www.bt-magazin.de 3.2011 Heft 6 Deutschland: € 14,90 Österreich: € 16,80 Schweiz: sFr 29,80 Luxemburg: € 16,90

Business Technology

Business Technology

Architektur & Management Magazin

Expertenwissen für IT-Architekten, Projektleiter und Berater

JP Rangaswami: „Das Fundament ist das Teilen.“

CLOUD COMPUTING

Wolkige Geschäfte – Wozu überhaupt Cloud?

Die Enterprise Cloud

Umdenken für Architekten

4 191858 414906 03

Sicherheit in der Kommunikation zwischen Unternehmen und Cloud-Anwendungen

Sicher in der Wolke

Erweitert man die Ideen von Enterprise SOA auf unternehmensübergreifende Kommunikation und insbesondere auch auf das Nutzen von Shared-Services, die sich nicht mehr im eigenen Rechenzentrum befinden, betritt man das Themenfeld, das heute unter dem Begriff „Cloud" diskutiert wird. Für die Cloud gelten selbstverständlich viele der Securityempfehlungen, die bereits innerhalb der Grenzen einzelner Unternehmen gelten. Aufgrund der Tatsache, dass die Unternehmensgrenzen überschritten werden, kommen zusätzliche Anforderungen dazu.

AUTOREN: MAMOON YUNUS UND DIRK KRAFZIG

Die Autoren haben bereits in einer Artikelserie in diesem Magazin [1 – 4] über das Thema Enterprise SOA Security geschrieben und dabei die Wichtigkeit von Sicherheitsmaßnahmen innerhalb großer Unternehmen, die sich in Richtung einer serviceorientierten Architektur bewegen, erörtert. Insbesondere wurden in den Artikeln die einzelnen Standards [3] beschrieben, auf die auch dieser Artikel Bezug nimmt. Mit der Version 2.1 der Guidance for Critical Areas of Focus in Cloud Computing [5] hat die Cloud Security Alliance (CSA) im Dezember 2009 eine umfassende Reihe von Empfehlungen herausgegeben, um Unternehmen zu helfen, Cloud Computing sinnvoll und sicher umzusetzen. Der Leitfaden enthält Empfehlungen für die operative Sicherheit und behandelt die Themen Applikationssicherheit, Verschlüsselung und Schlüsselmanagement sowie Identity und Access Management. In diesem Artikel sollen die Auswirkungen auf die Security bei REST- und SOAP-basierter Kommunikation zwischen Consumern und Infrastructure-as-a-Service-(IaaS-)Providern betrachtet werden.

SICHERHEIT VON CLOUD-ANWENDUNGEN

Die Umsetzung der Sicherheit von Cloud-Anwendungen beginnt mit klassischen Maßnahmen der IT-Sicherheit. Ein erster Schritt umfasst daher Maßnahmen wie die Einrichtung einer DMZ mit entsprechenden Firewalls. Dabei sollten auf der Providerseite nur die für die Kommunikation nötigen Ports geöffnet sein, also z. B. 80 und 443 (für HTTP und HTTPS). Ebenso sollten die erlaubten Consumer-Adressen fest vergeben werden. Analoge Maßnahmen sind auf der Consumer-Seite zu treffen. Im zweiten Schritt werden die Prinzipien der Web-Service-Sicherheit angewandt und im dritten Schritt die Sicherheitsmaßnahmen um weitere Anforderungen von Cloud-Anwendungen erweitert, z. B. um Anforderungen wie Mehrmandantenfähigkeit.

Abb. 1: Die Auslagerung von RZ-Diensten in die Cloud erfordert eine sorgfältige Planung von Sicherheitsaspekten

IaaS-Provider bieten in der Regel unterschiedliche APIs für verschiedene Nutzergruppen an. Beliebte IaaS-Provider (Amazon EC2, Rackspace, OpSource, GoGrid) veröffentlichen deshalb oftmals parallel REST und SOAP APIs. Damit stellen die Anbieter sicher, dass der Einstieg in ihre Plattformen mit REST einfach gehalten wird, für anspruchsvollere Anwendungen aber die Nutzung des komplexeren SOAP möglich ist (**Abb. 1**).

Bei näherer Betrachtung wird schnell deutlich, dass Cloud-Provider im Gegensatz zu den Cloud Consumern den größeren Teil der Verantwortung für die Umsetzung umfangreicher Maßnahmen zur IT-Sicherheit tragen. Für sie ist es eine Gratwanderung, auf der einen Seite eine möglichst einfache Nutzung des Cloud-Services zu ermöglichen, und auf der anderen die notwendige Sicherheit konsequent umzusetzen. An dieser Stelle ist es wichtig zu verstehen, dass Zuschnitt und Technologie der APIs für Cloud-Provider nicht allein eine sachliche Fragestellung ist, sondern auch durch Marketing- und Vertriebsaspekte überlagert wird.

Aber auch die Cloud Consumer müssen sicherstellen, dass ihre API-Aufrufe innerhalb der Cloud keinen Schaden anrichten. Beispielsweise können schlecht formulierte Anfragen (oder ungünstige Interaktionsmuster) im Backend, ähnlich einem Denial-of-Service-Angriff (DoS), eine so erhebliche Last erzeugen, dass die Cloud-Anwendung für alle anderen Consumer nicht mehr nutzbar ist.

AUSWIRKUNGEN FÜR CLOUD CONSUMER

Cloud Consumer verwenden in der Regel REST- oder SOAP-basierte APIs für den Aufruf eines IaaS-Providers, um sich Serverinstanzen bereitstellen zu lassen und sie zu verwalten. Standardbasierte API-Aufrufe bieten hierbei einen enormen Grad an Flexibilität und Benutzerfreundlichkeit. Gleichzeitig birgt die Flexibilität und Einfachheit jedoch auch Sicherheitsrisiken, die adressiert werden müssen. Im Folgenden werden Sicherheitsempfehlungen der CSA vorgestellt, die Cloud Consumer zur Senkung ihres Risikos bei Interaktionen mit IaaS-Providern berücksichtigen sollten:

1. **Verschlüsselung aktivieren:** Cloud Consumer sollten SSL (HTTPS) zur Verschlüsselung von Daten während des Transports von einem in das andere System verwenden. Sofern verfügbar, sollte die Verschlüsselung der Nachrichteninhalte per WS-Security erfolgen [4]. Durch die Nutzung von WS-Security sind die Nachrichten auch dann sicher, wenn sie z. B. in einem Queuing-System zwischengespeichert werden. Das gilt auch für den Aufruf von IaaS-Ma-

nagementservices. Verschlüsselungen für SOAP-und REST-Antworten stellen sicher, dass nur autorisierte Consumer die Antworten des Providers mit ihrem jeweiligen Private Key entschlüsseln können.

2. **Überprüfung der Nachrichten**: Vor dem Aufruf eines Service sollten die Consumer sicherstellen, dass der Aufruf im definierten Format erfolgt, keine Malware enthält und die Integrität der eigentlichen Nachricht gewährleistet ist. Die Antwort des Providers sollte ebenfalls auf Malware und Integrität gescannt werden. Glücklicherweise bieten strukturierte Datenformate wie XML und SOAP durch Schemavalidierung die Möglichkeit, eine einfache Überprüfung der Nachrichten durchzuführen. Das Durchführen der Schemavalidierung gewährleistet, dass die Nachricht in Form der definierten Struktur vorliegt. Ferner muss auch eine Kontrolle der Antwort des Providers zur Identifizierung von Malware durchgeführt werden. Solche Schutzmaßnahmen kann die Verteilung von Malware innerhalb des Unternehmens oder seines IaaS-Providers verhindern.
3. **Nutzung von SOAP**: Zur Erstellung eines robusten und sicheren Frameworks für die Interaktion mit

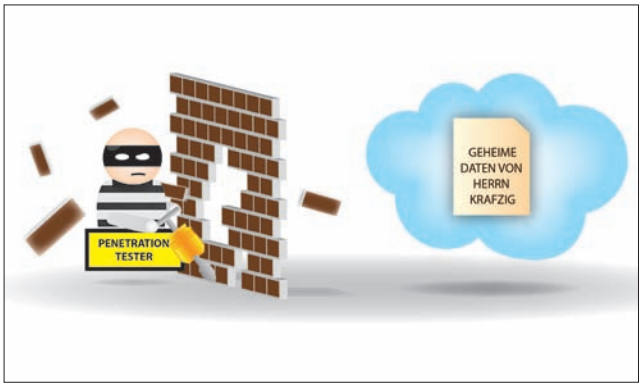

Abb. 2: Die Schutzmaßnahmen für Cloud-Anwendungen sollten Gegenstand intensiver Testbemühungen sein

IaaS-Anbietern bietet die SOAP-basierte Kommunikation einige Vorteile gegenüber der Nutzung von REST XML/JSON. Mit SOAP können Unternehmen ihre eigene Public-Key-Infrastruktur (PKI) nutzen und haben vollen Einfluss auf das Key-Lifecycle-Management, einschließlich der Fähigkeit zur Ausgabe, Signierung, dem Widerruf und der Validierung von in SOAP-Aufrufen genutzten

X.509-Zertifikaten. Durch die Verwendung von kryptografischen Verfahren haben die Unternehmen eine umfassende Kontrolle über die Authentifizierung, Integrität der Nachricht und die Privatsphäre während der Interaktion mit IaaS-Providern. Die Verwendung von X.509 mit GETs in einer REST-Umgebung ist hingegen schwierig und entspricht keinem Standard (außer für SSL „Mutual Authentication", die von vielen IaaS-Providern jedoch nicht unterstützt wird).

AUSWIRKUNGEN FÜR CLOUD-PROVIDER

IaaS-Provider verwenden in der Regel einfach zu benutzende webbasierte User Interfaces, die den Nutzern die Verwaltung der von ihnen verwendeten Cloud-basierten Server-Images ermöglichen. Für die Einrichtung einzelner Plattformen sind die webbasierten Interfaces eine hervorragende Möglichkeit zur schnellen Konfiguration und Bereitstellung. Für größere Unternehmen, die in der Regel eine große Anzahl von Cloud-basierten Server-Images bereitstellen möchten, ist jedoch die Möglichkeit des Einsatzes von automatisierten Skripts zur Konfiguration und Bereitstellung der Plattformen essenziell und unabdingbar. Die meisten IaaS-Provider ermöglichen ihren Kunden deshalb die Konfiguration und Bereitstellung der Server-Images über REST, SOAP oder Command Line Scripting. Im Folgenden werden Empfehlungen der CSA für Cloud-Provider vorgestellt:

1. **Einsatz von Standards zur Sicherung der Flexibilität:** Aufgrund des unterschiedlich ausgeprägten, technischen Hintergrundwissens müssen IaaS-Provider ein breites Spektrum an Kommunikationsprotokollen beherrschen. Dieses Spektrum kann von einer einfachen RESTful-XML/JSON-GET-Anfrage bis hin zur komplexen SOAP-Anfrage mit integrierten X.509-Schlüsseln reichen. Für große Unternehmenskunden ist es notwendig, Authentifizierung und semantisch hochwertige SOAP-Anfragen als Toolset bereitzustellen, wohingegen kleinere Unternehmen einfachere REST-Anfragen bevorzugt werden. Für die Interaktion über REST sind jedoch keine Standards in Bezug auf die Nutzung von Identity Tokens vorhanden. Unternehmen, die einen ernsthaften Einsatz von IaaS erwägen, werden auch über den Einsatz von Multi-Cloud-Plattformen nachdenken, um eine möglichst hohe Zuverlässigkeit zu erreichen. Standardbasierte Identity Tokens, beispielsweise OAuth für RESTful APIs und WS-X.509 für SOAP APIs, können ein Framework für den Aufbau von redundanten Systemen innerhalb von Multi-Cloud-Plattformen bieten.
2. **Umfassende Verschlüsselung ermöglichen:** IaaS-Provider müssen zur Erfüllung der Sicherheitsanforderungen ihrer Unternehmenskunden sowohl für im Transport befindliche Daten, Sicherheit durch Protokolle wie SSL als auch für gespeicherte Daten, Sicherheit durch Standards wie WS-Security ermöglichen. Alle bekannten IaaS-Provider ermöglichen die Nutzung einer SSL-Verschlüsselung beim Aufruf der Management-APIs. Die auf den Systemen gespeicherten Daten sind jedoch in der Regel nicht zusätzlich verschlüsselt. IaaS-Provider wie Amazon EC2 unterstützen X.509-Zertifikate für die Authentifizierung und bieten ebenso WS-Signature für ihr SOAP-basiertes API an. IaaS-Provider sollten SOAP APIs zusammen mit feingranular ausgestalteten Sicherheitsmechanismen anbieten. Sie sollten SOAP APIs unterstützen und Verschlüsselung für XML-/SOAP-Antworten als zusätzliche Ebene der Verschlüsselung anbieten, sodass nur Unternehmen, die über den eigenen privaten Schlüssel verfügen, auf verschlüsselte Informationen innerhalb einer XML-/SOAP-Antwort zugreifen können.
3. **Umfassende API-Tests durchführen:** Vor der Veröffentlichung von Cloud-Management-APIs an die Consumer sollten diese gründlich in allen angebotenen Kommunikationstypen z. B. JSON/XML REST und SOAP über HTTP(S) getestet werden. Hierbei sollte es sich um eine umfassende Prüfung innerhalb der vier Aspekte funktionale Prüfung, Performanceprüfung, Interoperabilitätsprüfung und Sicherheitsprüfung handeln. Wichtig ist, dass die Tests automatisiert und regressionsfähig sind, damit die Qualitätsmerkmale fortlaufend getestet werden können.

Funktionale Tests stellen sicher, dass das Cloud-Management-API sich wie erwartet verhält und keine Regressionsfehler eingefügt worden sind. Die funktionalen Tests sollten alle Nachrichtentypen, Identity Token und Securityartefakte abdecken. Performancetests geben Informationen zu den Durchsatzprofilen der APIs. Interoperabilitätstests stellen sicher, dass die APIs für eine breite Palette verschiedener Consumer nutzbar sind. Beispielsweise sorgt die Einhaltung des WS-I-Basic-Profile-Standards, dass die Servicebeschreibung (WSDL) für Cloud-Management-APIs in verschiedenen Umgebungen einschließlich .NET und Java leicht verwendet werden kann.

Zu guter Letzt sind die leider oft vernachlässigten Penetrations- und Sicherheitstests des IaaS-Management-APIs zur Aufdeckung von REST-, XML- und SOAP-basierten Schwachstellen elementar wichtig, bevor das IaaS-Management-API der Öffentlichkeit bereitgestellt wird. Die multiplizierende Wirkung eines

mehrmandantenfähigen Systems und mehrere Management-APIs sind eine dramatische Ausweitung der Angriffsfläche für den IaaS-Provider. Die Identifizierung und Beseitigung der angesprochenen Risiken durch umfassende Penetrationstests sollte deshalb ein wesentlicher Bestandteil der Sicherheitsplanung des IaaS-Providers werden (**Abb. 2**).

UMSETZUNG IN DER PRAXIS

In der Praxis können die in diesem Artikel beschriebenen Anforderungen, sowohl auf der Consumer- als auch auf der Providerseite mit XML Gateways umgesetzt werden. Die Autoren haben bereits dargelegt, dass XML Gateways auf Protokoll- und Content-Ebene Sicherheitsmechanismen bereitstellen [6]. Indem XML Gateways die Kommunikation zwischen Unternehmen und Cloud absichern, werden kritische Informationen während des Transports geschützt. Noch wichtiger ist allerdings, dass XML Gateways auf Nachrichtenebene die Vertraulichkeit der Daten sicherstellen können. Damit wird die Ablage von Daten in der Cloud um ein Vielfaches sicherer. In Umgebungen, die von mehreren Mandanten genutzt werden, wie es bei öffentlichen Clouds der Fall ist, ist Vertraulichkeit auf Content-Ebene besonders wichtig. XML Gateways liefern ebenfalls Identity-Management-Infrastrukturen, die dazu genutzt werden können, die Autorisierung des Zugriffs auf die Cloud-Anwendung zu regeln. Dabei ist die Fähigkeit, Identity Token zu erzeugen, zu konsumieren, zu transformieren etc. von entscheidender Bedeutung. Mit diesen Identity-Management- und Steuerungsfunktionen nehmen XML Gateways eine kritische Position ein, da sie den geregelten bzw. autorisierten Zugriff auf die Cloud-Dienste und Cloud-Daten sicherstellen.

FAZIT

Die Sicherheit von Cloud-Anwendungen erfordert eine über die Unternehmensgrenzen hinweg ausgeweitete Planung und Analyse. Unternehmen, die bereits erfolgreich Anwendungen in der DMZ mit externen Partnern nutzen, haben in der Regel bereits die ersten Grundlagen für die sichere Interaktion mit IaaS-Providern gelegt. Diese Unternehmen sind meist in der Lage, externe APIs via XML/SOAP aufzurufen, die Verwaltung von Identity Tokens durchzuführen, die Kommunikation zu verschlüsseln und den Datenverkehr zu überwachen. Die Nutzung von IaaS-Providern und der Aufbau von zuverlässigen Multi-Cloud-Plattformen erfordert jedoch eine Erweiterung der bestehenden Applikationsinfrastruktur um ein zentralisiertes Cloud-Management.

IaaS-Provider müssen einen größeren Beitrag zur Absicherung der Cloud-Anwendungen liefern als die IaaS-Consumer. Sie haben das Ziel, die notwendigen Sicherheitsmaßnahmen umzusetzen, ohne die Flexibilität und Einfachheit für die Anwender einzuschränken. Der Einsatz von starken Sicherheitsrichtlinien kann dazu führen, dass Anwender mit geringeren technischen Fertigkeiten den IaaS-Service nicht mehr nutzen können. Bei weniger starken Sicherheitsrichtlinien können eventuell die Sicherheitsanforderungen der Enterprise-Kunden nicht mehr erfüllt werden. Cloud-Provider sollten dennoch weiterhin auf die Bereitstellung flexibler Aufrufmöglichkeiten der von ihnen bereitgestellten APIs achten und optionale Erweiterungsmöglichkeiten in Bezug auf die Sicherheit ermöglichen. Sie sollten weiterhin die Nutzung standardbasierter Identity Tokens und Standard-APIs erwägen, um Unternehmen die Möglichkeit der Erstellung einer sicheren und zuverlässigen Multi-Cloud-Implementierung zu erleichtern.

Dr. Dirk Krafzig ist Gründer von SOAPARK. Als Sprecher auf Konferenzen und Autor von Artikeln und Büchern gilt Dr. Krafzig als ein Protagonist der serviceorientierten Architektur (SOA) und hat maßgeblich zu der Begriffsbildung in diesem Bereich beigetragen. Insbesondere die SOA-Fallstudien mit der Deutschen Post, Credit Suisse, Halifax Bank of Scotland und Winterthur Versicherung in seinem Bestseller „Enterprise SOA" haben viel Aufmerksamkeit auf sich gezogen. Derzeit arbeitet Dr. Krafzig in einem strategischen SOA-Programm bei einem Mobilfunkanbieter an dem Thema Security.

Mamoon Yunus ist CEO von Crosscheck Networks, einem führenden Technologieanbieter für Cloud- und Web-Service-Infrastrukturen. Als SOA-Pionier und Gründer von Forum Systems hat er wichtige Techniken für XML Appliances patentieren lassen. Er besitzt zwei Abschlüsse vom MIT. InfoWorld hat ihn 2004 als einen von vier „Up and coming CTOs to watch" ausgezeichnet.

Links & Literatur

[1] Krafzig, Becker, Mahnke und Pavkovic: Enterprise SOA Security, Teil 1: Herausforderungen, in Business Technology. Architektur & Management Magazin 1.2010, 2010

[2] Krafzig, Becker, Mahnke und Pavkovic: Enterprise SOA Security, Teil 2: Lösungsmuster, in Business Technology. Architektur & Management Magazin, 2.2010, 2010

[3] Krafzig, Becker, Mahnke und Mazur: Enterprise SOA Security, Teil 3: Web-Service-Standards, in Business Technology. Architektur & Management Magazin, 3.2010, 2010

[4] Krafzig, Becker, Mahnke und Pavkovic: Enterprise SOA Security, Teil 4: Organisatorische Maßnahmen, in Business Technology. Architektur & Management Magazin, 1.2011, 2011

[5] Cloud Security Alliance (CSA): Security Guidance for Critical Areas of Focus in Cloud Computing, Version 2.1, 17. Dezember 2009: https://cloudsecurityalliance.org/guidance/

[6] Yunus, Krafzig: Einführung in XML Gateways, in Business Technology. Architektur & Management Magazin, 2.2011, 2011