Verlässliche Online-Services für ISP auf Basis von Microsoft Technologien

Michael Kranawetter
Chief Security Advisor (CSA)
Microsoft Deutschland

Deutschland sicher im Netz DSIN – Workshop
24.01.2008, eco, Köln

Microsoft's Ausrichtung

Bedrohungen

Entwicklung der Bedrohungslandschaft

- Lokale Netzwerke
- Erster PC-Virus
- Bootsektor-Viren
- Schlechten Ruf erlangen oder Schaden verursachen
- Langsame Verbreitung
- 16-Bit DOS

1986–1995

- Internet-Ära
- Makro-Viren
- Skript-Viren
- Schlechten Ruf schaffen oder Schaden verursachen
- Schnellere Verbreitung
- 32-Bit Windows

1995–2000

- Verbreitung von Breitbandzugängen
- Spyware und Spam
- Phishing
- Botnets
- Rootkits
- Finanzielle Beweggründe
- Das Internet ermöglicht große Auswirkungen
- 32-Bit Windows

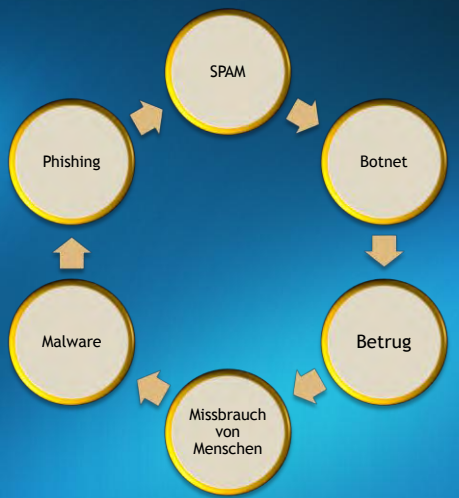
2000–2005

- Hyperjacking
- Peer-to-Peer
- Social-Engineering
- Angriffe auf Anwendungen
- Finanzielle Beweggründe
- Zielgerichtete Attacken
- 64-Bit Windows

2007

Entstehung von Bedrohungen

Online Bedrohungen



Sicherheitsbedrohungen adressieren

Menschen

Unternehmen versteht die Bedeutung von **Sicherheit am Arbeitsplatz**
Personen kennen ihre **Rolle** für die Sicherheitssteuerung und Compliance
IT-Personal verfügt über **Sicherheitskompetenzen** und -wissen, um Ihr Geschäft zu unterstützen

Prozesse

Prozesse für vertrauliche Daten zur effizienten Datenverwaltung
IT-Sicherheitsprozesse zur Implementierung, Verwaltung und Steuerung der Sicherheit
Finanzberichtsprozesse enthalten Angaben zur Unternehmenssicherheit

Technologie

Unterstützt Ihre täglichen Sicherheitsprozesse
Ermöglicht es, Geschäfte erfolgreich abzuwickeln
Hilft dabei, die IT in einen strategischen **Unternehmenswert** zu verwandeln, anstatt als Kostenstelle zu betrachten

Security Development Lifecycle

Sicherheitsstrategien von Microsoft

Netzwerksicherheit

- Sicherer Zugang von überall aus
- Durchgängige Sicherheit mit IPv6 und IPsec
- Zugangssteuerung anhand von Richtlinien anstatt der Topologie
- Zertifikatbasierte Multifaktor-Authentifizierung
- Zustandsprüfung u. Sanierung vor dem Zugang

Richtliniengesteuerte Lösungen für den Netzwerkzugang

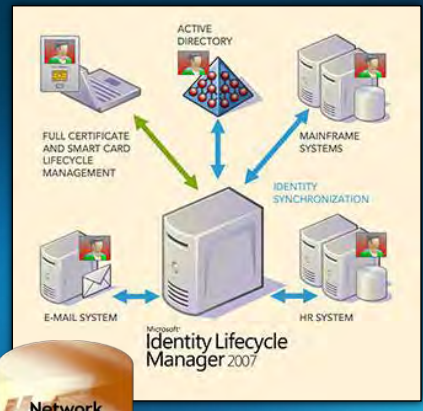
- Windows Firewall mit erw. Filterung
- Server- und Domänenisolation
- Netzwerkzugriffsschutz (NAP)
- ISA Server 2006
- Intelligent Application Gateway (2007)
- Windows Filtering Platform

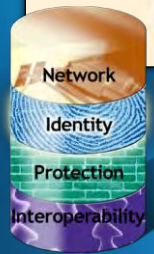
Identitäts- und Zugangssicherheit

- Sichere Collaboration
- Leichte Verwaltung mehrerer Identitäten
- Hardware-unterstützte , geschützte Plattform
- Synchronisation unterschiedl. Verzeichnisse
- Zentralisierte ID-Kontrollen und Verwalt.
- In Anwendungen eingebettete Identität
- Richtlinien steuerung/ Compliance
- Rollenbasierte Berechtigungen
- Privatsphäre für Identität und Daten

Windows Active Directory

Identity Lifecycle Manager





Identity Lifecycle Manager

- Stellt eine integrierte, umfang-reiche Lösung zur Verwaltung des gesamten Lebenszyklus von Benutzeridentitäten sowie der zugehörigen Credentials bereit
  - Identitätssynchronisation
  - Zertifikats- und Kennwort-verwaltung
  - Benutzer-Provisionierung
- IT-Organisationen können Prozesse definieren und automatisieren, die zur Verwaltung von Identitäten (von der Erstellung bis hin zum Ausscheiden) erforderlich sind

Microsoft Forefront Security for Exchange Server

Microsoft Forefront Server Security Management Console

Microsoft Forefront Security for SharePoint

Erweiterter Schutz
Mehrere Scan-Engines auf mehreren Ebenen über die gesamte Infrastruktur des Unternehmens hinweg bieten ein Maximum an Schutz gegen E-Mail- und Collaboration-Bedrohungen

Verfügbar-keit und Kontrolle
Enge Integration mit Microsoft Exchange, Windows-basiertem SMTP, SharePoint und Office Communications Servern maximiert die Verfügbarkeit und Verwaltungskontrolle

Sicherer Inhalt
Stellt sicher, dass Unternehmen unsachgemäße Sprachen sowie gefährliche Dateianhänge aus internen und externen Nachrichten beseitigen können

Interoperabilität

Industriestandards

- Web Services (WS-*)
- Offene Dokumentenformate (XPS)
- OpenID

Partnerprodukte

- Netzwerkzugriffsschutz
- EV-Zertifikatunterstützung im IE7
- Windows CardSpace
- Windows Security Center

Industriepartnerschaften

- SecureIT Alliance
- Microsoft Security Response Alliance
- Interop Vendor Alliance

Interoperabilität des Sicherheits-Stacks

- Integrierte Sicherheit vereinfacht die Bereitstellung einer umfassenden Abwehrarchitektur
- Einsatz offener Standards gestattet plattformübergreifende Integration

Integration von Management-Systemen

Windows Server 2008

Windows Server 2008
Herausforderungen

Windows Server 2008

- **Plattform Verlässlichkeit**
  - Dateisystem und Registry sich Angriffsziele
  - Wenige Schichten zwischen User und Kernel erhöhen die Plattform Verwundbarkeit
  - Server Applikationen sind aufgrund von schwachen Architekturen Risiken ausgesetzt

- **Schutz vor nicht autorisiertem Zugriff**
  - Nicht autorisierte Benutzer können auf das Netzwerk zugreifen
  - Geräte die nicht „compliant“ sind können in das Netzwerk aufgenommen werden und Schäden verursachen
  - Sicherheit für kabellose Netzwerke ist schwer einzurichten und zu managen

- **Datenschutz und Compliance**
  - Nicht autorisierte Benutzung von Daten, Dokumenten und eMails
  - Rechtliche Folgen durch den Verlust von Daten
  - Nachteile im Wettbewerb durch den Verlust von „Intellectual Property“

Windows Server 2008
Verbesserungen

Windows Server 2008

- **Sichere Plattform**
  - Gehärtete Plattform mit reduzierter Anzahl an Schichten
  - Verhinderung von anormaler Aktivität im Dateisystem und Registry
  - Neue Architektur der Plattform um das Kompromittierens des Systems zu minimieren

- **Sichere Zugriffs Kontrolle**
  - Richtlinienüberprüfung, Zustrandskontrolle und Systemaktualisierung auf Basis der definierten Sicherheitsrichtlinien
  - Verbesserung des Managements von mobilen Benutzern und ihren Geräten
  - Segregation von Zugriffsrechten basierend auf der Identität

- **Datenschutz und Compliance**
  - Verringerung des Risikos von Datenverlust durch Zugriffsrechtesteuerung bei Dokumenten und eMails
  - Unterstützung bei der Durchsetzung von Regeln im Netzwerk zur Unterstützung der „Compliance“
  - Verhinderung von Datenabfluss durch verbesserte Security Maßnahmen

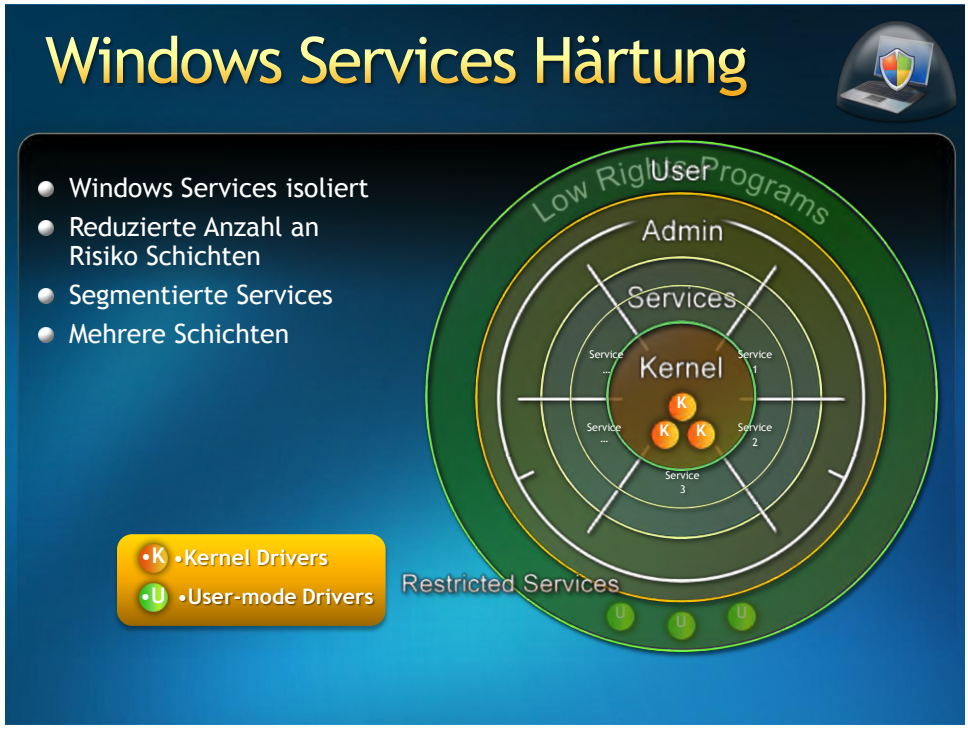
Windows Server 2008
Sicherheits Features

Windows Server 2008

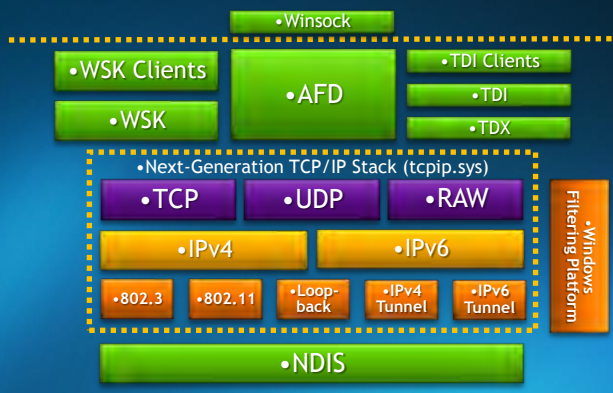
- **Sichere Plattform**
  - Windows Service Hardening
  - Windows Firewall mit Advanced Security
  - Verbesserter TCP/IP Stack

- **Sichere Zugriffs Kontrolle**
  - Network Access Protection
  - Server and Domain Isolation
  - Active Directory Federation Services

- **Datenschutz und Compliance**
  - BitLocker
  - Active Directory Rights Management Service
  - Verbesserter Auditing Infrastruktur



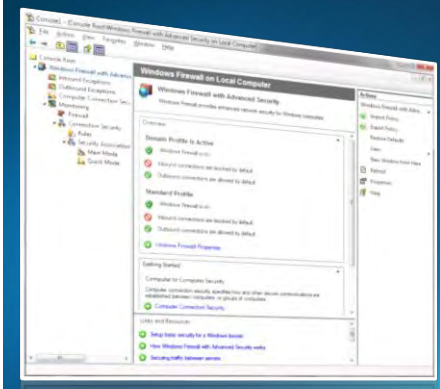
Weiterentwicklung des Server TCP/IP



•Next Generation Networking Highlights

- Neue dual-IP Layer Architektur für nativen IPv4 und IPv6 Support
- Erweiterte IPsec Integration
- Verbesserte Performance durch Hardwarebeschleunigung
- Neuer Netzwerk auto-tuning und Optimierungs Algorithms
- Verbesserung der Erweiterbarkeit durch mächtige APIs

Neue Windows Firewall



- Inbound und Outbound Filtering
- Neue Management Console
- Integrierte Firewall und IPsec Richtlinien
- Regel Konfiguration basieren auf Active Directory Gruppen und Benutzern
- Unterstützung für IPv4 u. IPv6
- Erweiterte Regel Optionen
- “by Default” an

Read-Only Domain Controller

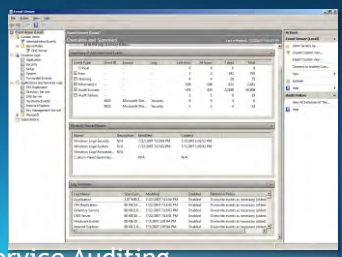
Features
- Read Only Active Directory
- Nur selektierte Kennworte sind im RODC gespeichert
- Unidirektionale Replication
- Rollen Separierung

Vorteile
- Verbesserte Sicherheit für entfernte Domain Controllers

Unterstützt
- ADFS,DNS, DHCP, FRS V1, DFSR (FRS V2), Group Policy, IAS/VPN, DFS, SMS, ADSI queries, MOM

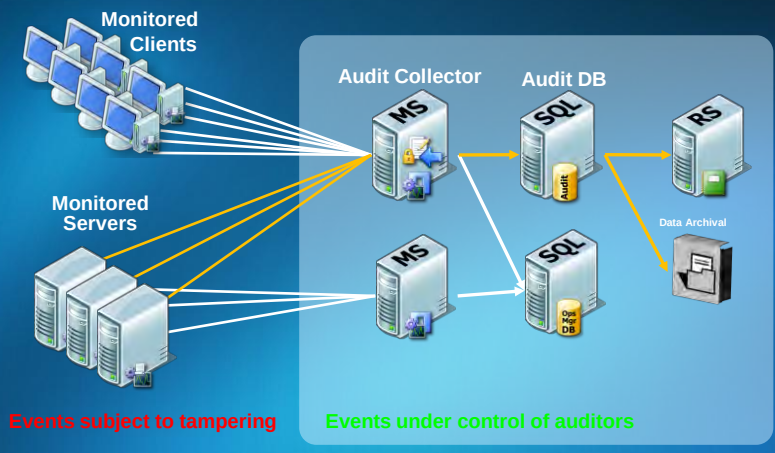
Windows Eventing 6.0

- Neues Auditing Subsystem in Windows Server 2008
  - 95% der Windows Server 2008 Features ist auch in Windows Vista
- Bestandteile
  - Erweiterter Event Erklärungstext
  - XML Event Format
  - Zugriff auch über WS-Management
  - Granular Audit Policy (GAP) mit vielen Untergruppen (AuditPol)
  - Verbesserte Scalieriung
  - Event Triggering
  - Verbessertes Registry und Directory Service Auditing
  - Event Subscriptions



Audit Collection

Überwachung von Clients und Servern auf Security relevante Ereignisse, mit forensischer Analyse und IDS System, im Backend sorgen für ein hohes Maß an Sicherheit und Transparenz



Zusammenfassung

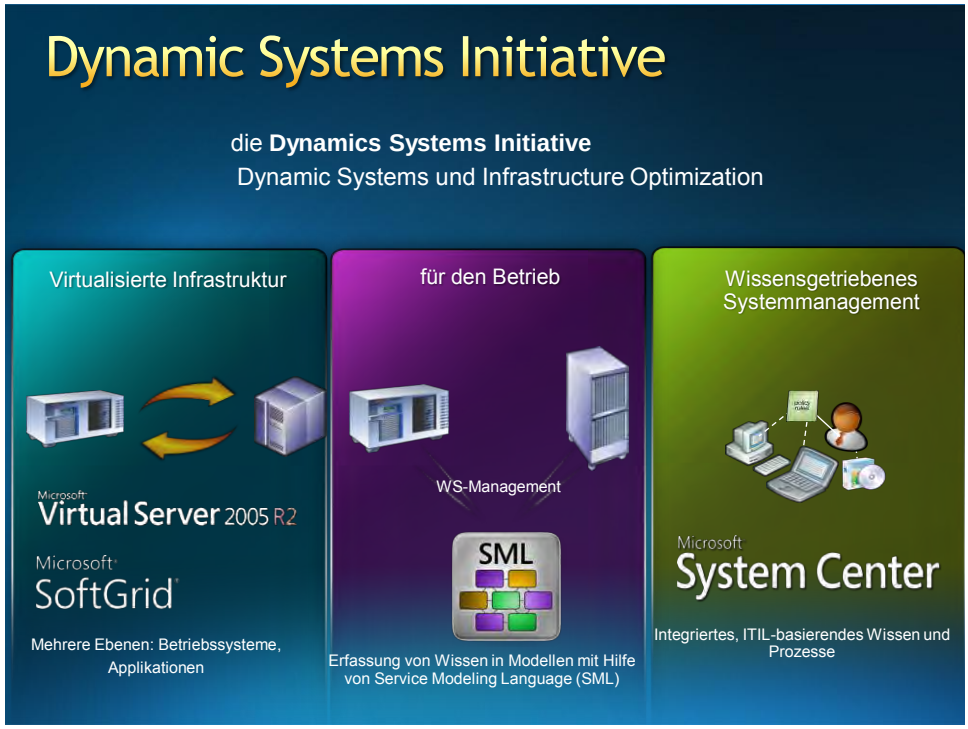
Windows Server 2008

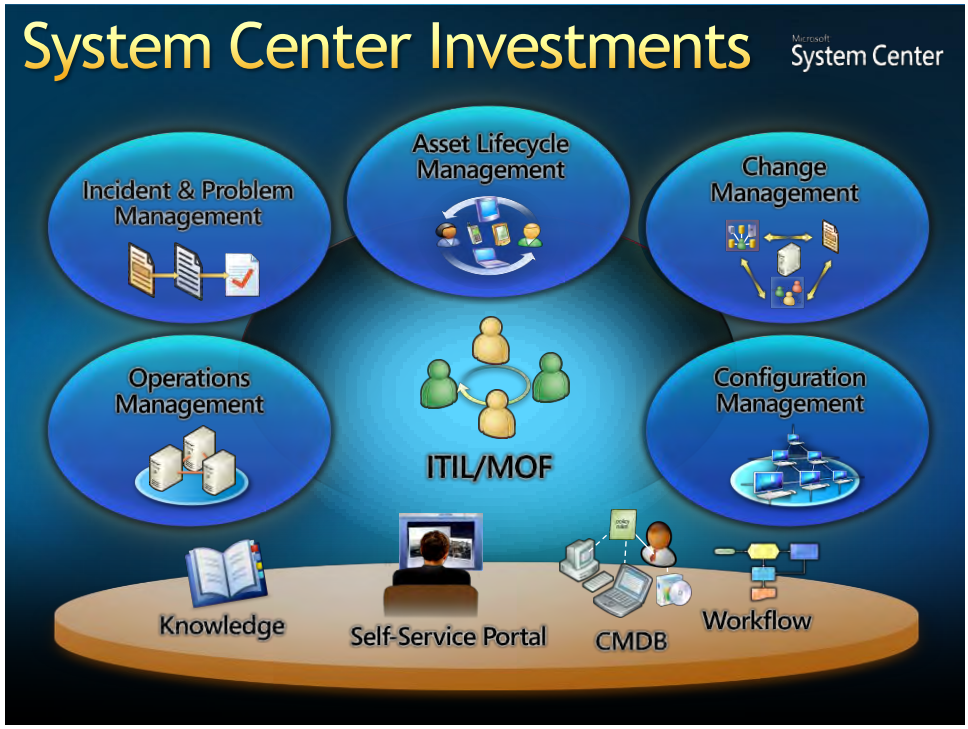
- Windows 2008 ist das bislang sicherste MS Betriebssystem
  - Netzwerkzugriffsschutz (Network Access Protection, NAP)
  - Microsoft BitLocker
  - Reduktion der Kernel Angriffsfläche
  - Read-Only Domain Controller (RODC)
  - Failover-Clustering
  - Server Manager - Server Core: DHCP-, DNS-, Datei- oder Webserver, Domänencontroller oder Windows Server Virtualization
  - Windows PowerShell
  - Windows Deployment Services (WDS)
  - Erweiterte Gruppenrichtlinien
  - Neuen Authentifizierungsarchitektur
  - Richtliniengesteuertes Netzwerk
  - Federated Rights Management
  - Verbessertes Auditing
  - Secure startup
  - Public Key Infrastructure (PKI) Erweiterungen
  - Neue bi-directionale Windows Firewall
  - Next-generation Kryptography Unterstützung
  - Windows Server TCP/IP.

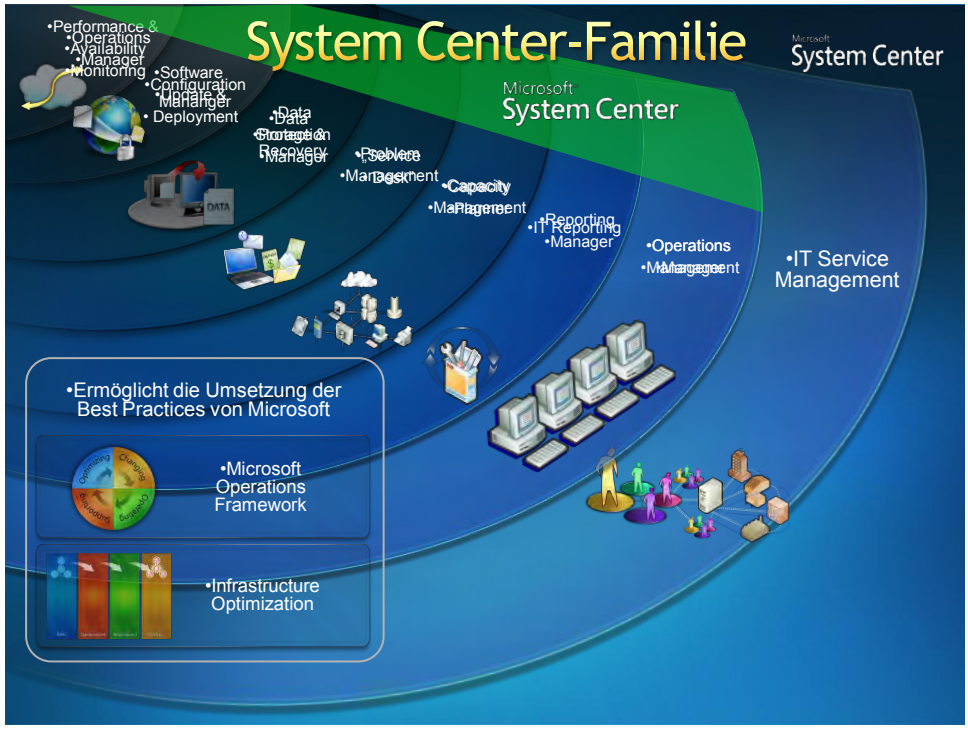
Server-Sicherheitsfortschritt

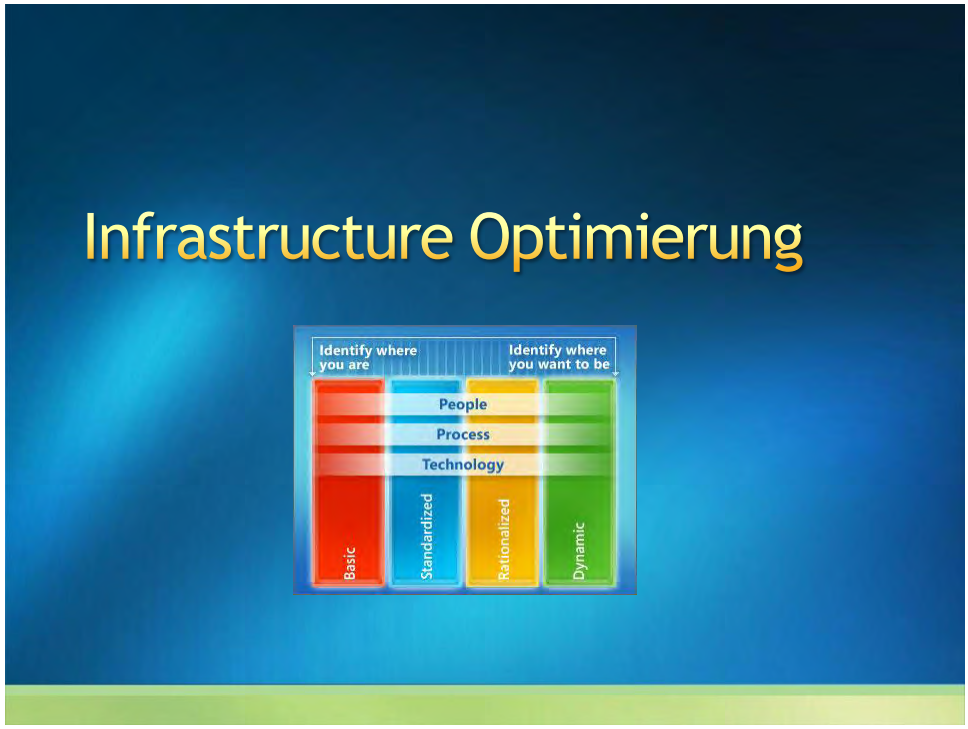
	Office	Exchange Server 2007	SQL Server 2005
Sichere Plattform	• Trust Center • Neues Modell zur Dokumentensicherheit • Open XML-Dateiformate	• Erweiterte Spam- und Virenabwehr • Compliance • Geschäftskontinuität	• Tool zur Konfiguration der Angriffsfläche • Durchsetzung von kennwortrrichtlinien; granulare Rollen • Eingebaute Verschlüsselung; Schlüsselverwaltung. • Auditing - Data Definition Language (DDL)
Schutz von Daten	• Dokumenten-Inspektor • Information Rights Management • Strenge Verschlüsselung, digitale Signaturen	• Grundlegende Sicherheitsverwaltung und Verwaltung mobiler Geräte • Eingebauter Schutz mit Geschäftskontinuität • Compliance-Unterstützung • Erweiterte Filterung von Nachrichten	• Reichhaltige Authentifizierung • Granulare Zugangskontrolle • Compliance und Überwachung • Hierarchische Verschlüsselung

Dynamic Systems Initiative





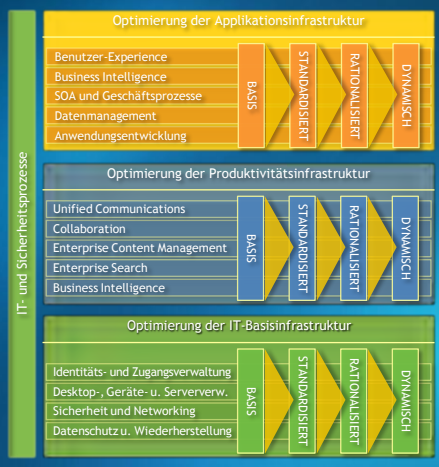




Infrastrukturoptimierung

Ein People-Ready Business schaffen

Modellbasierter Ansatz



- Stellt … Frame… bereit, das Ihne… hil… opti…rte In… a… n (…t Mi… z…
- Ve… em… W… für … we… Imple… ung
- Förde… Ko… nred… Sicher…it u… Eff… …hse
- Schaff… Agilität

Optimierung der IT-Basisinfrastruktur

Richtlinien und Compliance
Risikobewertung
Benutzeraufmerksamkeit

Basis	Standardisiert	Rationalisiert	Dynamisch
Identitäts- und Zugangsverwaltung			
Patch-Management			
Bedrohungs- und Schwachstellen-Milderung			
Sichere(s) Messaging und Collaboration			
Sichere Anwendungsarchitektur			
Migration älterer Plattformen			

Optimierung der IT-Basisinfrastruktur: Sicherheit

	Basis	Standardisiert	Rationalisiert	Dynamisch
Menschen	• IT-Personal wird nach operativen Herausforderungen eingestuft • Benutzer schaffen sich ihre eigenen IT-Lösungen	• IT-Mitarbeiter für empfohlene Vorgehensweisen wie MOF, ITIL etc. geschult • Benutzer erwarten Basisunterstützung von der IT	• IT-Personal verwaltet effizient kontrollt. Umgebung • Benutzer verfügen über die richtige Werkzeuge, Ve barkeit und zu Informa	• IT ist ein trachten ertvollen neue itiativen
Prozesse	• Keine IT-Prozesse definiert • Komplexität wg. ortsgebundener Prozesse, und nur minimale zentrale Kontrolle	• Zentrale Sicherheitsverwaltung u. -konfiguration • Standard-Arbeitsplatz-Images definiert, nur teilw. adaptie	• SLAs Ge te wandte herheit, empf. Vorgehensweisen	• Selbsteinschätzung und fortlaufende Verbesserung • Leichter, sicherer Zugriff auf Inform. Über das Internet von überall aus
Technologie	• Patch-Status von Arbeitsplatz-PCs ist unbekannt • Kein einheitliches Verzeichnis fü die Zug verwaltung	• Mehr Ve se zur fizierung grenzte automatisierte Software-verteilung	• Identitäts- und Zugangs-verwaltung ist automatisiert • Systemverwaltung ist automatisiert	• Selbst-Provisionierung und quarantäne-fähige Systeme stellen die Compliance und Hochverfügbarkeit sicher

IT-Reifegrad und ROI verbessern

Windows CardSpace

- Verwaltung der Digitalen Identitäten
- Authentifizierung gegenüber Web-Sites und Web-Services

Leichter

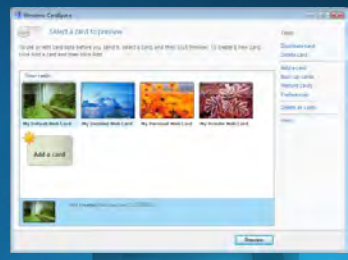
- Kein Username und Passwort
- Konsistentes Login und Registrierung

Sicherer

- Verhindert Phishing
- Multi-Factor Autentifizierung

Built on WS- Web Service Protocols*

Login mit der Managed Card



•Identity Provider

•Relying Party (website)

Auswahl der Managed Card

•User

•Identity Provider

•Relying Party (website)