Quelle: Fotolia / chombosan

Modernes API Management ist ein Muss

Die digitale Transformation treibt branchenübergreifend nahezu alle Unternehmen vor sich her. Im Zuge dessen spielen sogenannte APIs (englisch Application Programming Interfaces) eine wesentliche Rolle.

APIs sind in ihrer Funktion als Schnittstellen für die Anwendungsprogrammierung das Bindeglied zwischen Systemen, Daten und Menschen. Ihre Sicherheit ist darum unbedingt und stets zu gewährleisten – erst recht in Zeiten immer häufiger stattfindender Hackerangriffe.

Historie

Vor etwas mehr als einem Jahrzehnt war die Welt der APIs (hier speziell Webservices) noch relativ klein und undefiniert. Das sogenannte SOAP Protokoll war ein Quasi-Standard und hat das Arbeiten mit APIs (anders als das S für ‚Simple' im Namen vermuten lässt) nicht gerade angenehm gestaltet. SOAP-Calls waren kompliziert aufzurufen, eine entsprechende Infrastruktur musste erstmal aufgebaut werden und ein „Debuggen" für Antworten war – bedingt durch noch fehlende Statuscodes – schwer machbar. Über die Zeit hat sich die Situation deutlich verbessert und SOAP hat dazu gelernt (wobei „simple" in dem Zusammenhang immer noch nicht passt) und mit REST kam ein ganz neues Paradigma zur Erstellung von Webservices hinzu. Roy Fielding hatte es sich zur Jahrtausendwende zum Ziel gemacht, APIs end-

lich klar und einfach zu definieren. Durch seine klar umrissenen und einfach umzusetzenden universalen Regeln wurde die Art und Weise wie APIs aussehen müssen stark vereinfacht. Dadurch konnten sie nun einfach erstellt und gewartet werden und fanden durch die Verbreitung des Internets auch schnell einen großen Anwenderkreis.

Im Bereich des E-Commerce haben Branchengrößen wie beispielsweise Ebay und Amazon durch den Einsatz von APIs ihre eigene Verbreitung schnell gesteigert. Auch Dienste wie das Bilderportal Flickr konnten durch APIs ihre Dienstleistungen einfach auf viele verschiedene Plattformen verteilen und dadurch die eigene Präsenz ausweiten. Doch mit der zunehmenden Bedeutung der APIs wuchs auch ihre Attraktivität aus der Sicht von Angreifern.

Sicherheit im Fokus

Die Cyberkriminalität wächst und lässt IT-Sicherheitsexperten keine Ruhe. Es vergeht kaum ein Tag, wo nicht von Hackerangriffen auf Unternehmen oder Regierungsbehörden zu lesen ist. APIs in ihrer Kernfunktion als Bindeglied zwischen unterschiedlichen Systemen und Daten sind hier ein willkommenes Ziel solcher Attacken.

Immerhin liefern sie Zugänge zu Ressourcen. Ressourcen wiederum sind die wichtigsten Daten eines jeden Unternehmens: Seien es die Wetterinformationen eines Wetterdienstleisters, die Bestellhistorie eines Internetshops oder die Kreditinformationen einer Ratingagentur. Diese Daten sind die Kronjuwelen dieser Unternehmen und daher besonders wichtig. Gleichzeitig sind auch die gespeicherten Kundeninformationen besonders schützenswert. Wenn es einem Angreifer gelingt an diese Daten durch schlecht abgesicherte API Schnittstellen zu gelangen, kann dem Unternehmen nicht nur ein finanzieller Schaden entstehen, auch die Reputation nimmt dauerhaft einen Schaden – denn: Selbstverständlich lassen sich mit personenbezogenen Daten auch weitere Angriffe gegen die Kunden des Unternehmens starten durch beispielsweise Phishing. Zudem sind erhebliche rechtliche Konsequenzen zu befürchten.

Wenn eine API auf Daten Zugriff hat, die schützenswert sind, sind Authentifizierung und Autorisierung das A und O, was letztlich bedeutet, dass nur berechtigte Anwendungen bzw. Nutzer die API aufrufen dürfen, um an die Daten heranzukommen. Wird an dieser zentralen Stelle nicht mit der notwendigen Sorgfalt gearbeitet, öffnet sich einem potenziellen Angreifer Tür und Tor. Obwohl diese Regel einleuchtend und selbstverständlich klingt, gehört die Nachlässigkeit in diesem Bereich laut dem aktuellen Bericht der OWASP zu den zweit-verbreitetsten Fehlern im Bereich der Webdienste.

Neben der Zugriffsabsicherung müssen zusätzlich weitere technische Vorkehrungen getroffen werden. Fachverantwortliche können sich hier an den praktischen Empfehlungen der OWASP Top 10 orientieren. Dazu gehören beispielsweise sogenannte SQL-Injections, mit denen sich ein Angreifer bei ungesicherten Schnittstellen mit zusätzlichen SQL Befehlen in der Anfrage mehr Daten abgreift, als beim Design der API vorgesehen war.

Moderne API Management Lösungen (beispielsweise APIIDA API Gateway Manager in Verbindung mit CA API Management) helfen hier, genau diese Schwachstellen möglichst einfach und durchdacht abzusichern.

Folgen erfolgreicher Angriffe

Ist ein Angriff erfolgreich, kann dies verheerende Auswirkungen auf den Datenschutz, die Datensicherheit und den gesamten Geschäftsbetrieb haben. Um beispielsweise ein Kundenportal für die eigenen Lieferanten und Kunden anzubieten, bedarf es einer API Schnittstelle zur ERP Software. Dadurch kann ein Lieferant zum Beispiel seine Lieferungen überwachen und ein Kunde seine Bestellungen verwalten. Wird nun die Authentifizierung nicht richtig gelöst, könnte nun ein Wettbewerber an diese Informationen herankommen – um diese dann gegen das konkurrierende Unternehmen einzusetzen. Zusätzlich sind durch hoch personalisierte Informationen viel bessere Phishing Angriffe möglich, um etwa Schadsoftware in die andere Organisation einzuschleusen. Dass es soweit in der Praxis tatsächlich kommen kann, beweisen eindrucksvoll die verheerenden Cryptotrojaner (auch Ransomware oder Erpressungstrojaner) Angriffe aus dem letzten Jahr. Die meisten angegriffenen Unternehmen haben sich so einen Cryptotrojaner per Phishing eingefangen.

Die Sicherheit der APIs nachhaltig zu gewährleisten, ist für Unternehmen und Behörden folglich besonders wichtig. Damit der notwendige Schutz gelingt, brauchen Organisationen zunächst einmal ein intelligentes API-Management.

APIs effizient managen

Ein effizientes und intelligentes API-Management unterstützt die Administratoren dabei, die laufenden Prozesse von der Entwicklung über die Umsetzung bis hin zum Betrieb dauerhaft und ohne großen Zeitaufwand abzusichern. Um erfolgreich mit den sich ständig veränderten Marktgegebenheiten konform zu gehen, ist eine stetige Weiterentwicklung der eigenen Dienste notwendig. Auf der anderen Seite dürfen die bereits vorhandenen bei der Weiterentwicklung auf keinen Fall in Mitleidenschaft gezogen werden. Ein bewährter Ansatz dabei ist es, verschiedene Bereitstellungsumgebungen

APIs in ihrer Kernfunktion als Bindeglied zwischen unterschiedlichen Systemen und Daten sind ein willkommenes Ziel von Cyber-Attacken. Moderne API Management Lösungen helfen Schwachstellen möglichst einfach und durchdacht abzusichern.
(Bild: Fotolia / wladimir1804)

(Staging Environments) einzusetzen. So ließen sich etwa in einer speziell für Entwickler vorgesehenen Umgebung neue Funktionen ausprobieren. Eine Testumgebung für die Testabteilung um neue Funktionalitäten vor der Produktivstellung wäre beispielsweise hilfreich, mit möglichst realitätsnahen Daten zu testen. Unabhängig davon arbeitet schließlich die Produktivumgebung, die möglichst stabil laufen muss, um den Kunden eine gleichbleibende Qualität anbieten zu können.

Nun ist es selbstverständlich möglich, eine neue Funktionalität durch jede Umgebung zu kopieren und dabei manuell umfangreiche Test durchzuführen um die Funktionalität sicherzustellen. Diese Vorgehensweise hat sich in der Praxis aufgrund ihrer Fehleranfälligkeit und durch den hohen und damit kostenintensiven Ressourcenbedarf nicht bewährt. Hier helfen automatisierte API Management Lösungen, die die (optional automatische) Migration zwischen den Umgebungen übernehmen und im besten Fall auch die notwendigen Tests selbständig durchführen. So kann sich der Entwickler auf seine Kernaufgabe konzentrieren und die lästigen und zeitaufwändigen manuellen Tätigkeiten automatisieren.

Smart gelöst: Überwachung und Problembehebung in Echtzeit

Wollen Unternehmen und Behörden in intelligente API-Management-Lösungen investieren, sollten sie auf wichtige Details achten. So überwachen entsprechende Anwendungen beispielsweise die APIs idealerweise in Echtzeit und melden auftretende Probleme sofort. Bewährt hat sich in der Praxis zudem eine sogenannte „auto-healing"-Funktion: Hier reagiert das API Management auf erkannte Probleme oder Ausfälle automatisch mit Gegenmaßnahmen, beispielsweise mit einer Backuperstellung und der Wiederherstellung von vorherigen API-Versionen. Im Tagesgeschäft von Fertigungsunternehmen kann dies mitunter erfolgsentscheidend sein. Fast alle Automobilhersteller bieten beispielsweise als zusätzliches Extra den Automobilkäufern Onlinedienste im Auto an. Dazu gehören z.B. Echtzeit-Verkehrsinformationen für die Bordnavigation. Regelmäßige Erweiterungen der Dienste steigern die Kundenzufriedenheit, wie beispielsweise die Integration eines Musik Streamingangebotes. Auf der anderen Seite führt ein Ausfall eines solchen Dienstes sofort zu Unzufriedenheit, die durch die starke Verbreitung von Social Media spürbare Folgen für die Reputation haben kann. Umso wichtiger ist es Fehler, die neue Funktionen naturgemäß bringen können, schnell zu erkennen und zu beseitigen. Hierbei kann beispielsweise (als kurzfristige Maßnahme) die neue Funktion einfach auf die alte Version gesetzt werden um mehr Zeit zu haben, die Fehlerquelle zu lokalisieren.

Zudem sollte eine API Management Lösung die schnelle Umsetzung von Änderungen im Sinne von DevOps und Continous Delivery Ansätzen über alle Entwicklungsumgebungen (beispielsweise Entwicklungs-, Test- und Produktivumgebung) hinweg unterstützen – auf diese Weise sparen die Unternehmen Zeit und Geld. Schlussendlich muss eine einfache Migration neuer API-Versionen unkompliziert möglich sein und darf unter keinen Umständen zum Ausfall nachgelagerter oder korrelierender Systeme führen.

Fazit

APIs haben eine lange Historie. Inzwischen gehören die Application Programming Interfaces längst zu den technischen Standards mittlerer und großer Organisationen. Mit ihrer Marktdurchdringung wächst allerdings auch das Interesse von Cyberkriminellen, sie anzugreifen und mit ihrer Hilfe, (mitunter personenbezogene) Daten zu erlangen. Um diesen Gefahren adäquat zu begegnen, müssen Unternehmen sich mit präventiven Schutzmaßnahmen auseinandersetzen. Ein modernes API Management stellt dafür eine unersetzliche Basis dar.

Waldemar Rosenfeld, Berater, APIIDA AG

APIIDA AG
www.apiida.com