IBM Security

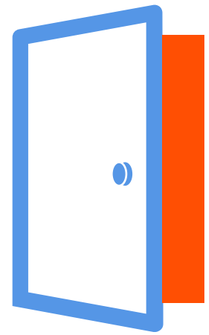
IBM

Effektives Managen von Risiken für die Anwendungssicherheit in der Cloud

Einfache, automatisierte Tests können Ihre Sicherheitsroutine optimieren und stärken

IBM Security Whitepaper

Warum ist Anwendungssicherheit so wichtig?



Sie haben sicherlich schon viel für Ihre Datensicherheit getan – doch kann es sein, dass die Anwendungen, die Sie nutzen, eine offene Tür zu Ihrem Unternehmen darstellt? Die Sicherheit der Daten, die sich in Ihrem Unternehmen befinden, hängt von deutlich mehr ab als vom Schutz einzelner Dateien und Aufzeichnungen. Sie müssen auch auf *Anwendungsebene* für Sicherheit sorgen, denn Anwendungen können den Zugriff auf Ihre Daten kontrollieren – und auch auf die Internet of Things (Internet der Dinge; IoT)-Infrastruktur Ihres Unternehmens.

Viele bekannte Sicherheitsverstöße sind nicht aufgrund von unzureichender Datensicherheit aufgetreten, sondern weil die Anwendungen ungeschützt waren. Der Einsatz von Anwendungssicherheit hilft, fehlerhafte oder ungeschützte Software davor zu schützen, dass Cyberkriminelle sicher geglaubte Daten erreichen.

Dennoch bleibt die Anwendungssicherheit ein häufig vernachlässigter Aspekt der Cybersicherheit[1] und es gibt weiterhin Verstöße. Warum? Zum Teil, weil der Schutz von Anwendungen schwieriger ist als das Verschlüsseln von Dateien oder die Sicherung von Netzwerken durch Firewalls. Außerdem ist die Anzahl und Vielfalt von Anwendungen gestiegen, seit es App Stores und spezielle Anwendungen für den Zugriff auf Cloud-basierte Infrastrukturen gibt. Gleichzeitig hat die immer größere Akzeptanz von „Bring-your-own-Device“ (BYOD)-Richtlinien dazu geführt, dass sich vermehrt unkontrollierte Anwendungen und mit Anwendungen verbundene IoT-Datenquellen immer mehr ausbreiten.

Anwendungssicherheit ist wichtig für:

- Vorbeugen von Schaden am Ruf des Unternehmens
- Aufrechterhalten des Kundenvertrauens
- Vermeiden von Sanierungskosten
- Erkennen von und Reaktion auf Sicherheitsrisiken, bevor sie Schäden anrichten.

In einer Studie gaben

77%

die befragten Entwickler an, dass Anwendungen anfällig sind, da Druck besteht, sie schnell auf den Markt zu bringen, wodurch es unmöglich ist, angemessene Tests durchzuführen.[2]

▸ Sehen Sie sich ein Demovideo darüber an, was IBM Application Security on Cloud für Sie bieten kann.

1 „How to Make Application Security a Strategically Managed Discipline,“ *Ponemon Institute.*, März 2016.

2 „The State of Mobile Application Insecurity,“ *Ponemon Institute.*, Februar 2015.

Warum ist es für Unternehmen so schwierig, Erfolge im Bereich Anwendungssicherheit zu erreichen?

Anwendungssicherheit wird durch Faktoren beeinflusst, die von Entwicklern über IT-Mitarbeiter bis hin zu den Endanwendern reichen. Diese Faktoren in Kombination können ein Unternehmen anfällig für Verletzungen machen.

Druck zur schnellen Freigabe
Eine ständige Atmosphäre, in der „Druck zur schnellen Freigabe“ herrscht, bedeutet häufig, dass Entwickler nicht über genügend Ressourcen zum Testen der Anwendungen verfügen. Doch Anwendungssicherheit liegt nicht nur in der Verantwortung der Entwickler. Endnutzer möchten Anwendungen schnell installieren, um die Eigenschaften der neuen Software umgehend zu nutzen.

Komplexe Anwendungen
Software variiert stark im Hinblick auf Umfang, Datenbedarf, Sprache und Plattform. Eine kompromittierte Anwendung mit direktem Zugriff auf die Daten eines Unternehmens kann genauso gefährlich sein wie ein verlorener Laptop, auf dem ähnliche Daten gespeichert sind – oder gar schlimmer, wenn die Sicherheitslücke nicht entdeckt wird. Eine unsichere oder bösartige Anwendung könnte Ihre Daten freigeben, egal, ob dafür eine Sicherheitsschwachstelle genutzt wurde oder sie bereits bei der Entwicklung unsicher war.

Anwendungssicherheit ist keine Priorität
Schwachstellen auf Anwendungsebene werden oft als niedrige Priorität angesehen und Unternehmen klassifizieren ihre Anwendungen meist nicht nach Risikogesichtspunkten. Außerdem befinden sich Anwendungen oft an vielen verschiedenen Stellen innerhalb eines Unternehmens – gemeinsam mit der Verantwortung für ihre Sicherheit – dabei ist oft kaum sichtbar, welche genutzt werden und welche am anfälligsten für Attacken sind.

Fehlende Standards
Anwender haben keine Zeit für Sicherheitstests und wissen nicht, wie sie ihre Anwendungen effektiv prüfen können. Es gibt wenige allgemeine Standards für die Anwendungssicherheit, weshalb es schwierig sein kann, Anleitungen oder Expertenwissen vor Ort zu finden und zu nutzen.

Eine aktuelle Studie des Ponemon Institute zeigte auf, dass

47%

der Befragten gaben an, dass die Risiken im Hinblick auf mobile Anwendungen in Ihren Unternehmen zunehmen oder stark zunehmen.[1]

- Erfahren Sie mehr über risikobasiertes Management von Anwendungssicherheit.

1 „How to Make Application Security a Strategically Managed Discipline,” *Ponemon Institute.*, März 2016.

Was ist effektive Anwendungssicherheit?

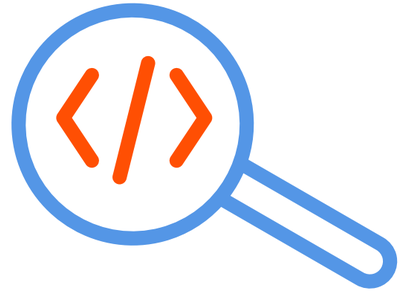
Effektive Praktiken für die Anwendungssicherheit bestätigen, dass Sicherheit als ein Prozess angesehen werden sollte, nicht als eine Reihe von Aufgaben, die abzuhaken sind. Daher muss das Testen von Anwendungssicherheit (Application Security Testing; AST) umfassend und ständig geschehen.

Für Entwickler sollte das AST-Verfahren Teil des Softwareentwicklungs-Lebenszyklus sein, inklusive ständiger Quellcodeanalyse. Bei Endanwender-Unternehmen geht der Prozess weiter: jegliche neue Software sollte geprüft werden, und Anwendungen, die bereits genutzt werden, müssen erneut getestet werden.

Umfassende Anwendungssicherheit sollte folgendes umfassen:

- Erkennen und Katalogisieren von Anwendungen, die derzeit genutzt werden
- Statisches Testen – Scannen des Anwendungs-Quellcodes auf Schwachstellen ist der direkteste Weg, um den tatsächlichen Code zu finden, der hinter einer bestimmten Sicherheitsschwachstelle steckt
- Dynamisches Testen – Evaluation des Software-Verhaltens beim Einsatz (ist sie zum Beispiel anfällig für mögliche Website-übergreifende Scripting- und SQL-Injection-Attacken?)
- Mobiles AST, aufgrund der Verbreitung neuer mobiler Anwendungen auf dem Markt
- Implementierung neuer Software nur nach eingehender Prüfung.

Anwendungen sollten regelmäßig neu bewertet werden, und dieser Evaluierung sollten Quellen wie die Top-Ten-Liste des Open Web Application Security Project (OWASP) zugrunde liegen[1] – neue Gefahren können ein Risiko für ehemals sichere Anwendungen darstellen.



Im September 2016 wurden

2 Millionen

Apple iOS-Anwendungen zum Download angeboten,[2] und über

2,4 Millionen

Google Android-Anwendungen.[3]

▸ Erfahren Sie mehr über Risiken, die Anwendungssicherheit so wichtig machen.

1 Paul Ionescu, „The 10 Most Common Application Attacks in Action," *IBM Security Intelligence*8. April 2015.

2 „Number of apps available in leading app stores as of June 2016," *Statista*, Juni 2016.

3 „Number of Android Applications," *AppBrain*, Zugriff 13. Oktober 2016.

Nutzen Sie unsere lange erprobten Best Practices für Anwendungssicherheit

Beim Prüfen der Anwendungen auf Sicherheitsrisiken unterliegen Unternehmen Einschränkungen, die von beschränkten Budgets bis zu hoher Arbeitsbelastung für Sicherheits- und IT-Mitarbeiter reichen. Doch diese Einschränkungen sollten der Verbesserung des Sicherheitsschutzes nicht im Wege stehen. Stattdessen sollte Ihr Unternehmen Best Practices einsetzen, die folgendes beinhalten:

- **Übersicht** – Geplante, automatisierte Tests ermöglichen genauere und zuverlässigere Ergebnisse als Ad-hoc-Tests
- **Kontinuität** – Anwendungen sollten erstellt und auf Sicherheit geprüft werden, und dann immer wieder getestet werden, um mit möglichen Schwachstellen Schritt zu halten
- **Priorisierung** – Einordnung von Problemen der Anwendungssicherheit auf Grundlage von Schwere und möglichen Auswirkungen auf den Geschäftsbetrieb, damit Probleme in der Reihenfolge beseitigt werden können, die am meisten Sinn für das Unternehmen ergibt
- **Flexibilität** – Die Vermeidung restriktiver Implementierungsanforderungen ist entscheidend, um die gesamte Bandbreite der von Ihrem Unternehmen eingesetzten Anwendungen zu bewerten.
- **Anpassbarkeit** – Bedrohungen ändern sich im Laufe der Zeit; ein flexibler Ansatz führt zu weniger Änderungen, um die Kontrolle über die Anwendungssicherheit zu behalten.
- **Aktualität** – Um Unterbrechungen – oder die nochmalige Durchführung – von Entwicklungsprozessen zu vermeiden, sollten Anwendungen auf allen Stufen des Entwicklungs-Lebenszyklus getestet werden.

Eine integrierte Anwendungssicherheits-Lösung wie IBM® Application Security on Cloud kann Ihnen helfen, Sicherheitslücken zu schließen und mögliche Schwachstellen zu erkennen. Die Integration mit anderen Sicherheitsprodukten und -praktiken macht die Risikominimierung für Anwendungen zu einem Teil eines umfassenden Sicherheitsprogramms, statt zu einem nachgelagerten Element.

58%

der Unternehmen geben an, dass Sicherheitsbedenken den vollständigen Einsatz einer mobilen Sicherheitsstrategie verhindern.[1]

▸ Finden Sie heraus, wie IBM Application Security on Cloud Schwachstellen erkennt und mindert.

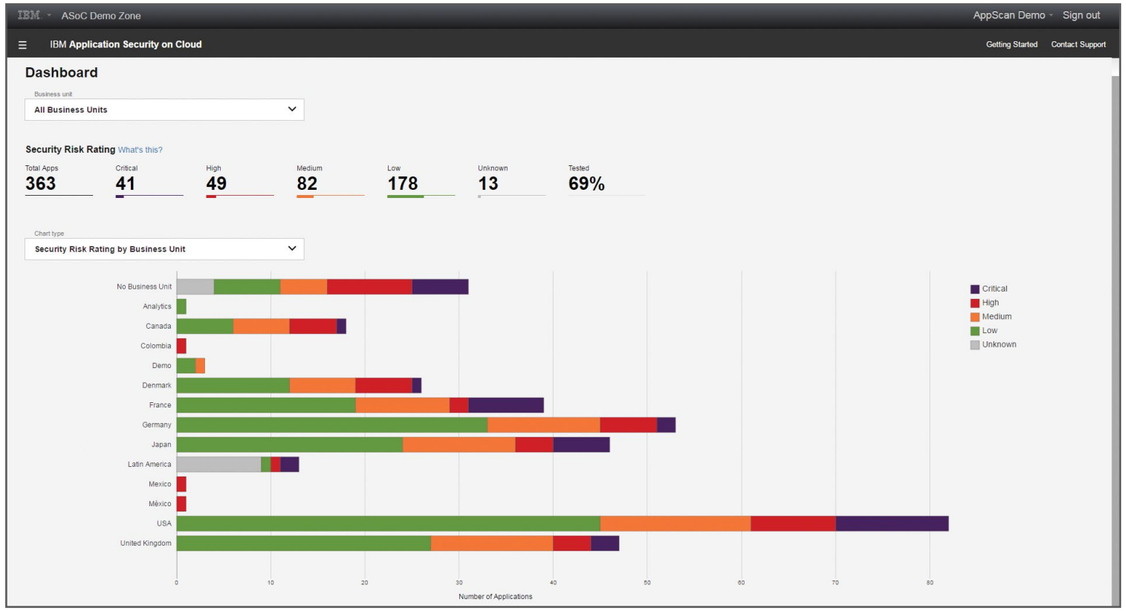
1 „2016 Mobile Security & Business Transformation Study," *Information Security Media Group*, gesponsert von IBM Corp., 2016.

Umfassendes, Cloud-basiertes AST

Unterstützen Sie Ihr Risikomanagement für Anwendungssicherheit durch die Implementierung einer integrierten Lösung, statt sich auf unterschiedliche Tools zu verlassen. IBM Application Security on Cloud ist eine umfassende, kosteneffiziente, anwenderfreundliche und einfach einsetzbare Cloud-basierte Lösung für Web- und Mobilanwendungen, die alle Phasen der Anwendungssicherheitstests vereinigt. Unser Cloud-basiertes Angebot basiert auf jahrelanger IBM-Erfahrung im Bereich standortbezogener Sicherheitstests und funktioniert gemeinsam mit anderen Sicherheits-Tools, um einen umfassenden Schutz gegen Cyberattacken zu ermöglichen.

Bei IBM Application Security on Cloud handelt es sich um eine vollständige, abonnementbasierte Lösung, die es Ihnen ermöglicht, Anwendungen zu testen und mithilfe handlungsorientierter Daten den Sicherheitsschutz zu verstärken. Mit IBM Application Security on Cloud können Sie schnell die Risikobewertungen für Anwendungen einschätzen und sich somit auf Sanierungsaufgaben für die wichtigsten Schwachstellen konzentrieren.

- Melden Sie sich für eine Testversion von IBM Application Security on Cloud an oder laden Sie eine standortbezogene Testversion von IBM Security AppScan herunter.



Dashboard-Ansicht für IBM Application Security on Cloud.

Sie können statische Sicherheitstests für Anwendungscodes in verschiedenen Programmiersprachen durchführen, dynamische Analysen für Software-Webanwendungen vor und während der Produktion erstellen, sowie Android- und iOS-Anwendungen vor ihrem Einsatz testen. IBM Application Security on Cloud erkennt und meldet Sicherheitsprobleme, ordnet sie im Hinblick auf ihre Verletzlichkeit und Bedrohung und schlägt Sanierungsschritte vor. Alle Ergebnisse können in verschiedene DevOps-Systeme und integrierte Entwicklungsumgebungen (IDEs) integriert werden.

Außerdem ist ein komplettes Sortiment an ergänzenden Beratungsleistungen verfügbar, wodurch Ihr Sicherheitsteam die Funktionen von IBM Security im vollen Umfang nutzen kann.

Echte Fallstudien zu IBM Application Security on Cloud

Unternehmen, die Lösungen für Anwendungssicherheit von IBM nutzen, erkennen den Wert von Integration und Automatisierung als Teil ihrer allgemeinen Sicherheitsstrategien – egal ob bei der Entwicklung oder beim Einsatz von Anwendungen.

Code-Schutz während des Softwareentwicklungs-Lebenszyklus

- Concur Technologies in Bellevue, Washington, ist Spezialist für Unternehmens-Kostenmanagement, verarbeitet also täglich vertrauliche finanzielle Informationen. Der Schutz dieser Informationen ist unabdingbar, aber auch schwierig. Concur ist ein Unternehmen mit starker Mobilpräsenz, einschließlich eigener Mobilanwendungen, und setzte daher AppScan mit der gleichen Schwachstellen-Testtechnologie ein, die IBM Application Security on Cloud nutzt. Mit AppScan kann Concur seine Anwendungen während der Entwicklung auf Sicherheitsrisiken testen und den Produktionscode analysieren.

Risikoverwaltung in einem schnell wachsenden Unternehmen

- Migros, ein türkischer Einzelhandels-Konzern mit hohem Wachstum im In- und Ausland muss seine groß angelegte Infrastruktur schützen, in der Anwendungen Bestands- und Zahlungsinformationen über ein Netzwerk von fast 1.500 Geschäften und mehr als 100.000 mit dem Internet verbundenen Endgeräten senden. Bei der Orchestrierung seines Wachstums sah sich das Unternehmen mit Herausforderungen konfrontiert, als es bei der Umsetzung einer BYOD-Richtlinie den Betrieb in die Cloud verlagerte. Durch die Nutzung von IBM-Lösungen für Anwendungssicherheit konnte Migros das Geschäft erweitern und gleichzeitig Risiken minimieren.

IBM bietet ein
vollständiges Portfolio von
AST-Tools, die von führenden Unternehmen genutzt werden, die von Fertigungs-[1] und Finanzdienstleistungen[2] reichen, um beim Schutz von Anwendungen, Geräten und Daten zu helfen.

▸ Registrieren Sie sich für einen kostenlosen Testplan für IBM Application Security on Cloud.

1 „Large global automaker: Protecting the Connected Car Ecosystem," *IBM Corp.*, Juli 2016.

2 „Progressive Insurance: Proactively Protecting Data by Creating Appropriate Controls," *IBM Corp.*, Mai 2016.

Weitere Informationen

Weitere Informationen über die IBM Security-Lösungen erhalten Sie von Ihrem IBM Ansprechpartner, Ihrem IBM Business Partner oder unter: **ibm**.com/applicationsecurity

Über IBM Security Lösungen

IBM Security bietet eines der modernsten und perfekt integrierten Portfolios mit Sicherheitsprodukten und -services für Unternehmen an. Das Portfolio, das von der weltweit bekannten IBM X Force Forschungs- und Entwicklungsabteilung unterstützt wird, umfasst eine umfangreiche Sicherheitsexpertise, damit Unternehmen Mitarbeiter, Infrastrukturen, Daten und Anwendungen zuverlässig schützen können. Wir bieten Lösungen für die Identitäts- und Zugriffsverwaltung, Datenbanksicherheit, Anwendungsentwicklung, Risikoverwaltung, Endpunktverwaltung, Netzwerksicherheit und vieles mehr an. Mit unseren Lösungen können Unternehmen Risiken erfolgreich verwalten und integrierte Sicherheitsverfahren für mobile und Cloud-basierte Umgebungen, soziale Medien sowie andere geschäftliche Architekturen implementieren. IBM verfügt über eine der weltweit größten Abteilungen für Forschung, Entwicklung und Bereitstellung im Bereich Sicherheit, überwacht in über 130 Ländern 15 Milliarden Sicherheitsereignisse am Tag und kann mehr als 3.000 Sicherheitspatente vorweisen.

Sie können IBM Security Services auch den wechselnden Bedürfnissen Ihres Unternehmens anpassen, wenn Sie Sicherheitsprogramme für Anwendungen erstellen und ausführen. Dadurch erhalten Sie Zugriff auf Fachkenntnisse im Bereich Anwendungssicherheit, wenn, wo und wie lange Sie es brauchen. Ob Sie Ihr Team kurzfristig auf den neuesten Stand bringen möchten, tiefgreifende Beratungsleistungen benötigen, ethische Hacker einsetzen möchten, um Ihre Anwendungen manuell zu erproben, oder sonstige Dienste wünschen – IBM ist für Sie da.

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

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

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

WGW03254-DEDE-02