Benutzer der IBM Rational AppScan Source Edition können Schwachstellen in Softwareprogrammen für das gesamte Softwareportfolio analysieren und messen. Unterstützt werden sie hierbei durch einheitliche Messverfahren und Kennzahlen und die Möglichkeit, die Informationen so aufzubereiten, wie es den Anforderungen im Unternehmen entspricht.

Dezember 2009

Rational. software

Vertrauen ist gut, Kontrolle ist besser

Risikomanagement beim Anwendungsoutsourcing

Ryan Berg
IBM Senior Security Architect
IBM Software Group

Kernaussagen

„84 Prozent der InformationWeek 500-Unternehmen haben die Anwendungsentwicklung und -integration ausgelagert.“
– InformationWeek-Studie

Überblick

Kosteneinsparungen, beschleunigte Entwicklung, Entlastung des eigenen Personals oder Nutzung von Know-how, das intern nicht verfügbar ist. Es gibt viele und unterschiedlichste Gründe, die dafür sprechen, die Entwicklung von Anwendungen auszulagern. In der modernen, internetbasierten Wirtschaft kann Outsourcing eine kostengünstige und wirtschaftliche Strategie sein, um die Nachfrage nach neuen und spezialisierten Anwendungen zu bedienen.

Bei der Bewertung der ausgelagerten Anwendung muss die Frage der Sicherheit jedoch angemessen berücksichtigt werden, bevor ein Release abgenommen werden kann. Es muss einen von beiden Seiten akzeptierten Prozess geben, mit dem die Sicherheit der gelieferten Lösung beschrieben und bestätigt werden kann. Anhand dieser Informationen ist es Organisationen möglich, Anwendungsrisiken zu kontrollieren und die Wichtigkeit von Korrekturmaßnahmen abzuwägen. Dieses White Paper beschäftigt sich mit folgenden Fragen:

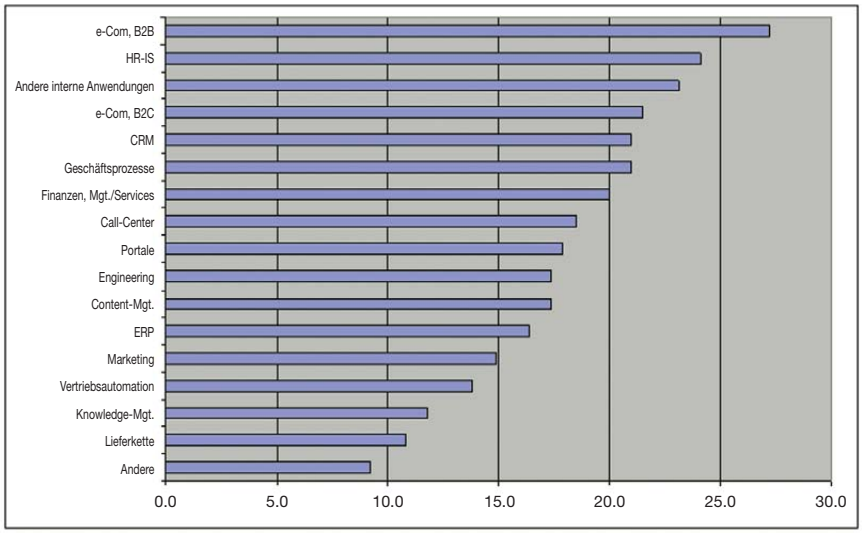
- *Warum sollten Sicherheitsfragen beim Anwendungsoutsourcing eine wichtige Rolle spielen?*
- *Wie können diese Fragestellungen gemeinsam mit Outsourcingpartnern aufgegriffen werden?*
- *Welche Rolle spielen Technologien für die Quellcodeprüfung und vergleichbare Technologien für die Bewertung und Zertifizierung ausgelagerter Anwendungen?*

Outsourcing im Vormarsch

Outsourcing ist weiterhin eine wichtige Ressource im Rahmen der Anwendungsentwicklung. Wie eine InformationWeek-Studie zeigt, setzen 84 Prozent der InformationWeek 500-Unternehmen bei der Anwendungsentwicklung und -integration auf Outsourcing.[1] Branchenübergreifend gehen immer mehr Unternehmen dazu über, die Entwicklung auch wichtiger Anwendungen auszulagern, um ihre Flexibilität

zu erhöhen, Kosten zu kontrollieren und das intern verfügbare Know-how zu ergänzen. Andere Berichte gehen davon aus, dass beim Outsourcing von Unternehmensanwendungen bis 2007 mit einer Wachstumsrate von 7,3 Prozent rechnen ist. Laut Tower Group ist zu erwarten, dass der Umfang der IT-Arbeiten, die von den 15 größten Finanzinstituten weltweit an ausländische Firmen ausgelagert werden, in den nächsten vier Jahren um jährlich 34 Prozent und somit von derzeit 1 Mrd. US-Dollar auf 2,5 Mrd. US-Dollar in 2008 ansteigen wird.[2]

Abb. 1: Anwendungen, deren Entwicklung ausgelagert werden soll



Quelle: CIO Insight

Kernaussagen

Organisationen entscheiden sich in zunehmendem Maße für das Outsourcing ihrer wichtigsten und sensibelsten Anwendungsprojekte.

Es ist jedoch nicht nur eine allgemein Zunahme beim Outsourcing der Anwendungsentwicklung zu verzeichnen; immer mehr Unternehmen entscheiden sich dafür, auch ihre wichtigsten und sensibelsten Anwendungsprojekte auszulagern (Abb. 1). E-Commerce-Anwendungen, Informationssysteme für das Personalwesen oder Anwendungen für Finanzdienstleistungen, die mit extrem wichtigen und vertraulichen Daten arbeiten und unternehmenskritische Prozesse steuern, werden immer häufiger extern und im Ausland entwickelt.[3] Für Unternehmen, die solche Anwendungen regelmäßig auslagern, ist es unverzichtbar, den Sicherheitsstatus der gelieferten Lösungen zu kontrollieren.

Ausgelagerte Entwicklung: die wichtigsten Fragestellungen

Beim Outsourcing von Entwicklungsarbeiten sind im Hinblick auf das Thema Sicherheit verschiedene Aspekte zu beachten. Diese Aspekte erfordern eine sorgfältige Planung, Umsetzung und Kontrolle, um vor der Abnahme der gelieferten Software sicherzustellen, dass ihnen angemessen Rechnung getragen wurde. Folgendes ist zu berücksichtigen:

Sachgerechter Einsatz von Sicherheitsmechanismen: Wurden die erforderlichen Sicherheitsmechanismen eingebunden, um sicherzustellen, dass die Anwendung nur die gewünschten Funktionen erfüllt? Wurden diese Sicherheitsmechanismen ordnungsgemäß implementiert? Einwandfreier Entwurf und ordnungsgemäße Implementierung müssen überprüft werden, um sicherzustellen, dass die Voraussetzungen für wirksame Sicherheit erfüllt sind.

Bewährte Verfahren für die sichere Softwareentwicklung: Greift der Outsourcingpartner auf eine genau definierte Sammlung bewährter Verfahren für die sichere Softwareentwicklung zurück? Wie sind diese Verfahren dokumentiert, und wie wird ihre Einhaltung überprüft? Verfahren für die sichere Softwareentwicklung basieren auf festgelegten und genau beschriebenen Standards und müssen fester Bestandteil der Entwicklungsprozesse des Outsourcingpartners sein.

Kernaussagen

Erfahrung und Qualifikation der Programmierer: Verfügen die Programmierer über das Know-how, um die Techniken für die sichere Softwareentwicklung umzusetzen? Wie wird dies dokumentiert und definiert? Welche Prozesse wurden definiert, um die Einhaltung der Techniken zur sicheren Softwareentwicklung sicherzustellen? Es ist unerlässlich, dass die an einem Outsourcingprojekt beteiligten Entwickler über das entsprechende Know-how und das Wissen um die Bedeutung dieser Strategien verfügen. Die meisten Entwickler sind für die sichere Programmierung nicht hinreichend ausgebildet, unabhängig davon, ob sie für ein Outsourcingunternehmen arbeiten oder nicht.

Existenz bösartigen Programmcodes: Gibt es ein Prüfverfahren, um sicherzustellen, dass die Software keinen bösartigen Code enthält? Sind die Prüfer darin geschult, bösartigen Code in Softwareprodukten zu identifizieren? Es empfiehlt sich, einen Prozess für die Überprüfung wichtigen Codes im Hinblick auf Gefahren wie Viren, Würmer, Backdoors und Trojanische Pferde zu definieren.

Gesetzliche Vorgaben

„Die Festlegung von Sicherheitsanforderungen, Abnahmekriterien und Testplänen sowie die Prüfung und das Testen von Quellcode im Hinblick auf Sicherheitslücken müssen fester Bestandteil von Programmen für das Lieferantenmanagement sein.“

– FFIEC Information Security Handbook

Das regulatorische Umfeld spiegelt das steigende Bewusstsein dafür wider, dass Anwendungssicherheit, insbesondere bei ausgelagerten Anwendungen, ein unverzichtbarer Bestandteil für die Sicherheit wichtiger Infrastrukturen sowie für die Integrität und den Schutz von Daten ist. Für jede Branche gelten eigene behördliche Vorgaben, die erfüllt werden müssen. So wird beispielsweise im Information Security Handbook des Federal Financial Institutions Examination Councils (FFIEC), das ein Leitfaden für die Implementierung des Gramm-Leach-Bliley Act (GLBA) ist, explizit festgestellt, dass die betreffenden Unternehmen ein Programm für das Lieferantenmanagement einführen müssen, das die Festlegung von Sicherheitsanforderungen, Abnahmekriterien und Testplänen sowie die Prüfung und das Testen von Quellcode im Hinblick auf Sicherheitslücken umfasst.[4] Gemäß dem Federal Information Security Management Act von 2002 (FISMA) müssen Behörden Schwachstellen in Informationssystemen, einschließlich Anwendungen, identifizieren und beseitigen. Diese Anforderungen gelten unabhängig davon,

Kernaussagen

ob die Anwendungen intern entwickelt oder von einer anderen Behörde, einem Lieferanten oder einer anderen Quelle bereitgestellt oder verwaltet werden.[5] Viele Behörden schnitten in den offiziellen Beurteilungen für 2005 und 2006 mit einem Durchschnittsergebnis von C- ausgesprochen schlecht ab, wobei im Vergleich zu früheren Jahren nur geringfügige Verbesserungen zu verzeichnen waren.[6]

Die Besorgnis der amerikanischen Regierung hinsichtlich der Sicherheit ausgelagerter Anwendungen, insbesondere, wenn es um wichtige Infrastrukturanwendungen und militärische Waffensysteme geht, wurde besonders nachdrücklich in einem kürzlich vom Government Accountability Office (GAO) vorgelegten Bericht mit dem Titel „Defence Acquisitions: Knowledge of Software Suppliers Needed to Manage Risk" formuliert. Obwohl sich die Hauptlieferanten des Verteidigungsministeriums bei der Entwicklung von Software für Waffensysteme zunehmend auf die Arbeit externer Vertragspartner stützen, ergab die Prüfung des GAO, dass Programm-Manager nach den Richtlinien des Verteidigungsministeriums den Erwerb und die Sicherheit von Software betreffend nicht verpflichtet sind, die Risiken des Einsatzes externer Lieferanten für die Entwicklung von Software für Waffensysteme zu identifizieren und zu kontrollieren. GAO und Verteidigungsministerium erkannten hierin ein schwerwiegendes Problem und kamen zu dem Schluss, dass das Verteidigungsministerium mittels entsprechender Maßnahmen sicherzustellen hat, dass der Frage der Sicherheit ein fester Platz im Rahmen der Entscheidungsfindung zukommen muss und Programm-Manager die Risiken entsprechend kontrollieren müssen.[7] Gesetzgeberische und regulatorische Aktivitäten unterschiedlichster Regierungsstellen untermauern eindeutig die Erkenntnis, dass für Anwendungen, die mit sensiblen Daten arbeiten, eine klare und einheitliche Methode erforderlich ist, um Sicherheitsanforderungen genau definieren, ausformulieren, implementieren und überprüfen zu können.

Sicherheitsaspekte beim Outsourcing berücksichtigen

Sicherheitsanforderungen sollten ein fester Bestandteil der funktionalen Anforderungen eines Service-Level-Agreements (SLA) sein.

Sicherheitsfragen müssen systematisch und gewissenhaft im gesamten Softwareentwicklungszyklus Rechnung getragen werden, angefangen beim Entwurf bis hin zur Bereitstellung der fertigen Lösung. Dies gilt insbesondere dann, wenn ein Outsourcingpartner mit der Entwicklung beauftragt wird. Zwei wesentliche Schritte sind erforderlich, um eine Due-Diligence-Struktur zu schaffen, damit vor der Abnahme der Software sichergestellt werden kann,

dass diese die geforderten Sicherheitsmerkmale erfüllt. Dieser Rahmen ist unerlässlich, um Outsourcingpartner hinreichend für die Sicherheitsanforderungen der zu entwickelnden Anwendung zu sensibilisieren:

Detaillierte Definition wichtiger Daten und Prozesse: Sicherheitsanforderungen müssen ein fester Bestandteil innerhalb der funktionalen Anforderungen an das Projekt insgesamt sein. Zu diesen Anforderungen können beispielsweise Details wie die folgenden gehören:

- *Proprietäre Daten*
- *Vertrauliche Daten*
- *Datenschutzüberlegungen*
- *Berechtigung für wichtige Funktionen*

Genaue Beschreibung des geschäftlichen Nutzens, der Zielgruppe und der Offenlegung: Bei dieser Analyse werden Informationen zum Nutzen der geplanten Anwendungen für die Ziele einer Organisation unter operativen und/oder finanziellen Gesichtspunkten erfasst. Es wird außerdem abgeschätzt, in welchem Umfang die Anwendung einer breiten Öffentlichkeit zugänglich sein wird und welche Zielgruppe(n) sie anspricht.

Geschäftlicher Nutzen: Welche Bedeutung hat diese Anwendung oder das Netzwerk im Hinblick auf das finanzielle oder operative Wohl der Organisation? Bestimmen lässt sich dies auf der Basis der Einnahmen, die mit einer Anwendung generiert würden, oder anhand der internen Kosten, die durch eine nicht mehr funktionierende Anwendung verursacht würden.

Zielgruppe und Offenlegung: Wem dient die Anwendung oder das Netzwerk und wie zugänglich muss sie bzw. es sein, um dieser Zielgruppe zu dienen? Inwiefern ist die Anwendung für externe Benutzer zugänglich? Die Offenlegung wird bestimmt durch die Anzahl der Personen, die Zugriff auf das Netzwerk oder die Anwendung benötigen, die Funktion, die sie innerhalb der Organisation erfüllen, und die Berechtigungen, die diesen Personen eingeräumt werden. Einfache Informationswebsites ohne interaktive Komponenten

verzeichnen ein hohes Maß an Datenverkehr, legen jedoch nur wenig Funktionalität für die Besucher der Site offen. E-Commerce-Websites ermöglichen es hingegen nahezu jedem, einzukaufen und dabei echtes Geld auszugeben und vertrauliche Informationen auszutauschen. Zur Definition des Grads der Offenlegung muss auch eine Beschreibung der Sicherheit der Bereitstellungsumgebung gehören, um die Bedingungen darzustellen, unter denen die einzelne Anwendung möglicherweise Back-End-Daten und -Ressourcen offen legen kann.

Abb. 2: Adäquate Sicherheitsmechanismen

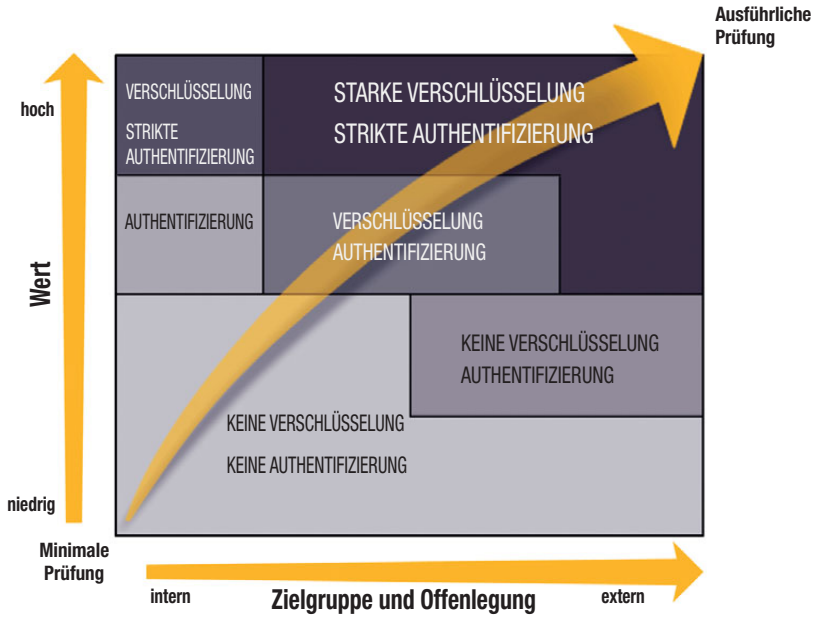


Abbildung 2 zeigt, welche Sicherheitsmechanismen für die Anwendung oder den Prozess bezogen auf den geschäftlichen Nutzen und die Zugänglichkeit angemessen sind. Diese Analyse muss dem Outsourcingpartner zur Verfügung gestellt werden, um ihn hinreichend über die Zusammenhänge und die Bedeutung des Projekts für die übergeordneten Ziele der Organisation zu informieren.

Sicherheit als vertraglich festgeschriebene Leistung

Nachdem die Sicherheitsanforderungen identifiziert wurden, müssen diese Anforderungen sowie ein Prüfprozess zur Bestätigung der erfolgreichen Implementierung in die Ausschreibung und den endgültigen Vertrag aufgenommen werden. Angesichts des Trends, Entwicklungsarbeiten auszulagern, wurde bereits viel über die Prozesse geschrieben, die ein unter zeitlichen und finanziellen Gesichtspunkten erfolgreiches Projekt sicherstellen sollen. In vielen Organisationen werden Service-Level-Agreements definiert, die Erwartungen und Bedingungen, Meilensteine und Liefergegenstände auf der Grundlage eines vorgegebenen Zeitplans festlegen. Abnahmekriterien für die Sicherheit der gelieferten Anwendungen werden jedoch in vielen Verträgen nicht angemessen definiert, bewertet und festgelegt. Und auch unter den Unternehmen, die ihre Sicherheitsanforderungen vertraglich festschreiben, finden sich nur wenige, die über eine Methode verfügen, um vor der Abnahme und Bereitstellung des betreffenden Produkts untersuchen oder bestätigen zu können, ob der Code sicher ist. Angesichts der sensiblen Natur etlicher Anwendungen ist es jedoch unverzichtbar, wirksame Methoden und Kriterien einzuführen, um die Vertraulichkeit und Integrität der Daten sicherzustellen, die mit ausgelagerten Anwendungen verarbeitet werden.

Bekannte Sicherheitsanalytiker betonen regelmäßig die Notwendigkeit, die Sicherheit des zu liefernden Codes in die Vertragsbedingungen von Entwicklungsverträgen aufzunehmen. Zu diesen Bedingungen sollten das Recht zur Prüfung des Codes, die Beseitigung von Sicherheitslücken, die Definition von Methoden für die sichere Entwicklung sowie eine Software Security Assurance-Garantie (SSA) gehören.

Diesen Experten zufolge sollte ein entsprechender Vertragszusatz vier Hauptbereiche benennen:

Das Recht zur Prüfung: Die Organisation schreibt vor, dass SSA Teil des Prozesses ist und dass über die Zuständigkeiten beider Parteien vor der Endabnahme Einvernehmen besteht.

Korrekturen: Werden bei der Prüfung Mängel festgestellt, muss es einen klar definierten Prozess für die Beseitigung schwerwiegender Schwachstellen vor der Endabnahme geben. Die Details dieser Korrekturphase müssen im Vertrag eindeutig dargelegt sein.

Entwicklungsmethoden: Verfahren für die sichere Softwareentwicklung, die während der Entwicklung des Projekts oder der Anwendung einzuhalten sind, müssen klar definiert und dokumentiert sein.

Sicherheitsgarantie: Falls identifizierte Schwachstellen nicht beseitigt werden, müssen Richtwerte verfügbar sein, auf deren Grundlage die Software als unsicher eingestuft und somit eine Verletzung der Bedingungen des Vertragszusatzes festgestellt werden kann.[8]

Die Abstimmung von finanziellen Vereinbarungen, Vertragsstrafen und Anreizen mit Geschäftszielen sorgt bei den Beteiligten für mehr Sicherheit im Hinblick auf die Erwartungen der jeweils anderen Seite und beseitigt potenzielle Konfliktquellen, falls Korrekturmaßnahmen erforderlich sein sollten. Durch die Sicherheitsgarantie ist für beide Seiten klar geregelt, wie im Falle von Mängeln zu verfahren ist. Hierdurch werden nicht nur Risiken für den Kunden vermieden; auch dem Outsourcingpartner bietet sich auf diese Weise eine gute Möglichkeit, um sich mit dem eigenen Angebot abzusetzen und gleichzeitig eine dauerhafte Partnerschaft aufzubauen.

Die Notwendigkeit von Codesicherheitsprüfungen

Im Rahmen der Sicherheitsprüfung muss der Quellcode eingehend auf Sicherheitslücken untersucht werden. Nicht sichere Software führt zu Einkommensverlusten, geringerem Nutzen für die beteiligten Interessengruppen, Haftbarkeit, Nichteinhaltung behördlicher Vorschriften und Reputationsverlust.

Die Analyse des Anwendungsquellcodes erfüllt vier Funktionen: Zertifizierung, Priorisierung, Verfolgung und Korrekturmaßnahmen. Bei der Auswahl eines Tools für die Quellcodeanalyse oder eines Audit-Anbieters muss das Tool danach bewertet werden, ob und wie gut es auf der Basis Ihrer Prioritäten konsistente, kennzahlenbasierte Daten zur Schwachstellenanalyse in diesen vier Bereichen bereitstellen kann:

Zertifizierung

Zertifizierungs- und Zulassungsaktivitäten gehen für gewöhnlich auf externe oder interne Prüfauflagen zurück und dienen dazu, behördlichen, datenschutztechnischen und stabilitätsbezogenen Vorgaben für neue, aktualisierte oder erneut implementierte Anwendungen Rechnung zu tragen. Bei ausgelagerten Anwendungen ist dieser Aspekt von höchster Bedeutung, denn die Zertifizierung wird hier zum letzten Abnahmekriterium, bevor die Zahlung erfolgt. Für alle Zertifizierungs- und Zulassungsaktivitäten ist Folgendes unerlässlich:

- *Verständliche Berichte in verschiedenen Formaten, um sie online oder in gedruckter Form lesen zu können*
- *Zuverlässige Kennzahlen, um Bewertungen anhand von Richt- und Schwellenwerten zu ermöglichen*

Priorisierung

Sicherheitsbudgets decken nur sehr selten die Kosten für die anwendungsübergreifende Analyse und Mängelkorrektur. Aus diesem Grund müssen Tools für die Analyse der Softwaresicherheit, die zur Priorisierung dieser Bemühungen eingesetzt werden, zwei verschiedene Maßzahlen für die Kritikalität liefern. Mithilfe dieser Maßzahlen können sich Anbieter und auftraggebende Organisation auf die zu behebenden Mängel auf der Grundlage ihrer Dringlichkeit oder Position konzentrieren.

- *Anfälligkeit mehrerer Anwendungen, Projekte oder Gruppen gemäß der Anzahl und Dringlichkeit der identifizierten Schwachstellen*
- *Dringlichkeit einzelner Anwendungsschwachstellen gemäß Typ und Auswirkungen*

Verfolgung

Sicherheit ist keine statische, sondern eine veränderliche Größe, wobei absolute Sicherheit weder bezahlbar noch erreichbar ist. Organisationen müssen daher ein Ziel im Hinblick auf einen angemessenen Grad an Sicherheit definieren. Jedes Produkt für die Schwachstellenanalyse muss die Möglichkeit bieten, die Anfälligkeit ausgelagerter Anwendungen zu einem bestimmten Zeitpunkt als Ausgangswert festzulegen, um dann einheitliche Methoden anzuwenden, mit deren Hilfe der Fortschritt von Korrekturmaßnahmen verfolgt werden kann. Damit diese Informationen möglichst aussagekräftig sind, muss die Verfolgung und Fortschrittsprotokollierung zwei Kriterien erfüllen.

- ***Detailgenauigkeit der bewerteten Objekte:*** *Während verschiedene Kennzahlen auf unterschiedlichen Organisationsebenen allgemein für die gesamte Organisation verfolgt werden, können Entwicklungsmanager die Verfolgung im Laufe eines Outsourcingprojekts auch auf Anwendungs-, Projekt- oder Dateiebene steuern. Damit Kennzahlen allgemein gültig und nachvollziehbar sind, muss die Datenverfolgung auf unterschiedlichen Aggregationsebenen unterstützt werden.*
- ***Regelmäßige Bewertungen:*** *Einheitliche, geplante Bewertungen als Grundlage für Fortschrittsberichte sind in den meisten Fällen sinnvoll und aufgrund verschiedener behördlicher Vorgaben oftmals obligatorisch. Die Automatisierung des Bewertungsprozesses oder eine geplante Analyse ist ein effektives Verfahren, um regelmäßige und reproduzierbare Berichte für interne und externe Prüfungen sicherzustellen.*

Korrekturmaßnahmen

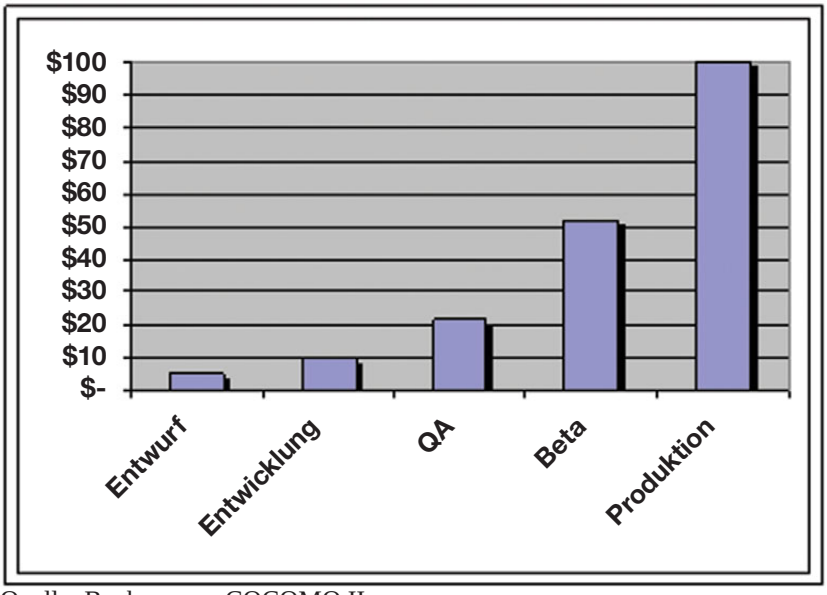
Die Beseitigung von Schwachstellen kann je nach Art der Anwendung, der Sicherheitslücke und der Organisation auf unterschiedliche Weise erfolgen. Die Abnahme ausgelagerter Anwendungen erfolgt auf der Grundlage klar definierter Richt- und Schwellenwerte, und alle erforderliche Korrekturen müssen vor der Bereitstellung und vollständigen Bezahlung vorgenommen werden. Durch diesen Ansatz wird nicht nur das von ausgelagerten Anwendungen ausgehende Risiko für organisationsinterne Prozesse verringert, er trägt auch zu einer Senkung der Entwicklungs- und Supportkosten bei. Im Rahmen seiner Arbeiten zum Kostenmodell COCOMO II am Zentrum für Software Engineering der University of Southern California konnte Dr. Barry Boehm feststellen, dass die Kosten für die Korrektur eines Programmfehlers, dessen Beseitigung in der Entwurfsphase einen US-Dollar kostet, in der Produktionsumgebung auf 100 US-Dollar ansteigen. (Abb. 3).

Bei einigen Entwicklungsprojekten übernimmt der Outsourcingpartner die Verantwortung für die Korrektur sämtlicher Fehler, die festgestellt und als bedeutsam identifiziert werden. Den Entwicklern müssen die folgenden Informationen zur Verfügung stehen, damit sie alle erkannten Probleme nachvollziehen und beseitigen können.

1. Genaue Kennzeichnung der Position des Problems, einschließlich Angaben zur Datei, Zeile und Spalte. Der zeitliche und finanzielle Aufwand für Korrekturmaßnahmen kann auf diese Weise drastisch reduziert werden.

2. Mit eindeutigen Beschreibungen des identifizierten Problems, einschließlich Angaben zu möglichen Auswirkungen und zur Schwere des Missbrauchs, können Entwickler für die Verfahren der sicheren Programmierung sensibilisiert werden. Dies ist erforderlich, um nachhaltige Verbesserungen bei laufenden und zukünftigen Projekte zu erzielen.

Abb. 3: Kosten für Korrekturmaßnahmen



Quelle: Boehm u. a., COCOMO II

3. Schlüssige Vorschläge zu Verbesserungen, ob mittels alternativer Strukturen oder sichererer Routinen, sind notwendig, um den zeitlichen Aufwand für die Behebung von Problemen zu minimieren.

4. Die Zusammenstellung von Problemen nach Position, Fehlertyp oder anfälliger Routine ist notwendig, um die Arbeiten zur Schwachstellenbeseitigung mit anderen Entwicklungsprozessen verbinden zu können und auf diese Weise die Effektivität zu erhöhen.

Kernaussagen

Eine Sicherheitsprüfung des Quellcodes ist unverzichtbar, um die Sicherheit der gelieferten Anwendung sicherzustellen. Bis vor kurzem gab es nur ein bewährtes Verfahren, um den Sicherheitsstatus einer Anwendung präzise zu ermitteln. Eine Organisation beauftragt ein spezielles Team – interne Ressourcen oder einen externen Dienstleister mit entsprechendem Know-how – mit der manuellen Untersuchung des Quellcodes, um auf diese Weise Schwachstellen identifizieren und Korrekturmaßnahmen vom Outsourcingpartner anfordern zu können. Auch wenn es sich hierbei um ein effektives Verfahren zur Bewertung von Quellcode handelt, ist diese Vorgehensweise normalerweise sehr teuer und zeitaufwändig und lässt sich maximal ein- oder zweimal pro Jahr realisieren. Um die Prüf- und Zertifizierungsvorgaben eines Service-Level-Agreements für Outsourcing-projekte zu erfüllen, ist daher ein kostengünstigeres, einheitlicheres und kennzahlenbasiertes Verfahren für die Schwachstellenanalyse und -korrektur erforderlich.

Softwarerisikoanalyse und IBM

Mittlerweile stehen erprobte Technologien für Sicherheitstests zur Verfügung, um zentrale Elemente dieses Prozesses zu automatisieren. Zu den im Handel erhältlichen Lösungen zählen Produkte, die Quellcode automatisch im Hinblick auf Sicherheitslücken analysieren können. Ein Beispiel für eine Lösung zur Analyse von Softwarerisiken ist IBM Rational AppScan Source Edition. Dieses Produkt bietet Funktionen, um Quellcode auf Sicherheitslücken zu überprüfen, und stellt präzise Detailinformationen und Korrekturempfehlungen zu Programmierungsfehlern, Mängeln im Programmentwurf und Richtlinienverletzungen bereit. Mithilfe dieser Informationen können Sicherheitsmanager, Analytiker und Entwickler die Sicherheitsprüfung von Softwareprodukten unterstützen, die Risiken gefährdeter Software kontrollieren und Sicherheitslücken in der Software bereits im Quellcode beseitigen.

Eine Sicherheitsprüfung des Quellcodes ist unverzichtbar, um die Sicherheit der gelieferten Anwendung sicherzustellen.

Rational AppScan Source Edition bietet Organisationen zahlreiche Vorteile, wenn es um Fragen der Sicherheit bei der ausgelagerten Anwendungsentwicklung geht:

Schnelle Identifizierung der schwerwiegendsten Sicherheitsrisiken:

Fester Bestandteil jeder Analyse muss die Untersuchung grundlegender Fragestellungen wie Pufferüberlauf und Eingabe- oder Ausgabeüberprüfung sein. Die bloße Identifizierung dieser Bereiche macht eine Anwendung jedoch nicht sicher. Die unsachgemäße Implementierung anderer Sicherheitsmechanismen, was auch die Verwendung der Kryptografie, Methoden für sichere Netzwerkverbindungen und die Zugriffssteuerung umfasst, kann für die Organisation ein deutlich größeres Risiko darstellen.

Bei der ausgelagerten Anwendungsentwicklung ist die Identifizierung dieser eher unscheinbaren Schwachstellen eine noch anspruchsvollere Aufgabe. So ist das Know-how zum sachgerechten Umgang mit Kryptografie, um Complianceanforderungen zu erfüllen, intern möglicherweise vorhanden. Es ist jedoch alles andere als leicht, diese Anforderungen präzise zu formulieren und dann sicherzustellen, dass sie tatsächlich erfüllt wurden.

Mit der patentierten Automatisierungslösung Rational AppScan Source Edition können die unterschiedlichsten Programmierungsfehler und Entwurfsmängel erkannt werden. Auf diese Weise lässt sich problemlos feststellen, ob der gelieferte Code die definierten Sicherheitsanforderungen erfüllt und ob, ausgehend von den Bedingungen des Service-Level-Agreements, ggf. Korrekturmaßnahmen erforderlich sind. Bei der Beurteilung von Zertifizierungs- und Zulassungsmethoden für die Abnahme ausgelagerten Codes werden diese Leistungsmerkmale sehr leicht außer Acht gelassen.

Effektivitätsmaximierung im Bereich der Sicherheitsverwaltung

Softwaresicherheit ist kein Thema, das nur innerhalb einer einzelnen Abteilung relevant ist, sondern im Gegenteil eine unternehmensweite Aufgabe, die Sicherheitsanalytiker, Entwickler, Führungskräfte und Prüfer betrifft. Codeprüfer und Zertifizierungs- und Zulassungsexperten benötigen Ergebnisse innerhalb von Minuten und nicht erst nach mehreren Tagen. Berichte müssen anpassbar sein, um auf das aktuell geltende SLA abgestimmt zu sein, und die jeweils kritischen Bereiche hervorheben können. Auf diese Weise können Abweichungen vom SLA und entsprechende Lösungen schnell und eindeutig identifiziert und ausgehandelt werden. Dank der präzisen, handlungsrelevanten Ergebnisse, Berichte und Korrekturvorschläge von Rational AppScan Source Edition können notwendige Maßnahmen in kürzester Zeit ergriffen werden.

Rational AppScan Source Edition unterstützt Organisationen bei sicherheitsrelevanten Prüfungen und Kontrollen während des gesamten Softwareentwicklungszyklus und stellt eine Lösung bereit, die von unterschiedlichen Interessengruppen und Verantwortlichen genutzt werden kann, angefangen bei Sicherheitsanalytikern über Qualitätssicherungsanalytiker und -entwickler bis hin zu Führungskräften und Sicherheitsmanagern. Es liefert ausführliche Management- und Sicherheitsberichte, die Entwurfsmängel und Richtlinienverletzungen genau identifizieren, was auch Mängel in den Bereichen Zugriffssteuerung, Kryptografie, Eingabeüberprüfung und Protokollierung umfasst. Ein zentrales Verwaltungsdashboard stellt zusammengefasste Informationen für ein vollständiges Softwareportfolio zur Verfügung und trägt mit spezifischen Kennzahlen und Trendberichten zu Sicherheitsrisiken dazu bei, die Entscheidungsfindung zu optimieren.

Entwickler können Rational AppScan Source Edition in der integrierten Entwicklungsumgebung ausführen, was die schnelle Identifizierung von Sicherheitslücken auf Codeebene und den problemlosen Zugriff auf ausführliche Handlungsanweisungen zu konkreten Problemstellungen ermöglicht. Durch den Einsatz dieser Lösung sind Entwickler bei der Entwicklung und Wartung sicheren Codes gleichberechtigte Akteure. Sie kann außerdem mit führenden Fehlererfassungssystemen verknüpft werden, um die Zeit zwischen Schwachstellenerkennung und -beseitigung zu verkürzen.

Mit Rational AppScan Source Edition stehen der gesamten Organisation die Tools und Informationen zur Verfügung, die notwendig sind, um Sicherheitslücken in jeder Phase des Entwicklungszyklus identifizieren und beheben zu können. Insbesondere bei engen Entwicklungszeitplänen bietet Rational AppScan Source Edition ein kostengünstiges, zweckmäßiges und konsistente Ergebnisse produzierendes Verfahren, um die Sicherheit ausgelagerter Anwendungen vor der endgültigen Abnahme zu überprüfen.

Risikomanagement für das gesamte Unternehmensportfolio:

Für die effektive Steuerung einer Anwendungssicherheitsstrategie ist ein Verfahren unverzichtbar, das es ermöglicht, relative Risiken für das gesamten Anwendungsportfolio zu messen und zu vergleichen und gegen die damit verbundenen geschäftlichen Risiken abzuwägen.

Dank einheitlicher Messungen und Kennzahlen, die Rational AppScan Source Edition unterstützt, können Benutzer die Softwarerisiken für das gesamte Softwareportfolio leichter messen und nachvollziehen und die Ergebnisse so aufbereiten, wie es den Anforderungen im Unternehmen entspricht. Die patentierte, compilerbasierte Analysetechnologie ermöglicht die schnelle Analyse auch bei einigen der komplexesten Anwendungen, die derzeit eingesetzt werden. Dank der flexiblen Bereitstellungsoptionen kann das Tool so genutzt werden, wie es sich für die jeweilige Organisation am besten eignet: lokal in der integrierten Entwicklungsumgebung, um überall im Netzwerk darauf zugreifen und Code analysieren zu können, oder als Remoteinstallation, sodass mobile Benutzer von ihrem Laptop jederzeit darauf zugreifen können.

Integrierte Sicherheit

Die Frage der Sicherheit von Anwendungen, die das Fundament für wichtige Prozesse innerhalb einer Organisation bilden, darf nicht länger eine untergeordnete Rolle spielen. Natürlich wird niemand unterstellen, dass ein Softwarelieferant absichtlich und böswillig Sicherheitslücken in eine Anwendung einbaut. Es ist vielmehr so, dass die meisten Schwachstellen auf unzureichendes Know-how im Hinblick auf bewährte Verfahren für die

sichere Softwareentwicklung oder – angesichts knapper Zeitpläne und immer neuer Anforderungen – auf mangelnde Sorgfalt bei der Programmierung zurückzuführen sind. Glücklicherweise stehen nun Verfahren zur Verfügung, um die Sicherheit unternehmenswichtiger Anwendungen zu untersuchen, Fehler ggf. zu korrigieren und das Ergebnis erneut zu überprüfen, und zwar unabhängig davon, ob die Anwendungen intern oder von einem Outsourcingpartner entwickelt werden. Software Security Assurance bietet einer Organisation u. a. folgende Vorteile:

- **Geringeres Risiko.** *Indem Sicherheitslücken bereits vor der Bereitstellung behandelt werden, sind Anwendungen weniger anfällig für externe und interne Bedrohungen.*
- **Compliance.** *Die Berichts- und Prüfauflagen sind Teil des Abnahmeverfahrens. Prüfer, Kontrollbeauftragte und Regulierungsbehörden können den SSA-Prozess problemlos überwachen.*
- **Datenintegrität.** *Software Security Assurance erhöht das Vertrauen in die Integrität von Daten und in die Geschäftsprozesse, die für die Ziele der Organisation wichtig sind.*
- **Kostenkontrolle.** *Die Kosten für die Identifizierung und Beseitigung von Sicherheitslücken in Code, der von Drittanbietern entwickelt wurde, machen einen Großteil der ungeplanten Ausgaben aus, sofern dieser Aspekt nicht proaktiv im SLA geregelt ist. Die durch Sicherheitsverletzungen verursachten Kosten können für ein Unternehmen verheerende Folgen haben.*
- **Verfügbarkeit und Stabilität.** *Sicherere Software bedeutet größere Widerstandsfähigkeit bei Angriffen und Gefahren und höhere Verfügbarkeit wichtiger Systeme.*

Die explizite und frühzeitige Benennung der Sicherheitsanforderungen an eine ausgelagertes Projekt, das Wissen um die Bedeutung, die ein Projekt für die Ziele einer Organisation hat, und die vertragliche Festlegung von Abnahmekriterien sind wesentliche Faktoren, um sicherzustellen, dass der vom Outsourcingpartner gelieferte Code sicher ist. Nun sind das Know-how und die Tools verfügbar, die eine zweckmäßige Bewertung der Sicherheit von Quellcode vor der Endabnahme sowie die Überprüfung der Einhaltung von Auflagen und Vorschriften auf Seiten des Lieferanten ermöglichen.

Weitere Informationen

Weitere Informationen zu IBM Rational AppScan Source Edition erhalten Sie bei Ihrem IBM Ansprechpartner oder IBM Business Partner oder unter:

ibm.com/software/rational/products/appscan/source/

Ryan Berg ist Senior Security Architect bei IBM. Er ist ein bekannter Referent, Schulungsleiter und Autor für Sicherheits-, Risikomanagement- und sichere Entwicklungsprozesse. Er hält in folgenden Bereichen Patente bzw. hat Patente angemeldet: Sicherheitsanalysen in mehreren Sprachen, Sicherheit auf Kernel-Ebene, Sprachen für zwischengeschaltete Sicherheitsanalysen und sichere Remote-Übertragungsprotokolle.

IBM Deutschland
IBM-Allee 1
D-71139 Ehningen
Germany
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter: **ibm.com**

IBM leistet keine rechtliche Beratung oder Beratung bei Fragen der Buchführung und Rechnungsprüfung. IBM gewährleistet und garantiert nicht, dass seine Produkte oder sonstigen Leistungen die Einhaltung bestimmter Rechtsvorschriften sicherstellen. Der Kunde ist für die Einhaltung anwendbarer Sicherheitsvorschriften und sonstiger Vorschriften des nationalen und internationalen Rechts verantwortlich.

[1] Larry Greenmeier, „Companies Reconsider Offshore Outsourcing“, InformationWeek, 10. Dezember 2001

[2] Diane E. Lewis, „Increase in Tech Outsourcing Seen“, The Boston Globe, 14. Mai 2004

[3] Mike Perkowski, „Outsourcing: The CIO Insight Research Study“, CIO Insight, Mai 2002.

[4] Federal Financial Institutions Examination Council, „Information Security IT Examination Handbook“, Dezember 2002

[5] Federal Information Security Management Act von 2002, Public Law 107-347, 17. Dezember 2002

[6] Federal Information Security Management Act: 2006 Report to Congress from White House

[7] Katherine Schinasi, „Defence Acquisitions: Knowledge of Software Suppliers Needed to Manage Risk“, GAO-04-768, Mai 2004

[8] Michael Rasmussen, „Security Assurance in Software Development Contracts“, Forrester Research, 24. Mai 2004

TAKE BACK CONTROL WITH Rational.

RAW14200-DEDE-00