Sicheres Cloud Computing mit Linux on System z

Siegfried Langer
IBM Deutschland Research & Development GmbH
Böblingen

Schlüsselworte

Cloud Computing, Sicherheitskonzept, IT Management, Risikomanagement, Linux on System z, Methoden, Architektur, Kryptographie, Mandantenfähigkeit, Virtualisierung, IBM, z/VM, Mainframe

Einleitung

Eines der aktuellsten IT Themen ist Cloud Computing. Die klare Serviceausrichtung bedingt die Anpassung von Methoden und verlangt eine Architektur, die neue Wege für die Optimierung der IT Umgebung und deren Management bietet. Während das Cloud Konzept attraktive Vorteile bieten kann, gehören Sicherheitsbedenken zu den größten Hindernissen für die Einführung und Nutzung solcher Services. Tatsächlich unterscheiden sich die Sicherheits-anforderungen an eine Cloud-Umgebung nur unwesentlich von sicheren IT Implementierungen, aber das Risiko erhöht sich durch die veränderten Nutzerszenarien. Der Vortrag soll Hilfestellungen für ein durchgehendes Sicherheitskonzept geben und zeigt am Beispiel von Linux on System z auf, wie Methoden, Architektur und geeignete Produkte eine sichere und gleichzeitig virtualisierte Basis für Cloud Computing bieten können.

Sicherheitsbedenken in der Cloud

Die Bedeutung von Informationssicherheit ist unbestritten. Sich häufende Pressemeldungen über kompromittierte Kundendaten sind nur ein Indikator dafür, dass das Problem präsent ist und zu erheblichem Vertrauensverlust und Umsatzeinbußen führen kann. Der Schutz der Informationen und Werte ist eine fundamentale Anforderung an die Informationstechnologie.

Warum wird Sicherheit in der Cloud als besonders großes Problem angesehen? In der Cloud – und insbesondere in öffentlichen Clouds (Public Cloud) – liegt die Kontrolle über zahlreiche Aspekt nicht mehr im eigenen Hause, sondern beim Serviceanbieter: wo sind meine Daten gespeichert? Wie sicher ist das System? Wer hat Zugriff? Wie wird auditiert? usw. Der Nutzer der Cloud muss dem Betreiber vertrauen, dass dieser alle Sicherheitsaspekte wirkungsvoll implementiert und verwaltet. Neben technischen Voraussetzungen spielt hier aber auch die persönliche Risikoeinschätzung und Bewertung eine entscheidende Rolle. Viele Unternehmen setzen daher für kritische Daten auf die private Cloud, die im eigenen Unternehmen und im eigenen Rechenzentrum betrieben wird.

Sicherheitsanforderungen an die Cloud unterscheiden sich nicht wesentlich von den grundsätzlichen Maßnahmen für eine sichere Datenverarbeitung. Allerdings steigt die Komplexität durch ein hohes Maß an Virtualisierung, Automation, Mandantenfähigkeit und Selbstbedienung – alles wichtige Voraussetzungen für den effektiven Betrieb einer Cloud-Umgebung.

Beste Praktiken und Empfehlungen

Das Ziel der IT Sicherheitsmaßnahmen muss sein, dass das Risiko auf ein vertretbares Niveau gesenkt wird. Um dies zu erreichen, müssen die Werte und Sicherheitsanforderungen verstanden werden und mögliche Risiken sind zu untersuchen. Dazu gehört auch das Monitoring, um wachsende Risiken möglichst früh zu erkennen. Einige der Risiken können abgesichert werden, während verbleibende

Risiken akzeptiert werden müssen. Dies sollte bewusst geschehen. Eine Cloud kann nicht sicherer sein, als ihre physische Rechnerinfrastruktur.

Das IBM Security Framework ist ein geschäftsorientierter Ansatz, der die Diskussion der Sicherheitsfragen unterstützt und strukturiert. Dieses wird ergänzt durch eine Sicherheitsarchitektur (IBM Security Blueprint), die das Thema weiter in einzelne Disziplinen aufbricht. Weitere Informationen dazu sind im Internet verfügbar (siehe „Weitere Informationen“ am Ende dieses Vortragsmanuskripts).

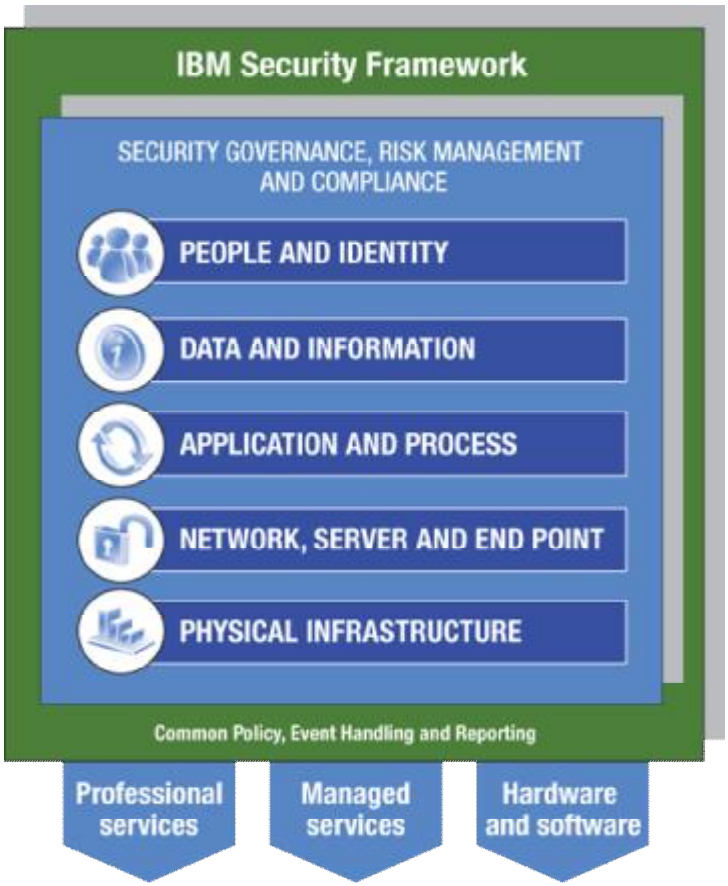

Abb. 1: IBM Security Framework

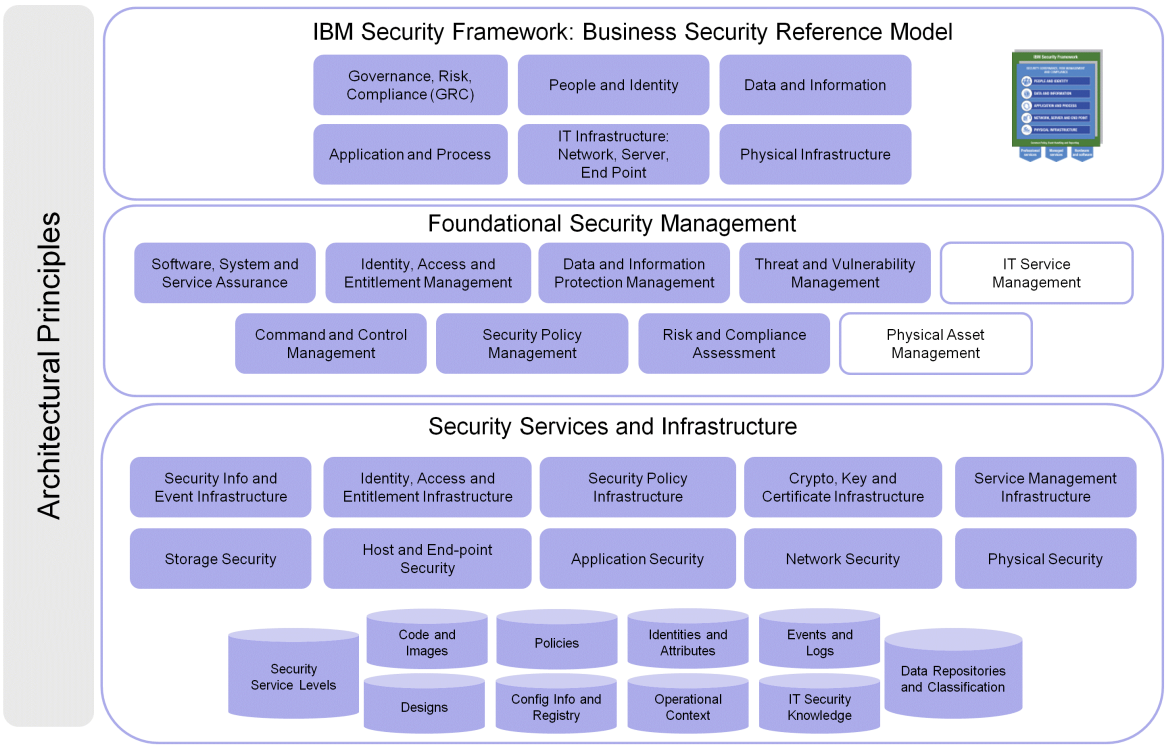

Abb. 2: IBM Security Blueprint

Anwendungs-Beispiel - Integrierte Sicherheit mit Linux on System z

Das IT-Sicherheits-Risikomanagement umfasst zahlreiche Disziplinen. Im Bereich der Sicherheitstechnologie kann die Server- und Betriebssystemarchitektur entscheidende Beiträge zur Betriebssicherheit liefern und ein hohes Maß an Flexibilität erlauben ohne die Sicherheitsaspekte zu vernachlässigen. Am Beispiel von „Linux on System z“ soll dies verdeutlicht werden.

Linux on System z

Linux on System z ist eine Linux-Implementierung auf den hochskalierbaren IBM Großsystemen, die häufig auch als Mainframe bezeichnet werden. Die neueste Generation „zEnterprise“ bietet bis zu 96 Kerne (Cores) mit einer Taktrate von erstaunlichen 5,2 GHz. IBM arbeitet eng mit SUSE und Red Hat zusammen und unterstützt SLES und RHEL auf System z. Neben zahlreichen Anwendungen und Lösungen sind Oracle 11*g* R2 und Oracle E-Business Suite für Linux on System z zertifiziert.

Mehrdimensionale Virtualisierung

Virtualisierung ist eine unabdingbare Voraussetzung für eine hoch flexible und kosteneffektive Cloudumgebung. Die System z Architektur beinhaltet eine in der Hardware integrierte Virtualisierung, die es erlaubt, das physische System in bis zu 60 logische Partitionen (LPAR) aufzuteilen.

Jede dieser LPARs ist nach Common Criteria als EAL 5 zertifiziert, was der Sicherheitseinstufung von physisch separierten Servern entspricht. Dadurch ist es möglich, beispielsweise Produktions- und Testsysteme gleichzeitig auf einer physischen Serverumgebung zu betreiben.

Für den Betrieb zahlreicher Linux-Server wird eine weitere Virtualisierungsebene empfohlen. Die IBM z/VM Virtualisierungssoftware erlaubt den Betrieb von hunderten – theoretisch tausenden – von individuellen Linux-Servern mit einer hohen gegenseitigen Isolation, die mit EAL 4+ zertifiziert ist. Gleichzeitig steht eine Vielzahl von Virtualisierungsfunktionen, wie Memory Overcommitment (den einzelnen virtuellen Servern kann mehr Speicher als die Summe des verfügbaren physischen Speichers zugewiesen werden), virtuelle LANs (VLAN) und Switches (VSWITCH), wie auch Plattenspeicher-Virtualisierung zur Verfügung. Die virtualisierten Netzwerkfunktionen können wie ein externes Netzwerk administriert werden und durch erweiterte Sicherheitsmechanismen, wie Zonen (Zoning), VLAN tagging, Port-Isolation, zusätzlich geschützt werden. Ein virtuelles Netzwerk benutzt keine physischen Verbindungen, sondern kommuniziert von Speicherbereich zu Speicherbereich, was neben der höheren Bandbreite und Geschwindigkeit mögliche Angriffspunkte und Fehlerquellen stark reduziert.

Kryptographie

Verschlüsselungstechnologien sind ein wichtiges Sicherheitswerkzeug. Das System z verfügt über integrierte Verschlüsselungshardware, die symmetrische Verschlüsselungsalgorithmen, wie z.B. DES, TDES, AES und auch Hashing stark beschleunigt.

Für Public Key Kryptographie steht eine spezielle integrierte Hardwarefunktion mit geschütztem Speicher und Sicherheitsmodul zur Verfügung, die z.B. RSA mit Schlüssellängen bis zu 4096 Bits unterstützt.

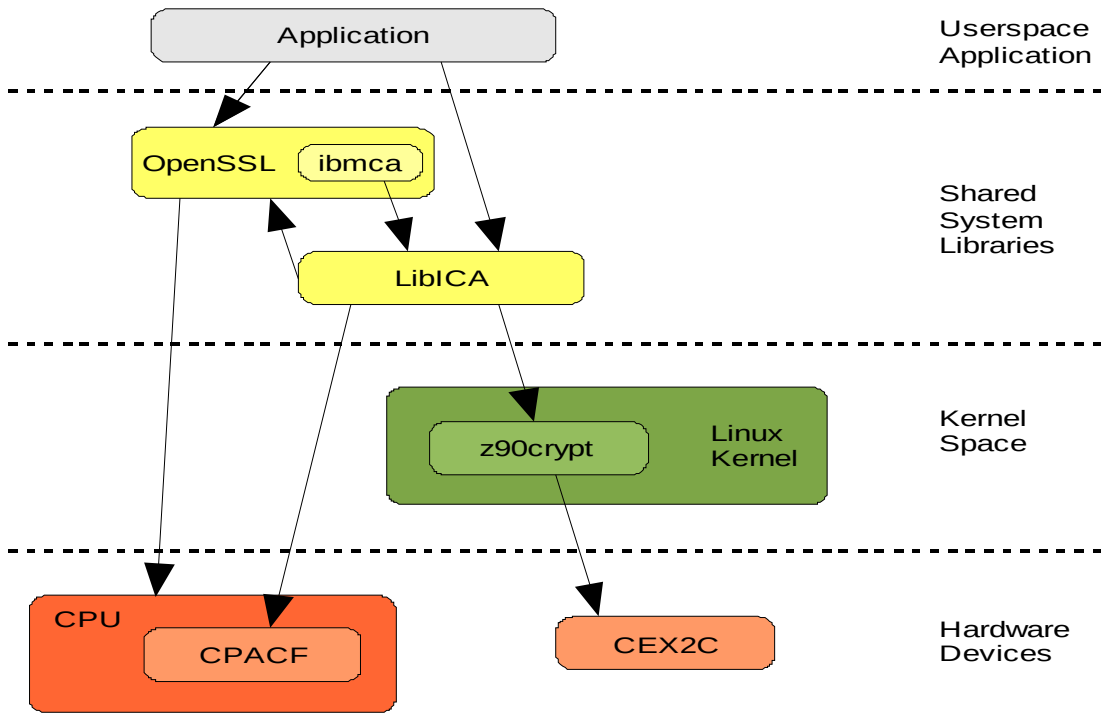

Abb. 3: Linux on System z Kryptographie-Softwareunterstützung

Ergänzt wird diese Hardwarefunktionalität durch Open Source Bibliotheken für Linux und deren Erweiterungen für Linux on System z.

Mandantenfähigkeit

Als Cloud-Serviceanbieter ist die Flexibilität, auf unterschiedliche Anforderungen reagieren zu können und gleichzeitig ein hohes Maß an Integration zu bieten, ein Erfolgskriterium. Unterschiedliche Nutzer müssen sauber getrennt voneinander die IT-Infrastruktur nutzen können – bei einem Höchstmaß an Sicherheit. Es muss garantiert werden, dass jeder Nutzer nur die eigenen Daten sehen kann. Die Fähigkeit eines Systems oder einer Datenbank, mehrere Nutzer mit garantierter Datentrennung bedienen zu können, wird mit Mandantenfähigkeit bezeichnet.

Bezogen auf Datenbanken heißt Mandantenfähigkeit, dass es möglich ist, mehrere Klienten je nach Datenmenge nicht nur mit getrennten Instanzen einer Datenbank, sondern auch über geschützte Tabellen (Table) oder Zeilen (Row) sicher zu bedienen. Daten müssen eindeutig voneinander isolierbar sein, um die Datensicherheit bei gleichzeitiger Integration zu gewährleisten.

Empfehlungen für Sicherheitsmaßnahmen in einer virtualisierten Umgebung

Die folgende Liste stellt die Minimalanforderungen an eine virtuelle Umgebung dar:

- Schutz der physikalischen IT Infrastruktur
- Absicherung des Zugriffs auf die Virtualisierungssoftware (z/VM)
- Schutz der Daten
- Schutz des virtuellen Netzwerks
- Absicherung des Zugriffs auf die virtualisierten Server (Linux)
- Schutz des Systems durch konsistente und auditierbare Systemlogs

Im Einzelnen erfordert dies verschiedenste technische Sicherheitsmaßnahmen. Für Linux on System z mit z/VM Hypervisor ergeben sich folgende Empfehlungen, die noch durch zahlreiche spezielle Sicherheitsprogramme ergänzt werden können.

Ein externes Sicherheits-Managementsystems, wie RACF (Resource Access Control Facility), bietet einen übergeordneten und von den Subsystemen unabhängigen Schutzmechanismus. Unter anderem kontrolliert und sichert es den logischen Zugriff auf z/VM, das Netzwerk, auf Daten und Programme. Darüber hinaus wird jeder Zugriff registriert (Audit Trail).

Im z/VM Hypervisor, der Virtualisierungssoftware, ist die richtige Auswahl der Privilegienklassen wichtig. Ein Linux-Gast sollte nur auf die eigene virtuelle Maschine und deren Ressourcen zugreifen dürfen. Er sollte nicht über zusätzliche Privilegien verfügen, die es erlauben, system-weite Parameter des z/VM oder anderer virtueller Gastsysteme zu verändern.

Zwingende Zugriffskontrolle (mandatory access control – MAC) ist zu implementieren. Ein zentralisiertes Zugriffsverzeichnis, wie LDAP Server, erhöht die Sicherheit und vereinfacht die Verwaltung der Identitäten.

Alle Netzwerkzugriffe (z.B. Telnet) sollten einen sicheren Kanal, wie SSL, verwenden.

Eine goldene Regel für IT-Management ist, dass Informationen nur in einer Lokation existieren sollten, also nicht mehrere Lokationen zu synchronisieren und zu überwachen sind. Mit gemeinsamen Plattenspeicherbereichen (shared Disks) über mehrere virtuelle Gäste innerhalb eines Systems kann die Anzahl der Angriffspunkte deutlich reduziert werden.

Kritische Daten sollten durch Datenverschlüsselung (encrypted file systems) zusätzlich geschützt werden.

Virtuelle Netzwerk-Switches sollten VLAN-Tagging und Port-Isolation verwenden. Dies ist ein übergeordneter Schutzmechanismus, der auch bei Fehladressierung greift. Datennetzwerke sollten von administrativen Netzwerken (Management-Netzwerke) getrennt sein.

Hinzu kommt der Schutz in der eigenen Organisation. Neben dem Audit-Log ist die Trennung von Aufgaben und Personen (separation of duties) eine essentielle Sicherheitsmaßnahme.

Zusammenfassung

Sicherheit ist mehr als nur der Schutz der Umgebung, eine Brandmauer (Firewall) reicht nicht aus! Sicherheit fängt mit den zur Verfügung stehenden Sicherheitsfunktionen und –einrichtungen an, von denen dem Betreiber von Linux und System z ein großes Portfolio zur Verfügung steht. Für Linux auf dem System z beinhaltet dies einzigartige Hardwarefunktionen, Unterstützung von vertrauten Verschlüsselungsalgorithmen, eine sichere Open Source Implementation und Softwareebenen, die es ermöglichen diese Hardwarefunktionalität von der Anwendungsebene aus zu nutzen.

Kontaktadresse:

Siegfried Langer

IBM Deutschland Research & Development GmbH

Schönaicher Strasse 220

D-71032 Böblingen

Telefon: +49 (0) 7031-16 4228

Fax: +49 (0) 7031-16 3456

E-Mail: Siegfried.Langer@de.ibm.com

Internet: www.ibm.com

Weitere Informationen:

Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security

http://www.redbooks.ibm.com/abstracts/redp4528.html?Open

Cloud Security Guidance IBM Recommendations for the Implementation of Cloud Security

http://www.redbooks.ibm.com/abstracts/redp4614.html

Security for Linux on System z

http://www.redbooks.ibm.com/abstracts/sg247728.html?Open