IBM Software Partner Academy Program

Telefonkonferenz am 07.08.2009

Security@IBM
Wie IBM Software Sie bei der Minimierung von Risiken für Ihr Unternehmen unterstützt

Susanne Kurz (SWG Channel IT Architect)

1 **Security@IBM Überblick**

2 **Governance, Risk & Compliance**

3 **Innere Sicherheit**

4 **Äußere Sicherheit**

5 **Weitere Informationen**

CSO müssen eine Vielzahl von Themen adressieren Security@IBM liefert hierfür einen flexiblen, wertbasierten Ansatz.


Bedrohungslage verstehen


Risiken priorisieren + beherrschen

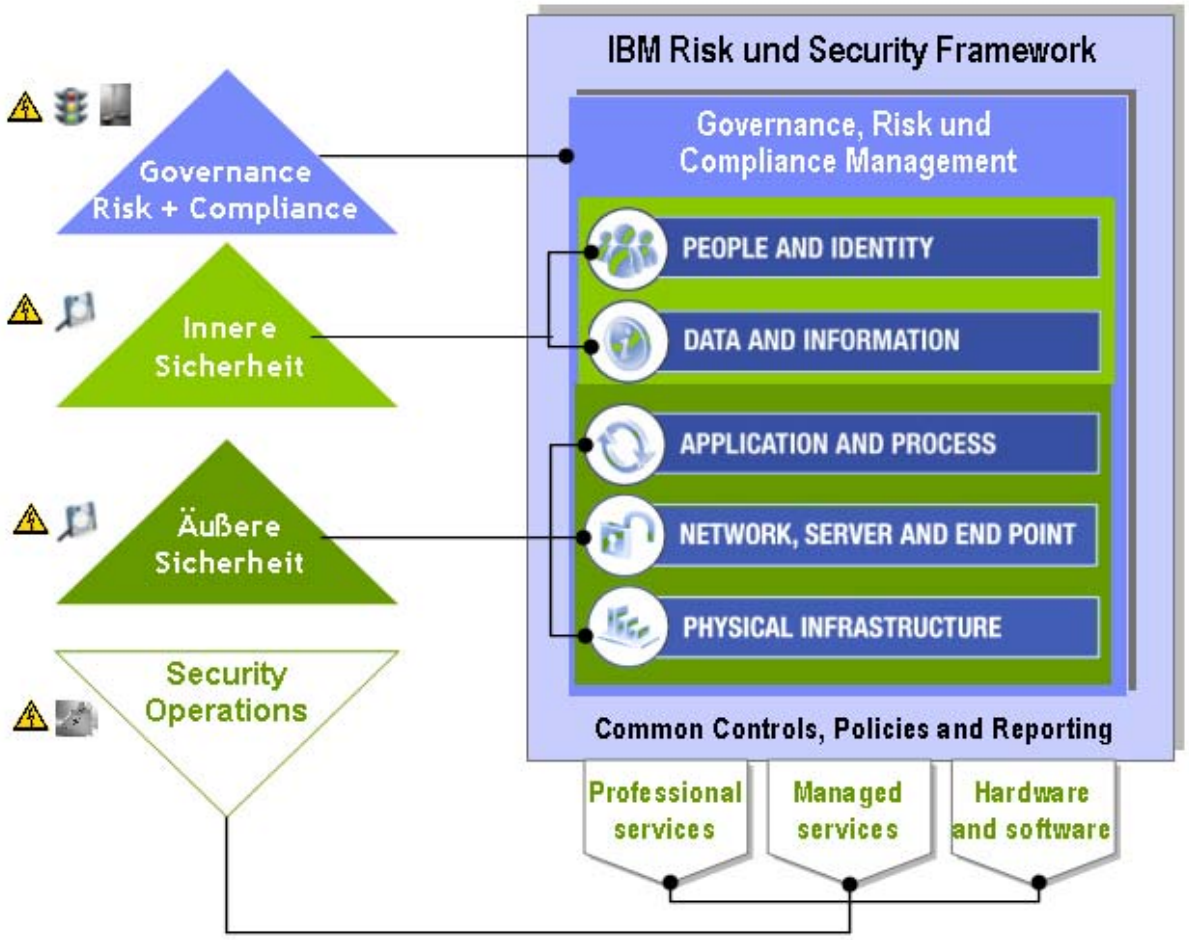

Compliance Anforderungen erfüllen


Informationen + Infrastruktur schützen


Kosten managen

Security@IBM ordnet diese wesentlichen Sicherheitsthemen und Risikodimensionen vier Kategorien zu

Alle Bereiche fußen methodisch auf dem IBM Risk und Security Framework



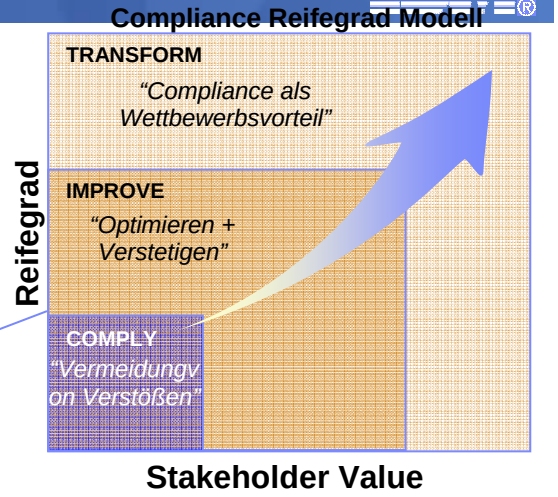
- Jeder Lösungsbereich aus dem Framework besteht aus den Bausteinen Organisation, Prozesse und Architektur
- Alle Bereiche haben untereinander Beziehungen, die durch das Security@IBM Beratungs- und Reifegrad- modell hergestellt werden

Die IBM Portfolio Elemente in der Übersicht

IBM Lösungsspektrum
- Schaffung nachhaltiger Risiko Management Strukturen
- Bewertung aktueller Risk Management Modelle via COSO und BRM Standards
- Operational Risk Management Design
- GRC Cockpit Design + Rollout

Bedrohungslage
- Fahrlässigkeit
- Persönliche Haftung
- Strafzahlungen
- Existenzbedrohung

Governance Risk + Compliance



Bedrohungslage
- Systemmanipulation
- Kontrollverlust
- Systemausfall
- Datendiebstahl

Security Operation

Bedrohungslage
- Daten + Identitätsdiebstahl
- Betrug + Erpressung
- Plagiate + Manipulation
- Interna in der Presse

Innere Sicherheit

Äußere Sicherheit

Bedrohungslage
- Trojaner, Viren, etc.
- Spam, Botnetze
- Diebstahl,
- Vandalismus

IBM Lösungsspektrum
- Bewertung/Verbesserung der Applikationssicherheit
- Sicherung von Identitäten und Zugängen
- Überwachung privilegierter Benutzer
- Datenschutz/Sicherung geistigen Eigentums
- Data Loss Prevention / Encryption Lösungen
- Security Awareness Programme

IBM Lösungsspektrum
- Managed Security Services
- Managed Identity Management
- Security Betriebskonzepte
- Operatives Compliance Modell

IBM Lösungsspektrum
- Penetrations-Tests und Schwachstellen-Scans
- Intrusion Detection und Prevention
- Security Information und Event Management
- Web Service/Security Konzepte + Lösungen
- Netzwerkzugangskontrolle (NAC)
- Netzwerk DLP + Content Filter
- DR und BCM Analyse

1 Security@IBM Überblick

2 **Governance, Risk & Compliance**

3 Innere Sicherheit

4 Äußere Sicherheit

5 Weitere Informationen

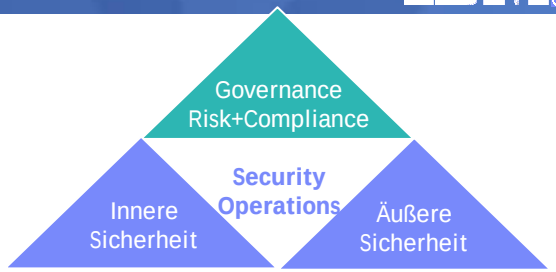
Governance, Risk & Compliance

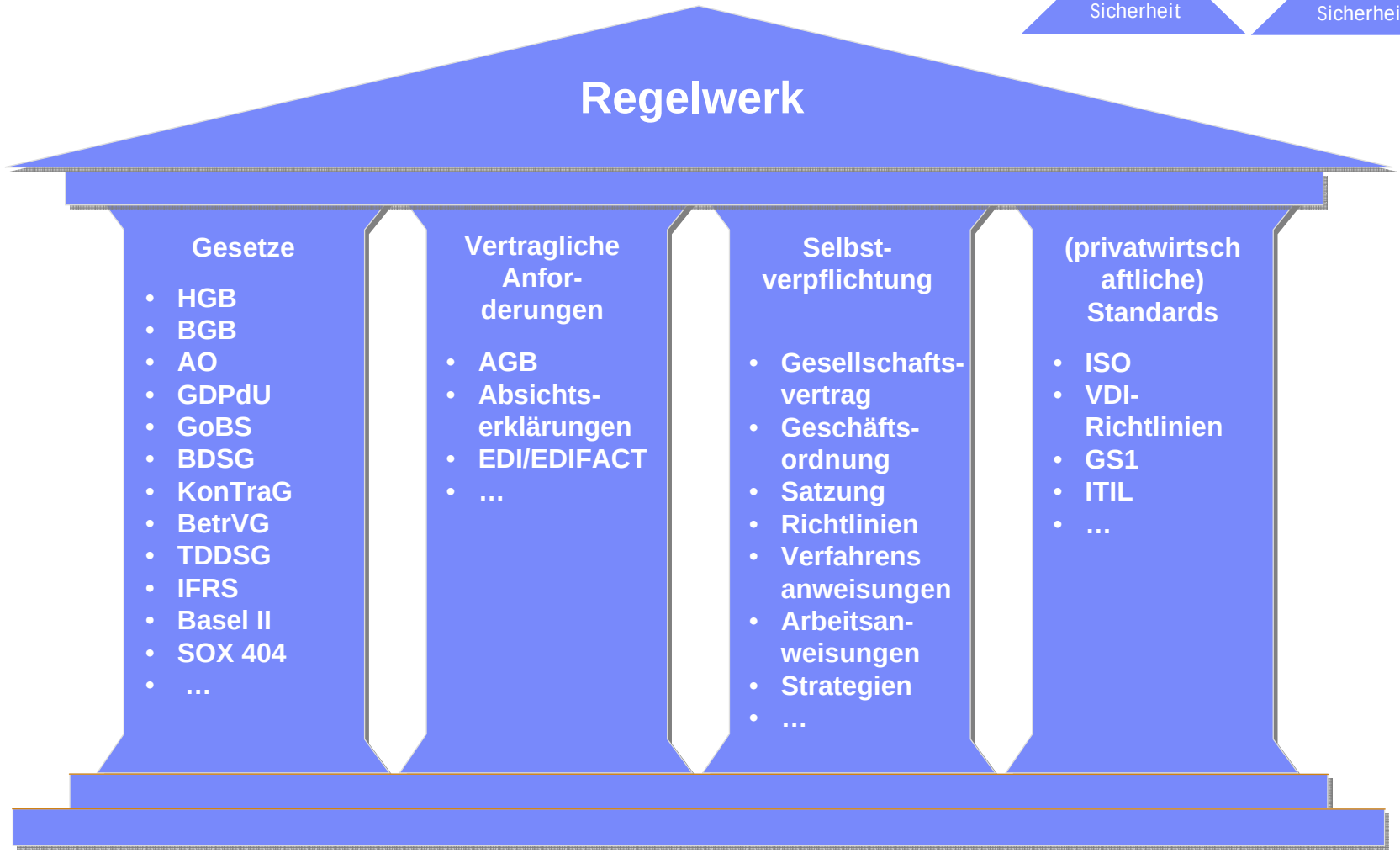
Der Begriff **Compliance** bezeichnet die Einhaltung von:

- **Gesetzen** (compliance i.e.S.)
- **Richtlinien/ Verordnungen/ Verträgen**
- **freiwilligen Regelungen in Unternehmen** (z.B. Code of Conduct)

und zielt somit auf die Legalität unternehmerischen Handelns und die Konformität des Verhaltens von Management und Mitarbeitern

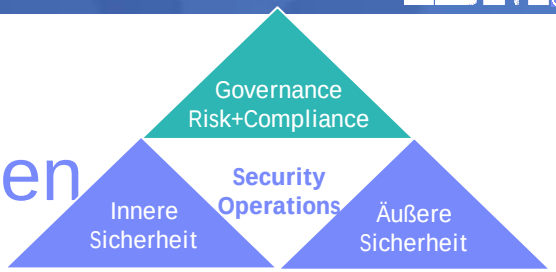
Welche Regeln sind zu beachten?





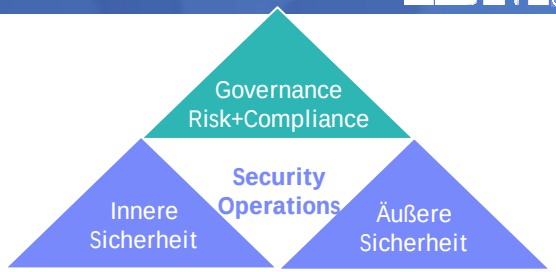
Quelle: © 2009 KPMG AG Wirtschaftsprüfungsgesellschaft

Anforderungen an Compliance Lösungen



- Hohes Sicherheitsniveau für Systeme, Anwendungen, Daten im Ruhezustand und Daten in Bewegung
- Vollständiges und integriertes Benutzeridentitäts- und Zugriffsmanagement
- Anwendungsentwicklungsprozesse und -werkzeuge, die bereits im Voraus Sicherheits- und Leistungsprobleme berücksichtigen
- Archivierung und Abfrage von Daten und Inhalten, die eine Abstimmung zwischen täglicher Leistung der Geschäfts-anwendungen einerseits und Datenspeicherung und Daten-sicherheit andererseits ermöglichen
- Werkzeuge für die Erstellung von Berichten zu Standards hinsichtlich Sicherheit, Business-Continuity und Leistung

Compliance-Management-Lösungen



- **Compliance Management mit Rational-Software**
  IBM Rational-Software unterstützt die Ausrichtung von Softwareentwicklungsprozessen an allgemein anerkannten, bewährten Verfahren und Standards für das IT- und Systemmanagement, wie COBIT™ (Control Objectives for Information and related Technology), CMMI® (Capability Model Maturity Integration) und den ITIL®-Standards (IT Infrastructure Library)

- **Compliance Management für Enterprise Content Management**
  ECM Compliance-Produkte archivieren und verwalten E-Mails und andere elektronische Nachrichten als Records, unterstützen die Einhaltung von Vorschriften und senken die Kosten für die Speicherplatzverwaltung

- **Tivoli Security Compliance Manager**
  Beurteilt IT-Systeme im Hinblick auf die Erfüllung von Sicherheitsrichtlinien und ermöglicht bessere Sicherheitsverfahren durch Automatisierung und Zentralisierung. Unterstützt bei der Umsetzung von Sicherheitsrichtlinien, die zur Erfüllung von Unternehmens- und Branchenstandards beitragen. Und ermöglicht eine rasche Ermittlung, ob Ihre Betriebssysteme Ihren Sicherheitsrichtlinien entsprechen.

1 Security@IBM Überblick

2 Governance, Risk & Compliance

3 **Innere Sicherheit**

4 Äußere Sicherheit

5 Weitere Informationen

Innere Sicherheit

Die innere Sicherheit stellt den Schutz von Unternehmensinformationen, geistigem Eigentum und Applikationen in den Vordergrund. Im Rahmen der inneren Sicherheit ist es erforderlich, den Zugang zu und die Kommunikation von kritischen Informationen zu steuern und zu auditieren, um Missbrauch frühzeitig erkennen und eindämmen zu können.

Aus der Corporate und Security Governance leiten sich damit folgende Disziplinen für den Bereich der Inneren Sicherheit her:

- **Datenschutz** (Privacy) und Vier-Augen-Prinzip (Segregation of Duty)
- **Datensicherheit** (Data Security Management)
- **Application Security**
- **Identity & Access Management**
- **Persönliche Sicherheit**

Identity & Access Management

Identity Management

- Zentrale Verwaltung aller Accounts
  - Anlegen, Löschen, Ändern, Sperren, Freigeben
- Password Management
  - Ein Kommando ändert alle Passwörter
- Automatisierung durch Rollen und Regeln
  - Änderung an Rollen und Regeln führt zu Provisionierungsaktivitäten
  - Policy Enforcement
- Genehmigungsprozesse / Workflows
  - Einholen von Genehmigungen, egal ob Provisionierung aufgrund von Anträgen oder durch Rollen und Regeln initiiert wurde
- Delegierte Administration
  - Administration durch Fachbereichskoordinatoren, Standortverantwortliche
  - Administration durch Vorgesetzte
  - Self-Service
- Auditing und Reporting
  - Alle Aktivitäten müssen protokolliert werden

Access Management

- Zentrale Verwaltung von Zugriffsrechten
  - für Web-Zugriffe, eigene Anwendungen, …
- Authentifizierung
  - Unterstützung unterschiedlicher Authentifizierungsmechanismen
- Single Sign-On
  - für Web- und Desktopanwendungen
- Autorisierung
  - auf URL Basis oder anwendungsspezifisch
- Auditing und Reporting
  - Alle Zugriffe müssen protokolliert werden

Anforderungen an eine zentrale Benutzer-verwaltung

Was soll erreicht werden?

- Kostenreduktion
- Entlastung der Administratoren
- Erhöhung der Sicherheit, Revisionsfähigkeit
- Mehr Akzeptanz bei den Benutzern

Wie soll es erreicht werden?

- **Importierung von Benutzerdaten aus HR Systemen**
- **Automatisierte Vergabe und Entzug von Rechten/Resourcen**
- **Rollen-basierte Berechtigungsvergabe**
- **Webbasierte Benutzerschnittstelle**
- **„User Self-Service“**
- **Integriertes flexibles Genehmigungsverfahren**
- **Einheitliche Unterstützung „aller“ Zielsysteme und Anwendungen**
- **Auditing und Reporting**

1 Security@IBM Überblick

2 Governance, Risk & Compliance

3 Innere Sicherheit

4 Äußere Sicherheit

5 Weitere Informationen

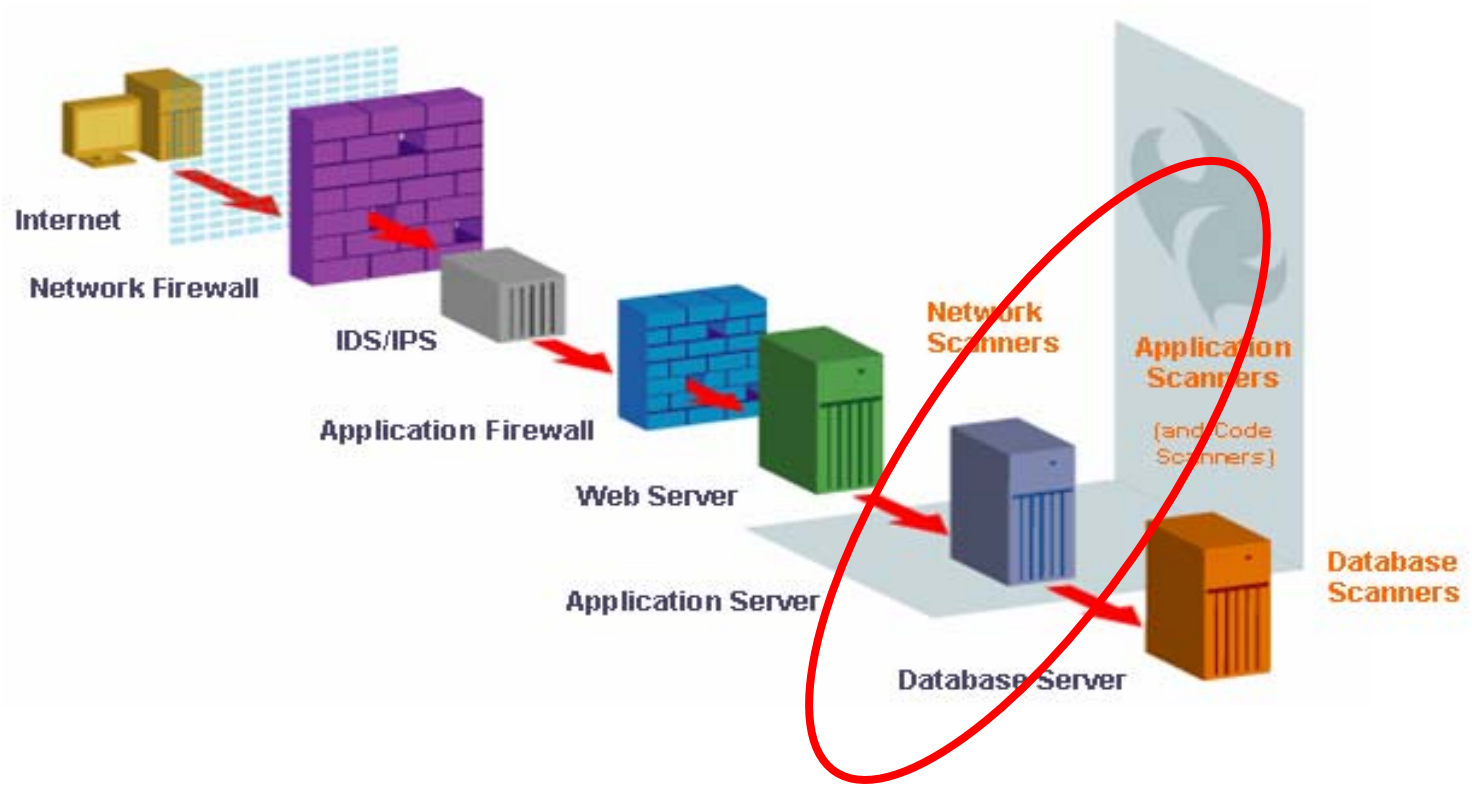
Äußere Sicherheit

- Die äußere Sicherheit fokussiert auf den Schutz der Peripherie eines Unternehmens, ganz egal ob es sich dabei um die physische oder informationstechnische Hülle handelt. Die äußere Sicherheit wurde historisch durch die Abwehr von isolierten externen Angriffen auf die Netzwerk-Infrastruktur bestimmt.
- Aufgrund des technologischen und gesellschaftlichen Wandels muss die Herstellung der äußeren Sicherheit mittlerweile auch das strukturierte und äußerst professionelle Vorgehen krimineller und geheimdienstlicher Gruppen berücksichtigen.
- Somit umfasst die äußere Sicherheit die Disziplinen:
  - **Threat Mitigation** (Pro-aktiver Peripherieschutz)
  - **Physische Sicherheit**

Beispiel Rational AppScan

Lösungen für die Automatisierung von Softwaretests für eine höhere Software-Qualität

- Einordnung der „Application Security“



Warum ist “Application Security” so wichtig?

- **Web Applikationen stehen an erster Stelle der Hacker Attacken**
  - 75% aller Attacken betreffen die Applikationsschicht (Gartner)
  - “XSS” und “SQL Injection” stehen an erster und zweiter Stelle der Attacken
- **Die meisten Sites sind angreifbar**
  - 90% aller Seiten sind angreifbar durch Applikations-Attacken (Watchfire)
  - 78% der einfach anwendbaren Attacken betreffen Web Applikationen (Symantec)
  - 80% aller Unternehmen werden bis 2010 mit Sicherheitsvorfällen konfrontiert werden (Gartner)
- **Web Applikationen sind für Hacker höchst interessant**
  - Zugriff auf persönliche Daten, Kundendaten, Unternehmensdaten, Kreditkarten usw.
- **Compliance Anforderungen werden verletzt**
  - Basel II, Datenschutzgesetze, SOX, Payment Card Industry (PCI) Standards, GLBA, HIPPA, FISMA.

Rational AppScan

- AppScan ist eine automatisierte Sicherheitslösung für Webanwendungen, die exakt kritische Schwachstellen lokalisiert, diese erläutert und Empfehlungen zur Bereinigung angibt (z.B. mit Beispielcode)

- Zielgruppe: Sicherheitsprüfer, Penetration Tester, QA Tester, Entwickler

VALUE PROPOSITION

- End-to-End Solution mit dem Ziel, Anzahl der Schwachstellen in Zukunft zu minimieren (andere Anbieter melden lediglich die Schwachstellen).
- Webanwendungen verfügen meist über zu wenig programmierte"Sicherheitsvorkehrungen Angriffe für Hacker zum Zugriff/Diebstahl auf Unternehmensdaten oder persönlichen Daten werden dadurch einfacher; Sicherheitsvorkehrungen im Netzwerk helfen hier nicht.
- Rational AppScan ist die umfassendste Lösung für Compliancereporting schafft Transparenz in den Themen, die Auswirkung auf die Erfüllung von Sicherheits- und Complianceanforderungen haben.
- Zeitersparnis durch Automation für Entwickler, Prüfer, Penetrationtester und Consultants.
- Reports mit Lösungsempfehlungen erhöhen Effizienz der Entwickler und Prüfer.
- Schnellere Audits (intern/extern) bietet 40 verschiedene Reporting Templates für Industrie- und Complianceanforderungen.

1 Security@IBM Überblick

2 Governance, Risk & Compliance

3 Innere Sicherheit

4 Äußere Sicherheit

5 Weitere Informationen

Weitere Infos

- www.ibm.com/de/security
- Workshop
  360° Rundumblick über IBM Security Software
  Wie IBM SW Sie bei der Minimierung von Risken für Ihr Unternemen unterstützt
  - 1.9. Frankfurt
  - 7.9. Hamburg
  - 17.9. Stuttgart

Zeit	Vortrag
10:00	**Security@IBM** *Matthias Lehmann, Manager Tivoli Technical Sales*
10:30	**Governance, Risk & Compliance** *Walter Karl, Tivoli Technical Sales Specialist*
11:30	**Innere Sicherheit** Application Security Assessment mit Rational AppScan *Thomas Neudert, Product Sales Specialist Rational*
13:15	Identity & Access Management *Walter Karl, Tivoli Technical Sales Specialist*
14:00	**Äußere Sicherheit** Proaktiver Peripherie Schutz *Peter Häufel , Partner Account Manager IBM Internet Security Systems*
15:00	Lotus Protector *Ingo Karge, Lotus Technical Sales Specialist*
15:45	**Zusammenfassung und Diskussion**

Kontaktdaten:

Susanne Kurz
SWG Channel IT Architect
Tel: 0171 9706362
Email: KURZ@de.ibm.com

Vielen Dank für Ihre Aufmerksamkeit!