affaires intérieures afin de procéder à un échange d'expériences. Celui-ci aura lieu dans les deux semaines à venir.

Mme Taina Bofferding (LSAP) s'interroge sur l'avancement des travaux ministériels concernant la refonte du système d'alerte LU-Alert, qui se base sur une approche multicanale. Le système utilisera à l'avenir divers canaux de communication, dont notamment les réseaux sociaux, une application mobile, les SMS géolocalisés ou encore les messages envoyés par diffusion cellulaire (« *Cell Broadcast* »).

Rappelant que lesdits travaux ont débuté il y a deux ans et ont depuis bien avancé, de sorte qu'il a été estimé que le nouveau système d'alerte à la population pourrait être opérationnel avant la fin de l'année 2023 ou début 2024, l'oratrice demande dans quel délai ces travaux pourront être définitivement finalisés.

Renvoyant à sa réponse à la question parlementaire n° 146[13] de M. Marc Goergen, Monsieur le Ministre indique qu'il souhaite que le nouveau système d'alerte soit opérationnel au plus tard en septembre 2024.

M. Marc Goergen (Piraten) se rallie aux explications du Directeur du CERT gouvernemental selon lesquelles le système d'alerte étatique n'a pas été piraté, mais que des messages d'alerte ont été usurpés par des cybercriminels. Il en résulte que l'incident ne peut pas être qualifié de piratage informatique (« *Hacking* »), mais d'usurpation d'identité (« *smishing* »).

Bien qu'il apprécie le fait que les acteurs nationaux tentent de trouver des solutions dans la lutte contre les problématiques du *smishing* et du *phishing*, l'orateur estime qu'il sera

[12] Ladite instance est également connue sous son nom français « Organe des régulateurs européens des communications électroniques (ORECE) ».
[13] https://www.chd.lu/fr/question/26255

très difficile, voire impossible, d'endiguer complètement de tels incidents en raison du fait qu'ils se produisent dans le monde entier.

Étant donné que certains services de messagerie électronique, comme *Google Mail*, recourent à l'envoi de SMS pour authentifier les utilisateurs de leurs services, l'orateur doute que le *Whitelisting* soit la bonne solution pour empêcher le *smishing*. À cet égard, il estime qu'il faudrait plutôt développer une solution logicielle, téléchargeable sur un téléphone mobile, qui soit en mesure de vérifier l'identité d'un expéditeur d'un SMS ou d'un courriel électronique.

À ses yeux, de nombreuses personnes sont régulièrement victimes d'attaques de *smishing* parce qu'elles n'ont pas été suffisamment informées de ces risques. Il conviendrait ainsi de sensibiliser davantage la population, et notamment les enfants dans les écoles, aux SMS frauduleux.

En outre, l'orateur estime que les possibilités pour la Police grand-ducale de trouver les auteurs d'attaques par *smishing* sont limitées si les serveurs concernés se trouvent à l'étranger. À son avis, une telle enquête policière ne pourrait aboutir qu'avec l'implication d'Europol ou d'Interpol.

Le Directeur du CERT gouvernemental partage l'affirmation de M. Goergen selon laquelle il est très difficile de trouver une solution qui permet d'endiguer complètement le *smishing*. Néanmoins, selon lui, une approche comprenant différents volets, tels que la sensibilisation de la population, la mise en place de solutions techniques et l'adaptation pertinente des textes législatifs en la matière, pourrait réduire le nombre de victimes d'attaques de *phishing* et de *smishing* au Luxembourg. En outre, l'orateur rend attentif au fait que BEE SECURE[14] et GOVCERT.LU lancent régulièrement des campagnes d'information à ces sujets.

M. Marc Baum (déi Lénk) s'interroge sur l'ampleur du phénomène du *smishing* et demande si des statistiques existent qui permettent de se faire une idée de l'évolution de celui-ci.

Le Directeur du CERT gouvernemental indique que, bien que le trafic annuel de SMS soit en baisse, 928 millions de SMS sont encore envoyés chaque heure dans le monde entier. Le nombre des SMS envoyés en 2023 au Luxembourg s'élève à 161 millions d'unités.

Le phénomène du *smishing*, qui désigne uniquement l'hameçonnage qui se fait par SMS, connaît actuellement une tendance à la hausse. Or, selon l'orateur, le nombre de tentatives de *phishing* est toutefois plus important que celui du *smishing*.

M. Meris Sehovic conclut des explications précédentes qu'il n'est pas possible d'éviter que des attaques de *smishing* surviennent à l'avenir.

Selon l'orateur, il se pose ainsi la question des procédures que Monsieur le Ministre envisage de mettre en place pour sensibiliser au mieux les citoyens à l'égard des risques du *smishing* et par quels canaux de communication ces informations devraient être transmises.

[14] BEE SECURE vise à sensibiliser le grand public à une utilisation plus sûre et responsable des technologies numériques, et à renforcer en particulier les enfants, les jeunes et leur entourage (parents, enseignants, éducateurs et autres) par des offres ciblées. BEE SECURE est une initiative gouvernementale du Grand-Duché de Luxembourg, opérée par le Service national de la jeunesse (SNJ) et le *Kanner-Jugendtelefon* (KJT), en partenariat avec *Luxembourg House of Cybersecurity*, la Police *Lëtzebuerg* ainsi que le Parquet général du Grand-Duché de Luxembourg.

Monsieur le Ministre souligne qu'il importe d'informer rapidement la population en cas d'incident. Bien que l'approche multicanale du nouveau système d'alerte à la population constitue un avantage dans ce contexte, il ne peut jamais être totalement exclu que des messages d'alerte puissent être usurpés.

Le ministère des Affaires intérieures continuera à analyser, en collaboration avec les autres acteurs impliqués dans la gestion dudit incident de *smishing*, s'il est possible de renforcer davantage la sécurité du système LU-Alert. Au cas où il s'avérait nécessaire, des adaptations législatives pourraient également être envisagées.

4. Divers

M. Marc Goergen signale qu'il souhaite poser plusieurs questions à Monsieur le Ministre des Affaires intérieures concernant l'imposition des indemnités de congé politique des élus communaux ayant le statut d'indépendant.

Il rappelle que les élus communaux ont récemment reçu une circulaire ministérielle[15] les informant sur les modalités de demande de remboursement ou d'indemnisation des heures de congé politique de l'année 2023 et que les députés ont été informés, par le biais d'un document interne de l'Administration parlementaire, que les indemnités de congé politique des députés qui exercent une profession indépendante doivent être déclarées sur la déclaration d'impôts dans la catégorie de revenu provenant d'une occupation salariée avec le traitement de base.

Aux yeux de l'orateur, le fait que les indemnités de congé politique des élus, qui exercent une profession indépendante parallèlement à leur mandat parlementaire ou communal, ne sont désormais plus considérées comme des revenus provenant de l'exercice d'une profession libérale, mais comme revenus provenant d'une occupation salariée, constitue une nouvelle interprétation de l'Administration des contributions directes. Étant d'avis que ce changement aura un impact significatif sur l'imposition tant des députés que des élus locaux qui exercent une profession indépendante, l'orateur souhaite avoir de plus amples informations de la part de Monsieur le Ministre à ce sujet.

Monsieur le Ministre fait savoir qu'il n'a pas connaissance des informations échangées entre l'Administration parlementaire et les députés et que les questions relatives à l'imposition sur le revenu relèvent de la compétence du ministre des Finances.

Pour ces raisons, il ne peut, à ce stade, pas fournir de réponse aux questions de M. Goergen et propose de collecter les informations nécessaires et de revenir ultérieurement sur ce point.

Étant d'avis que le sujet en question est d'une certaine actualité, M. Marc Goergen exprime son souhait de le mettre à l'ordre du jour de la prochaine réunion de la Commission des Affaires intérieures.

Procès-verbal approuvé et certifié exact

[15] Circulaire n° 2024-010 du ministère des Affaires intérieures :
https://maint.gouvernement.lu/fr/circulaires/circulaires2024/circulaire-2024-010.html