PRÜFUNG

Prüfung der Produktivsetzung von Anwendungen in einem agilen Umfeld

Bundesamt für Informatik und Telekommunikation

DAS WESENTLICHE IN KÜRZE

Das Bundesamt für Informatik und Telekommunikation (BIT) hat kürzlich seine IT-Infrastruktur in der Private Cloud Atlantica auf den neuesten Stand gebracht. Das BIT hat insbesondere eine neue Plattform zur Verwaltung von Software-Containern eingeführt. Diese Technologie ermöglicht es, den Anwendungscode mit den Konfigurationsdateien und den für die Ausführung der Anwendung erforderlichen Komponenten zu bündeln. Die Arbeiten, die im Rahmen des Programms «Amboss» durchgeführt wurden, wurden Ende Dezember 2023 abgeschlossen und kosteten rund 13,2 Millionen Franken. Sie umfassten auch die Realisierung neuer Prozess- und Toolketten für die automatisierte Produktivsetzung der als «CNCICD-Pipelines» bezeichneten Anwendungen. Diese Ketten haben eine besondere Bedeutung im Hinblick auf das interne Kontrollsystem (IKS). Sie sollen nämlich sicherstellen, dass die Tests der Anforderungen an eine Anwendung bestanden wurden, bevor diese produktiv gesetzt wird.

In dieser Prüfung untersucht die Eidgenössische Finanzkontrolle (EFK), ob die Vorgaben und Prozesse des BIT gewährleisten, dass die Anforderungen – und insbesondere die nicht-funktionalen Anforderungen wie die Sicherheit, die Architekturkonformität, die Einbeziehung der IKS-Erfordernisse usw. – bei sämtlichen Produktivsetzungen von Anwendungen erfüllt werden. Die EFK hat festgestellt, dass eine erste Version der CNCICD-Pipelines betriebsbereit ist und bereits verwendet wird. Bei den Produktivsetzungen decken die automatischen Tests jedoch nur einen Teil der nicht-funktionalen Anforderungen ab. Die übrigen Anforderungskategorien können über manuelle Validierungsschritte getestet werden. Mehrere Punkte sind noch offen, an welchen das BIT aber arbeitet. Die EFK hat zudem empfohlen, die Perspektive des IKS bei diesen Arbeiten stärker zu berücksichtigen.

Eine erste Version der Pipelines ist implementiert, die Tests decken jedoch nur einen Teil der Anforderungen ab

Bei der Umsetzung der CNCICD-Pipelines wurde ein strukturierter Ansatz verfolgt. Gemäss Pflichtenheft sollten die sich durch die Cloud-Umgebungen bietenden Möglichkeiten voll ausgeschöpft werden, dies bei gleichzeitiger Gewährleistung der Sicherheit. Das Ergebnis dieser Arbeiten war eine komplexe Kombination von Tools und Prozessen, welche die Phasen der Anwendungsentwicklung und der kontinuierlichen Bereitstellung von Lösungen abdecken. Die Pipelines führen die Entwicklungsteams und die Betreibenden demnach bei der Verwaltung der Versionen von Codeobjekten und bei den Test- und Validierungsaktivitäten (Integration). In einem zweiten Schritt begleiten die Pipelines sie bei der Vorbereitung der Software-Pakete und deren Verteilung auf die produktiven Infrastrukturen (Deployment). Verschiedene Nebenfunktionen, wie die Protokollierung von Ereignissen und die Speicherung sensibler Informationen, werden ebenfalls bereitgestellt. Zwar bleiben noch einige offene Punkte, doch hat diese erste Version ihre Funktionsfähigkeit unter Beweis gestellt: Vier Anwendungen konnten bereits über die Pipelines produktiv gesetzt werden, mehr als hundert sind noch in Arbeit. Der Übernahmeprozess schreitet voran und das BIT und die Leistungsempfängerinnen und -empfänger sammeln Erkenntnisse. Anpassungen sind nach wie vor möglich.

Die Produktivsetzung von Anwendungen muss über eine Pipeline erfolgen. Um den internen und externen Entwicklerinnen und Entwicklern die Anwendung dieses Grundsatzes zu erleichtern, hat das BIT eine umfangreiche Dokumentation in Form von Beschreibungen, Leitfäden, Standards, Videos und Checklisten zusammengestellt.

Für von externen Anbietern schlüsselfertig gelieferte Container-Anwendungen wurde eine spezielle Art von Pipeline eingerichtet. Diese Anwendungen müssen demnach ebenfalls die in den Toolketten festgelegten Tests durchlaufen, um in der produktiven Zielinfrastruktur bereitgestellt zu werden. Damit sind die Bedingungen erfüllt, dass sowohl interne als auch externe Entwicklerinnen und Entwickler die CNCICD-Pipelines sinnvoll nutzen und sicherstellen können, dass die festgelegten Anforderungen erfüllt sind.

Die in die CNCICD-Pipelines eingebetteten automatischen Tests decken nur Anforderungen im Zusammenhang mit dem IT-Grundschutz ab. Diese Tests, von denen nicht alle obligatorisch sind, konzentrieren sich auf die Ermittlung von Schwachstellen und von in Codezeilen sichtbaren Anmeldedaten sowie auf die Qualität des Anwendungscodes. Für die anderen Arten von Anforderungen – ob funktional oder nicht – wurden keine automatischen Tests verwendet. In diesen Fällen wären nämlich aufwändige, anwendungsspezifische Definitionen erforderlich. Das BIT zog es vor, manuelle Validierungsschritte festlegen zu können oder eine Testschleife in ein Ad-hoc-Tool einbauen zu können. Um die Akzeptanz seitens der Leistungsempfängerinnen und -empfänger zu fördern, wurde daher ein Mittelweg zwischen Automatisierung und der Integration manueller Schritte gewählt. Damit bleibt jedoch immer noch ein grosser Teil der Verantwortung für die korrekte Umsetzung der Anforderungen bei den Entwicklungsteams. Nach Ansicht der EFK stellt diese erste Version der CNCICD-Pipelines eine angemessene Ausgangsbasis hinsichtlich der Einbettung der Anforderungstests dar. Sie geht davon aus, dass das BIT die technologische Entwicklung der Testtools weiterverfolgen und die Automatisierung so weit wie möglich ausbauen wird.

Es bestehen Möglichkeiten für die vorübergehende Umgehung von Tests

In Anbetracht der Tatsache, dass automatische Tests manchmal fälschlicherweise positive Ergebnisse hervorbringen oder nicht immer für eine bestimmte Umgebung relevant sind, wurde eine Möglichkeit geschaffen, sie zu deaktivieren (Whitelisting). Gemäss dem dafür festgelegten Verfahren muss eine solche Ausnahme ordnungsgemäss dokumentiert und von der oder dem Leistungsempfangenden und der oder dem Leistungserbringenden bestätigt werden. Die Ausnahme gilt nur für eine begrenzte Zeit. Für die EFK ist diese kontrollierte Abweichung von der Pflicht, Anwendungen zu testen, vertretbar.

Es gibt weitere Möglichkeiten für eine Umgehung. Unter anderem können die Entwicklerinnen und Entwickler eine bestehende Pipeline kopieren und die Kopie abändern, indem sie obligatorische Testschritte entfernen. Sie können sie dann theoretisch dafür verwenden, Anwendungen produktiv zu setzen, ohne sie zu testen. Im Programm Amboss waren Mechanismen zum Schutz der Pipeline-Definitionen mittels kryptografischer Signatur vorgesehen. Sie konnten jedoch noch nicht implementiert werden, da es kein kompatibles Produkt auf dem Markt gibt. Momentan sind die Pipelines also unzureichend geschützt, was jedoch einer der noch offenen Punkte auf der Liste des BIT ist. Eine nachträgliche Erkennung solcher Umgehungsfälle ist aber nach wie vor durch eine Analyse der Ausführungsprotokolle der Pipelines möglich. Aus diesen Gründen verzichtet die EFK auf eine Empfehlung zu diesem Punkt.

Die EFK weist darauf hin, dass sie die Wirksamkeit der im Zusammenhang mit den CNCICD-Pipelines implementierten Kontrollen nicht beurteilen konnte. Das BIT konnte zeigen, dass die Daten hierfür vorhanden sind, deren Analyse ist für eine repräsentative Stichprobe von Produktivsetzungen aber noch nicht ausreichend industrialisiert.

Operationalisierung läuft, Perspektive des IKS muss stärker berücksichtigt werden

Für die Steuerung der CNCICD-Plattform, die Festlegung der Plattform-Governance und die Schwerpunkte für deren zukünftige Entwicklung ist ein Komitee zuständig. Darin sitzen Vertreterinnen und Vertreter der Bereiche Business Solutions und Plattform Services des BIT sowie Sicherheitsexpertinnen und-experten. Die Perspektive des IKS ist in dem Komitee jedoch nicht speziell vertreten.

Ein Referenzrahmen, der die wichtigsten Tätigkeiten im Zusammenhang mit den Pipelines beschreibt, steht kurz vor der Verabschiedung. Von diesen Tätigkeiten werden bereits einige übergeordnete ausgeführt. Diese umfassen insbesondere die Überwachung der Funktionsfähigkeit und die Kontrolle der Sicherheit und des ordnungsgemässen Zustands der Pipelines und Anwendungen. Ende Dezember 2023 wurde dementsprechend ein Sicherheitsaudit der Pipelines durchgeführt.

Die Prozesse und Verantwortlichkeiten, die sich aus den im Referenzrahmen beschriebenen Tätigkeiten ergeben, sind jedoch noch nicht alle definiert und institutionalisiert, ihre Operationalisierung steht jedoch auf der Agenda des Komitees. Die EFK verzichtet daher diesbezüglich auf eine Empfehlung. Sie hat aber empfohlen, die Perspektive des IKS innerhalb des Komitees und auf dessen Agenda stärker zu berücksichtigen.

Originaltext auf Französisch