www.bt-magazin.de 4.2011 Heft 7 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

Detlev Klage:
„Das Verständnis für Architektur zählt."

BUSINESS VALUE

Wertschöpfung durch IT?

Kostentransparenz im EAM-Modell

Der ROI der Cloud

4 191858 414906 04

Kosten- und Risikominimierung durch Einsatz von zentraler SOA-Security

Zentrale Sicherheit

In diesem Artikel möchten wir zentrale und dezentrale Security-Implementierungen in großen Anwendungs- und Systemlandschaften miteinander vergleichen. Unser Fokus liegt hierbei auf der Betrachtung von Kosten und organisatorischen Herausforderungen. Bei einer genaueren Untersuchung wird deutlich, dass zentrale Security-Implementierungen erhebliche Vorteile gegenüber dezentralen Security-Implementierungen haben. Als besonderer Vorzug zentraler Security-Implementierungen muss hier neben den gewonnenen Kostensenkungspotenzialen und dem geringeren Risiko vor allen Dingen auch eine Vereinfachung auf der Seite der Anwendungsentwickler genannt werden. Diese können bei der Nutzung einer zentralen Security-Implementierung voll und ganz auf die Umsetzung der fachlichen Anforderungen konzentrieren. Security ist „out of the Box“ für sie und auch jedes weitere Projekt verfügbar.

AUTOREN: MAMOON YUNUS UND DR. DIRK KRAFZIG

Der durch die weltweite Vernetzung der Märkte verschärfte Konkurrenzdruck treibt die Unternehmen stetig an, ihre Dienstleistungen zu verbessern. Gleichzeitig wird gefordert, dass Ressourcen effektiver genutzt werden und sparsam mit ihnen umgegangen wird. Von den IT-Abteilungen wird vor dem Hintergrund dieser Einflüsse gefordert, fachliche Anforderungen in minimaler Zeit, bei minimalen Kosten in funktionsfähige Anwendungen umzusetzen. Glücklicherweise liefern Methodiken wie agile Softwareentwicklung, SOA oder Cloud Computing – um nur einige Beispiele zu nennen – einen Werkzeugkasten, der dabei hilft, flexible und kostengünstige IT-Strukturen aufzubauen, welche gleichzeitig einen guten Zuschnitt auf die geschäftlichen Bedürfnisse ermöglichen.

Moderne Anwendungen, die aktuellen Geschäftsanforderungen gerecht werden wollen, müssen in der Regel Informationen aus den verschiedensten Quellen verarbeiten. Dies können neben mehreren internen Quellen innerhalb des eigenen Unternehmens auch externe Quellen sein. Unternehmen begegnen dem Verlangen nach mehr Vernetzung in der Regel durch die Implementierung von Rich Internet Application-, API-, Virtualisierungs- und Cloud-Services, um einen direkten Zugriff auf die Datenbasis ihrer Anwendung zu ermöglichen. Das globale Bereitstellen von ausgewählten Informationen hat neben vielen Vorteilen aber auch einen Preis: Die Anwendungssicherheit leidet. Denn durch die zur Verfügung gestellten Schnittstellen wird ein potenzielles Einfallstor für Schadcode oder unautorisierten Abgriff von sensiblen Daten geschaffen. In diesem Artikel untersuchen wir zentrale und dezentrale Security-Implementierungen und zeigen, wie Unternehmen mit zentralen Security-Implementierungen kostengünstige, konsistente und handhabbare Security-Lösungen aufbauen können.

SECURITY-MODELLE IN DER ÜBERSICHT

Anwendungssicherheit kann innerhalb von Unternehmen in der Regel in drei Ausprägungen existieren: Zentralisierte Security-Implementierungen (hub-spoke), dezentrale Security-Implementierungen (Point to Point) oder eine Mischform der beiden Modelle. Zu Beginn der Anwendungsentwicklung stehen in der Regel die fachlichen Anforderungen im Vordergrund. Der Fokus liegt nicht auf der Schaffung eines gemeinsamen Rahmens oder einer gemeinsamen Infrastruktur. Das Thema Security wird in den meisten Fällen nur am Rande behandelt. Erst zum Schluss wird beispielsweise versucht durch das Aktivieren von Mechanismen wie HTTP Basic Authentication oder SSL ein minimales Maß an Security in die erstellte Anwendung zu implementieren.

Abbildung 1 zeigt eine dezentrale Systemimplementierung in der m Applikationen mit n Services kommunizieren. Hierbei können die Services neben internen Services auch Services von Partnerunternehmen, also externe Services sein. Je mehr Applikationen und Services im Laufe der Zeit in der schemenhaft dargestellten Systemlandschaft genutzt werden, desto größer wird die Anzahl der Verbindungen. Insgesamt müssen für m x n-Verbindungen Security-Richtlinien eingehalten werden.

Um der mit der Zeit steigenden Anzahl an Verbindungen Herr zu werden, kann ein zentrales Security Gateway eingesetzt werden, das die Verbindungen zwischen Applikationen und fachlichen Services herstellt. Durch die Integration dieses zentralen Gateways wird die Anzahl der Verbindungen von m x n auf m + n reduziert. Das Thema Security wird bei diesem zentralen Modell Aufgabe des zentralen Gateways und die Komplexität für die Einhaltung von Security-Richtlinien reduziert sich.

Statt m x n-Security-Richtlinien zu programmieren, kann in einem zentralem Modell durch die Nutzung

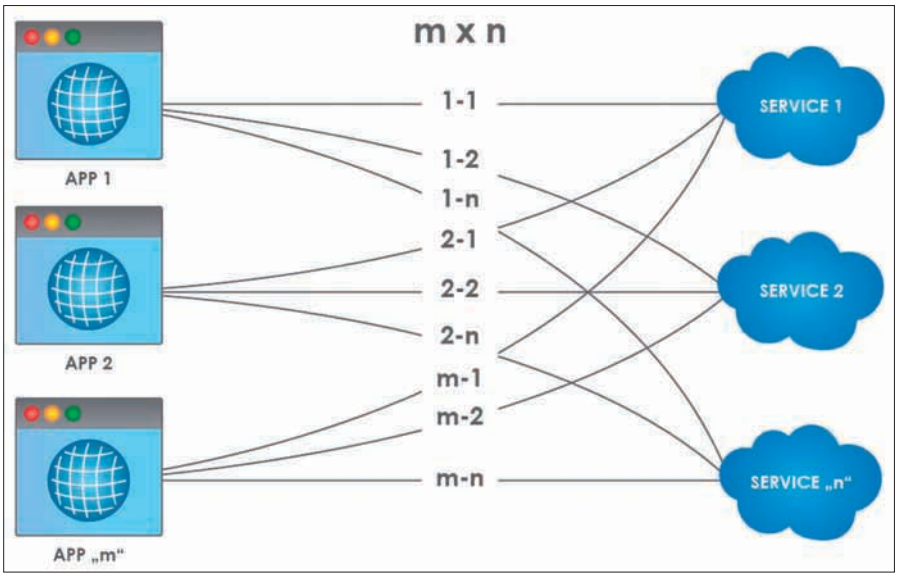

Abb.1: m x n-Verbindungen mit eigenen Security-Richtlinien bei dezentraler Security-Implementierung

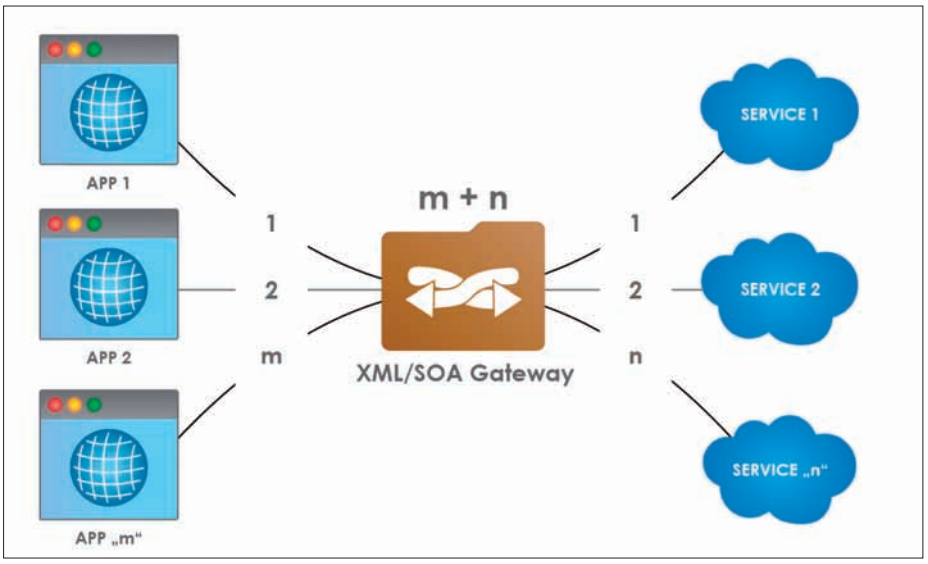

Abb. 2: m + n-Verbindungen mit Security-Richtlinien bei zentraler Security-Implementierung

eines zentralen Gateways der Aufwand für die Security-Implementierung reduziert werden. Typische Security-Anforderungen wie Identity, Privacy, Integrität, Prüfung und Schutz von Informationen werden zentral und wiederverwendbar bereitgestellt und helfen eine sichere Anwendungs- und Systemlandschaft zu gestalten.

Um zu verstehen, mit welchen Auswirkungen durch die Anwendung von zentralen Security-Implementierungen im Vergleich zu dezentralen Security-Implementierungen zu rechnen ist, möchten wir im Folgenden die Services 1 – n betrachten. Unsere Services, sowohl in **Abbildung 1**, wie auch in **Abbildung 2** verlangen die Einhaltung folgender, unterschiedlicher Anmelde-Security-Richtlinien:

- Service 1: HTTP Basic Authentication
- Service 2: SAML Token
- Service n: Adhoc Token-Typ

Im dezentralen Integrationsszenario (**Abb. 1**) muss jede Applikation, die auf Services zugreifen möchte, „n“ verschiedene Security-Richtlinien implementieren um Zugriff auf alle Services zu erhalten. Je mehr Applikationen entstehen, die auf „n“ Services zugreifen möchten, desto öfter wird immer wiederkehrend der gleiche Code programmiert und implementiert werden müssen. Denn jede Applikation ist für die Umsetzung der Security-Richtlinien selbst verantwortlich. Im Vergleich dazu werden die Security-Richtlinien in einem zentralen Integrationsszenario (**Abb. 2**) nur einmal zentral programmiert und im Gateway abgelegt. Wird dann für den Zugriff auf das Gateway nur eine Anmelde-Security-Richtlinie, wie beispielsweise HTTP Basic Authentication definiert, kann der Aufwand bei der Applikationserstellung immens reduziert werden, da nicht mehr in jeder Applikation „n“ verschiedene Anmeldeszenarien programmiert werden müssen, sondern nur eines, um auf das zentrale Gateway zugreifen zu können.

Erweitert man die Security-Anforderungen über die reine Identifikation des Servicekonsumenten um Bereiche wie Vertraulichkeit, Integrität und Audit-Richtlinien, wird der Vorteil eines zentralisierten Modells im Vergleich zu einem dezentralen Modell sogar noch deutlicher. Zusätzlich zu den beschriebenen Vorteilen ist in der Regel davon auszugehen, dass die Implementierung von Security in einem zentralen Modell lediglich einer Konfiguration bedarf, während im Vergleich dazu in einer dezentralen Point-to-Point-Implementierung oftmals eine Programmierung der Sicherheitsrichtlinien erforderlich ist.

Abbildung 2 zeigt ein physisches Gateway, das zentrale Applikationssicherheit ermöglicht. Eine logisch zentralisierte Implementierung, mit der ähnliche Vorteile erzielt werden können, kann jedoch auch physisch dezentral erfolgen. Entscheidet sich ein Unternehmen für diesen Weg, muss die Einhaltung von Security-Standards und der Aufbau eines Governance-Frameworks sorgfältig überwacht werden. Für den Rest dieses Artikels konzentrieren wir uns aber auf die Betrachtung von physisch zentralen Security-Implementierungen auf der Basis von Gateways.

KOSTENBETRACHTUNG

In diesem Abschnitt vergleichen wir die Kosten zentraler und dezentraler Security-Implementierungen miteinander. Dies geschieht durch einen Vergleich der Kosten der für die Anwendung wichtigsten Security-Richtlinien. Wie in Tabelle 1 dargestellt, werden die verschiedenen Security-Richtlinien in drei Kategorien aufgeteilt: Anfänger, Fortgeschrittene und Experten. Um einen quantitativen Vergleich zu ermöglichen, bewerten wir den Schwierigkeitsgrad für die Implementierung einer Security-Richtlinien auf einer Skala von 1 bis 10. Hierbei bedeutet Level 1, dass die Implementierung sehr einfach ist, während Level 10 bedeutet, dass die Implementierung schwierig und aufwändig ist. Wir gehen davon aus, dass bei einer

Anzeige

dezentralen Implementierung zur Einhaltung der Security-Richtlinien programmiert werden muss und bewerten somit den Aufwand für die Programmierung (Coding). Innerhalb der zentralen Implementierung gehen wir davon aus, dass eine Konfiguration (Configuration) des Gateways zur Implementierung der Security-Richtlinien notwendig ist. Das Coding-Configuration-Verhältnis zeigt die relative Schwierigkeit zwischen Programmierung und Konfiguration jeder Sicherheitsrichtlinie. Zum Beispiel kann die Entwicklung eines WS SAML Token und die Programmierung der zur Auswertung benötigten Software zehn Tage dauern, während die Konfiguration einer gleichwertigen Sicherheitsrichtlinie lediglich zwei Tage in Anspruch nimmt. In der nachfolgenden Tabelle stellen wir das Verhältnis als 10:2 (= 10 Tage Programmierung vs. 2 Tage Konfiguration) dar. Gleichzeitig ermöglicht das Verhältnis einen Vergleich des Schwierigkeitsgrades der Implementierung der einzelnen Security-Richtlinien.

Der Aufwand für die Implementierungen der Security-Richtlinien im Bereich der Expertenstufe ist deutlich höher als der Aufwand im Bereich der Anfängerstufe. Bei den besonders schwierig zu implementierenden Sicherheitsrichtlinien ergibt sich ein Verhältnis von 72 Tagen zu 17 Tagen, wobei 72 Tage für die Programmierung der Umsetzung der Security-Richtlinien anfallen und nur 17 Tage für die Konfiguration.

Die oben gezeigten Schwierigkeitsgrade sind Schätzungen und sollen einen Anhaltspunkt für Unternehmen bieten, die sich mit der Integration von Security-Richtlinien auseinandersetzen. Die Einteilung in Anfänger, Fortgeschrittene und Experten erfolgt auf der Basis von den Erfahrungen, welche die Autoren in zahlreichen Kundenprojekten machen durften. Es sollte jedoch beachtet werden, dass jedes Unternehmen bei genauerer Betrachtung aufgrund der jeweils vorherrschenden Voraussetzungen zu leicht unterschiedlichen Ergebnissen kommen kann.

Der Kontrast zwischen den Aufwänden für die Programmierung gegenüber denen für die Konfiguration wird noch deutlicher, wenn weitere Security-Richtlinien erfüllt werden müssen. Die Aufwände steigen mit jeder neuen Sicherheitsrichtlinie um den Faktor S. Im dezentralen Modell bedeutet das einen Anstieg der Aufwände um (m x n) x S, während im zentralen Modell lediglich (m + n) x S Aufwände entstehen.

Um einen Vergleich der beiden Security-Implementierungen zu ermöglichen, sollten weiterhin folgende Aspekte betrachtet werden:

- Initiale Kosten für den Erwerb eines Gateways mit laufenden Supportkosten
- Kosten für die Änderung von Artefakten für bestehende Security-Richtlinien. Beispielsweise kann ein X.509-Zertifikat ablaufen und Auswirkungen auf SSL und SAML, sowie Content-Security-Richtlinien haben
- Performancebetrachtungen bei steigender Nutzung, evtl. wird dann zusätzliche Hardware benötigt
- Komplexität der Verwaltung mehrerer Security-Richtlinien in einer einzigen Anwendung gegenüber der Konfiguration in ein Gateway

Unternehmen, die lediglich ein paar wenige Systeme und Security-Richtlinien aus dem Anfängerbereich integrie-

Security-Richtlinie	Aufwand Kodierung	Aufwand Konfiguration
Anfänger	**8**	**3**
Simple Authentication	2	1
Authorization	2	1
SSL	4	2
Fortgeschrittene	**30**	**9**
Threat – DoS/Malware	8	2
Threat – Data Leak	8	2
Data Transformation	6	2
Experten	**72**	**17**
PKI Management	8	2
Content Security	9	2
WS-SAML Tokens	10	2
Enrichment	5	1
Reliability Management	10	1

Tab. 1: Typische Aufgaben im Bereich Security – Vergleich Programmierung/Konfiguration

ren müssen (2 bis 4) werden die dezentrale Lösung präferieren. Bei einem Anstieg der Anzahl an Systemen und Forderungen nach Security-Richtlinien aus den Schwierigkeitsgraden Fortgeschrittene und Experten, wird diese Lösung schnell äußerst schwierig zu handhaben.

ORGANISATORISCHE EFFEKTE

Security-Modelle haben einen signifikanten Einfluss auf die Organisation, Rollen und Verantwortlichkeiten in einem Unternehmen. In einem dezentralen Modell bestehen Projekte zur Umsetzung fachlicher Anforderung in der Regel aus Projektmanagern, technischen Architekten und Anwendungsentwicklern. Selten werden Security-Profis Teil des Teams sein. Die Aufgabe, Sicherheitsrichtlinien in die Anwendung zu implementieren, wird auf die Anwendungsentwickler abgewälzt. Sollte es besonderen Beratungsbedarf geben, werden externe Personen damit beauftragt, die Sicherheitsrichtlinien innerhalb des Projekts umzusetzen. Nach dem Projekt sind sie nicht mehr greifbar. Nach Projektende werden in der Regel Supportverträge abgeschlossen, welche die Funktionsfähigkeit der Anwendung sicherstellen sollen. Die Überprüfung und Aufrechterhaltung der Security-Richtlinien ist in den meisten Fällen keine besonders definierte Aufgabe im Rahmen des Supportvertrags.

Auf der anderen Seite hat man die Möglichkeit, in einer zentralen Sicherheitsumgebung die Kontrolle der Einhaltung der Security-Richtlinien an ein qualifiziertes Team abzugeben, welches sich ausschließlich auf Minderung von Risiken über alle Anwendungen innerhalb des Unternehmens konzentriert. Die organisatorischen Aufgaben und Verantwortlichkeiten im Rahmen des zentralisierten Modells sind im Gegensatz zu den Adhoc-Rollen in dem dezentralen Modell eindeutig und klar definiert. Im Falle einer Security-Verletzung können im zentralisierten Modell rasch Lösungen gefunden werden. Wenn Anwendungen erweitert werden, können neue Security-Richtlinien einfach konfiguriert werden. Das macht die laufende Betreuung und Wartung unter Kosten- und Risikogesichtspunkten im zentralisierten Modell effektiver.

Ein CIO sollte finanzielle Mittel für den Aufbau eines zentralen Security-Implementierungsteams bereitstellen, um Security als Software as a Service (SaaS) innerhalb des Unternehmens anbieten zu können. Das SaaS-Modell bietet erhebliche Vorteile im Bereich der Wiederverwendung und Standardisierung. In einem zentralen Modell ist das Security-Team dafür verantwortlich, dass Sicherheitsrichtlinien aktualisiert werden, damit die Anwendungs- und Systemlandschaft gegen aktuelle Angriffsmethoden geschützt ist. Corporate-Risk-Governance-Regeln können zentral gepflegt werden und durchgesetzt werden. Die Kosten der zentralisierten SaaS Security können leicht nachvollzogen und auf die nutzenden Anwendungen verteilt werden.

ZUSAMMENFASSUNG

Ein zentralisiertes Security-Modell hat erhebliche Vorteile. Es reduziert das Sicherheitsrisiko unter Beibehaltung niedriger Kosten. Ein zentrales Security-Team, ähnlich wie die Personalabteilung oder juristische Abteilungen innerhalb eines Unternehmens, widmet sich ausschließlich dem Thema Security. Rollen und Aufgaben sind klar definiert. In modernen, agilen Entwicklungsumgebungen soll Funktionalität innerhalb weniger Tage zur Verfügung gestellt werden. Die Erwartungen an die Entwicklerteams steigen damit dramatisch an. Gleichzeitig erhöht diese beschleunigte Entwicklungszeit, die nur durch die Bereitstellung von zentraler Security aus den einzelnen Projekten abgekoppelt und somit gemildert werden kann, das Risiko-Profil. Zentrales Security-Management ist die einzig kluge Entscheidung für den Schutz von geschäftskritischen Anwendungen unter betriebswirtschaftlichen Gesichtspunkten.

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.

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.