Département fédéral de justice et police, Secrétariat général, Palais fédéral, 3003 Berne

Consultation relative à un projet de directive sur les prescriptions de sécurité régissant l'accès aux systèmes d'information du DFJP par des utilisateurs externes à la Confédération

Madame, Monsieur,

Votre courrier du 19 juillet dernier relatif à l'objet susmentionné nous est bien parvenu et il a retenu toute notre attention.

De manière générale, nous saluons la directive et les mesures qui l'accompagnent étant donné que celles-ci répondent à un besoin réel, actuel et commun à toutes les autorités et administrations dotées de systèmes d'information.

Basées sur la norme ISO27001, les prescriptions découlant de la directive et du tableau annexé, représentent un niveau de qualité incontestable. Elles suscitent néanmoins les quelques remarques et préoccupations suivantes de notre part.

En préambule, permettez-nous de regretter que ce soit la deuxième demande de ce type qui émane de la Confédération, après celle en lien avec les directives de sécurité dans le cadre de l'assurance chômage. En effet, l'on est en droit de s'inquiéter sur l'éventuel manque de coordination entre départements et offices nous soumettant des directives, notamment au niveau des éventuelles dérogations qui pourraient être sollicitées.

L'introduction de la directive, qui se limite à évoquer les bases légales relatives aux systèmes d'information VOSTRA et RIPOL, laisse penser que celle-ci ne s'applique qu'à ce domaine. Or, nous nous posons la question de savoir ce qu'il en est des autres systèmes que la Confédération met à disposition des cantons (SYMIC, ISA etc.).

Si nous avons bien saisi le caractère contraignant des prescriptions minimales de base, il nous manque toutefois les éléments nécessaires (analyse de risque, champ d'application, périmètre d'action) et le temps pour évaluer les conséquences concrètes de leur mise en œuvre.

Selon notre analyse préliminaire, les éléments techniques des exigences de base suivantes ne pourront pas être réalisés dans le délai imparti :

- L'accès par des personnes aux systèmes de postes de travail et de serveurs doit être possible uniquement via une authentification à deux facteurs.
- L'administration des systèmes doit avoir lieu sur un réseau (logique) séparé et être effectuée sur des systèmes informatiques dédiés et sécurisés à part. Ce réseau ne peut pas permettre l'accès à Internet ou aux outils bureautiques (par ex. boîte aux lettres électronique).
- Les activités suivantes doivent être enregistrées, surveillées et analysées rapidement pour les systèmes informatiques et les applications, en fonction de leur utilisation et de manière à pouvoir être tracées : démarrage et arrêt du système; tentatives d'authentification ayant échoué; tentatives d'accès à des objets qui ont échoué; octroi et modification de privilèges; toutes les actions nécessitant des privilèges accrus.

- Les systèmes de serveurs nécessitant une protection élevée doivent être soumis périodiquement à un examen d'intégrité afin de déceler les modifications non autorisées.
- L'authenticité des logiciels doit être vérifiée, les modifications non autorisées doivent être analysées et clarifiées.
- L'accès à distance pour les fournisseurs doit être préautorisé via un concept de JumpHost (serveur permettant de gérer les accès externes vers l'interne).

En ce qui concerne l'aspect financier, la prise en charge par les cantons n'est nullement remise en cause. Il n'en demeure pas moins que les coûts relatifs au niveau de protection exigé dans ce contexte représentera une charge non négligeable et inégale pour les cantons. C'est aussi pour tenir compte de ce facteur qu'il paraît essentiel, si aucun soutien ne peut être accordé dans ce contexte, de différer le délai de mise en œuvre de cette directive.

Tout en vous remerciant de nous avoir associés à cette consultation, nous vous prions de croire, Madame, Monsieur, à l'assurance de notre parfaite considération.

Neuchâtel, le 30 septembre 2019

Au nom du Conseil d'État :

Le président,	*La chancelière,*
A. RIBAUX	S. DESPLAND