

# IT-Security in Deutschland 2010

Deutschland 2010

.....  
Unternehmensdarstellung und Fallstudie: IBM  
.....

- ANGABEN OHNE GEWÄHR -

IDC Multi-Client-Projekt • Juli 2010 • Analyst: Lynn-Kristin Thorenz

## METHODIK

Das nachfolgend dargestellte Unternehmensprofil sowie die Fallstudie basieren auf Informationen, die von IBM zur Verfügung gestellt wurden. Für diese Angaben übernimmt IDC keine Gewähr.

## IBM

---

### Unternehmensdarstellung IBM

#### *Informationen zum Unternehmen*

IBM gehört mit einem Umsatz von 95,8 Milliarden US-Dollar im Jahr 2009 zu den weltweit größten Anbietern im Bereich Informationstechnologie (Hardware, Software und Services). Das Unternehmen beschäftigt derzeit 399.400 Mitarbeiter in über 170 Ländern. Die IBM in Deutschland mit Hauptsitz bei Stuttgart ist die größte Ländergesellschaft in Europa.

#### *Positionierung im Bereich IT Security*

IBM verfügt im Bereich Security nach eigenen Angaben mehr als 200 Produkte und etwa 3.500 Mitarbeiter. IBM betreibt zudem weltweit sechs Forschungseinrichtungen, in denen Sicherheitstechnologien entwickelt werden. Außerdem verfügt IBM über acht Security Operations Center.

#### *Darstellung des Darstellung des IT Security Portfolios*

IBM bietet im Security Bereich Lösungsstrategien und –szenarien an – von der strategischen Beratung, Design und Lösungskonzeption bis hin zu Software, Hardware und den Sicherheitsbetrieb. Im Einzelnen konzentriert sich IBM dabei auf:

- Eine ganzheitliche Risk und Compliance Beratung, inklusive der Entwicklung von Risiko Management- und Sicherheitskonzepten unter Einhaltung und Kontrolle der entsprechenden Richtlinien (IBM Security Governance Solutions). Lösungen in diesem Bereich sind z.B.:

**IBM Tivoli Security Information and Event Manager**, eine Sicherheits- und Compliance-Management-Lösung, die Unternehmen dabei unterstützt, ihre Sicherheitsrisiken transparent zu machen. Die Lösung hilft, sicherheitsrelevante Ereignisse zu zentralisieren und die konsolidierten Daten zu analysieren, um hieraus Erkenntnisse in Bezug auf Sicherheit und Compliance zu erlangen.

**IBM Tivoli Compliance Insight Manager**, eine automatisierte Lösung für die Überwachung, Überprüfung und Dokumentation von Benutzeraktivitäten im gesamten Unternehmen. Tivoli Compliance Insight Manager unterstützt Unternehmen bei der Überprüfung und Dokumentation darüber, ob Daten und Systeme in Übereinstimmung mit geltenden Unternehmensrichtlinien verwaltet werden.

- ☒ Die Verwaltung von Nutzern und deren Zugriffsrechten auf Daten und Anwendungen zum Schutz der inneren Sicherheit eines Unternehmens (IBM Identity und Access Management). Lösungen in diesem Bereich sind z.B.:

**IBM Tivoli Identity Manager**, eine Lösung für die Verwaltung von Benutzerkonten, Zugriffsberechtigungen und Kennwörtern. Sie automatisiert nach Angaben von IBM die Prozesse der Erstellung und Einrichtung oder Löschung von Benutzerberechtigungen für heterogene IT-Ressourcen während des gesamten Lebenszyklus des Benutzerkontos.

**IBM Tivoli Access Manager Enterprise Single Sign on** ermöglicht die Authentifizierung für sämtliche Anwendungen in einem Schritt und stellt für die Anwendungen an allen Unternehmensendpunkten strikte Authentifizierung, Zugriffsautomatisierung und Konformitätsberichte bereit.

- ☒ Den sicheren Umgang mit geschäftskritischen oder personenbezogenen Daten sowie die Abwehr von Viren und Spam (IBM Data Security Solutions).
- ☒ Die Erkennung und präventive Abwehr externer Bedrohungen (IBM Threat Mitigation Solutions). Schutz gegen unbekannte Bedrohungen liefern die Lösungen von Internet Security Systems (ISS). IBM hat das Sicherheitsunternehmen im Oktober 2007 übernommen. Das sogenannte X-Force Team von ISS ist darauf spezialisiert, Schwachstellen in Netzwerken, Systemen und Anwendungen zu finden.

Mit **IBM Rational AppScan** können Eingabeparameter einer Webanwendung, wie Formularfelder, Abfragezeichenfolgen, Cookies und HTTP-Header, automatisiert auf bekannte Sicherheitslücken überprüft werden. Alle erkannten Sicherheitslücken werden protokolliert, beschrieben und risikoklassifiziert und Empfehlungen zur Fehlerbehebung ausgegeben.

- ☒ Die physikalische Sicherheit mit dem Schwerpunkt digitale Videoüberwachung und dem Bau von sicheren Rechenzentren (IBM Physical Security).

### ***Referenzen im IT Security Umfeld***

- ☒ Herz- und Diabeteszentrum NRW
- ☒ Münster Osnabrück International Airport
- ☒ Meyer Werft

---

## **Fallstudie: Meyer Werft**

### ***Informationen zum Kunden***

Die Meyer Werft in Papenburg an der Ems ist eine der ältesten und modernsten Werften der Welt. Sie hat sich international vor allem durch den Bau von luxuriösen Kreuzfahrtschiffen einen exzellenten Ruf erworben. Die Werft wurde 1795 gegründet und befindet sich in sechster Generation in Familienbesitz. Schiffe können dank der modularen Bauweise in kürzester Zeit gebaut werden. Möglich wird dies durch zwei überdachte Baudockhallen, effiziente Fertigungsanlagen, innovative Produktionsmethoden und kurze Wege – sowohl organisatorisch als auch räumlich. Seit 1997 gehört die Neptun Werft in Rostock-Warnemünde zur Unternehmensgruppe. Diese beschäftigt ca. 2.500 Mitarbeiter in Papenburg und ca. 400 in Warnemünde.

### ***Anforderungen des Kunden***

Etwa 1.800 Lieferanten weltweit sowie einige hundert Partnerfirmen bauen gemeinsam an den Schiffsprojekten der Werft. Die Vertreter der beauftragenden Reedereien haben eigene Büros auf dem Werftgelände. „Zu unseren strategischen Zielen gehört es, Kunden und Partnerfirmen einen sicheren und zentralen Zugang zu ausgewählten Anwendungen zu eröffnen“, sagt Yvonne Tepe, IT-Architektin bei der Meyer Werft GmbH. Dadurch soll eine effizientere, unternehmensübergreifende Zusammenarbeit gestärkt werden. Das Web-basierte Meyer Neptun Portal ist ein wichtiger Baustein dieser Strategie. Besonders wichtig ist hierbei eine sichere Authentifizierung und Autorisierung der Benutzer.

### ***Darstellung der Lösung***

IBM unterstützte die Meyer Werft bei der Erstellung des Sicherheitskonzepts. Eingeführt wurde der "Tivoli Access Manager for e-business", über dem die Autorisierung der Zugriffe auf ausgewählte Informationen erfolgt. Benutzer ohne korrekte Zugangsdaten werden bereits vom "Tivoli Access Manager WebSEAL" abgewiesen. Die unterschiedlichen Berechtigungen sind im Policy Server abgelegt, die Benutzerdaten werden im Directory Server verwaltet. Über HTTP Server und "WebSphere Application Server" und abgesichert durch Firewalls erfolgt dann der Zugriff auf die jeweils erlaubten Informationen.

Den Zugang über personalisierte Login-Daten erhalten Lieferanten nach ihrer Bewerbung und einer erfolgreichen internen Prüfung. Für Kunden ist der Zugang darüber hinaus durch eine USB-PKI-Token-Lösung abgesichert. Der "Tivoli Access Manager" unterstützt unterschiedliche Authentifizierungsmöglichkeiten. So kann abhängig von der Sensibilität der zugänglichen Informationen flexibel über den Sicherheits-Level und das Maß an Authentifizierung und Autorisierung entschieden werden.

"Tivoli Access Manager" verwaltet die Sicherheitsrichtlinien zentral für mehrere "WebSphere Application Server". Das Benutzer-Registry wird von "WebSphere Application Server" und "Tivoli Access Manager" gemeinsam verwendet. Innerhalb von nur fünf Tagen hatte nach Unternehmensangaben ein Mitarbeiter von IBM die komplette "Tivoli Access Manager"-Testumgebung installiert, einschließlich

Hochverfügbarkeit, Einbindung der "WebSphere Application Server" und Dokumentation der Konfiguration. Das Aufsetzen der Produktivumgebung erfolgte dann selbstständig durch die IT-Fachleute der Meyer Werft.

### ***Projekthighlights***

- Unternehmensübergreifende Zusammenarbeit in Übereinstimmung mit den strategischen Unternehmenszielen.
- Flexible Unterstützung verschiedener Authentifizierungsstufen je nach Sicherheitsanforderungen.
- Installation der kompletten "Tivoli Access Manager"-Testumgebung innerhalb von fünf Tagen.

### ***Zitate des Kunden zum Projekt***

- „Tivoli Access Manager for e-business und WebSphere Application Server sind sehr gut miteinander integriert und harmonisieren bestens“.

Hans Hermann Zumsande, Administrator Systemumgebung. Meyer Werft

- „Das System ist flexibel und verfügt über gut dokumentierte Schnittstellen. So konnten administrative Prozesse durch uns automatisiert werden.“

Matthias Müller, Softwareintegrator, Meyer Werft

---

## **Copyright Hinweis**

Die externe Veröffentlichung von IDC Information und Daten – dies umfasst alle IDC Daten und Aussagen, die für Werbezwecke, Presseerklärungen oder anderweitige Publikation verwendet werden, setzt eine schriftliche Genehmigung des zuständigen IDC Vice Presidents oder des jeweiligen Country-Managers bzw. Geschäftsführers voraus. Ein Entwurf des zu veröffentlichenden Textes muss der Anfrage beigelegt werden. IDC behält sich das Recht vor, eine externe Veröffentlichung der Daten abzulehnen.

Für weitere Informationen bezüglich dieser Veröffentlichung kontaktieren Sie bitte: Katja Schmalen, Marketing Manager, +49 (0)69/905020 oder [kschmalen@idc.com](mailto:kschmalen@idc.com).

Urheberrecht: IDC, 2010. Die Vervielfältigung dieses Dokuments ist ohne schriftliche Erlaubnis strengstens untersagt.