AUDIT

Audit de la mise en production d'applications dans un environnement agile

Office fédéral de l'informatique et de la télécommunication

L'ESSENTIEL EN BREF

L'Office fédéral de l'informatique et de la télécommunication (OFIT) a récemment mis à jour son infrastructure informatique en nuage privé Atlantica. Il a notamment mis en œuvre une nouvelle plateforme de gestion des conteneurs logiciels. Cette technologie permet de regrouper le code d'une application avec les fichiers de configuration et les composantes nécessaires à son exécution. Réalisés dans le cadre du programme Amboss, les travaux se sont achevés à fin décembre 2023 et ont coûté quelque 13,2 millions de francs. Ils ont aussi porté sur la réalisation de nouvelles chaînes de processus et d'outils pour la mise en production automatisée des applications nommées « pipelines CNCICD ». Ces chaînes ont une importance particulière en termes de système de contrôle interne (SCI). Elles doivent en effet assurer que les tests du respect des exigences posées à une solution applicative ont été réussis avant que celle-ci passe en mode productif.

Dans cet audit, le Contrôle fédéral des finances (CDF) examine si les prescriptions et les processus de l'OFIT garantissent que les exigences – et particulièrement les exigences non-fonctionnelles telles que la sécurité, la conformité architecturale, l'incorporation des besoins du SCI, etc. – sont remplies dans toutes les mises en production d'applications. Le CDF a constaté qu'une première version des pipelines CNCICD est opérationnelle et déjà utilisée. Cependant, seule une partie des exigences non-fonctionnelles sont couvertes par les tests automatiques dans les mises en production. Les autres catégories d'exigences peuvent être testées au travers d'étapes manuelles de validation. Plusieurs points sont encore en suspens, l'OFIT y travaille. Le CDF a par ailleurs recommandé de renforcer la perspective du SCI dans ces travaux.

Une première version des pipelines est en place, mais la couverture des exigences par les tests automatiques est limitée

Une approche structurée a présidé à la mise en œuvre des pipelines CNCICD. Selon le cahier des charges, les possibilités offertes par les environnements en nuage devaient être exploitées au maximum, tout en garantissant la sécurité. Ces travaux ont débouché sur une combinaison complexe d'outils et de processus, qui couvrent les étapes du développement applicatif et du déploiement des solutions en mode continu. Ainsi, les pipelines guident les développeurs et les exploitants durant la gestion des versions des objets de code et les activités de test et de validation (intégration). Dans un deuxième temps, ils les accompagnent en vue de la préparation des paquets logiciels et leur distribution sur les infrastructures productives (déploiement). Diverses fonctions annexes, telles que la journalisation des événements et le stockage d'informations sensibles, sont aussi mises à disposition. Certains points ouverts subsistent, mais cette première version a pu faire la preuve de son fonctionnement : quatre solutions applicatives ont déjà pu être mises en production au travers des pipelines, plus d'une centaine d'entre elles sont en cours de travail. Le processus d'adoption suit son cours, l'OFIT et les bénéficiaires de prestations gagnent en expérience. Des ajustements restent possibles.

La mise en production des applications ne peut se faire que par le biais d'un pipeline. Pour faciliter l'adoption de ce principe par les développeurs internes et externes, l'OFIT a mis en place une abondante documentation sous forme de descriptions, de guides, de standards, de vidéos et de listes de contrôle. Pour les applications en conteneurs livrées clés en main par des fournisseurs externes, un type spécifique de pipeline a été mis en œuvre.

Ces applications doivent donc aussi passer par les tests définis dans les chaînes d'outils pour être déployées sur l'infrastructure productive cible. Ainsi, les conditions sont réunies pour que les développeurs internes aussi bien qu'externes puissent utiliser judicieusement les pipelines CNCICD et s'assurer que les exigences définies soient respectées.

Les tests automatiques incorporés dans les pipelines CNCICD ne couvrent que des exigences relatives à la protection informatique de base. Ces tests, qui ne sont pas tous obligatoires, se concentrent sur la recherche de vulnérabilités, d'identifiants apparents dans les lignes de programmes et de qualité du code des applications. Par contre, pour les autres types d'exigences, fonctionnelles ou non, des tests automatiques n'ont pas été utilisés. En effet, dans ces cas, des définitions fastidieuses et spécifiques à chaque application seraient nécessaires. L'OFIT a plutôt privilégié la possibilité de définir des étapes de validation manuelle ou d'incorporer une boucle de test dans un outil ad hoc. Pour favoriser l'acceptation par les bénéficiaires de prestations, une voie médiane entre automatisation et intégration d'étapes manuelles a donc été choisie. Elle laisse toutefois encore une grande partie de la responsabilité de la mise en œuvre correcte des exigences aux équipes de développement. Le CDF estime que cette première version des pipelines CNCICD offre un point de départ raisonnable en termes d'incorporation du contrôle des exigences. Il part du principe que l'OFIT continuera de suivre l'évolution technologique en matière d'outils de test et de pousser l'automatisation dans la mesure du possible.

Des possibilités de contournement temporaire des tests existent

Parce que les tests automatiques retournent parfois des résultats faux-positifs ou qu'ils ne sont pas toujours pertinents pour un environnement donné, une possibilité de les désactiver a été mise en place (« whitelisting »). Selon le processus défini, cette exception doit être dûment documentée et validée par le bénéficiaire et le fournisseur de prestations. La validité de l'exception est limitée dans le temps. Pour le CDF, cette entorse contrôlée à l'obligation de tester les applications est acceptable.

D'autres possibilités de contournement existent. D'une part, les développeurs peuvent copier un pipeline existant et modifier la copie pour en retirer les étapes de tests obligatoires. Ils peuvent alors théoriquement l'utiliser pour mettre en production des applications sans les tester. Des mécanismes de protection des définitions de pipelines par signature cryptographique étaient prévus dans le programme Amboss. Ils n'ont toutefois pas encore pu être mis en place, faute d'un produit compatible sur le marché. La protection des pipelines est donc insuffisante pour l'instant, mais l'OFIT garde cette lacune sur sa liste de points en suspens. D'autre part, la détection a posteriori de tels cas reste possible au travers de l'analyse des journaux d'exécution des pipelines. Pour ces raisons, le CDF renonce à une recommandation sur ce point.

Le CDF précise qu'il n'a pas pu évaluer l'efficacité des contrôles mis en œuvre dans le cadre des pipelines CNCICD. L'OFIT a pu montrer que les données à cet effet sont disponibles, mais leur analyse pour un échantillon représentatif de mises en production n'est pas encore industrialisée.

Opérationnalisation en cours, la perspective du SCI doit être mieux prise en compte

Un comité est en charge du pilotage de la plateforme CNCICD, de la définition de sa gouvernance et des priorités de son futur développement. Des représentants des domaines Business Solutions et Plattform Services de l'OFIT, ainsi que des spécialistes de la sécurité y siègent. Par contre, la perspective du SCI n'est pas explicitement représentée au sein du comité.

Un cadre de référence décrivant les principales fonctions liées aux pipelines est en passe d'être adopté. Parmi ces fonctions, des activités d'ordre supérieur sont d'ailleurs déjà menées. Elles portent notamment sur la surveillance du fonctionnement et les contrôles de la sécurité et de la bonne santé des pipelines et des applications. Un audit de sécurité des pipelines a ainsi été réalisé fin décembre 2023. Les processus et les responsabilités découlant des fonctions décrites dans le cadre de référence ne sont toutefois pas encore tous définis et institutionnalisés, mais leur opérationnalisation est à l'agenda du comité. Par conséquent, le CDF renonce à une recommandation sur ce point. En revanche, il a recommandé de renforcer la perspective du SCI au sein du comité et de son agenda.