

Was tut Microsoft im Bereich Security?

Martin Saalfeld
Senior Presales Consultant

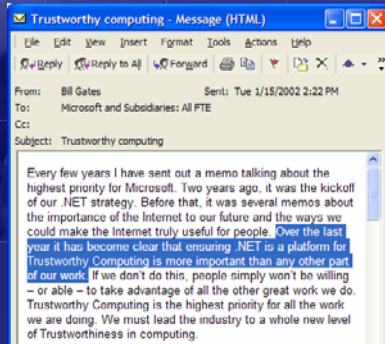
Microsoft

Agenda

- **Trustworthy Computing**
- Einflußbereich
- Security Herausforderungen
- Summary

Trustworthy Computing:

“To do everything possible to make certain that every customer can work, communicate, and transact securely over the Internet.”



Vision

Trustworthy Computing

Security

Privacy

Reliability

Business Integrity

Agenda

- Trustworthy Computing
- **Einflußbereich**
- Security Herausforderungen
- Summary

Einflussbereich

bestehende Plattform und Produkte

- Windows 2000/ XP /Server 2003 Familie
- .Net Enterprise Server Familie
- ISA – Internet Security & Acceleration Server
- SMS, MOM

Tools und Services

- Security Toolkit
- Software Update Service
- Security Notification Service

Design/ Entwicklung/ Response

bestehende Plattform und Produkte

Office XP

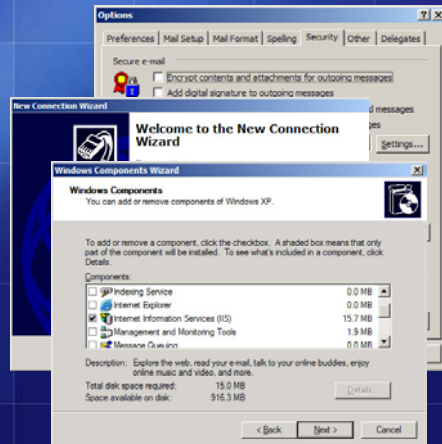
- .exe Ausführung, Script Zugriff begrenzen

Windows XP

- Internet Connection Firewall
- Software Restriction Policies

Reduzieren der Angriffsfläche

- Windows Server 2003, IIS6
- IIS5.x Lockdown
- ISA



Tools und Services

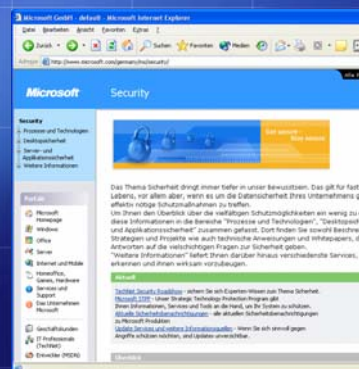
STPP - Get Secure

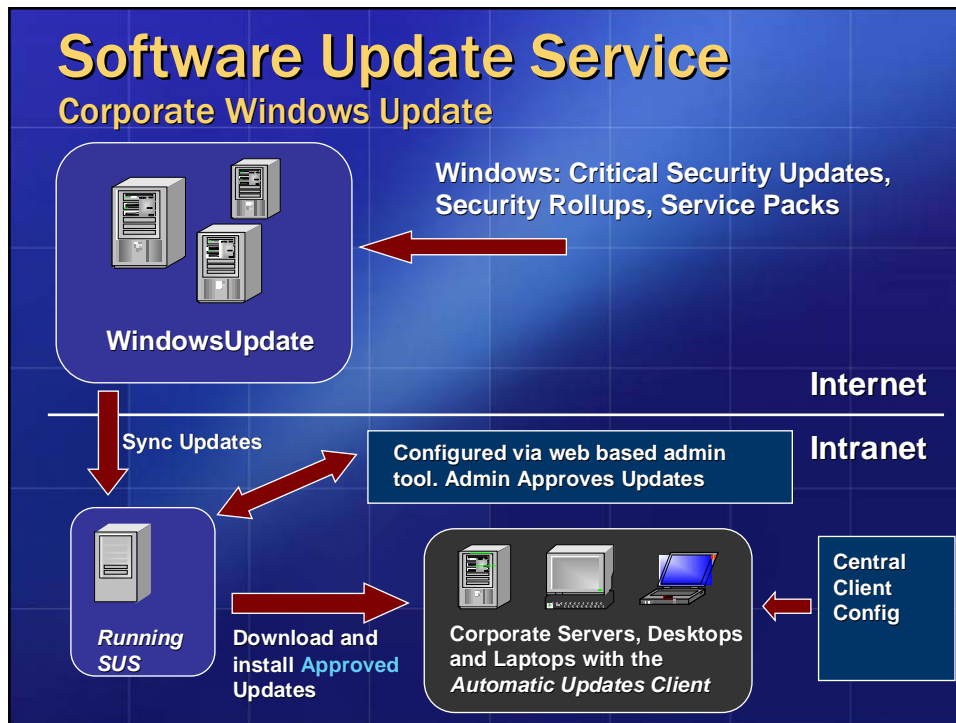
- Microsoft Security Toolkit
- Microsoft Baseline Security Analyzer
- Security Assessment Program

STPP - Stay Secure

- Microsoft Security Response Center
- Software Update Service
- Security Notification Service
- Windows Update

kostenloser Support für Security Themen





Design/ Entwicklung/ Response

Externer Security Review

Common Criteria Zertifizierung von Windows 2000

FIPS 140-1 Bewertung des Cryptographic Service Provider (CSP)

Source Code bereitgestellt an mehr als 80 Universitäten, Labs und Regierungseinrichtungen

Design/ Entwicklung/ Response **Interner Security Review**

Einsatz neuer Tools und Compiler bei der Entwicklung

Training für Entwickler, Tester, Produktmanager (8 Wochen im März 2002)

Verdreifachung des R&D Budget im Bereich Security

Einbindung des internen ITG KnowHows in die Entwicklung - FaceIT

Design/ Entwicklung/ Response **Microsoft Security Response Center**

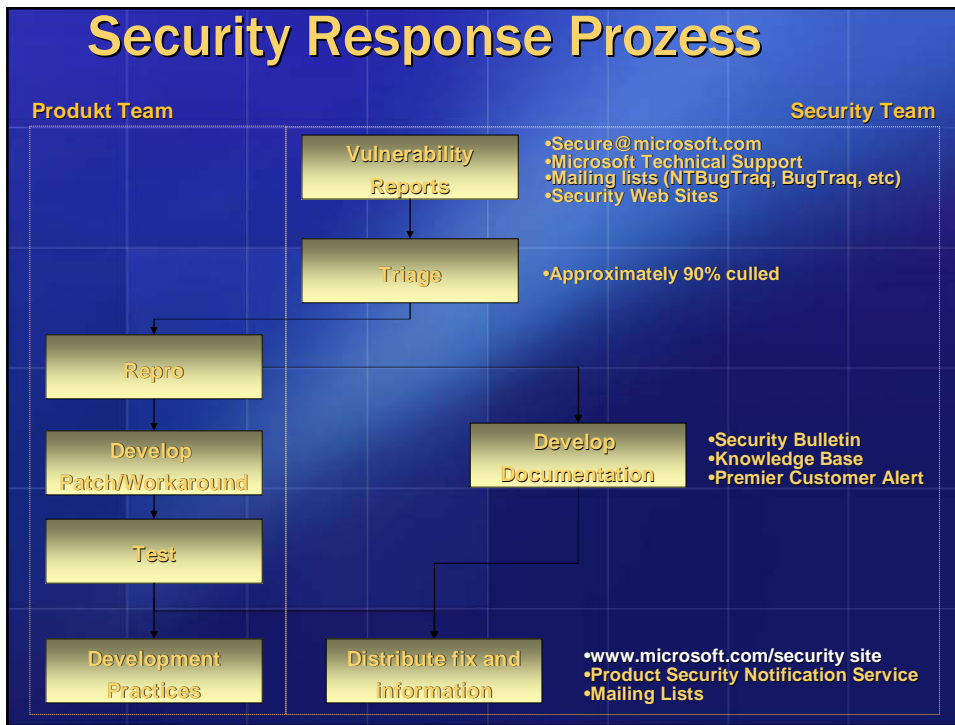
Arbeitet mit den Security relevanten Stellen

- Reaktion auf jeden eingehenden Report 7x24
- Schnittstelle zu den Produktgruppen
- Erstellen von Bulletins und Webveröffentlichung von Patches oder Workarounds

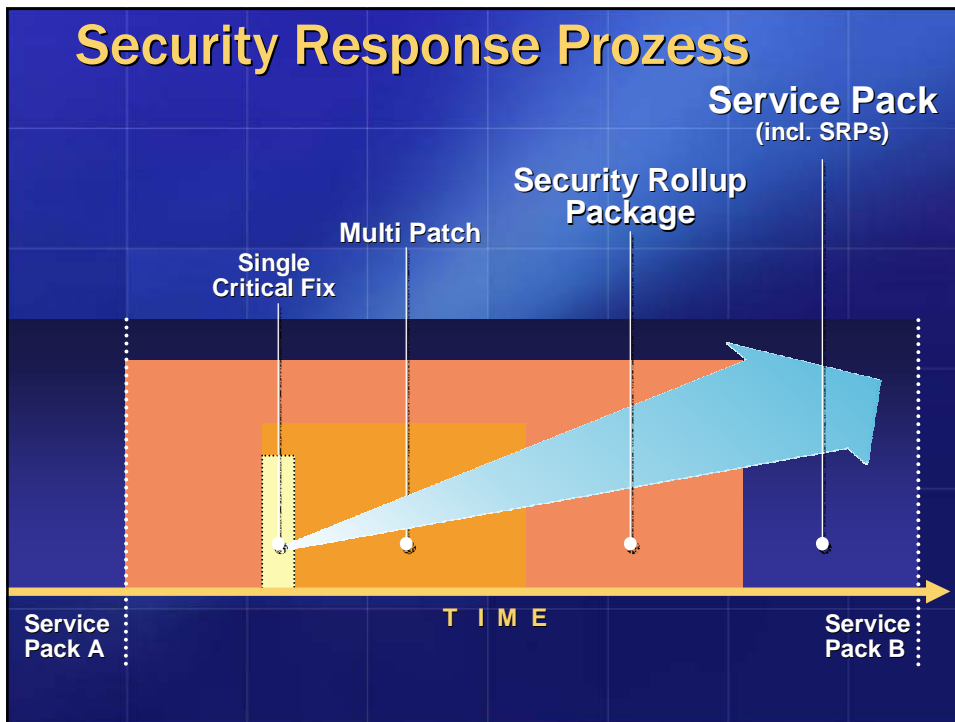
Sichert die breite Information

- Email Liste
- Proaktive Benachrichtigung
- Key Priorität "getting patches to more customers"

Security Response Prozess



Security Response Prozess



Agenda

- Trustworthy Computing
- Einflußbereich
- **Security Herausforderungen**
- Summary

Security Herausforderungen

Angebot an
Sicherheitsfunktionen
Reduzierung möglicher
Fehler durch Design und
Entwicklung
Neue Technologische
Möglichkeiten

Bewertung und Anwendung
der Technologie
Security Design
Einsatz der Technologie
Response Plan
Stay Up-to-Date



Technologie

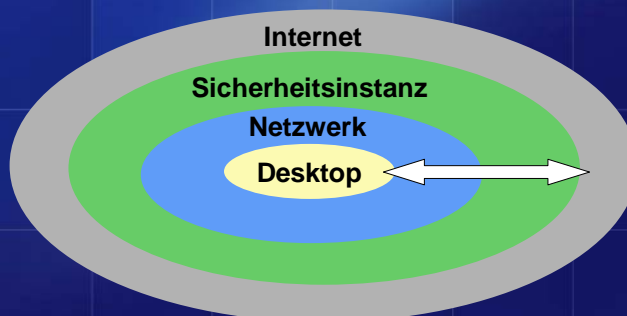
Windows 2000 / Windows Server 2003

- SECURITY INTEGRATED INTO ACTIVE DIRECTORY
- KERBEROS V. 5 vs. NTLM
- GROUP POLICY
- INTEGRATED PKI
- SECURE WEB SERVICES
- ENCRYPTING FILE SYSTEM
- NATIVE SMART CARD SUPPORT
- IPSEC AND L2TP SUPPORT

Prozesse

•Welche Risiken sieht der Kunde für sein Unternehmen?

- Bewertung des Schutzes
- Aufwand, um eine Lösung zu implementieren
- Mögliches Risiko eines Angriffs
- Auswahl geeigneter Konzepte, Tools oder Lösungen



Prozesse

Bsp: Smart Cards

Fragen:

- Ist Single SignOn gewünscht, sinnvoll, möglich?
- Ist die Hardware geeignet?
- Welche Funktionen können, sollen müssen abgedeckt werden?
- Zieht die Implementierung bauliche Veränderungen am Gebäude nach sich?
- Ist die Implementierung für alle MA notwendig?
- In welchem Zeitrahmen kann, soll, muß eine Integration erfolgen.....

Prozesse

Existierende Umgebung

TECHNOLOGIE INFRASTRUKTUR

- Logisch
- Physikalisch

SECURITY PRODUKTE/SERVICES/TECHNOLOGIEN

- aktuelle Security-Konfiguration der Servers, Desktops und des Netzwerks
- Security-Produkte z.B VPN Server, Firewall, IDS

ADMIN MODEL, GESCHÄFTSPROZESSE

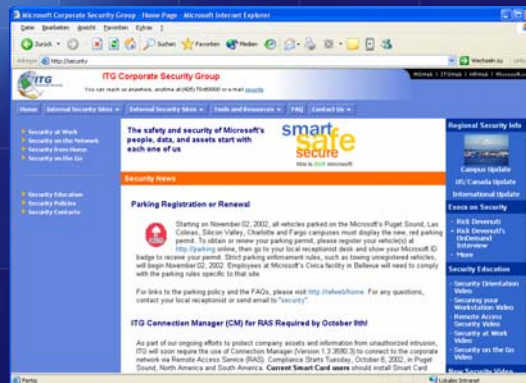
- Business Units / Filialen
- Sites

EXISTIERENDE HARDWARE/SOFTWARE

- Server
- Client
- Security Hardware/ Software
- Applikationen

Mensch

- Training – Know How
- Sensibilisierung
- Verantwortung



Summary

Microsoft bietet:

- zuverlässige Sicherheitstechnologie
- Tools und Lösungen zum Implementieren der Prozesse
- Trustworthy Computing

MS Security IT Showcase Microsoft



<http://www.microsoft.com/technet/itsolutions/techsol/showcase/default.asp>

Security Implementierung
Konfigurationsempfehlung
Best Practise

MS Security IT Showcase Microsoft



Abgeschlossene Aktionen

- Security Patch Management
- >96% der PCs in ITG gemanagten Domänen bekommen Patches automatisch via Internet (Autoupdate, GroupPolicies)
- NT4 Domänen migriert zu Active Directory
- Nebeneffekt des Network Intrusion Detection Projektes
 - Reduzieren der nötigen Internet Proxy Server
 - Erhöhende Bandbreite für andere Services

MS Security

IT Showcase Microsoft

Security Management

- bis zu 5000 Attacken pro Tag
 - ca. 95 % einfache Tools, vertippen, etc.
- 24h Emergency Response Center
 - Status Weltweit
 - Responseplan (Scripts, Policies, Serversetting, etc.)
 - Verantwortlichkeiten
- Design/ Security Reviews 14tägig
- Technologie Integration in die Entwicklung

The Microsoft logo is centered on a dark blue background with a light blue grid pattern. The logo is rendered in a white, 3D-style font with a slight shadow effect.

© 2002 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.