Contrôle subséquent de la mise en œuvre dans les cantons de la politique de sécurité du réseau de la Conférence suisse sur l'informatique
Office fédéral de l'informatique et de la télécommunication

L'essentiel en bref

En 2009, le Contrôle fédéral des finances (CDF) a examiné dans quelle mesure les cantons avaient mis en œuvre la politique de sécurité du réseau (*Network Security Policy, NSP*) dictée par la Conférence suisse sur l'informatique (CSI)[1]. Sur la base des résultats de cet audit, une recommandation a été adressée à l'Office fédéral de l'informatique et de la télécommunication (OFIT) qui, selon le CDF, n'a pas été mise en œuvre jusqu'ici. Les contrats entre l'OFIT et les cantons devaient être complétés par des dispositions de sécurité. De plus, les cantons devraient fournir la preuve que leurs réseaux répondent aux exigences convenues en la matière. S'ils ne respectent pas ces accords, l'OFIT ou les organisations tierces mandatées doivent mener de tels audits de sécurité.

L'OFIT a appliqué cette recommandation autant que possible dans les accords de niveau de service (*Service Level Agreement, SLA*) conclus avec les cantons. Toutefois, il ne se considère pas en mesure ni obligé de mener des audits dans des domaines relatifs à la sécurité auprès des cantons. Les bases juridiques manquent dans le système fédéraliste suisse pour qu'un office fédéral ait le droit d'empiéter sur la souveraineté des cantons, ou inversement. C'est pourquoi le CDF va classer la recommandation en suspens comme liquidée.

Chaque partie doit protéger elle-même ses réseaux des menaces

Depuis le rapport du CDF, les menaces et le potentiel de risques qui en résulte ont augmenté. Auparavant, la tendance voulait que la confiance réciproque règne au sein des structures de réseaux. Aujourd'hui, la protection très ciblée des données sensibles des unités administratives se trouve au premier plan. C'est pourquoi non seulement les limites extérieures d'un réseau sont pourvues de barrières aussi élevées que possible, mais en plus son trafic interne de données est surveillé en permanence.

Du point de vue de la Confédération, le réseau de transmission de données entre les réseaux cantonaux et son pendant fédéral (KOMBV-KTV) est considéré comme un réseau tiers. Par son biais, les cantons disposent d'une liaison hautement disponible et performante pour accéder aux applications de la Confédération dans le cadre de leurs tâches légales. Dans ce but, ils doivent suivre une procédure d'authentification à deux facteurs (première barrière de sécurité). Les profils ainsi personnalisés permettent de libérer uniquement l'accès aux applications auxquelles la personne connectée a réellement droit (deuxième élément de sécurité). Le cryptage assure la confidentialité des données transmises.

La sécurité des réseaux relève de la souveraineté cantonale

Dans leur propre intérêt, les cantons devraient appliquer le même niveau de sécurité que la Confédération pour protéger leurs réseaux et données. Hormis la NSP de la CSI, il existe d'autres bases et directives permettant à chaque canton de mettre en place les mesures de sécurité minimales

[1] « Audit de la mise en œuvre dans les cantons de la politique de sécurité du réseau (*Network Security Policy*) de la Conférence suisse sur l'informatique », 8421, 2009

requises. De plus, la collaboration entre les représentants de la Confédération et des cantons se concrétise au sein de différents organes de la CSI, toujours dans le but d'uniformiser les procédures. Cependant, il manque une instance supérieure contrôlant régulièrement le respect des directives contraignantes et qui puisse aussi les faire appliquer. Une plus grande attention devrait être portée à ces exigences lors du remaniement de la NSP de la CSI, ce que le CDF salue.

Texte original en allemand