CSV FRAKTIOUN

CHAMBRE DES DÉPUTÉS
Entrée le:
14 MARS 2017
2836

Monsieur Mars Di Bartolomeo
Président de la Chambre des Députés

Luxembourg, le 14 mars 2017

Monsieur le Président,

Par la présente nous avons l'honneur de vous informer que conformément à l'article 80 du Règlement de la Chambre des Députés, nous souhaiterions poser une question parlementaire à Monsieur le Ministre de l'Economie concernant la sécurité informatique des entreprises.

Au fil des années, l'Etat a lancé diverses initiatives visant à sensibiliser et assister des acteurs privés (particuliers et entreprises) face aux risques que comporte une digitalisation toujours accrue de notre vie quotidienne.

C'est dans ce contexte que nous aimerions poser les questions suivantes à Monsieur le Ministre :

- Monsieur le Ministre peut-il nous indiquer combien de fois les divers services de l'Etat ont été sollicités en la matière par des entreprises luxembourgeoises ces dernières années, (i) de manière préventive et (ii) après avoir subi une cyberattaque ?

- Monsieur le Ministre peut-il confirmer que les services étatiques ont toujours été à la hauteur des attentes des entreprises, i.e. qu'ils ont pu fournir des réponses adéquates aux demandes desdites entreprises ?

- Quels sont les problèmes majeurs auxquels sont confrontées les entreprises en termes de sécurité informatique ?

- A combien de reprises les sites internet des différents services étatiques sont-ils consultés par jour / mois par des acteurs implantés au Luxembourg respectivement depuis l'étranger ?

Nous vous prions d'agréer, Monsieur le Président, l'expression de notre parfaite considération.

Diane Adehm
Députée

Gilles Roth
Député

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

Le Ministre

Luxembourg, le 26 avril 2017

CHAMBRE DES DÉPUTÉS
Entrée le:
26 AVR. 2017

Le Ministre de l'Économie
à
Monsieur le Ministre aux
Relations avec le Parlement

L-2450 LUXEMBOURG

Réf. : Co/QP2836-04/JM-dm

Objet: **Question parlementaire N° 2836 du 14 mars 2017 des députés Diane Adehm et Gilles Roth**

J'ai l'honneur de vous communiquer en annexe la réponse de Monsieur le ministre de l'Économie à la question parlementaire sous objet, avec prière de bien vouloir en assurer la transmission à Monsieur le Président de la Chambre des Députés.

Étienne Schneider

Dossier suivi par : Judith Meyers, tél : 247-84349 ; email : judith.meyers@eco.etat.lu

19-21, boulevard Royal
L-2449 Luxembourg
TVA LU 158 52 112

Tél. (+352) 247-82478
Fax (+352) 26 20 04 95
IBLC 158 52 112

Adresse postale:
L-2914 Luxembourg

info@eco.etat.lu
www.gouvernement.lu
www.eco.public.lu

Réponse de M. le Vice-Premier ministre, ministre de l'Economie, Etienne Schneider, à la question parlementaire nr 2836 du 14 mars 2017 des députés Diane Adehm et Gilles Roth

La sécurité informatique des entreprises au Luxembourg est soutenue par le ministère de l'Economie par le biais de CASES.LU depuis 2003. Les différents moyens relatifs à la sécurité informatique, dont CASES.LU ont été regroupés au sein de l'initiative SECURITYMADEIN.LU depuis 2010.

Les initiatives de l'Etat en matière de cybersécurité ont souvent précédé les besoins des entreprises en les alertant sur des dangers qu'elles n'avaient pas encore perçus. En effet, de nombreuses entreprises n'ont pas conscience des risques liés aux technologies de l'information ni des moyens pour se protéger. Ainsi, les services de l'Etat ont répondu à leurs besoins à trois niveaux :

- en matière de prévention, d'information et de formation aux bonnes pratiques ;
- en matière d'analyse et de gestion des risques ;
- en matière d'analyse de la menace, de réaction et de réponse sur incident.

La qualité des méthodes et des approches utilisées a permis au Luxembourg de se distinguer à plusieurs reprises à l'étranger, lors de visites officielles, de foires ou de conférences internationales.

Pour aider les entreprises à progresser en maturité et à adopter les bonnes pratiques, le gouvernement est déterminé à démocratiser davantage l'accès à la sécurité de l'information, notamment en mutualisant certains services et en capitalisant sur les synergies existantes.

Depuis la création de SECURITYMADEIN.LU, les équipes ont été en contact avec environ 6.000 entreprises au Luxembourg. Le plus grand nombre de ces contacts concerne des situations où un acteur a été victime d'une cyberattaque. Ces contacts se font avec le département *CIRCL*[1].

De plus, les équipes de SECURITY MADEIN.LU ont contacté de manière proactive bien au-delà de 10.000 acteurs privés au Luxembourg et à l'étranger, suite à des informations sur des brèches ou d'autres soucis de sécurité obtenues via les réseaux de confiance spécialisés de la part d'homologues internationaux ou encore par le biais de services d'alerte et de veille (« early-warning ») du type MISP[2] ou AIL[3].

Les problèmes majeurs que les entreprises rencontrent en matière de sécurité informatique sont (top 5) :

- Côté menaces :

    1. Le « vol » et l'usurpation de mots de passe, via des attaques dites de « *phishing* », qui sont facilitées par le manque de rigueur et de bonnes pratiques lié à la gestion et l'utilisation des mots de passe ;

---

[1] https://www.circl.lu/mission/
[2] MISP - Malware Information Sharing Platform - https://www.circl.lu/services/misp-malware-information-sharing-platform/
[3] AIL - framework for Analysis of Information Leaks - https://github.com/CIRCL/AIL-framework

2. Les « *malwares* » (virus, trojans ou autres logiciels malicieux), en particulier des demandes de rançons après prise d'otage par chiffrement des données ;
3. Les « fraudes au président » ou autres tentatives de type *ingénierie sociale* qui visent à obtenir des informations sensibles par des techniques de manipulation ;

- Côté vulnérabilités :

4. Le manque de *mise à jour* des logiciels et systèmes utilisés ;
5. Le manque de *sauvegardes* régulières, fonctionnelles et testées.

Sur un plan préventif, les axes de développement se concentrent sur la sensibilisation des acteurs via

- des conférences : plus de 70 participations de SECURITYMADEIN.LU en tant qu'orateur et/ou organisateur, au niveau national, mais aussi international ;
- de campagnes d'information;
- de formations de type « sensibilisation de base » : une quarantaine de ces formations sont délivrées par CASES.LU par an ce qui correspond à environ 900 personnes formées par an ;
- de formations spécialisées : pour MISP, 15 séances de formations ont été organisées depuis 2013 et pour MONARC, 5 séances depuis 2015. Ces formations ont atteint une audience de 530 personnes au total.

La formation sera d'ailleurs renforcée prochainement avec la mise en place, au sein de SECURITYMADEIN.LU, d'un département dédié, à savoir, le *centre de compétences en cybersécurité C3*. Le C3 offrira également un espace de test aux entreprises. Cette approche fait partie de la stratégie « TIRLUX » (Etude Rifkin) qui veut faire du Luxembourg une « Smart Nation ».

En outre, le département CASES.LU a accompagné depuis 2012, quelques 220 entreprises dans leurs démarches de cybersécurité en termes de diagnostic et d'analyse des risques, ceci en vue de les aider à identifier « les grands chantiers » et à trouver des prestataires du marché pour la mise en sécurité.

Finalement, les sites internet www.securitymadein.lu, www.cases.lu et www.circl.lu reçoivent chaque mois plusieurs milliers de visiteurs. Or, ces chiffres ont peu d'intérêt, contrairement à ceux relatifs à l'utilisation des services en ligne offerts par CASES.LU et CIRCL.LU et qui améliore sensiblement l'état de la sécurité de l'information au Luxembourg:

- 720 organisations utilisent plusieurs fois par jour MISP (Malware Information Sharing Platform), dont 30% sont des entreprises luxembourgeoises. Ainsi plus de 2000 « indicateurs de compromission (IOC[4]) » sont échangés par jour ;
- 288 organisations ont accès au service « Passive SSL »[5] ;
- 299 organisations ont accès au service « Passive DNS »[6] ;
- 36 organisations utilisent le service AIL[7] ;
- 68 organisations ont testé leur sécurité via l'auto-évaluation en ligne "start-up kit"[8] ;
- 25 organisations utilisent la plateforme MONARC[9] pour analyser et gérer leurs risques. Parmi ces 25 organisations on compte 16 organismes publics et 9 entreprises privées dont 5 sont également des « providers ».

---

[4] Indicator of compromise (IOC) in computer forensics is an artifact observed on a network or in an operating system that with high confidence indicates a computer intrusion. (https://en.wikipedia.org/wiki/Indicator_of_compromise)

[5] https://www.circl.lu/services/passive-ssl/

[6] https://www.circl.lu/services/passive-dns/

[7] AIL - framework for Analysis of Information Leaks - https://github.com/CIRCL/AIL-framework

[8] https://eval.startup.cases.lu/

[9] Méthode optimisée d'analyse des risques (https://www.cases.lu/monarc.html), outil phare de la plateforme my.cases.lu qui d'ailleurs à gagner le prix "security solution of the year" en 2014 (https://securitymadein.lu/mycases_fr/)