VERIFICA

Verifica della messa in produzione di applicazioni in un ambiente agile

Ufficio federale dell'informatica e della telecomunicazione

L'ESSENZIALE IN BREVE

Recentemente l'Ufficio federale dell'informatica e della telecomunicazione (UFIT) ha aggiornato la sua infrastruttura di cloud privato Atlantica. Nello specifico ha introdotto una nuova piattaforma di gestione dei container. Questi ultimi consentono di raggruppare il codice di un'applicazione, i relativi file di configurazione e le componenti necessarie alla sua esecuzione. I lavori di realizzazione della nuova piattaforma sono stati eseguiti nel quadro del programma AMBOSS e completati alla fine di dicembre 2023 per un costo di circa 13,2 milioni di franchi. In questo contesto sono state sviluppate anche nuove catene di processi e strumenti per la messa in produzione automatizzata delle applicazioni, denominate «pipeline CNCICD» (integrazione, distribuzione e deployment continui in base agli standard del cloud nativo). Tali catene di processi e strumenti ricoprono particolare importanza nell'ambito del sistema di controllo interno (SCI). Servono infatti a garantire che i test di verifica della conformità dei requisiti imposti a una soluzione applicativa siano stati superati prima che questa entri in funzione nell'ambiente produttivo.

Nell'ambito della presente verifica, il Controllo federale delle finanze (CDF) ha esaminato il rispetto da parte dell'UFIT delle sue prescrizioni e dei suoi processi che garantiscono l'osservanza dei requisiti per quanto riguarda la messa in produzione di tutte le applicazioni, in particolare dei requisiti non funzionali, ad esempio in materia di sicurezza, conformità architetturale e osservanza delle necessità del SCI. Il CDF ha potuto constatare che una prima versione delle pipeline CNCICD è già operativa. Tuttavia i test automatici nell'ambito della messa in esercizio soddisfano solo una parte delle esigenze non funzionali. Le altre categorie di esigenze possono essere testate tramite processi manuali di validazione. L'UFIT è impegnato a risolvere numerose questioni ancora in sospeso in questo ambito. Al riguardo, il CDF ha inoltre raccomandato di riservare maggiore attenzione al SCI.

Prima versione delle pipeline già in funzione, limitato tuttavia il rispetto delle esigenze da parte dei test automatici

Per implementare le pipeline CNCICD è stato adottato un approccio strutturato. Il capitolato d'oneri imponeva di sfruttare al massimo le possibilità offerte dagli ambienti cloud, garantendo al contempo la sicurezza. Da questi lavori è risultata una complessa combinazione di strumenti e processi che assicurano lo svolgimento continuativo delle fasi di sviluppo delle applicazioni e di distribuzione delle soluzioni. Le pipeline guidano dunque gli sviluppatori e i gestori nell'esercizio delle versioni dei codici oggetto e nelle attività di test e validazione (integrazione). Successivamente li supportano nella preparazione dei pacchetti software e nella loro distribuzione sulle infrastrutture produttive (deployment). Inoltre vengono messe a disposizione diverse funzioni aggiuntive, come la registrazione degli eventi e l'archiviazione di informazioni sensibili. Nonostante alcuni aspetti in sospeso, questa prima versione delle pipeline si è dimostrata efficace: quattro soluzioni applicative sono già in funzione nell'ambiente produttivo e oltre un centinaio sono in fase di elaborazione. Il processo di adozione delle pipeline sta seguendo il suo corso e l'UFIT, così come i beneficiari delle prestazioni, stanno acquisendo sempre più dimestichezza nel loro impiego. Ciononostante è possibile attuare alcuni miglioramenti.

La messa in produzione delle applicazioni è realizzabile unicamente sulla base di una pipeline. Per sostenere gli sviluppatori interni ed esterni nel rispetto di questo principio, l'UFIT ha elaborato una ricca documentazione composta di descrizioni, guide, standard, video e liste di controllo. Per le applicazioni in container consegnate, pronte per l'uso, da fornitori esterni è stata attuata una pipeline specifica.

Anche queste applicazioni devono quindi superare i test stabiliti nelle catene di strumenti prima di essere distribuite sull'infrastruttura produttiva di destinazione. Così facendo gli sviluppatori interni ed esterni possono utilizzare le pipeline correttamente e assicurarsi che le esigenze prestabilite siano rispettate.

I test automatici previsti dalle pipeline CNCICD soddisfano solo i requisiti relativi alla protezione informatica di base. Questi test, non tutti obbligatori, si focalizzano sulla ricerca delle vulnerabilità, di identificativi figuranti nelle linee di codice nonché della qualità del codice delle applicazione.

Per contro non sono stati effettuati test automatici su altre categorie di esigenze, né funzionali né d'altro genere. In questi casi occorrerebbe elaborare complicate definizioni specifiche in riferimento a ogni singola applicazione. L'UFIT ha preferito la possibilità di definire tappe di validazione manuale o di integrare un ciclo di test in uno strumento ad hoc. Per agevolare l'accettazione da parte dei beneficiari delle prestazioni, l'UFIT ha dunque scelto una via di mezzo tra l'automazione e l'integrazione di tappe manuali. Tuttavia questo approccio attribuisce ancora una grande responsabilità in merito all'attuazione corretta delle esigenze ai team di sviluppo. Il CDF ritiene che la prima versione delle pipeline CNCICD rappresenti un buon punto di partenza per l'integrazione del controllo delle esigenze, ma presuppone che l'UFIT continui a seguire lo sviluppo tecnologico in materia di strumenti di test e a favorire, per quanto possibile, l'automazione.

Possibilità di disattivare temporaneamente i test

Dato che, talvolta, i test automatici forniscono risultati falsamente positivi o non pertinenti nel rispettivo ambiente, è stata prevista la possibilità di disattivarli («whitelisting»). In base alla procedura stabilita, si tratta di una deroga che deve essere debitamente documentata e convalidata dal beneficiario e dal fornitore delle prestazioni. La validità di tale deroga deve essere limitata nel tempo. Il CDF considera accettabile questa eccezione controllata all'obbligo di testare le applicazioni.

Esistono inoltre altre possibilità per evitare i test. Gli sviluppatori possono innanzitutto copiare una pipeline esistente e modificarne la copia per rimuovere le tappe di test obbligatorie. In tal modo riescono, in teoria, a mettere in funzione le applicazioni in ambiente produttivo senza prima testarle. Il programma AMBOSS prevede meccanismi di protezione delle definizioni di pipeline tramite firma crittografata. Tuttavia, a causa della mancanza di un prodotto compatibile sul mercato, tali meccanismi non sono ancora operativi. Al momento la protezione delle pipeline risulta quindi insufficiente, ma l'UFIT ha inserito questa lacuna tra i punti in sospeso da risolvere. Inoltre le analisi dei protocolli di esecuzione delle pipeline consentono di rilevare a posteriori i casi in cui è avvenuta una messa in esercizio non conforme. Per queste ragioni il CDF ha deciso di non formulare alcuna raccomandazione al riguardo.

Il CDF precisa di non aver potuto valutare l'efficacia dei controlli impiegati nel quadro delle pipeline CNCICD. L'UFIT ha dimostrato di disporre di dati che attestano l'efficacia dei controlli, ma non vi è ancora una soluzione industrializzata per un'analisi rappresentativa delle procedure di messa in produzione.

Messa in funzione in corso: necessaria una maggiore considerazione dell'approccio del SCI

Un comitato, composto da rappresentanti delle divisioni Business Solutions e Platform Services dell'UFIT nonché da esperti di sicurezza, è stato incaricato di gestire la piattaforma CNCICD, di definirne la governance e stabilire le priorità del suo futuro sviluppo. Tuttavia l'approccio del SCI non è rappresentato esplicitamente all'interno del comitato.

Attualmente è in fase di approvazione un quadro di riferimento che descrive le principali funzioni relative alle pipeline. Tra queste funzioni, alcune attività prioritarie sono d'altronde già operative. Si tratta, in particolare, di attività incentrate sulla sorveglianza dell'esercizio e sui controlli della sicurezza e del buon funzionamento delle pipeline e delle applicazioni. A fine dicembre è stato eseguito un controllo sulla sicurezza delle pipeline. Non sono ancora stati definiti né consolidati tutti i processi e le responsabilità inerenti alle funzioni descritte nel quadro di riferimento, tuttavia la loro messa in esercizio rientra tra le priorità del comitato. Di conseguenza, il CDF ha deciso di non formulare una relativa raccomandazione. Ha invece raccomandato di rafforzare l'approccio del SCI all'interno del comitato e della sua agenda.

Testo originale in francese