MEMORIAL
Journal Officiel
du Grand-Duché de
Luxembourg

MEMORIAL
Amtsblatt
des Großherzogtums
Luxemburg

RECUEIL DE LEGISLATION

A — N° 30 20 février 2015

Sommaire

Arrêté grand-ducal du 10 février 2015

1. **portant fixation de la gouvernance en matière de gestion de la sécurité de l'information**
2. **modifiant 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».**

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,

Vu l'article 76 de la Constitution;

Vu l'arrêté royal grand-ducal du 9 juillet 1857 portant organisation du Gouvernement grand-ducal, tel qu'il a été modifié;

Vu l'arrêté grand-ducal du 28 janvier 2015 portant constitution des Ministères;

Sur le rapport de Notre Premier Ministre, Ministre d'Etat et après délibération du Gouvernement en Conseil;

Arrêtons:

Art. 1er. Aux fins du présent arrêté grand-ducal, on entend par:

- «Sécurité de l'information»: sécurité autour des systèmes d'information classifiés et non classifiés installés et exploités par l'Etat et les opérateurs d'infrastructures critiques pour leurs besoins propres,
- «Systèmes de communication et d'information»: tout système d'information et de communication et tout autre système électronique traitant des informations,
- «Système de communication et d'information classifié»: tout système de communication et d'information où sont traitées des pièces classifiées telles que définies dans la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité,
- «Informations classifiées»: toute information ou tout matériel identifié comme tel par la classification de sécurité de l'entité correspondante, dont la divulgation non autorisée pourrait porter atteinte à des degrés divers aux intérêts de l'entité correspondante,
- «Bureau d'ordre central»: entité nationale responsable de la réception, de la comptabilisation, de la distribution et de la destruction de toutes les pièces classifiées au Grand-Duché de Luxembourg,
- «Bureau d'ordre auxiliaire»: entité décentralisée d'un département ministériel, administration, service ou autre structure spécifique responsable de la réception, de la comptabilisation, de la distribution et de la destruction des pièces classifiées de ce département ministériel, administration, service ou autre structure,
- «Agence nationale de la sécurité des systèmes d'information (ANSSI)»: autorité nationale en matière de sécurité des systèmes d'information classifiés et non classifiés installés et exploités par l'Etat et les opérateurs d'infrastructures critiques pour leurs besoins propres,
- «Computer Emergency Response Team Gouvernemental (CERT gouvernemental)»: centre gouvernemental de traitement des urgences informatiques tel que 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»,
- «Computer Emergency Response Team National (CERT national)»: centre national de traitement des urgences informatiques.

Art. 2.- La gouvernance de la gestion de la sécurité de l'information classifiée et non classifiée, est organisée autour des trois autorités suivantes:

- autorité régulatrice et gestionnaire d'incidents
- autorité opérationnelle
- autorité homologative.

Art. 3. (1) Le Haut-Commissariat à la Protection Nationale assure la fonction d'ANSSI. Celle-ci est considérée comme autorité régulatrice et gestionnaire d'incidents.

(2) L'ANSSI a pour missions:

1. de définir les politiques et lignes directrices en matière de la sécurité de l'information (classifiée et non classifiée) et d'en surveiller l'efficacité et la pertinence;
2. de veiller à ce que les mesures concernant la sécurité des systèmes d'informations soient mises en place et que leur application soit garantie;
3. de certifier les moyens de traitement de l'information non classifiée (systèmes, services, infrastructures, ou locaux les abritant);
4. d'assurer la fonction de CERT national et gouvernemental;
5. de coordonner la formation à la sécurité de l'information classifiée et non classifiée;
6. de veiller à ce que les utilisateurs soient sensibilisés de façon adéquate aux risques spécifiques liés à l'utilisation des systèmes de communication et d'information; notamment aux risques en relation avec les attaques électroniques;
7. d'assurer la fonction d'autorité Tempest;
8. d'assurer la fonction d'autorité d'agrément cryptographique.

Dans sa fonction de CERT national, il lui incombe:

a) d'opérer comme le point de contact officiel national pour les CERTs nationaux et gouvernementaux étrangers;

b) d'opérer comme le point de contact officiel national pour la collecte et la distribution d'informations relatives aux incidents de sécurité qui concernent les systèmes d'information et de communication implantés au Luxembourg;

c) de servir d'interlocuteur pour les personnes physiques et morales, nationales et internationales;

d) après réception d'informations, de relayer ces informations aux CERTs sectoriels en charge de la victime concernée ou à défaut de CERT sectoriel, directement à la victime;

e) de renseigner sur les points de contact spécifiques en fonction du secteur visé.

Dans sa fonction d'autorité Tempest, il lui incombe:

a) de veiller à la conformité des systèmes de communication et d'information classifiés aux stratégies et lignes directrices TEMPEST;

b) d'approuver les contre-mesures TEMPEST pour les installations et les produits destinés à protéger des informations classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel.

Dans sa fonction d'autorité d'agrément cryptographique, il lui incombe:

a) de veiller à ce que les produits cryptographiques soient conformes aux politiques de sécurité respectives en matière cryptographique;

b) d'évaluer et d'agréer les produits cryptographiques pour la protection des informations classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel;

c) de conserver et de gérer les données techniques relatives aux produits cryptographiques.

Art. 4. Sont considérées comme autorités opérationnelles, les administrations et services ayant dans leurs attributions les missions telles que définies d'une part par la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat ainsi que d'autre part par le présent texte. Les missions sont les suivantes:

1. concevoir, développer, déployer, exploiter et maintenir des systèmes de communication et d'information classifiés nationaux et internationaux;
2. acquérir les produits essentiels à la protection des systèmes de communication et d'information classifiés;
3. assurer la formation des utilisateurs des systèmes de communication et d'information classifiés;
4. assurer le respect des règles et procédures de sécurité, notamment en cas d'interconnexion de systèmes;
5. assurer la fonction d'Autorité de distribution cryptographique;
6. assumer la fonction d'autorité responsable du fonctionnement d'un bureau d'ordre central et de la supervision des bureaux d'ordre auxiliaires.

En tant qu'autorité de distribution cryptographique, il leur incombe:

a) de gérer et d'assurer la manutention, le stockage et la distribution du matériel cryptographique en toute sécurité;

b) d'assurer le transfert et la reprise du matériel cryptographique auprès des personnes ou des services utilisateurs.

Art. 5. Est considérée comme autorité homologative l'Autorité nationale de Sécurité, qui a pour missions celles définies par la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité.

Art. 6. Les principes et les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne s'appliquent mutatis mutandis à chaque fois qu'aucune disposition n'existe au niveau national pour la sécurité des informations classifiées nationales.

A titre subsidiaire, à chaque fois qu'aucune disposition n'existe ni au niveau national ni au niveau européen pour la sécurité des informations classifiées nationales, les principes et les règles de sécurité aux fins de la protection des informations classifiées de l'Organisation du traité de l'Atlantique du Nord s'appliquent mutatis mutandis.

Art. 7. A l'article 1er de 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», il est ajouté une deuxième phrase ayant la teneur suivante:

«Le CERT Gouvernemental est soumis à l'autorité du Haut-Commissariat à la Protection nationale.»

Art. 8. Notre Premier Ministre, Ministre d'État, est chargé de l'exécution du présent arrêté qui sera publié au Mémorial.

Le Premier Ministre,
Ministre d'Etat,
Xavier Bettel

Palais de Luxembourg, le 10 février 2015.
Henri

Convention sur la protection physique des matières nucléaires, ouverte à la signature à Vienne et New York, le 3 mars 1980. – Adhésion de la République de Saint-Marin.

Il résulte d'une notification du Directeur Général de l'Agence Internationale de l'Energie Atomique qu'en date du 19 janvier 2015 la République de Saint-Marin a adhéré à la Convention désignée ci-dessus, qui est entrée en vigueur à l'égard de cet Etat le 18 février 2015.

Convention sur la cybercriminalité, ouverte à la signature, à Budapest, le 23 novembre 2001 et 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, ouvert à la signature, à Strasbourg, le 28 janvier 2003. – Ratification du Monténégro.

Il résulte de plusieurs notifications du Conseil de l'Europe

- qu'en date du 3 mars 2010 le Monténégro a ratifié la Convention désignée ci-dessus, qui est entrée en vigueur à l'égard de cet Etat le 1er juillet 2010, conformément à l'article 48 de la Convention;
- qu'en date du 3 mars 2010 le Monténégro a ratifié le Protocole additionnel désigné ci-dessus qui est entré en vigueur à l'égard de cet Etat le 1er juillet 2010, conformément à l'article 16 du Protocole.

Editeur: Service Central de Législation, 43, boulevard F.-D. Roosevelt, L-2450 Luxembourg
Imprimeur: Association momentanée Imprimerie Centrale / Victor Buck