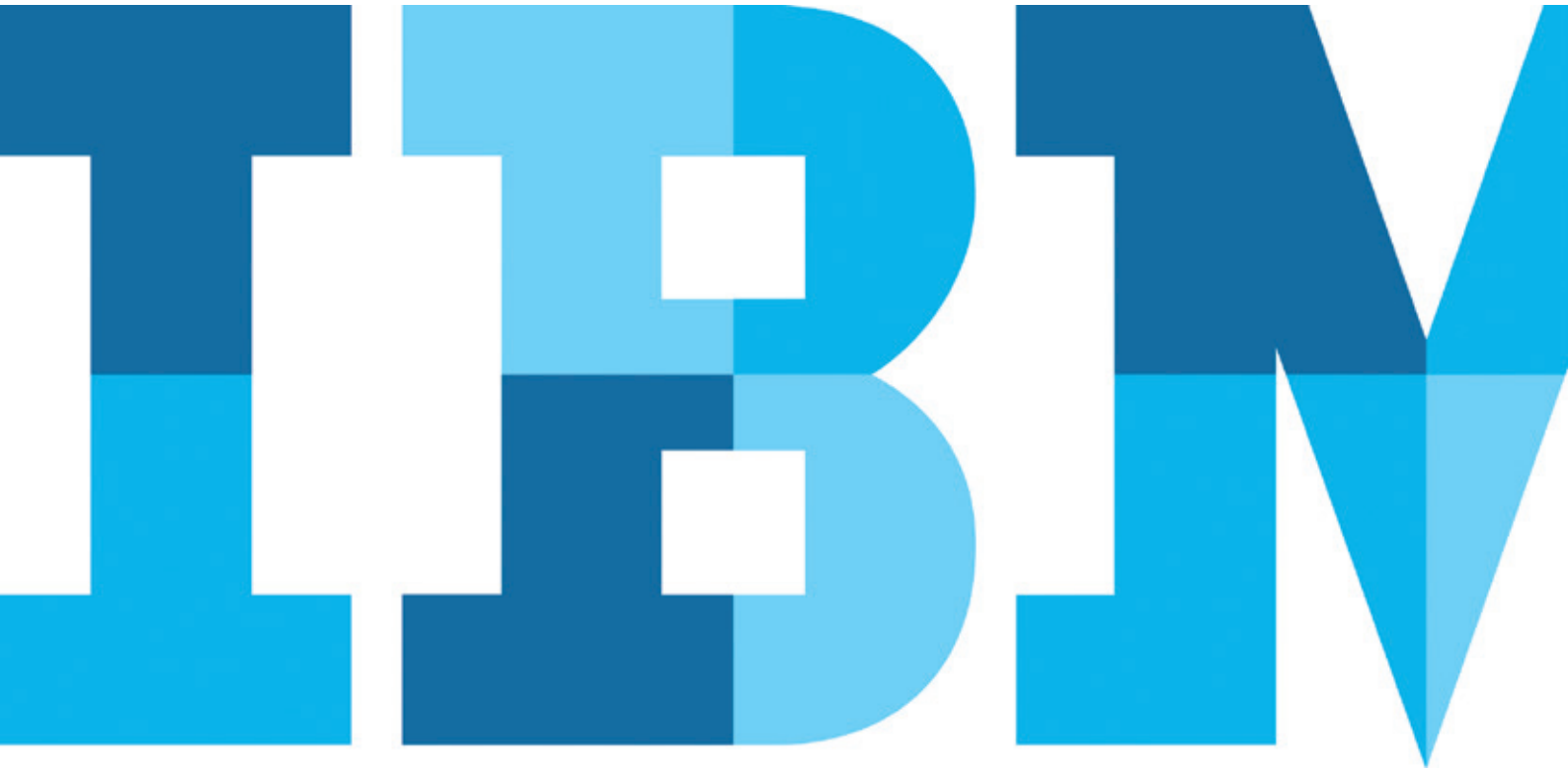
Dezember 2017

Steuern Sie die Sicherheitsrisiken für Ihre Anwendungen, um wichtige Daten Ihres Unternehmens zu schützen

Umfassende IBM Application Security Testing-Lösungen tragen dazu bei, Schwachstellen zu erkennen und Anwendungsrisiken zu minimieren



IBM

Warum Anwendungssicherheit wichtig ist

Viele Unternehmen setzen auf Softwareanwendungen, um kritische Geschäftsprozesse zu steuern, Transaktionen mit Lieferanten durchzuführen und Ihren Kunden komplexe Dienstleistungen anzubieten. Obwohl die Geschäftsmodelle vieler Unternehmen interessanterweise von solchen Anwendungen abhängig sind, machen sich viele wenig bis keine Mühe, diese Anwendungen auch angemessen zu schützen. Viele Firmen verwenden für Routineaufgaben im Geschäftsbetrieb oder Netzwerk sowie für Sicherheitsverfahren wie Zugangskontrolle und Authentifizierung ausgereifte Sicherheitstechnik, doch bei Implementierung, Verwaltung und Pflege wirksamer Sicherheitsprogramme für Ihre Anwendungen kommen sie ins Straucheln. Doch angesichts von immer häufigeren und zunehmend ausgereifteren Bedrohungsszenarien muss man die Latte deutlich höher legen. Da einzelne Anwendungen die Sicherheit eines ganzen Unternehmens kompromittieren können, muss die Anwendungssicherheit oberste Priorität haben.

Die Auswirkungen im Falle nicht angemessen geschützter Anwendungen können katastrophal sein. Sicherheitslücken, die sich versehentlich während des Entwicklungsprozesses einschleichen, können Hackern Tür und Tor öffnen, um Anwendungen zu destabilisieren und sich auf diese Weise ungehindert Zugang zu vertraulichen Unternehmensinformationen oder persönlichen Kundendaten zu verschaffen. Diese Form des Datenverlusts kann eine Marke ernsthaft beschädigen, das Vertrauen der Kunden erschüttern, das operative Geschäft nachhaltig beeinträchtigen, die Lieferkette unterbrechen sowie gerichtliche Schritte und/oder behördliche Auflagen nach sich ziehen – all diese Konsequenzen wirken sich letztendlich auf die Profitabilität eines Unternehmens aus.

Das Thema Anwendungssicherheit ist durchaus eine Herausforderung. Große Unternehmen verwalten tausende von Anwendungen. Die Aufgabe, deren Sicherheit zu gewährleisten, lastet jedoch meist auf den Schultern eines kleinen, überlasteten Sicherheitsteams. Um sich gegen diese Konsequenzen zu wappnen, sollte ein Unternehmen wie das Ihre auf ein risikobasiertes Management der Anwendungssicherheit setzen. Dafür brauchen Sie Lösungen, die Ihnen einen umfassenden Überblick über Ihre Infrastruktur geben, Anwendungen basierend auf den Auswirkungen für Ihr Unternehmen identifizieren und priorisieren, Anwendungen hinsichtlich von Schwachstellen beurteilen und Sicherheitslücken im Kontext betrachten können, um deren Risikograd zu bestimmen. Zudem muss eine solche Lösung in der Lage sein, Risiken zu minimieren, indem erforderliche Fixes im Code implementiert oder anderweitig geeignete Maßnahmen ergriffen werden. Eine Strategie zur Anwendungssicherheit einzuführen, mit der webbasierte und mobile Anwendungen geschützt werden, und das über den gesamten Lebenszyklus der Anwendung hinweg, ist ein wichtiger erster Schritt.

Eine Strategie zur Anwendungssicherheit einführen

Vielen Unternehmen gelingt es nicht, die Sicherheit ihrer Anwendungen zur obersten Priorität zu machen – damit setzen Sie jedoch das gesamte Unternehmen aufs Spiel. Laut einer Studie des Ponemon Institutes bewerten nur 25 Prozent der Teilnehmer die Fähigkeit ihres Unternehmens, Sicherheitslücken erfolgreich zu schließen oder einzudämmen, als hoch effektiv ein. Mit Blick auf Sicherheitsprüfungen gaben nur 44 Prozent der Befragten an, Anwendungen auf Schwachstellen zu testen.[1] Eine weitere Untersuchung zeigt, dass nur 39 Prozent der Befragten angeben, dass ihre mobilen Anwendungen während der Produktion getestet werden.[2] Teilen Sie Ihr Sicherheitsbudget entsprechend ein, um diesen aufkommenden Sicherheitsrisiken begegnen zu können?

Wirksame Sicherheit beginnt beim Risikomanagement. Es ist unerlässlich, dass Sie die Risiken für Ihre wichtigsten Ressourcen kennen, steuern und minimieren. Für eine effektive Anwendungssicherheit sollten Sie auf Folgendes achten:

1. **Machen Sie eine Bestandsaufnahme:** Sie müssen Ihre Ressourcen kennen und wissen, welche die größte Bedeutung für Ihr Unternehmen haben. Zunächst sollten Sie sich auf die wichtigsten Anwendungen fokussieren, anstatt alle Anwendungen auf einmal schützen zu wollen.
2. **Schätzen Sie die Auswirkungen ein:** Nachdem Sie Ihre Ressourcen priorisiert haben, analysieren Sie sie auf Schwachstellen. Bewerten Sie das Risiko, dem jede einzelne Anwendung ausgesetzt ist, basierend auf den Auswirkungen für Ihr Unternehmen und dem Schweregrad der Sicherheitslücke.
3. **Priorisieren Sie die Sicherheitslücken:** Nachdem Sie für jede Anwendung eine Risikoeinstufung vorgenommen haben, konzentrieren Sie sich in einem ersten Schritt auf die Anwendungen mit dem höchsten Risiko und fokussieren sich zunächst auf die größten Sicherheitslücken.
4. **Erstellen Sie einen Plan zur Schadensbehebung:** Zur Risikominderung gehören das Beheben von Kodierungsfehlern oder die Erstellung virtueller Patches über eine Web Application Firewall. In einigen Fällen kann es auch erforderlich sein, eine Anwendung vorübergehend offline zu nehmen.
5. **Messen Sie den Return on Investment (ROI):** Anhand verschiedener Kennzahlen können Sie den Status der Anwendungssicherheit überwachen und die Wirksamkeit Ihrer fortlaufenden Maßnahmen messen. Eine kürzlich durchgeführte Studie einer führenden Analystenfirma hat ergeben, dass IBM Kunden durch das Implementieren von IBM Security AppScan Source einen dreistelligen ROI erzielen.[3]

Auf dem Weg zu mehr Anwendungssicherheit

Für ein risikobasiertes Management der Anwendungssicherheit sind fünf entscheidende Kriterien zu beachten.

Erfahren Sie mehr über das integrierte Management der Anwendungssicherheit von IBM

Das Thema Anwendungssicherheit in einer großen Organisation umzusetzen, kann eine Herausforderung sein. Häufig ist ein kleines Sicherheitsteam verantwortlich für den Schutz tausender Anwendungen, die wiederum von unterschiedlichen Entwicklungsteams programmiert wurden. IBM bietet integrierte Funktionen für das Management der Anwendungssicherheit, somit können Sicherheitsteams die Schwachstellen angehen, mit denen sie sich jeden Tag herumschlagen müssen. Das Portfolio umfasst lokale und cloudbasierte Optionen, die auf Ihre spezifischen Anforderungen zugeschnitten sind.

Wie oben beschrieben, richten die erfolgreichsten Testprogramme im Bereich Anwendungssicherheit den Fokus auf die Risikominimierung. Unternehmen, die ihre Anwendungen bislang keinen Sicherheitstests unterzogen haben, können den Bedarf mit der Durchführung von Dynamic Application Security Testings (DAST) rechtfertigen und damit zunächst die wertvollsten Anwendungen testen, um die schwerwiegendsten Sicherheitslücken zu erkennen. DAST erlauben es zudem, auf die größten Risiken im Anwendungsportfolio des Unternehmens zu reagieren und schnell Erfolge vorweisen zu können. Jedes Unternehmen muss nun entscheiden, ob es zunächst Sicherheitslücken bei Anwendungen mit dem höchsten Risiko erkennen und angehen möchte oder eine sichere Kodierung auf den Weg bringen und Best Practices forcieren will. Mithilfe von DAST können Entwickler den Kodierungsprozess mit der Zeit sicherer machen und einen Anwendungsfall für das Testen der Anwendungssicherheit entwickeln. Static Application Security Testing (SAST) erfordert meist einen höheren strategischen Aufwand, der darauf abzielt, Best Practices für die sichere Kodierung durchzusetzen und somit schließlich Risiken, die die Anwendungen bergen, mit der Verbesserung des Codes zu minimieren.

Lokale Lösungen

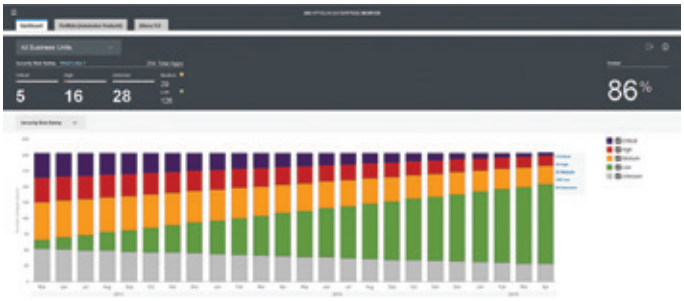
IBM Security AppScan Lösungen bieten speziell konzipierte Komponenten, um Anwendungssicherheitsmanagern und Entwicklungsteams in Unternehmen jeder Größenordnung die Arbeit zu erleichtern. Diese lokalen Lösungen beinhalten:

- **IBM Security AppScan Standard:** minimiert das Risiko für Attacken auf Webanwendungen und Datenschutzverstöße, indem Tests auf Sicherheitslücken in Anwendungen automatisiert und modernste DAST-Funktionen genutzt werden

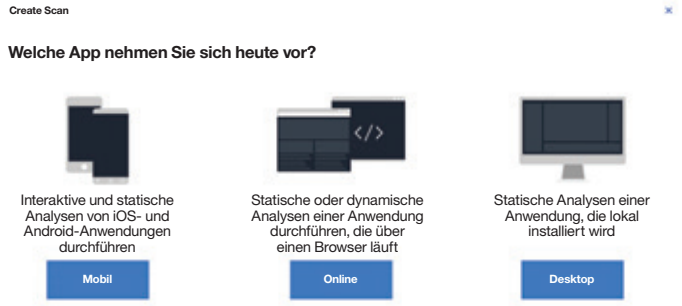
- **IBM Security AppScan Source:** senkt die Kosten und reduziert das Risikopotenzial, indem SAST in die DevOps-Automatisierung für das Testen von Anwendungen frühzeitig im Softwareentwicklungszyklus integriert werden, damit sich Schwachstellen vor der Implementierung beseitigen lassen

Mit der Software AppScan Source können Sie Sicherheitslücken für Ihre Anwendungen erfassen und Schwachstellen erkennen, die Ihre Anwendungen beeinträchtigen können.

- **IBM Security AppScan Enterprise:** Hilft Unternehmen dabei, die Risiken für die Anwendungssicherheit zu minimieren und gesetzliche Bestimmungen einzuhalten. Zudem können Sicherheits- und Entwicklungsteams eine Bestandsaufnahme ihrer Ressourcen vornehmen, Anwendungen basierend auf den Auswirkungen für das Unternehmen klassifizieren und priorisieren sowie Sicherheitslücken während des gesamten Anwendungslebenszyklus beseitigen.



Dank der vielfältigen Funktionen zur Anwendungssicherheit von AppScan können Sicherheitsteams die Schwachstellen angehen, mit denen sie sich jeden Tag herumschlagen müssen.



Mit IBM Application Security on Cloud wird das Testen von mobilen Anwendungen, Web- oder Desktop-Anwendungen zum Kinderspiel. Der Nutzer wählt einfach aus, welche Art der Anwendung getestet werden soll.

Cloudbasierte Lösungen

IBM Application Security on Cloud schützt mobile und Webanwendungen Ihres Unternehmens, indem dutzende der heute am häufigsten eingesetzten Arten ausgenutzter Sicherheitslücken erkannt werden. IBM Application Security on Cloud bietet DAST, Mobile Application Security Testing (MAST), SAST und Open Source Analyser, um Sicherheitslücken in Anwendungen zu erkennen, bevor diese in die Produktion gehen und implementiert werden. Dank praktischer Detailberichte können Sie Risiken für die Anwendungssicherheit wirksam angehen und diese ermöglichen es Nutzern, Ihre Anwendungen sicher zu verwenden.

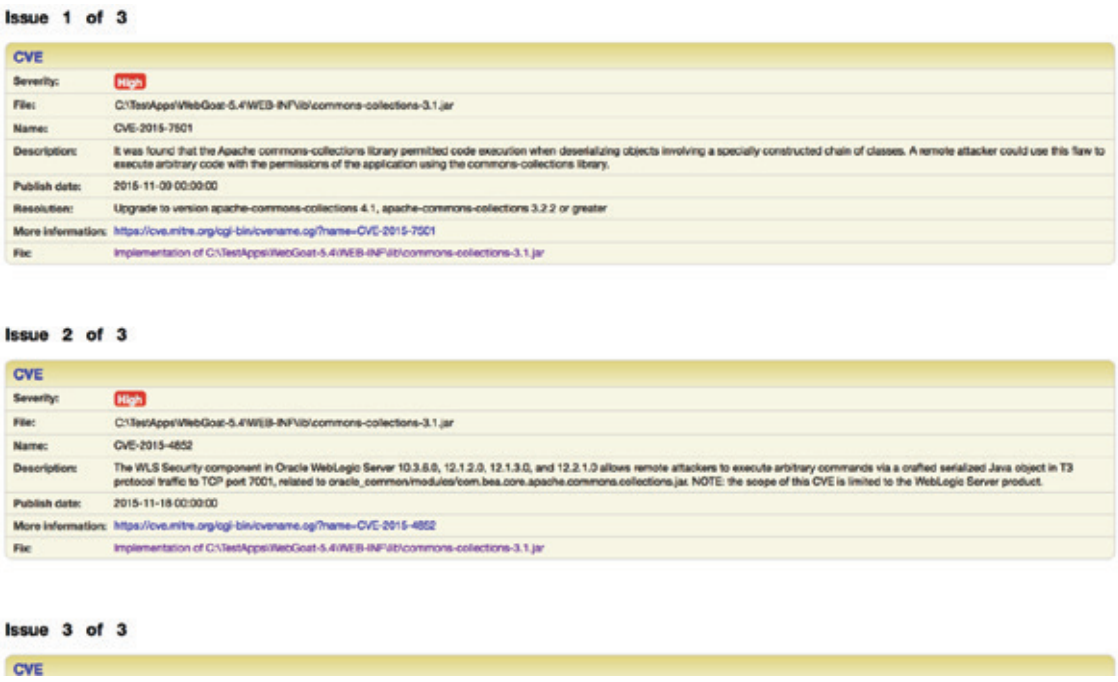
IBM Application Security on Cloud bietet folgende entscheidende Vorteile:

- Intelligent Finding Analytics nutzt maschinelles Lernen, um Scanbefunde zu analysieren, falsche Positivmeldungen intelligent zu reduzieren und die Scanzeiten deutlich zu minimieren, auf die wiederum die Sicherheitsexperten angewiesen sind, die die Überprüfung der Scanergebnisse verantworten
- Intelligent Code Analytics automatisiert die Analyse sämtlicher Code-Frameworks, die Entwicklungsteams benutzen, und eliminiert damit die kostenintensive manuelle Überprüfung sowie falsche Negativmeldungen, während gleichzeitig ein vollautomatisiertes DevOps-Testing möglich ist.

Merkmale der Lösung

IBM Lösungen zum Testen der Anwendungssicherheit einschließlich AppScan und IBM Application Security on Cloud erlauben es Unternehmen, die Sicherheit ihrer Anwendungen während des gesamten Lebenszyklus zu gewährleisten. Zu den wichtigsten Funktionen gehören:

- **Skalierbare Tests der Anwendungssicherheit** – Sie können die Lösung wählen, die zu Ihrem Unternehmen passt und mit dem Heranreifen Ihres Anwendungssicherheitsprogramms individuell Komponenten hinzufügen
- **Hohes Maß an Sichtbarkeit** – Bietet über ein spezielles Dashboard Sichtbarkeit der Enterprise-Klasse hinsichtlich Sicherheitsstatus und Compliance-Risiken von Anwendungen und Prozessen für das gesamte Unternehmen
- **Sichere DevOps-Strategie** – Integration mit den wichtigsten Build-Umgebungen und integrierten Entwicklungsumgebungen (IDEs) für ein nahtloses Testen und eine schnelle, zielgerichtete Schadensbehebung für Ihre Anwendungen
- **Fixgruppen** – Lokalisierung und Erfassung von Befunden, die eine oder mehrere Positionen oder Schnittpunkte teilen, in Gruppen, damit die Überprüfung und Schadensbehebung für diese Befunde erleichtert wird und die Entwickler schlussendlich weniger Arbeit haben, die DevOps-Bearbeitungszeit verkürzt wird und die zu implementierenden Anwendungen sicherer werden
- **Umgang mit behördlichen Auflagen** – Nutzer können aus mehr als 40 vordefinierten Berichten wählen und Scanbefunde mit den wichtigsten Compliance-Standards seitens Industrie und Behörden verknüpfen, um somit den wichtigsten Compliance-Vorgaben hinsichtlich der Webanwendungen des Unternehmens gerecht zu werden
- **Steuerung der Sicherheitstests** – Damit können Sie für das gesamte Unternehmen durchgängige Sicherheitsrichtlinien erarbeiten, vorantreiben und durchsetzen sowie dafür bereitgestellte Testrichtlinien und Scanvorlagen nutzen
- **Schadensbehebung** – Erstellen Sie mit jedem Scan eine vollständig priorisierte Liste von Sicherheitslücken, damit Sie sich zunächst um die Probleme mit den höchsten Risiken kümmern können
- **Sicherheitsinformationen** – Integration mit weiteren IBM Security Lösungen, um die Evaluierung von Bedrohungen und die Priorisierung von Sicherheitsproblemen noch weiter zu optimieren



Der IBM Open Source Analyser zeigt Schwachstellen als Fixgruppen an, um so Überprüfung und Behebung zu erleichtern.

Erweiterte Anwendungstests

Da es unterschiedliche Möglichkeiten gibt, die Sicherheit von Anwendungen zu gewährleisten, setzt AppScan auf eine Reihe von umfassenden Testverfahren, um die gründliche Überprüfung einer Anwendung bereits frühzeitig im DevOps-Prozess zu automatisieren. Das frühzeitige Aufspüren von Sicherheitslücken wirkt sich positiv auf den ROI aus, da die Entwickler die Schwachstellen bereits vor Implementierung der Anwendung beheben können.

IBM Application Security Testing-Lösungen bieten DAST, SAST und Open-Source-Testoptionen, damit Nutzer den neuesten Bedrohungen immer einen Schritt voraus sind und genaue sowie nutzbare Ergebnisse erzielen. AppScan Testverfahren beinhalten außerdem:

- **Interaktive Analysen:** Platzierung von Agenten in der Anwendungsmaschine und Analyse von Anwendungen während diese getestet werden. Durch die Kombination dynamischer und statischer Analysen zur Laufzeit lassen sich mehr Schwachstellen mit höherer Genauigkeit ermitteln
- **Hybride Analysen:** Kombination dynamischer und statischer Analysen für die Korrelation und Verifikation von Ergebnissen. Ermittlung von Problemen durch dynamische Analyse bis zur betreffenden Codezeile und Validierung der identifizierten Probleme aus der statischen Analyse anhand externer Tests
- **IBM Application Security Open Source Analyser:** Schützt und verwaltet Ihre Open-Source-Komponenten durch automatisierte Sicherheitstests und das Konfigurieren der Scanfunktion hinsichtlich Open-Source-Schwachstellen. Die Lösung ermöglicht es Ihnen, Ihr Open-Source-Risiko zu erkennen und zu steuern, indem kontinuierlich gefährdete Softwarekomponenten identifiziert werden
- **JavaScript™ clientseitige Analyse:** Hilft Ihnen dabei, Code zu analysieren, der auf den Client heruntergeladen wurde. Je mehr Funktionalität das Unternehmen clientseitig anbietet, desto größer ist clientseitig auch das Risiko von Sicherheitslücken und dem Ausnutzen solcher Probleme.

Wer profitiert von IBM Application Security Testing-Lösungen?

IBM Application Security Testing-Lösungen®wurden in erster Linie für drei Zielgruppen konzipiert:

- **Fachanwender oder Chief Information Security Officers (CIOs):** Anwender, die letztlich verantwortlich sind für die Anwendungssicherheit – und die Konsequenzen im Falle eines unzureichenden Schutzes tragen – können von einem besseren Verständnis der Sicherheitsrisiken Ihres Unternehmens und des gesamtes Compliance-Prozesses profitieren
- **Team für die Anwendungssicherheit:** Das Team, das innerhalb des Unternehmens Steuerung und Risikominimierung der Anwendungssicherheit verantwortet, profitiert davon, die vorhandenen Ressourcen sowie deren Priorisierung und Sicherheitsniveau und die wichtigsten Schwachstellen genau zu kennen
- **Team für die Anwendungsentwicklung:** Das Team im Bereich Anwendungsentwicklung profitiert davon, Tests zur Anwendungssicherheit in seinen DevOps-Prozess integrieren und somit Sicherheitslücken bereits im Entwicklungszyklus mühelos erkennen zu können.

Durchgängige Sicherheitslösungen

Beim Thema Anwendungssicherheit geht es nicht nur darum, Scans durchzuführen und Sicherheitslücken aufzuspüren – vielmehr geht es um die Steuerung von Risiken. Die Implementierung integrierter und automatisierter Lösungen zur Anwendungssicherheit bringen auch optimierte, kosteneffiziente und zuverlässige Ergebnisse mit sich. Integration ermöglicht einen risikobasierten Ansatz, denn Ihr Unternehmen kann unmöglich alle Anwendungen auf einmal und sofort schützen. Sicherheitsinformationen sind beispielsweise erforderlich, um Anwendungen zu priorisieren und festzulegen, wann welche Anwendung wie an der Reihe ist.

Daher wurden die IBM Application Security Testing-Lösungen so konzipiert, dass eine Integration weiterer IBM Security-Lösungen möglich ist. Damit steht ihr Unternehmen nicht nur in Sachen Anwendungssicherheit gut da, sondern verfügt auch über die Möglichkeiten, Bedrohungen besser zu bewerten und Sicherheitslücken anhand ihrer Risiken zu priorisieren. Zu den Lösungen gehören:

- **IBM QRadar Security Intelligence Platform**bietet Sicherheitsinformations- und Ereignismanagement (SIEM), Protokollverwaltung, Anomalieerkennung sowie Konfiguration und Schwachstellenmanagement für eine optimale Erkennung von Bedrohungen, größere Benutzerfreundlichkeit und geringere Betriebskosten
- **IBM Security Guardium**bietet eine umfassende Datensicherheitsplattform mit der vollen Bandbreite an Funktionen – von der Erkennung und Klassifizierung sensibler Daten, über die Verwundbarkeitsanalyse von Daten und Dateiaktivität bis hin zu Monitoring, Maskierung, Verschlüsselung, Blockierung, Alarmierung und Isolierung zum Schutz sensibler Daten
- **IBM Mobile Security Solutions**lassen sich mit den mobilen Testfunktionen für die Anwendungssicherheit von IBM Application Security on Cloud integrieren, um proaktiv potenzielle Sicherheitslücken bei mobilen Anwendungen zu schließen und die operative Effizienz zu optimieren
- **IBM Cloud Security Solutions**bieten über das Internet On-Demand Rechenkapazitäten – alles von Anwendungen bis zum Rechenzentrum – auf Pay-per-Use-Basis.

Zusammenfassung

Die Sicherheit von Anwendungen ist heute wichtiger denn je und die Herausforderungen sind komplex. Ohne die erforderliche Sichtbarkeit in der Infrastruktur und die richtigen Sicherheitslösungen kann Ihnen die Aufgabe, Ihr Unternehmen vor Bedrohungen zu schützen, schier unmöglich erscheinen. IBM verfolgt in Sachen Anwendungssicherheit eine klare Strategie und unterstützt Sie dabei zunächst die wichtigsten Schritte zu unternehmen, damit Sie ein wirksames, erfolgreiches Testprogramm zur Anwendungssicherheit auflegen können.

Dank modernster Sicherheitstests und einer Plattform zur Steuerung der Anwendungsrisiken unterstützt AppScan Unternehmen dabei, ihre neuesten Sicherheitsstrategien viel einfacher implementieren und umsetzen zu können. Mit dieser Lösung haben Sie die Sicherheitskompetenz und die Integration mit Ihrem Application Lifecyle Management, die Sie brauchen, um nicht nur Sicherheitslücken aufzuspüren, sondern auch das Gesamtrisiko für Ihre Anwendungen zu minimieren.

Wenn die Anwendungssicherheit in Ihrem Unternehmen zunehmend ausgereifter wird, können Sie zudem die IBM Application Security Testing-Lösungen auf Ihre Bedürfnisse anpassen und die Komponenten ergänzen, die sich für Ihre spezifischen Anforderungen am besten eignen.

Wenn Sie AppScan noch heute testen möchten, besuchen Sie bitte die AppScan Webseite.

Wenn Sie IBM Application Security on Cloud noch heute testen möchten, besuchen Sie bitte die IBM Application Security Analyser Webseite.

Weitere Informationen

Weitere Informationen zu den IBM Application Security Testing-Lösungen oder weitere komplementäre IBM Security-Lösungen erhalten Sie von Ihrem IBM Vertriebsmitarbeiter bzw. IBM Business Partner (BP) oder unter:
ibm.com/security/application-security/appscan/

Für detaillierte Systemvoraussetzungen zu den einzelnen Testlösungen zur Anwendungssicherheit, klicken Sie bitte auf folgenden Link:

- AppScan Standard
- AppScan Source
- AppScan Enterprise
- IBM Application Security on Cloud

[1] „How to Make Application Security a Strategically Managed Discipline“, *Ponemon Institute*, mit Unterstützung von IBM Security, März 2016. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGL03106USEN&attachment=WGL03106USEN.PDF

[2] „2017 Study on Mobile and Internet of Things Application Security“, *Ponemon Institute*, mit Unterstützung von IBM und Arxan Technologies, Januar 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03136USEN&

[3] Neil Jones, „Recently Released Industry Research Study Reveals Triple-Digit ROI for IBM Application Security Testing Solution“, *SecurityIntelligence*, 19. Juli 2016. https://securityintelligence.com/recently-released-industry-research-study-reveals-triple-digit-roi-for-ibm-application-security-testing-solution/

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
Deutschland

IBM Österreich
Obere Donaustraße 95
1020 Wien

IBM Deutschland und IBM Österreich finden Sie im Internet unter **ibm.com**

Please Recycle

WGB03009-DEDE-06