Audit de l'efficacité de la gestion des incidents dans la protection des TIC fédérales contre les cyber-risques

Centre national pour la cybersécurité

L'essentiel en bref

Comme service spécialisé dans la sécurité des technologies de l'information et de la communication (TIC) de l'administration fédérale, le Centre national pour la cybersécurité (NCSC) édicte des directives en matière de cybersécurité au sein de l'administration fédérale, en vérifie le respect et aide les fournisseurs de prestations à éliminer les vulnérabilités.

Adoptée par le Conseil fédéral, l'Ordonnance sur la protection contre les cyber-risques dans l'administration fédérale est en vigueur depuis le 1er juillet 2020. Elle constitue la base juridique pour la création et le développement du NCSC et définit la structure, les tâches et les compétences des autorités impliquées. Le NCSC y est habilité à prendre la direction des opérations en cas de cyber-incident présentant une menace pour le bon fonctionnement de l'administration fédérale, en concertation avec les services concernés.

Lors de cet audit, le Contrôle fédéral des finances (CDF) a vérifié l'efficacité du processus en place. Il a évalué en particulier les échanges en temps réel entre les sources d'information et le NCSC ainsi que le regroupement de ces informations avec les résultats de la propre activité de surveillance du NCSC. En outre, son évaluation a porté sur l'identification d'un cyber-incident et la mise en œuvre de mesures en temps utile ainsi que sur la transmission des informations aux services concernés.

Le processus de gestion des incidents est défini, publié et appliqué. Les rôles et responsabilités sont en principe attribués, mais le rôle des délégués à la sécurité informatique des unités administratives (DSIO) doit être renforcé. Des améliorations sont nécessaires en ce qui concerne la vue d'ensemble des acteurs lorsque des fournisseurs de prestations externes sont impliqués. Les conditions-cadres sont généralement appropriées, mais les canaux de communication et l'actualité des notifications doivent être améliorées.

La notification d'un cyber-incident doit être plus rapide

La notification immédiate d'un cyber-incident est importante, pour permettre une analyse et une évaluation globales du risque. Cela permet de limiter ou, dans le meilleur des cas, d'éviter le risque de propagation latérale dans toute l'administration fédérale. Lors de son audit, le CDF a constaté que la communication avec le NCSC doit encore être développée. Ainsi, la gestion des incidents au niveau horizontal, notamment les échanges d'informations entre fournisseurs de prestations (FP), n'est pas encore assurée partout. En outre, les délégués à la sécurité informatique des départements (DSID) doivent être informés plus vite.

La coordination ou l'harmonisation de la classification des cyber-incidents, lorsqu'ils concernent plusieurs FP, constitue également un défi. Sinon il est à craindre que les différents FP n'accordent pas la même priorité aux incidents. Une telle situation peut aussi conduire à une communication incohérente avec des tiers.

Le rôle du DSIO devrait être renforcé et une vue d'ensemble des fournisseurs de prestations externes devrait être créée

Les DSIO jouent un rôle important dans la notification des cyber-incidents : en tant que bénéficiaires de prestations (BP), ils signalent ces incidents à leurs FP, qui informent à leur tour le NCSC. Comme il existe différents niveaux de maturité en fonction de la taille des BP, il n'est toutefois pas toujours possible de définir une suppléance. En l'absence du DSIO, la notification d'un cyber-incident peut être retardée, de même que la notification immédiate au NCSC. Cette situation doit être corrigée sans délai.

En cas de cyber-incident, il n'est pas possible de déterminer rapidement quelles applications et quels services sont gérés par quel fournisseur pour quelle unité administrative (UA). Par conséquent, si un incident de sécurité informatique est signalé à un FP externe, il n'est pas possible d'informer immédiatement les UA concernées, ce qui augmente en principe la vulnérabilité de l'administration fédérale. Il faudrait donc songer à établir un inventaire général.

Les outils devraient être utilisés plus efficacement

L'acquisition d'outils de surveillance devrait être harmonisée au niveau de l'administration fédérale et centralisée pour éviter l'utilisation d'outils différents dotés de fonctions identiques ou similaires. Cela permet de profiter d'éventuelles économies d'échelles en termes de coûts et d'acquisition de savoir-faire.

La clause contractuelle type doit être optimisée

La Conférence des achats de la Confédération a élaboré une clause contractuelle type pour les cyber-risques. Les points de cette disposition concernant la sécurité informatique vont dans la bonne direction. Cependant, les délais de notification des cyber-incidents ne sont pas fixés de manière uniforme et devraient être définis en conséquence. En outre, cette clause devrait être renégociée dans les contrats de longue durée.

Texte original en allemand