Improving Security

Neue Initiativen und mehr Sicherheit von Microsoft

Wojciech Micka
Presales Consultant Microsoft Deutschland GmbH

Microsoft

Agenda

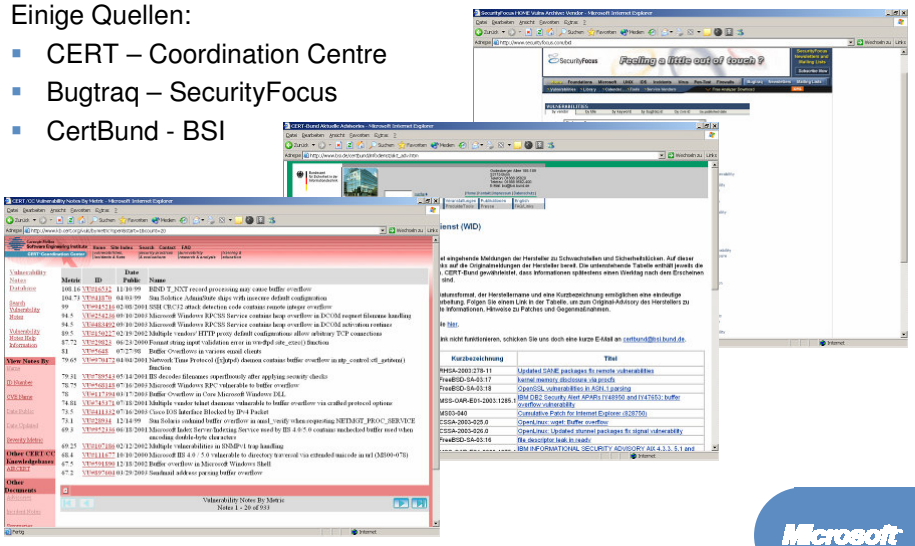
- Sicherheitskrise und Ursachen
- Unsere Kommunikation zu Vulnerabilities, Patches, Bulletins
- Microsofts Sicherheits-Initiative
- Ergebnisse von Trustworthy Computing bis heute
- Roadmap und Resümee
- Windows Rights Management Services

Microsoft

Sicherheitskrise in der Software-Branche

Einige Quellen:

- CERT – Coordination Centre
- Bugtraq – SecurityFocus
- CertBund - BSI



Folie 3

Wie Microsoft Sicherheitsanfälligkeiten kommuniziert

- Sicherheitsanfälligkeit (security vulnerability) in Software
  - Eine Sicherheitsanfälligkeit ist ein Defekt im Produkt, der trotz korrekter Nutzung des Produktes dazu führt, dass ein Angreifer Privilegien auf dem System (Computer) des Benutzers erlangen könnte, die seinen Missbrauch möglich machen. Missbrauch kann bedeuten:
    - Daten zu kompromittieren
    - Das System zu zweckentfremden
    - Vertrauensstellungen des Benutzers zu übernehmen
- Komplette Definition „security vulnerability“ in Englisch
  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/vulnrbl.asp
- Veröffentlichung von Sicherheitsanfälligkeiten
  - Microsoft gibt Sicherheitsanfälligkeiten in Software **nach** Verfügbarkeit eines entsprechenden Patches preis, um Kunden zu schützen

Folie 5

Patches und Sicherheits-Bulletins bei Microsoft

- Patches beheben gefundene Sicherheitsanfälligkeiten und werden von Microsoft in **Sicherheits-Bulletins** veröffentlicht:
  - *Deutsch*: http://www.microsoft.com/germany/ms/technetservicedesk/bulletin/
  - *Englisch*: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp
- Sicherheitsanfälligkeiten werden von Microsoft in 4 **Schweregrade** eingeteilt: Kritisch, Hoch, Mittel, Niedrig
  - *Deutsch*: http://www.microsoft.com/germany/security
  - *Englisch*: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/revsbwp.asp
- **Herausgabe-Richtlinie für Bulletins** bei Microsoft (neu seit 10/2003)
  - *Deutsch*: http://www.microsoft.com/germany/security
  - *Englisch*: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/revsbwp.asp

Folie 6

Situation

Patches im Software-Lebenszyklus

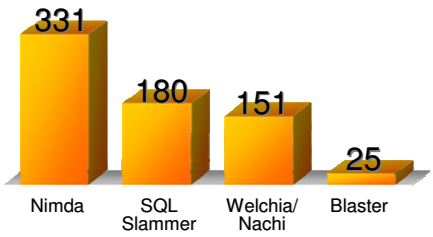
Wieviel Angriffe gibt es, die diese Lücke ausnutzen?

Produkt kommt auf den Markt	Sicherheitslücke entdeckt	Komponente Modifiziert bzw. gefixt	Patch wird herausge-geben	Patch wird bei Kunden eingespielt

Folie 8

Verstärkung der Sicherheitskrise

Zeitraum in Tagen zwischen Patchverfügbarkeit Und Angriff auf die Sicherheitslüscke



- Tage zwischen Patch und Exploit
  - Heute ist ein Patch im Durchschnitt nach 9 Tagen entziffert (Reverse Engineering)
  - Die Spanne wird immer kürzer und Kunden bleibt kaum noch Zeit zum Patchen
  - Ansatz Patchmanagement reicht nicht alleine

Folie 9

Neue Sicherheits-Initiative: Zeitrahmen

Kurzfristig	„People and Process“ - → Kostenlose KnowHow-Vermittlung zu Sicherheitskonzepten, Patchmanagement, u.a.m. – Fester Patch-Herausgabe-Zeitplan
Mittelfristig	„Technology“→ Schutztechnologien für mehr Resistenz gegen Angriffe, auch wenn Computer ungepatcht ist
Langfristig/ parallel	Kontinuierliche Verbesserung der Qualität in unserer Software und neue Technologien wie Next Generation Secure Computing Base

Folie 10

Hauptmaßnahmen der Sicherheitsinitiative

Kunden-Feedback	*Microsofts Antwort*
“Einfacheres Patching”	Neuer verbindlicher Zeitplan und vereinheitlichte Patchtechnologie
“Sicherer Betrieb”	Leitfäden und Trainings
“Prophylaxe, OS-Härtung”	Schutztechnik auch wenn ungepatcht
“Bessere Qualität”	Voller Fokus auf neue Qualität

Folie 11

Neuer Zeitplan für Patches

- Sicherheits-Patches jetzt ***monatlich***
  - Jeder 2. Dienstag im Monat: Microsoft Patchpaket
  - Bessere Test- und Deployment Planung möglich
  - Option: Patches als ein Gesamtpaket oder nur einzelne Patches
- Notfall-Patches (Exploit aufgetaucht)
  - Sofortige Bereitstellung des Patches
- Verlängerter Sicherheits-Support bis Ende Juni 2004 für
  - Windows NT4 Workstation SP6a

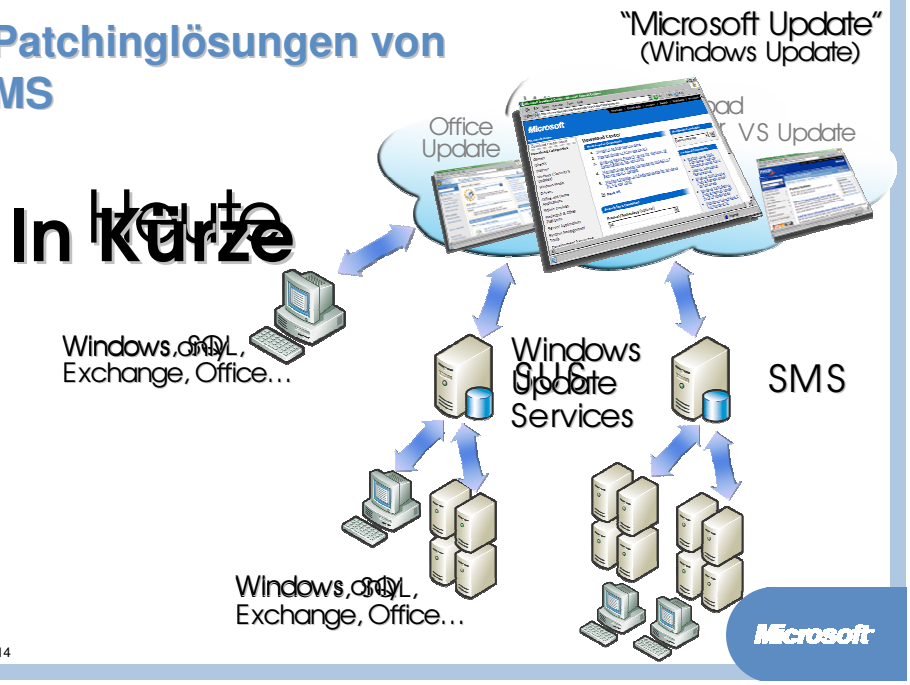
Folie 12

Patching vereinfachen

Patch Komplexität reduzieren	**Bis Mai 2004: Nur noch 2 Patch Installer. Alle Patches verhalten sich gleich und sind gleich zu installieren (SUS 2.0, MSI 3.0)**
Patch-Risiko minimieren	**Bis Mai 2004: Durchgängige Patch-Rollback- Fähigkeit für Windows, SQL, Exchange, Office**
Patch Grösse reduzieren	**Bis Mai 2004: 80% Reduktion der Grösse. (Delta patching Technologie, Optimierungen in MSI 3.0)**
Downtime reduzieren	**Bis Mai 2004: 30% weniger Reboots bei Win 2003 (mit SP1). Bis 70% Reduktion bei nächster Server-Generation**
Patch Automation für alle Produkte	**Bis Ende 2004: Alle Patches auf *"MS Update". 11/2003:* SMS 2003 kann alle Patches für aktuelle MS Apps verteilen**

Folie 13

Patchinglösungen von MS



Folie 14

SUS 2.0 Patchmanagement

- Unterstützung für zusätzliche MS Produkte
  - Office 2003, SQL Server 2000, Exchange 2000
  - zusätzliche Unterstützung weiterer Produkte
- Administrative Kontrolle
  - Möglichkeit der automatischen Deinstallation
  - Anpassung der Client Abfrageintervalle
  - Festlegen des Zeitpunktes bis Installation ausgeführt werden muss
  - Zusätzliche Regeln für automatische Installation

Folie 15

SUS 2.0 Patchmanagement

- Ausrollen & Zielbestimmung
  - Angepasste Synchronisation mit WU
    - z.B. alle WinXP Patches, aber keine Win2K Inhalte
  - Automatische Aktualisierung des SUS Clients
- Statusprüfung der installierten Updates
- Verbessertes Reporting
  - GUI Report-Tool sammelt den Aktualisierunsstatus per Computer-Group oder per Update

Folie 16

Leitfäden und Trainings

- **Globales Trainings-Programm**
  - 2 Tage TechNet Sicherheits-Seminare
  - Sicherheits-Webcast Serien
  - Developer Security Trainings
- **Neue Leitfäden**
  - Patterns and practices
  - How-Tos für sichere Konfiguration
  - How Microsoft Secures Microsoft
- **Security Guidance Center**
  - Patterns und Best Pratice

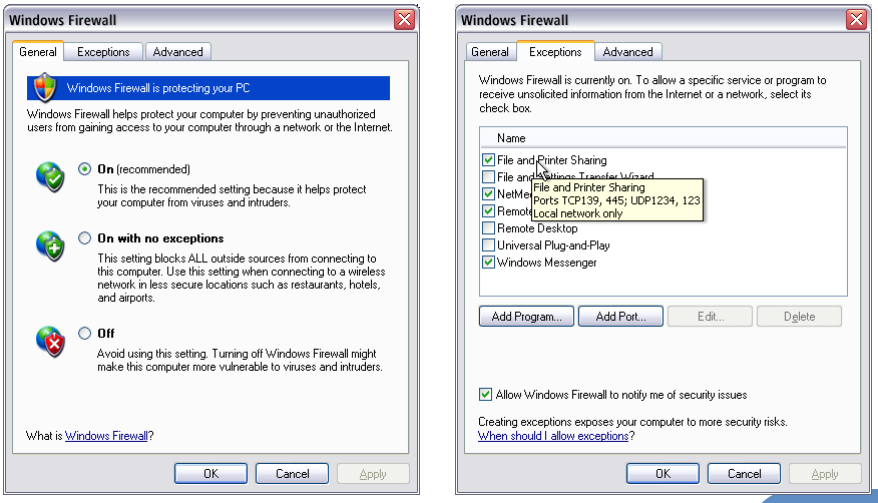
Folie 17

Windows XP SP2 - Reduktion der Angriffsfläche

- Netzwerkschutz
- Sichere Email und IM
- Sicheres Browsen
- Schutz vor Buffer Overruns

Folie 18

Vorschau: Windows XP SP2



Folie 19

Neue Schutztechnologien in Windows XP SP2

- Stark verbesserte, neue “Windows Firewall”
  - Neuer „Shielded-Mode“
  - Standardmäßig aktiviert
  - Sicherheit während des Startvorganges
  - Alternativ Dateinamen anstelle von Ports
- Email, IM und Browsing sicherer
  - Kontrolle über ActiveX®-Steuerelementen und Spyware
  - Pop-Up Manager
  - Umfassendere Outlook Express Security
- Execution Protection (NX)
  - Verbesserter Schutz gegen Buffer Overflows
  - Trennt Anwendungscode von Datenseiten in der CPU
- RPC Schnittstelleneinschränkungen
  - Anonymer Zugriff weitestgehend eingeschränkt
- Verfügbar: H1 2004

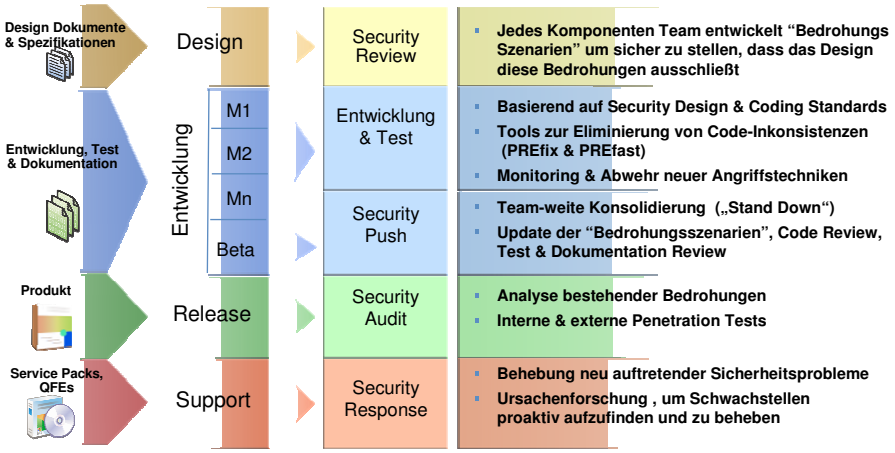
Folie 20

Windows Server 2003 SP 1

- Rollen-basierte Sicherheitskonfiguration
- RAS Client Inspection (Quarantäne Technologie)
- Locale Inspection bei Verbindungsaufbau im LAN
- Group Policy Unterstützung für WPA
- RTM ~ Q4 2004

Folie 21

Neue und bessere Qualität durch Trustworthy Computing: Software Release Prozess



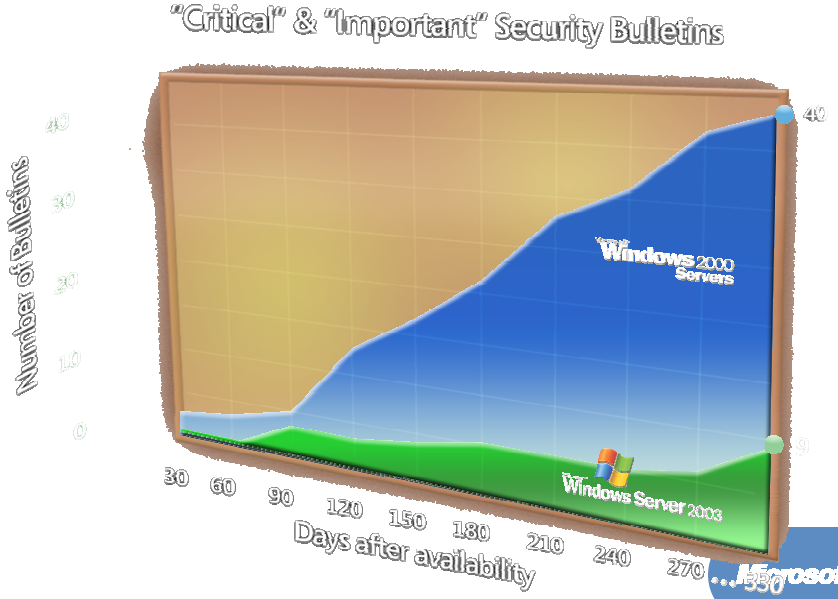
Folie 22

Produkte im TwC Release Prozess

.NET Framework (for 2002 & 2003)
ASP.NET (for 2002 & 2003)
Biztalk Server 2002 SP1
Commerce Server 2000 SP4
Commerce Server 2002 SP1
Content Management Server 2002
Exchange Server 2003
Host Integration Server 2002
Identity Integration Server 2003
Live Communications Server 2003
MapPoint.NET
Office 2003
Rights Mgmt Client & Server 1.0
Services For Unix 3.0
SQL Server 2000 SP3
Visual Studio .NET 2002
Visual Studio .NET 2003
Virtual PC
Virtual Server
Windows CE (Magneto)
Windows Server 2003
Windows Server 2003 ADAM

Microsoft

Höhere Qualität in Windows Server 2003

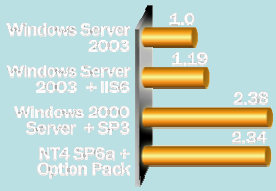


Microsoft

Trustworthy Computing: Konkret

Intensiv Security Trainings

Halbierung der Angriffsfläche



Leitfäden & Best Practices

msdn Microsoft TechNet

Windows Server 2003 | Microsoft Official Curriculum

patterns & practices

www.microsoft.com/practices/

SANS Institute – 2003 Information Security Leadership Awards:

- Führend in der Automatisierung von Updates
- Führend in Security Trainings für Software Entwickler
- Führend in Softwaretests für Sicherheitsschwachstellen

http://www.sans.org/press/isla.php

Folie 25

Trustworthy Computing: Konkret

- Microsoft hat sich Common Criteria Zertifizierungen verpflichtet
- Windows 2000 Zertifizierung abgeschlossen
  Windows 2000 Desktop und Server Konfigurationen
  - Active Directory, VPN, Single Sign-on, EFS, IPSEC u.a. mit evaluiert

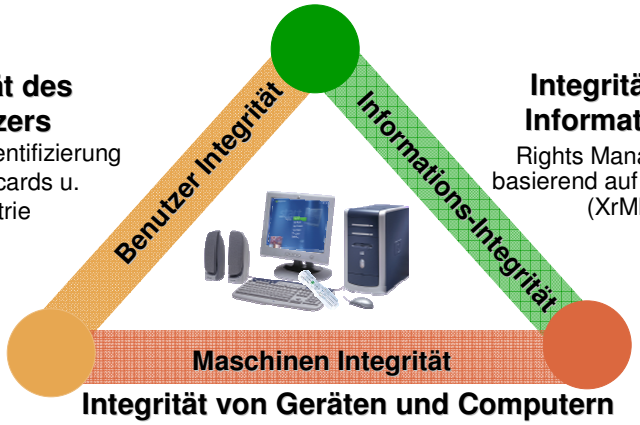
  Link: http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/cccert.asp
- Firewall ISA Server Zertifizierung abgeschlossen
  - Zertifiziert beim BSI in Deutschland
  - „Deutsches IT Sicherheits-Zertifikat“

  Link: http://www.bsi.bund.de/zertifiz/zert/reporte/0218a.pdf
- Weitere Produkte in Evaluierung: Windows XP, Windows Server 2003, Exchange Server 2003

Folie 26

Langfristige Verpflichtung für optimale Sicherheit

Integrität des Benutzers
Windows Authentifizierung inkl. Smartcards u. Biometrie



Integrität von Informationen
Rights Management basierend auf Standards (XrML)

Integrität von Geräten und Computern
Next Generation Secure Computing Base

Folie 27

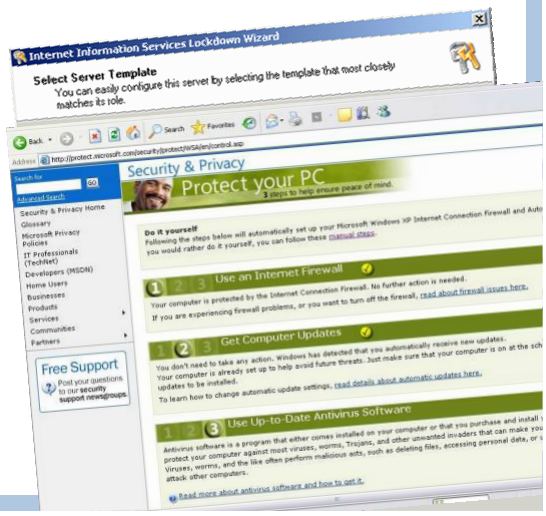
Schutztechnologien in MS Systemen

Netzwerk-sicherheit	IPSec Integration in Windows SSL, RPC over HTTP ISA Server 2004
Sicheres WLAN	Tiefgreifende Integration in Windows WPA, 802.1x, PEAP
Authentifizierung	Single sign-on, Smartcards MS Identity Integration Server
Daten-sicherheit	Rights Management Services Umfassende Autorisations-infrastruktur (AD, EFS, ACLs…)

Folie 28

Security Tools

- Microsoft Baseline Security Analyzer 1.2
- Security Bulletin Search Tool
- URLscan
- IIS Lockdown
- Blaster Cleaner auf Windows Update
- PYPC AutoKonfig



Folie 29

Community Engagement

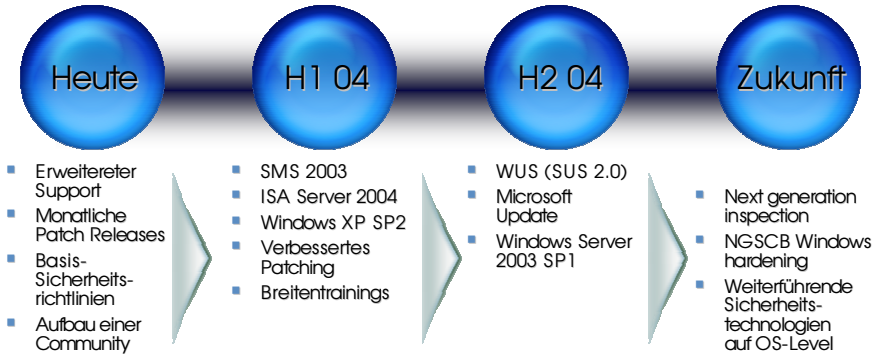
- Newsletter
- ITPro Security Zone
- Webcasts & Chats
  - Executive Updates
  - Security Bulletin
  - Technet/Msdn Security
- Security MVP Programm

Folie 30

Guidance And Training

- Security Developer's Center
- Security Guidance Center
  - How-to Articles, Checklists, Modules
- Microsoft Security E-Learning Clinics
- Security Hardening Guides
- Security Guidance Kit
- MCSA: Security und MCSE: Security Certifications

Security Roadmap



Entwicklung der Firewall-Technologien

- Was bedeutet heutzutage TCP Port 80?
  - Laut *iana.org* : „Hypertext Transfer Protokoll“
  - In der Realität : „Universal Firewall Bypass Protokoll“
    - Viele Unternehmen haben „Port 80“ an ihrer Firewall geöffnet
    - Viele Anwendungen tunneln ihre Daten über Port 80/HTTP
- Wie kann man dann die Protokollintegrität sicherstellen?
  - Einsatz von Application-Layer-Filtering (ALF)
    - Umsetzung als protokollspezifischer Proxy-Server
    - Umsetzung als transparente Datenstromfilter

Microsoft

ALF Funktionalitäten (Beispiel HTTP)

- Filterung anhand von Informationen wie…
  - Hostheader → gibt Auskunft über das Ziel
  - Dateiendung → gibt Auskunft über den Datentyp
  - Benutzerkennung, User-Agent, Mime-Type
  - Protokollspezifische Befehle
    - `PUT, DELETE, MOVE, OPTIONS, PROPFIND, POLL, …`
- Filterung von bekannten Angriffssignaturen
  - URL Encoding Probleme und Folder Traversal Bugs
    - `/scripts/..%255c../winnt/system32/cmd.exe?/c+…`
  - Buffer Overruns in eingesetzten Webserver
    - `/default.ida?xxxxxxxxx…xxxxxxxxx+SHELLCODE`

Microsoft

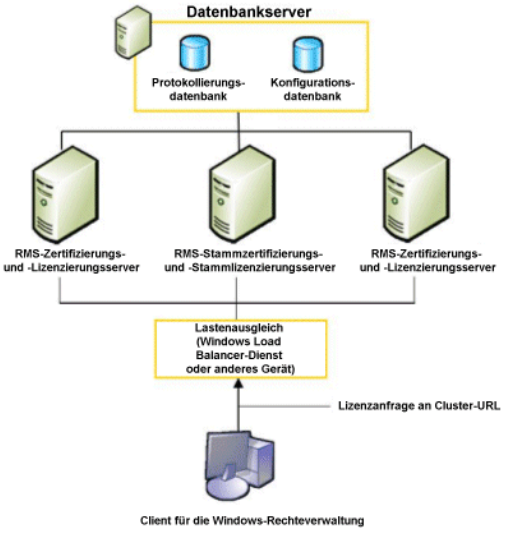
ISA Server 2004

- Künftige Firewall, VPN und Cache Lösung
  - Status: RC1
- Stateful- und Application-Layer-Filterung
  - ALF: HTTP, SMTP, FTP, DNS, POP3, RPC, H.323
  - Deep Content Inspection
- Erweitert VPN Dienst von Windows Server
  - VPN- und Quarantänenetzwerke
  - Statefull Inspection für VPN
- Multi-Networking Support
- Verbesserte GUI

Windows Rights Management Services

- Ermöglichen die Vergabe von unterschiedlichen Zugriffsrechten an Benutzer
- Basiert auf RMS Dienst
  - Webservices für Verwaltung und Clientinteraktion (IIS 6.0)
    - XrML für die Rechteverwaltung
  - Datenbank für Konfigurationsdaten (SQL oder MSDE)
  - Active Directory für Authentifizierung
- Information Rights Management schützt die Daten auf dem Desktop
  - Typische IRM Anwendungen: Email und Dokumente
  - IRM fähige Anwendung: Office 2003
  - Internet Explorer Add-on verfügbar

Rights Management Service - Infrastruktur



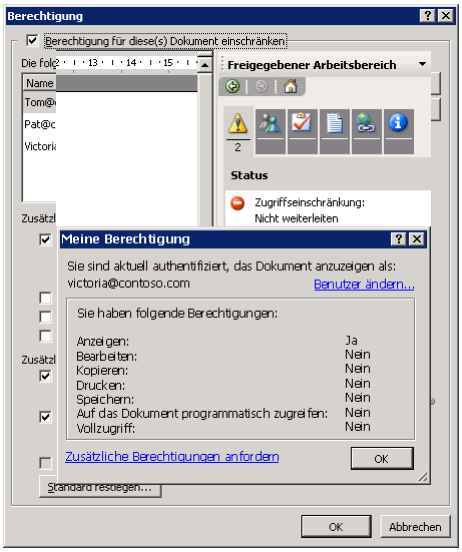
Folie 37

Rights Management Services - Technik

- RMS geschützte Daten sind immer verschlüsselt
  - 56 Bit DES oder 128 Bit AES
- Benutzerautorisierung Zertifikatsgesteuert
  - Signatur/Verschlüsselung mit RSA basierten Schlüsseln (1024 Bit)
- Client / Server Kommunikation ist immer geschützt
  - SSL

Folie 38

Rights Management Services – IRM Client



Folie 39

Die richtigen Schritte zu effizienter Sicherheit

- Durchführung eines Sicherheits-Assessment (Schutzbedarfs-Analyse)
- Erstellung eines Planes für Sicherheitmaßnahmen
- Einführen einer effizienten Patch Management Strategie
- Absicherung des Zugriffes auf das Netzwerk
- Absichern und Härten von Workstation und Servern

Folie 40

Weiterführende Informationen

- **Windows Rights Management Services**
  http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx

Folie 41

Vielen Dank
für Ihre Aufmerksamkeit!

Folie 42