Audit transversal des mesures en cas de défaillance des systèmes d'applications métier

Office fédéral de la douane et de la sécurité des frontières, Administration fédérale des contributions, Office fédéral de l'informatique et de la télécommunication

L'essentiel en bref

La gestion de la continuité des activités (*Business Continuity Management*, BCM) sert à maintenir les activités d'une organisation en cas de défaillance. Il inclut la préparation en vue d'une défaillance, la gestion et le suivi après une défaillance. Au printemps 2017, une réglementation relative à la BCM a été adoptée au sein de l'administration fédérale et mise en œuvre dans les départements et à la Chancellerie fédérale.

Le Contrôle fédéral des finances (CDF) a vérifié auprès de l'Office fédéral de la douane et de la sécurité des frontières (OFDF) ainsi que de l'Administration fédérale des contributions (AFC) l'avancement de la mise en œuvre de la BCM en évaluant son degré de maturité.

Étant donné que la sauvegarde des données et leur restauration à la suite d'une défaillance constituent une composante importante d'une BCM, l'application de sauvegarde « NetBackup » a été examinée dans un audit parallèle à l'Office fédéral de l'informatique et de la télécommunication (OFIT). La sécurité de l'exploitation et la fiabilité des processus de sauvegarde et de restauration ont été auditées.

Le système de BCM de l'OFDF a un degré de maturité élevé

À l'OFDF, la documentation et les plans relatifs à la BCM sont très détaillés. Les processus opérationnels critiques ont été identifiés et la marche à suivre en cas de défaillance est précisément décrite. Les mesures prévues sont compréhensibles et adéquates pour l'OFDF. Les moyens informatiques qui soutiennent ces processus sont installés de manière redondante et offrent une haute disponibilité.

Pour différentes raisons, les tests et la mise en pratique des mesures de BCM ont été négligés ces dernières années. Une liste détaillée des exercices prévus est disponible, ces derniers doivent couvrir tous les domaines concernés par la BCM dans les années à venir.

L'AFC a réalisé des progrès importants, mais certains travaux sont encore nécessaires

La BCM de l'AFC a beaucoup progressé par rapport à la dernière évaluation en 2016. Les documents nécessaires existent, mais sont parfois trop génériques. Ainsi, les processus opérationnels critiques identifiés dans l'analyse d'impact sur les activités ne sont pas traités systématiquement dans la planification.

Il n'existe pas de plan de test global définissant les types de tests à effectuer et les groupes concernés. Cependant, des plans distincts ont été établis pour certains exercices. Un exercice d'évacuation a pu être mené avec succès l'année dernière.

La protection contre les chevaux de Troie verrouillant les données est prioritaire

Les systèmes pour fournir la prestation de marché « Sauvegarde et restauration » de l'OFIT sont installés de manière redondante et offrent une haute disponibilité. Les mesures de sécurité implémentées répondent aux exigences actuelles.

Les délais de restauration convenus contractuellement ne peuvent toutefois pas être entièrement garantis pour les grandes bases de données en raison de leur volume.

Les chevaux de Troie verrouillant les données, appelés rançongiciels, constituent aujourd'hui l'un des plus grands risques pour la disponibilité des systèmes et des bases de données. Une protection spécifique contre ces logiciels malveillants n'est pas encore implémentée dans les systèmes de sauvegarde. L'OFIT traite cette question. De plus, une évaluation externe pour protéger les sauvegardes de données contre les rançongiciels est prévue. Cette thématique doit être considérée comme prioritaire et les éventuelles mesures à prendre doivent être mises en œuvre rapidement.

Texte original en allemand